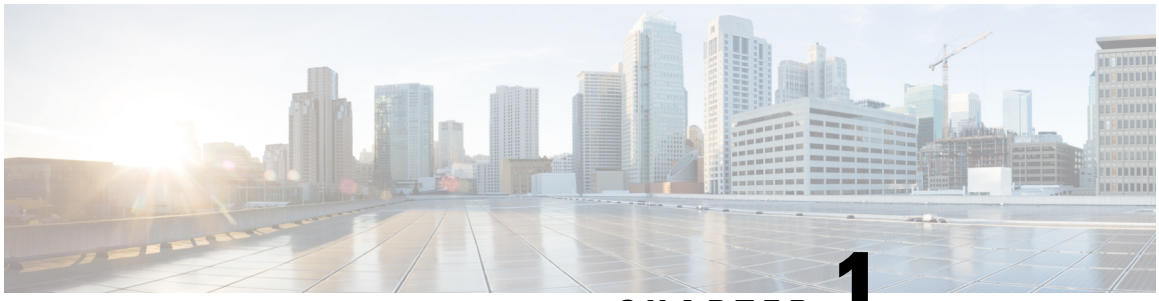
MGCP Configuration Guide, Cisco IOS Release 15M&T

Last Modified: 2015-07-31

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

Overview of MGCP and Related Protocols

This chapter provides overview information on Media Gateway Control Protocol (MGCP) and related protocols.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for MGCP and Related Protocols

- Configure IP routing.
- Configure voice ports.
- Configure VoIP.
- Configure the call agent. (For information on setting up call agents, see the documentation that accompanies the call agents used in your network configuration.)

Information About MGCP and Related Protocols

MGCP is an extension of the earlier version of the protocol Simple Gateway Control Protocol (SGCP) and supports SGCP functionality in addition to several enhancements. Systems using SGCP can easily migrate to MGCP, and MGCP commands are available to enable SGCP capabilities.

An MGCP gateway handles translation between audio signals and the packet network. Gateways interact with a call agent (CA)--also called a media gateway controller (MGC)--that performs signal and call processing on gateway calls. In the MGCP configurations that Cisco IOS supports, a gateway can be a Cisco router, access server, or cable modem, and the CA is a server from a third-party vendor.

Configuration commands for MGCP define the path between the call agent and the gateway, the type of gateway, and the type of calls handled by the gateway.

MGCP uses endpoints and connections to construct a call. Endpoints are sources of or destinations for data, and can be physical or logical locations in a device. Connections can be point-to-point or multipoint.

Similar to SGCP, MGCP uses User Datagram Protocol (UDP) for establishing audio connections over IP networks. However, MGCP also uses hairpinning to return a call to the PSTN when the packet network is not available.

Package Types

A call connection involves a series of events and signals--such as off-hook status, a ringing signal, or a signal to play an announcement--that are specific to the type of endpoint involved in the call.

MGCP groups these events and signals into packages. A trunk package, for example, is a group of events and signals relevant to a trunking gateway; an announcement package is a group of events and signals relevant to an announcement server. MGCP supports the following seven package types:

- Trunk
- Line
- Dual-tone multifrequency (DTMF)
- Generic media
- Real-Time Transport Protocol (RTP)
- Announcement server
- Script

The trunk package and line package are supported by default on certain types of gateways. Although configuring a gateway with additional endpoint package information is optional, you may want to specify packages for your endpoints to add to or override the defaults.

Protocol Benefits

MGCP provides the following benefits:

- Alternative dial tone for VoIP environments--Deregulation in the telecommunications industry gives competitive local-exchange carriers (CLECs) opportunities to provide toll bypass from the incumbent local-exchange carriers (ILECs) by means of VoIP. MGCP enables a VoIP system to control call setup and teardown and Custom Local Area Subscriber Services (CLASS) features for less sophisticated gateways.
- Simplified configuration for static VoIP network dial peers--When you use MGCP as the call agent in a VoIP environment, you need not configure static VoIP network dial peers. The MGCP call agent provides functions similar to VoIP-network dial peers.

Note Plain old telephone service (POTS) dial peer configuration is still required.

- Migration paths--Systems using earlier versions of the protocol can migrate easily to MGCP.
- Varied network needs supported for the following:
  - Interexchange carriers (IXCs) who have no legacy time-division multiplexing (TDM) equipment in their networks and want to deploy a fully featured network that offers both long-distance services to corporate customers and connectivity to local exchange carriers or other IXCs with traditional TDM equipment.
  - IXCs who have TDM equipment in their networks and want to relieve network congestion using data technologies to carry voice traffic or to cap the growth of TDM ports. In these situations, the packet network provides basic switched trunking without services or features.
  - Competitive competitive local-exchange carriers (CLECs) who want to provide residential and enhanced services.
  - Dial-access customers who want enhanced Signaling System 7 (SS7) access capabilities and increased performance, reliability, scalability, and economy.

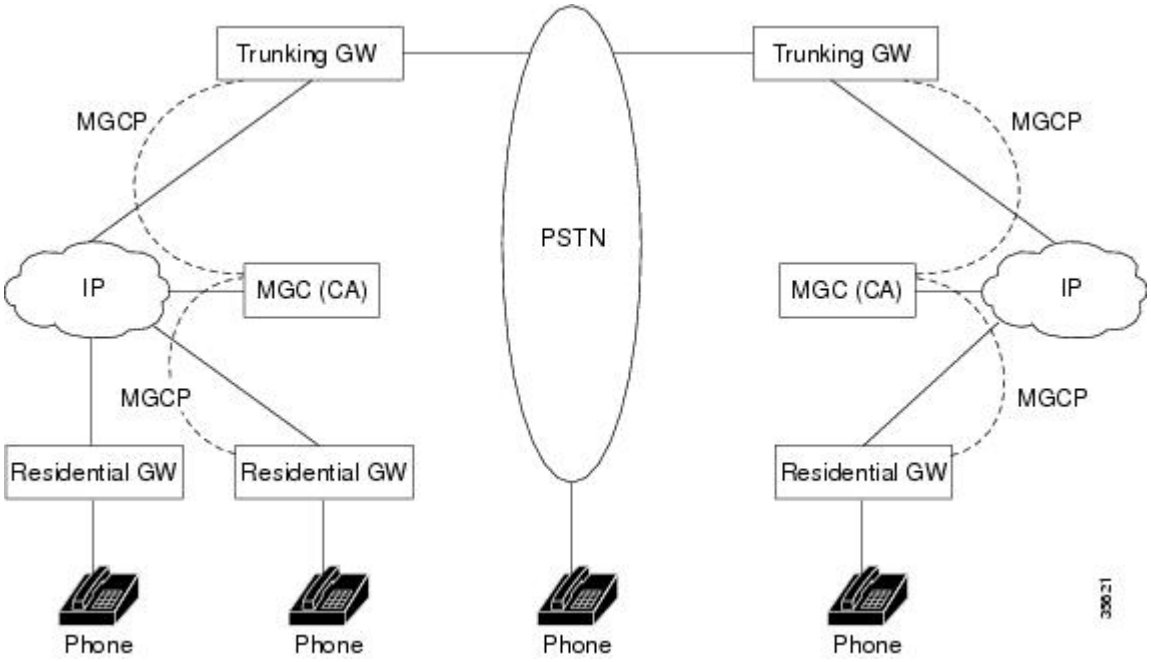
Supported Gateways

MGCP supports both residential and trunking gateways.

Residential Gateway

A residential gateway (RGW) provides an interface between analog (RJ-11) calls from a telephone and the VoIP network. Examples of RGWs include cable modems and Cisco 2600 series routers. The figure below shows an RGW configuration.

Figure 1: Residential and Trunking Gateways



RGW functionality supports analog POTS calls for both SGCP and MGCP on the Cisco 2600 series routers and Cisco uBR924 cable access router as shown in the table below.

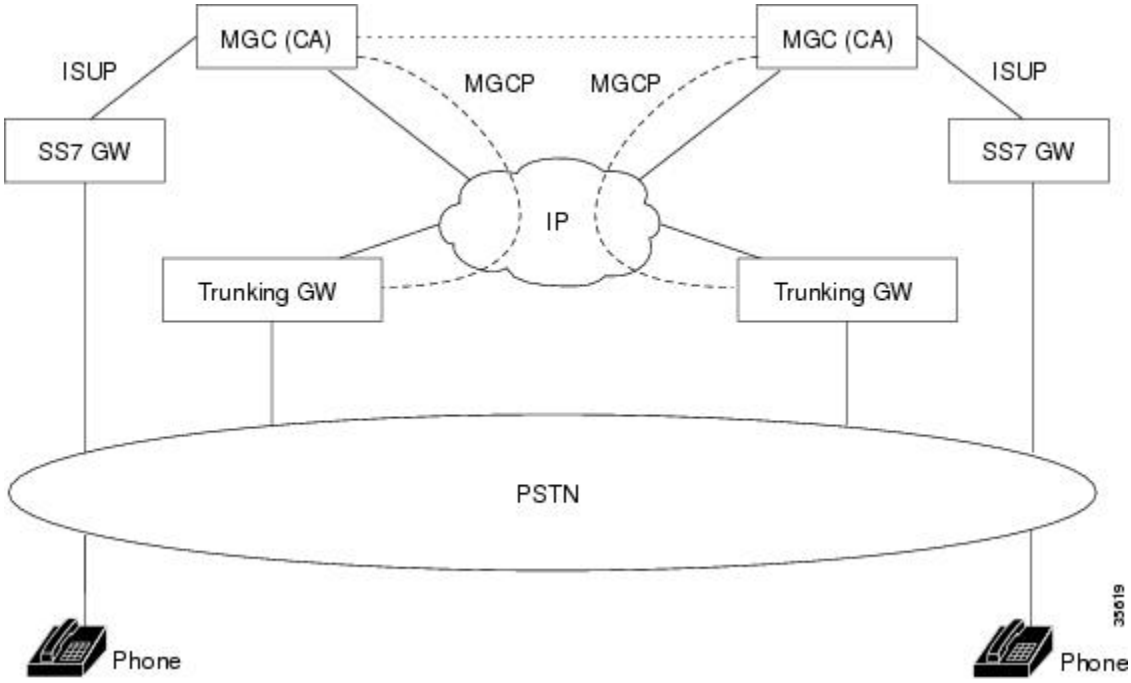
Table 1: RGW Functionality

Functionality	Platform	
Cisco 2600 Series	Cisco uBR924	
Call waiting	Yes	Yes
Default call-agent address specifiable for each foreign exchange station (FXS) port	--	Yes
Distinctive ringing	--	Yes
Fax and modem calls	Yes	Yes
On-hook caller identification (ID)	--	Yes
Ring splash	--	Yes
Stutter dial tone	Yes	Yes

Trunking Gateway

A trunking gateway (TGW) provides an interface between PSTN trunks and a VoIP network. A trunk can be a DS0, T1, or E1 line. Examples of TGWs include access servers and routers. The figure below shows a TGW configuration.

Figure 2: Trunking Gateways



TGW functionality supports SGCP and MGCP as shown in the table below.

Table 2: TGW Functionality

Functionality	Platform	
Cisco AS5300	Cisco 3660	
911 outgoing calls on T1 lines	Yes[1]	
Fax and modem calls	Yes	Yes
PRI/ISDN signaling (calls are backhauled to the call agent)	Yes	
SS7	Yes	Yes
T1 and E1 interfaces	Yes	Yes

[1] Server must have SGCP 1.1+ protocol for Feature Group D Operator Services (FGD-OS)

Toll Fraud Prevention

When a Cisco router platform is installed with a voice-capable Cisco IOS software image, appropriate features must be enabled on the platform to prevent potential toll fraud exploitation by unauthorized users. Deploy these features on all Cisco router Unified Communications applications that process voice calls, such as Cisco Unified Communications Manager Express (CME), Cisco Survivable Remote Site Telephony (SRST), Cisco Unified Border Element (UBE), Cisco IOS-based router and standalone analog and digital PBX and

public-switched telephone network (PSTN) gateways, and Cisco contact-center VoiceXML gateways. These features include, but are not limited to, the following:

- Disable secondary dial tone on voice ports--By default, secondary dial tone is presented on voice ports on Cisco router gateways. Use private line automatic ringdown (PLAR) for foreign exchange office (FXO) ports and direct-inward-dial (DID) for T1/E1 ports to prevent secondary dial tone from being presented to inbound callers.
- Cisco router access control lists (ACLs)--Define ACLs to allow only explicitly valid sources of calls to the router or gateway, and therefore to prevent unauthorized Session Initiation Protocol (SIP) or H.323 calls from unknown parties to be processed and connected by the router or gateway.
- Close unused SIP and H.323 ports--If either the SIP or H.323 protocol is not used in your deployment, close the associated protocol ports. If a Cisco voice gateway has dial peers configured to route calls outbound to the PSTN using either time division multiplex (TDM) trunks or IP, close the unused H.323 or SIP ports so that calls from unauthorized endpoints cannot connect calls. If the protocols are used and the ports must remain open, use ACLs to limit access to legitimate sources.
- Change SIP port 5060--If SIP is actively used, consider changing the port to something other than well-known port 5060.
- SIP registration--If SIP registration is available on SIP trunks, turn on this feature because it provides an extra level of authentication and validation that only legitimate sources can connect calls. If it is not available, ensure that the appropriate ACLs are in place.
- SIP Digest Authentication--If the SIP Digest Authentication feature is available for either registrations or invites, turn this feature on because it provides an extra level of authentication and validation that only legitimate sources can connect calls.
- Explicit incoming and outgoing dial peers--Use explicit dial peers to control the types and parameters of calls allowed by the router, especially in IP-to-IP connections used on CME, SRST, and Cisco UBE. Incoming dial peers offer additional control on the sources of calls, and outgoing dial peers on the destinations. Incoming dial peers are always used for calls. If a dial peer is not explicitly defined, the implicit dial peer 0 is used to allow all calls.
- Explicit destination patterns--Use dial peers with more granularity than .T for destination patterns to block disallowed off-net call destinations. Use class of restriction (COR) on dial peers with specific destination patterns to allow even more granular control of calls to different destinations on the PSTN.
- Translation rules--Use translation rules to manipulate dialed digits before calls connect to the PSTN to provide better control over who may dial PSTN destinations. Legitimate users dial an access code and an augmented number for PSTN for certain PSTN (for example, international) locations.
- Tcl and VoiceXML scripts--Attach a Tcl/VoiceXML script to dial peers to do database lookups or additional off-router authorization checks to allow or deny call flows based on origination or destination numbers. Tcl/VoiceXML scripts can also be used to add a prefix to inbound DID calls. If the prefix plus DID matches internal extensions, then the call is completed. Otherwise, a prompt can be played to the caller that an invalid number has been dialed.
- Host name validation--Use the "permit hostname" feature to validate initial SIP Invites that contain a fully qualified domain name (FQDN) host name in the Request Uniform Resource Identifier (Request URI) against a configured list of legitimate source hostnames.
- Dynamic Domain Name Service (DNS)--If you are using DNS as the "session target" on dial peers, the actual IP address destination of call connections can vary from one call to the next. Use voice source

groups and ACLs to restrict the valid address ranges expected in DNS responses (which are used subsequently for call setup destinations).

For more configuration guidance, see the " Cisco IOS Unified Communications Toll Fraud Prevention " paper.

Additional References

The following sections provide references related to MGCP.

Related Documents

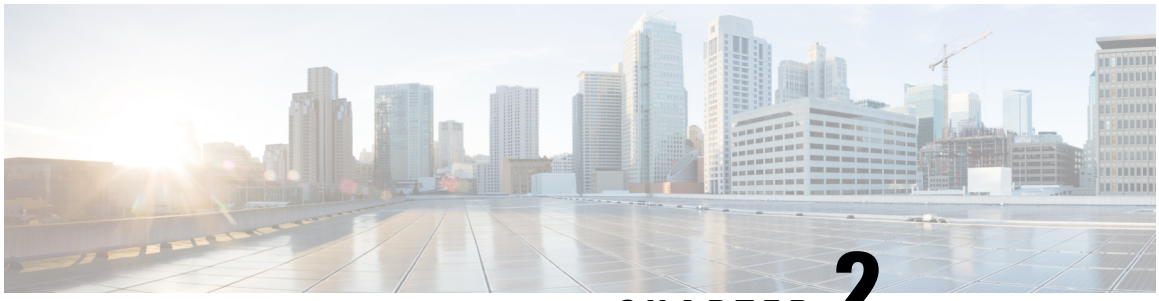
Related Topic	Document Title
Cisco IOS configuration examples	Cisco Systems Technologies website at http://cisco.com/en/US/tech/index.html . Select a technology category and subsequent hierarchy of subcategories. Click **Technical Documentation > Configuration Examples**.
Cisco IOS debug command reference	*Cisco IOS Debug Command Reference*
Cisco IOS troubleshooting information	*Cisco IOS Voice Troubleshooting and Monitoring Guide*
Cisco IOS voice command reference	*Cisco IOS Voice Command Reference*

MIBs

MIBs	MIBs Link
	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport



CHAPTER 2

Basic MGCP Configuration

This chapter provides basic configuration information for Media Gateway Control Protocol (MGCP) and related protocols.

For more information about related Cisco IOS voice features, see the following:

- "Overview of MGCP and Related Protocols" on page 3
- Entire Cisco IOS Voice Configuration Library--including library preface and glossary, other feature documents, and troubleshooting documentation--at http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/cisco_ios_voice_configuration_library_glossary/vcl.htm

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

How to Configure MGCP and Related Protocols

Note RGWs are configured only with MGCP.

Configuring a TGW for MGCP

To configure a trunking gateway (TGW) for MGCP, perform this task:

SUMMARY STEPS

1. **mgcp**
2. **mgcp call-agent** [*ipaddr*|*hostname*] [*port*] **service-type mgcp**
3. **controller t1** *number*
4. **ds0-group** *channel-number* **timeslots** *range* **type none service mgcp**
5. **exit**
6. **mgcp restart-delay** *value*
7. **mgcp package-capability** {**s-package** | **dtmf-package** | **gm-package** | **lcs-package** | **rtp-package** | **trunk-package** | **script-package**}
8. **mgcp default-package** {**as-package** | **dtmf-package** | **gm-package** | **rtp-package** | **trunk-package**}
9. **mgcp dtmf-relay** {**codec** | **low-bit-rate**} **mode** {**cisco** | **out-of-band**}
10. **mgcp modem passthru** {**cisco** | **ca**}
11. **mgcp sdp simple**
12. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**mgcp** **Example:** `Router(config)# mgcp`	Initiates the MGCP application.
Step 2	**mgcp call-agent** [*ipaddr*|*hostname*] [*port*] **service-type mgcp** **Example:** `Router(config)# mgcp call-agent [ipaddr |hostname ] [port ] service-type mgcp`	Specifies the call agent's IP address or domain name, the port, and gateway control service type.
Step 3	**controller t1** *number* **Example:** `Router(config)# controller t1 number`	Specifies the channel number of the T1 trunk to be used for analog calls and enters controller configuration mode.
Step 4	**ds0-group** *channel-number* **timeslots** *range* **type none service mgcp** **Example:** `Router(config-controller)# ds0-group channel-number`	Configures the channelized T1 time slots to accept the analog calls.

	Command or Action	Purpose
	`timeslots range` ` type none service mgcp`	
Step 5	**exit** **Example:** `Router(config-controller)# exit`	Exits the current mode.
Step 6	**mgcp restart-delay** *value* **Example:** `Router(config)# mgcp restart-delay value`	(Optional) Specifies the delay value sent in the RSIP graceful teardown method, in seconds. Range is from 0 to 600. Default is 0.

Step 7	**mgcp package-capability** {**s-package** | **dtmf-package** | **gm-package** | **lcs-package** | **rtp-package** | **trunk-package** | **script-package**}
	Example:
	`Router(config)#`
	`mgcp package-capability`
	`{trunk-package | dtmf-package | gm-package | lcs-package | rtp-package | as-package}`
		(Optional) Specifies the event packages that are supported on the trunking gateway. Default is **trunk-package**.

Step 8	**mgcp default-package** {**as-package** | **dtmf-package** | **gm-package** | **rtp-package** | **trunk-package**} **Example:** `Router(config)# mgcp default-package {as-package | dtmf-package | gm-package | rtp-package | trunk-package}`	(Optional) Specifies the default event package. Overrides the **mgcp package-capability** default package.
Step 9	**mgcp dtmf-relay** {**codec** | **low-bit-rate**} **mode** {**cisco** | **out-of-band**} **Example:** `Router(config)# mgcp dtmf-relay {codec | low-bit-rate} mode {cisco | out-of-band}`	(Optional) Used for relaying digits through the IP network. Default is **no mgcp dtmf-relay** for all codecs.
Step 10	**mgcp modem passthru** {**cisco** | **ca**} **Example:** `Router(config)# mgcp modem passthru {cisco | ca}`	(Optional) Configures the gateway for modem and fax data.
Step 11	**mgcp sdp simple** **Example:** `Router(config)# mgcp sdp simple`	(Optional) Specifies use of a subset of the session description protocol (SDP). Some call agents require this subset to send data through the network. Default is **no mgcp sdp simple**.

	Command or Action	Purpose
Step 12	**exit** **Example:** `Router(config)# exit`	Exits the current mode.

Configuring a TGW for SGCP

Perform this task to configure a trunking gateway (TGW) for Simple Gateway Control Protocol (SGCP):

SUMMARY STEPS

1. **mgcp**
2. **mgcp call-agent** [*ipaddr* | *hostname*] [*port*] **service-type sgcp**
3. **controller t1** *number*
4. **ds0-group** *channel-number* **timeslots** *range* **type** {**none** | **fgdos**} [*tone_type*] [*addr_info*] **service** {**sgcp** | **voice**}
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**mgcp** **Example:** `Router(config)# mgcp`	Initiates the MGCP application.
Step 2	**mgcp call-agent** [*ipaddr* | *hostname*] [*port*] **service-type sgcp** **Example:** `Router(config)# mgcp call-agent [ipaddr	hostname] [port] service-type sgcp`	Specifies the call agent's IP address or domain name, the port, and gateway control service type.
Step 3	**controller t1** *number* **Example:** `Router(config)# controller t1 number`	Specifies the channel number of the T1 trunk to be used for analog calls and enters controller configuration mode.
Step 4	**ds0-group** *channel-number* **timeslots** *range* **type** {**none** | **fgdos**} [*tone_type*] [*addr_info*] **service** {**sgcp** | **voice**} **Example:** `Router(config-controller)# ds0-group channel-number`	Configures the channelized T1 time slots to accept the analog calls. For type **none**, use **service sgcp**. For type **fgdos**, use **service voice**.

	Command or Action	Purpose
	`timeslots range type {none | fgdos} [tone_type] [addr_info] service {sgcp | voice}`	
Step 5	**exit** **Example:** `Router(config-controller)# exit`	Exits the current mode.

Configuring an RGW

To configure a residential gateway (RGW), perform this task:

SUMMARY STEPS

1. **mgcp**
2. **mgcp call-agent** [*ipaddr* | *hostname*] [*port*] **service-type sgcp**
3. **dial-peer voice** *number* **pots**
4. **application MGCPAPP**
5. **exit**
6. **mgcp package-capability** {**line-package** | **dtmf-package** | **gm-package** | **rtp-package**}
7. **mgcp default-package** [**line-package** | **dtmf-package** | **gm-package**]
8. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**mgcp** **Example:** `Router(config)# mgcp`	Initiates the MGCP application. **Note** RGWs are configured only with MGCP.
Step 2	**mgcp call-agent** [*ipaddr* | *hostname*] [*port*] **service-type sgcp** **Example:** `Router(config)# mgcp call-agent [ipaddr | hostname] [port] service-type mgcp`	Specifies the call-agent IP address or domain name, port, and gateway control service type.
Step 3	**dial-peer voice** *number* **pots** **Example:** `Router(config)# dial-peer voice number pots`	Sets up the dial peer for a voice port.

	Command or Action	Purpose
Step 4	**application MGCPAPP** **Example:** `Router(config-dial-peer)# application MGCPAPP`	Selects the MGCP application to run on the voice port.
Step 5	**exit** **Example:** `Router(config-dial-peer)# exit`	Exits the current mode.

Step 6	**mgcp package-capability** {**line-package** | **dtmf-package** | **gm-package** | **rtp-package**}
	Example:
	`Router(config)#`
	`mgcp package-capability`
	`{line-package | dtmf-package | gm-package | rtp-package}`
		(Optional) Specifies event packages that are supported on the residential gateway. Default is **line-package**.

Step 7	**mgcp default-package** [**line-package** | **dtmf-package** | **gm-package**] **Example:** `Router(config)# mgcp default-package [line-package | dtmf-package | gm-package]`	(Optional) Specifies the default event package. Overrides the **mgcp package-capability** command.
Step 8	**exit** **Example:** `Router(config)# exit`	Exits the current mode.

Configuring a SDP Aware NSE Mode

The Cisco IOS MGCP gateway relies only on the local modem or fax configuration to determine whether Named Signaling Event (NSE) should be used or not for the current call. SDP-aware NSE mode enables the Cisco IOS MGCP gateway to negotiate NSE-based modem and fax features by considering both the local configuration and the remote support for NSE.

Note Cisco Unified Call Manager (UCM) does not support modem or fax passthrough. This feature should not be enabled when Cisco UCM is the call agent.

>

SUMMARY STEPS

1. **mgcp**
2. **mgcp behavior negotiate-nse enable**
3. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**mgcp** **Example:** `Router(config)# mgcp`	Initiates the MGCP application.
Step 2	**mgcp behavior negotiate-nse enable** **Example:** `Router(config)# mgcp behavior negotiate-nse enable`	Enables SDP-aware NSE mode.
Step 3	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Verifying NSE Mode Configuration

SUMMARY STEPS

1. **show mgcp**

DETAILED STEPS

show mgcp

Use this command to display the state of the **mgcp behavior**command.

Example:

```
Router# show mgcp
MGCP Admin State ACTIVE, Oper State ACTIVE - Cause Code NONE
MGCP call-agent: 10.7.0.200 Initial protocol service is MGCP 0.1
```

The following lines show that the **mgcp behavior negotiate-nse enable**command is enabled:

Example:

```
mgcp modem passthrough voip mode nse
mgcp codec g723ar53 packetization-period 30
mgcp package-capability rtp-package
mgcp package-capability sst-package
mgcp package-capability pre-package
```

```
mgcp package-capability mdste-package
mgcp package-capability srtp-package
mgcp package-capability fm-package
no mgcp package-capability res-package
no mgcp timer receive-rtcp
mgcp sdp simple
mgcp sdp mdcx-ack
mgcp fax t38 ecm
mgcp fax t38 ls_redundancy 5
mgcp fax t38 hs_redundancy 2
mgcp behavior mdcx-sdp ack-with-sdp
mgcp behavior dynamically-change-codec-pt disable
mgcp behavior negotiate-nse enable
mgcp rtp payload-type nte 101
```

Verifying the TGW or RGW Configuration

SUMMARY STEPS

1. **show running-configuration**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show running-configuration** **Example:** `Router(config)# show running-configuration`	Displays the current configuration settings.

Blocking New Calls

You can block all new MGCP calls to the router (Step 1) and terminate all existing active calls (Step 2), which means that an active call is not terminated until the caller hangs up.

To block all new calls, use the following commands in global configuration mode:

SUMMARY STEPS

1. **mgcp block-newcalls**
2. **no mgcp block-newcalls**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**mgcp block-newcalls** **Example:** `Router(config)# mgcp block-newcalls`	Prevents the gateway from accepting new calls.

	Command or Action	Purpose
Step 2	**no mgcp block-newcalls** **Example:** `Router(config)# no mgcp block-newcalls`	Restarts normal MGCP call operation.

Configuration Examples for MGCP and Related Protocols

Configuring a Cisco AS5300 as a TGW with MGCP Example

The following example illustrates a configuration only for MGCP calls. FGD-OS calls are not supported.

```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname A
!
resource-pool disable
!
ip subnet-zero
ip ftp username smith
ip host B 209.165.200.225
ip host C 209.165.200.226
ip domain-name cisco.com
ip name-server 209.165.202.129
!
mgcp
mgcp request timeout 10000
mgcp call-agent 192.168.10.10 2302
mgcp restart-delay 5
mgcp package-capability gm-package
mgcp package-capability dtmf-package
mgcp package-capability trunk-package
mgcp package-capability rtp-package
mgcp package-capability as-package
mgcp package-capability mf-package
mgcp package-capability script-package
mgcp default-package trunk-package
mta receive maximum-recipients 0
!
controller T1 0
 framing esf
 clock source line primary
 linecode b8zs
 ds0-group 0 timeslots 1-24 type none service mgcp
!
controller T1 1
 framing esf
 clock source line secondary 1
 linecode b8zs
 ds0-group 0 timeslots 1-24 type none service mgcp
!
controller T1 2
```

```
 framing esf
 linecode b8zs
 ds0-group 0 timeslots 1-24 type none service mgcp
!
controller T1 3
 framing esf
 linecode b8zs
 ds0-group 0 timeslots 1-24 type none service mgcp
!
voice-port 0:0
!
voice-port 1:0
!
voice-port 2:0
!
voice-port 3:0
!
interface Ethernet0
 ip address 192.168.10.9 255.255.255.0
 no ip directed-broadcast
!
interface FastEthernet0
 ip address 172.22.91.73 255.255.255.0
 no ip directed-broadcast
 shutdown
 duplex auto
 speed auto
!
no ip classless
ip route 0.0.0.0 0.0.0.0 172.22.91.1
ip route 209.165.200.225 255.255.255.255 192.168.0.1
no ip http server
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
line vty 0 4
 login
!
end
```

Configuring a Cisco AS5300 as a TGW with SGCP Example

The following example illustrates a configuration that supports MGCP and FGD-OS calls:

```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname A
!
resource-pool disable
!
ip subnet-zero
ip ftp username smith
ip host B 209.165.200.225
ip host C 209.165.200.226
ip domain-name cisco.com
ip name-server 209.165.202.129
!
```

```
mgcp
mgcp request timeout 10000
mgcp call-agent 192.168.10.10 2302 sgcp
mta receive maximum-recipients 0
!
controller T1 0
 framing esf
 clock source line primary
 linecode b8zs
 ds0-group 0 timeslots 1-24 type none service mgcp
!
controller T1 1
 framing esf
 clock source line secondary 1
 linecode b8zs
 ds0-group 0 timeslots 1-24 type fgd-os mf dnis-ani service voice
!
controller T1 2
 framing esf
 linecode b8zs
 ds0-group 0 timeslots 1-24 type none service mgcp
!
controller T1 3
 framing esf
 linecode b8zs
 ds0-group 0 timeslots 1-24 type none service mgcp
!
!voice-port 0:0
!
voice-port 1:0
!
voice-port 2:0
!
voice-port 3:0
!
interface Ethernet0
 ip address 192.168.10.9 255.255.255.0
 no ip directed-broadcast
!
interface FastEthernet0
 ip address 172.22.91.73 255.255.255.0
 no ip directed-broadcast
 shutdown
 duplex auto
 speed auto
!
no ip classless
ip route 0.0.0.0 0.0.0.0 172.22.91.1
ip route 209.165.200.225 255.255.255.255 192.168.0.1
no ip http server
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
line vty 0 4
 login
!
end
```

Configuring a Cisco 3660 as a TGW with MGCP Example

The following example illustrates a platform that does not support FGD-OS calls.

```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname A
!
memory-size iomem 40
voice-card 1
!
ip subnet-zero
!
mgcp 4000
mgcp call-agent 209.165.202.129 4000
mgcp package-capability gm-package
mgcp package-capability dtmf-package
mgcp package-capability rtp-package
mgcp package-capability as-package
isdn voice-call-failure 0
cns event-service server
!
controller T1 1/0
 framing esf
 clock source internal
 ds0-group 1 timeslots 1-24 type none service mgcp
!
controller T1 1/1
 framing esf
 clock source internal
 ds0-group 1 timeslots 1-24 type none service mgcp
!
voice-port 1/0:1
!
voice-port 1/1:1
!
interface FastEthernet0/0
 ip address 209.165.202.140 255.255.255.0
 no ip directed-broadcast
 load-interval 30
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 load-interval 30
 shutdown
 duplex auto
 speed auto
!
ip default-gateway 209.165.202.130
ip classless
ip route 209.165.200.225 255.255.255.255 FastEthernet0/0
no ip http server
!
snmp-server engineID local 00000090200000107BD8CD80
snmp-server community public RO
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
```

```
line vty 0 4
 login
!
end
```

Configuring a Cisco uBR924 as an RGW Example

The following example illustrates a platform that does not support FGD-OS calls.

```
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname A
!
logging buffered 200000 debugging
!
clock timezone - -8
ip subnet-zero
no ip routing
no ip domain-lookup
ip host A 192.168.147.91
ip host C 209.165.200.224
ip host D 209.165.200.225
!
mgcp
mgcp call-agent 192.168.10.10 2490
mgcp package-capability gm-package
mgcp package-capability dtmf-package
mgcp package-capability line-package
mgcp default-package line-package
!
voice-port 0
 input gain -3
!
voice-port 1
 input gain -3
!
dial-peer voice 1 pots
 application MGCPAPP
 port 1
!
dial-peer voice 2 pots
 application MGCPAPP
 port 0
!
interface Ethernet0
 ip address 192.168.147.91 255.255.255.0
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
!
interface cable-modem0
 ip address negotiated
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
 cable-modem downstream saved channel 459000000 20
cable-modem downstream saved channel 699000000 19 2
 cable-modem mac-timer t2 100000
```

```
 no cable-modem compliant bridge
 bridge-group 59
 bridge-group 59 spanning-disabled
!
ip default-gateway 10.1.1.1
ip classless
no ip http server
!
line con 0
 exec-timeout 0 0
 transport input none
line vty 0 4
 login
!
end
```

Configuring a Cisco 2620 as an RGW Example

The following example illustrates a platform that does not support FGD-OS calls.

```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname D
!
memory-size iomem 10
ip subnet-zero
!
mgcp
mgcp call-agent 172.20.5.20
mgcp package-capability gm-package
mgcp package-capability dtmf-package
mgcp package-capability line-package
mgcp package-capability rtp-package
mgcp default-package line-package
cns event-service server
!
voice-port 1/0/0
!
voice-port 1/0/1
!
dial-peer voice 1 pots
 application MGCPAPP
 port 1/0/0
!
dial-peer voice 2 pots
 application MGCPAPP
 port 1/0/1
!
interface Ethernet0/0
 no ip address
 no ip directed-broadcast
 shutdown
!
interface Serial0/0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 shutdown
 no fair-queue
```

```
!
interface Ethernet0/1
 ip address 172.20.5.25 255.255.255.0
 no ip directed-broadcast
!
interface Serial0/1
 no ip address
 no ip directed-broadcast
 shutdown
!
ip default-gateway 209.165.202.130
ip classless
ip route 209.165.200.225 255.255.255.224 Ethernet0/1
no ip http server
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
line vty 0 4
 login
!
end
```

Tip See the "Additional References for MGCP and SGCP" section on page x for related documents, standards, and MIBs.

- See the " Glossary " for definitions of terms in this guide.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS Voice commands	*Cisco IOS Voice Command Reference*
Cisco IOS Voice Configuration Library	For more information about Cisco IOS voice features, including feature documents, and troubleshooti information--at http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/cisco_ios_voice_configuration_library_glossary/vcl.l

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

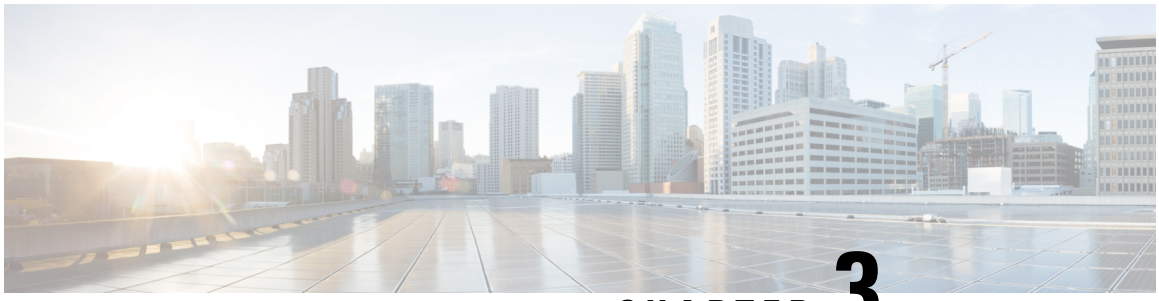
Feature Information for Basic MGCP Configuration

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 3: Feature Information for MGCP Basic Configuration

Feature Name	Releases	Feature Information
Configuring a TGW and RGW for MGCP	12.4(22)Y	
SDP Aware NSE Mode	15.1(3)T	Support was added for negotiating remote NSE support by configuring modem pass through on the gateway.



CHAPTER 3

Configuring MGCP 1.0

This chapter provides configuration information on configuring the MGCP 1.0 Including Network-based Call Signaling (NCS) 1.0 and Trunking Gateway Control Protocol (TGCP) 1.0 Profiles feature. The feature implements MGCP 1.0, NCS 1.0, and TGCP 1.0 support in existing MGCP stacks.

Feature benefits include the following:

- MGCP 1.0 provides flexible interoperability with a wide variety of call agents, thus enabling a wide range of solutions.
- MGCP 1.0 contains many improvements over its previous release.
- NCS 1.0 and TGCP 1.0 allow participation in packet cable solutions.
- The ability to interoperate with H.323 and Session Initiation Protocol (SIP) control agents allows leverage of the feature sets available in the different protocols and provides the ability to migrate smoothly from one protocol to another.

For more information about this and related Cisco IOS voice features, see the following:

- "Overview of MGCP and Related Protocols" on page 3
- Entire Cisco IOS Voice Configuration Library--including library preface and glossary, other feature documents, and troubleshooting documentation--at http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/cisco_ios_voice_configuration_library_glossary/vcl.htm

Feature History for MGCP 1.0 Including NCS 1.0 and TGCP 1.0 Profiles

Release	Modification
12.2(2)XA	This feature was introduced on the following platforms: Cisco CVA122, Cisco uBR924, and Cisco AS5300.
12.2(2)XA1	This feature was implemented on the following platforms: Cisco CVA122, Cisco uBR925, and Cisco AS5300
12.2(2)XB	This feature was implemented on the following platforms: Cisco AS5350 and Cisco AS5400.

Release	Modification
12.2(4)T	This feature was implemented on the following platforms: Cisco CVA122, Cisco CVA122E, Cisco uBR925, Cisco 2600 series, Cisco 2650, Cisco 3660, and Cisco MC3810. AAL2 PVC support was introduced for MGCP 1.0 on the Cisco MC3810. Certain gateway features were integrated into MGCP 1.0. **Note** The Cisco AS5300 is not supported in this release.
12.2(8)T	The voice-port (MGCP profile) command was changed to port (MGCP profile) for all platforms supported in this release. **Note** The Cisco AS5300 is not supported in this release.
12.2(13)T	The **fax** keyword was added to the **mgcp playout** command.
12.4(24)T3	The maximum number of MGCP profiles that can be configured was increased from 13 (12 plus 1 default) to 29 (28 plus 1 default).

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for MGCP 1.0

Prerequisites are described in the "Prerequisites for Configuring MGCP and Related Protocols" section. In addition, the following apply:

- Ensure that the minimum software requirements are met.Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn.
- Configure Voice over ATM AAL2 PVC (optional step that applies to Cisco MC3810 only). The router that is intending to use the VoAAL2 features must have hardware support for VoAAL2.
- Set up the cable modems, if any. See the documentation for the cable product as listed in the Preface.

Note IP addresses and host names in these examples are fictitious.

Information About MGCP 1.0

This feature implements the following MGCP protocols on supported Cisco media gateways:

- MGCP 1.0 (RFC 2705)
- Network-based Call Signaling (NCS) 1.0, the MGCP 1.0 profile for residential gateways (RGWs)
- Trunking Gateway Control Protocol (TGCP) 1.0, the MGCP 1.0 profile for trunking gateways (TGWs)
- VoIP--Includes signaling methods under VoIP.
- AAL2 PVC--Includes signaling methods under ATM adaptation layer 2 (AAL2) permanent virtual circuit (PVC).
- Basic/Extended RGW--Includes a collection of residential gateway features supporting channel-associated signaling (CAS). Digital CAS (recEive and transMit, or E&M) interfaces and analog (Foreign Exchange Office [FXO], Foreign Exchange Station [FXS], and E&M) interfaces are supported on platforms with the appropriate voice hardware.
- ISUP--Supports ISDN user part signaling for SS7 trunks.
- FGD-OS--Supports Feature Group D Operator Services signaling over T1 or E1 trunks.
- Incoming CAS--Supports digital CAS interfaces for digital incoming multifrequency tones (MF) CAS wink-start trunks in which an operator at an Operator Services Console can initiate the Operator Interrupt and Busy Line Verify (OI and BLV) functions.
- CAS PBX--Includes CAS private branch exchange (PBX) trunks, digit maps, CAS events, and quarantine buffer software. These features are supported on digital CAS interfaces.

MGCP1.0 is a protocol for the control of VoIP calls by external call-control elements known as media gateway controllers (MGCs) or call agents (CAs). It is described in the informational RFC 2705, published by the Internet Society.

PacketCable is an industry-wide initiative for developing interoperability standards for multimedia services over cable facilities using packet technology. PacketCable developed the NCS and TGCP protocols, which contain extensions and modifications to MGCP while preserving basic MGCP architecture and constructs. NCS is designed for use with analog, single-line user equipment on residential gateways, while TGCP is intended for use in VoIP-to-PSTN trunking gateways in a cable environment. To meet European cable requirements and equipment characteristics, the EuroPacketCable working group has adapted PacketCable standards under the name *IP Cablecom* .

MGCP Model

MGCP bases its call control and intelligence in centralized call agents, also called media gateway controllers. The call agents issue commands to simple, low-cost endpoints, which are housed in media gateways (MGs), and the call agents also receive event reports from the gateways. MGCP messages between call agents and media gateways are sent with Internet Protocol over User Datagram Protocol (IP/UDP).

The MGCP 1.0 Including NCS 1.0 and TGCP 1.0 Profiles feature provides protocols for RGWs and TGWs, which sit at the border of the packet network to provide an interface between traditional, circuit-based voice services and the packet network. Residential gateways offer a small number of analog line interfaces, while trunking gateways generally manage a large number of digital trunk circuits.

Two basic MGCP constructs are endpoints and connections. An endpoint is a source or sink for call data (RTP/IP) that is flowing through the gateway. A common type of endpoint is found at the physical interface between the POTS (plain old telephone service) or Public Switched Telephone Network (PSTN) service and the gateway; this type of endpoint might be an analog voice port or a digital DS0 group. There are other types of endpoints as well, and some are logical rather than physical. An endpoint is identified by a two-part endpoint name that contains the name of the entity on which it exists (for example, an access server or router) and the local name by which it is known (for example, a port identifier).

A connection is a temporary allocation of resources that enables a call to be completed. One or more connections is necessary to complete a call. Connections have names that identify them with the call to which they belong. Connections can be one-to-one or multipoint. Calls and connections are initiated, modified, and deleted on instructions from call agents.

Call agents manage call flow through standard MGCP commands that are sent to the endpoints under their control. The commands are delivered in standard ASCII text, and may contain session descriptions transmitted in Session Description Protocol (SDP), a text-based protocol. These messages are sent over IP/UDP.

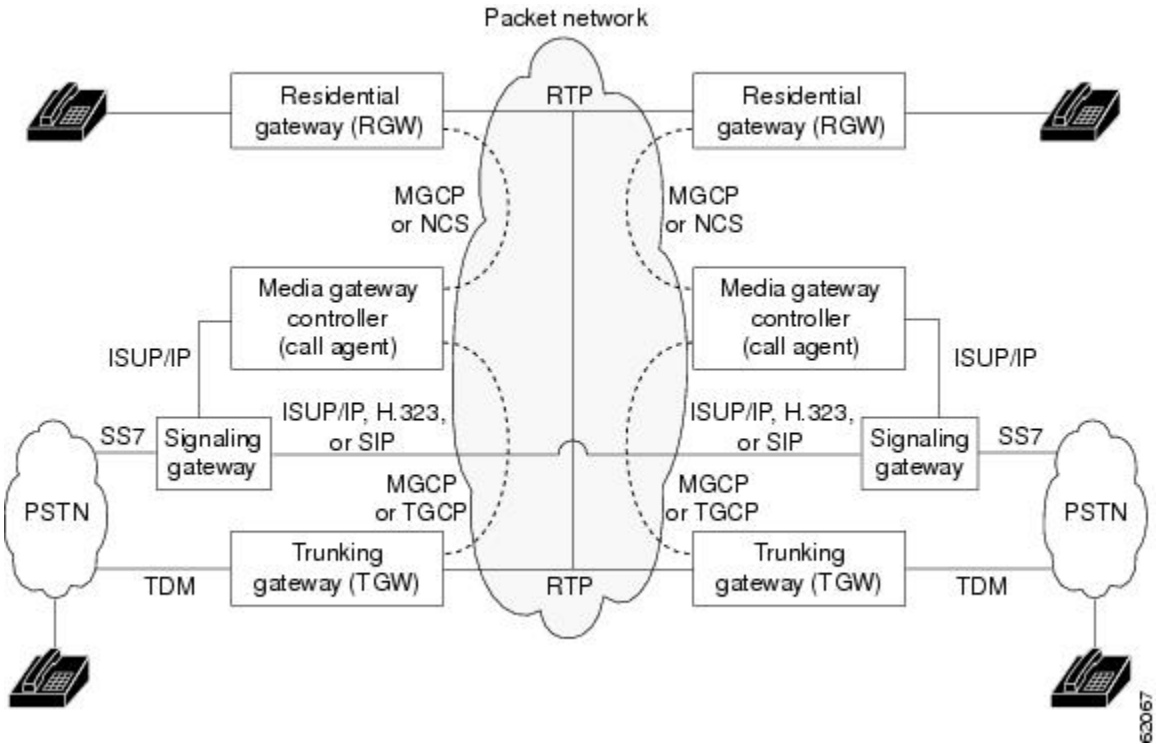
Call agents keep track of endpoint and connection status through the gateway's reporting of standard events that are detected from endpoints and connections. Call agents also direct gateways to apply certain standard signals when a POTS or PSTN connection expects them. For example, when someone picks up a telephone handset, an off-hook event is detected on an endpoint on the residential gateway to which the telephone is connected. The gateway reports the event to a call agent, which orders the gateway to apply the dial-tone signal to the endpoint reporting the off-hook event. The person picking up the handset hears dial tone.

Related events and signals are grouped into standard packages that apply to particular types of endpoints. For instance, the off-hook event is found in the line package, which is associated with analog-line endpoints, which in turn are associated with residential gateways. Standard events, signals, and packages are defined in the NCS, TGCP, and MGCP standards and RFCs listed in the " Preface ."

The figure below shows a hypothetical MGCP network with both residential and trunking gateways. The residential gateway has telephone sets connected to the gateway's FXS voice ports. MGCP or NCS over IP/UDP is used for call control and reporting to the call agent, while Real-Time Transport Protocol (RTP) is used to transmit the actual voice data.

The figure below also shows two trunking gateways with T1 (or E1) connections to the PSTN. Incoming time-division multiplexing (TDM) data is sent through the gateway into the packet network using RTP. MGCP or TGCP over IP/UDP is used for call control and reporting to the call agent. Signaling System 7 (SS7) data travels a different route, however, bypassing the trunking gateway entirely in favor of a specialized signaling gateway, where the signaling data is transformed to ISUP/IP format and relayed to the call agent. Communication between two signaling gateways in the same packet network can be done with Integrated Services Digital Networks User Part over Internet Protocol (ISUP/IP), H.323, or Session Initiation Protocol (SIP).

Figure 3: MGCP Network Model



How to Configure MGCP 1.0

The three tasks listed below configure the MGCP 1.0 Including NCS 1.0 and TGCP 1.0 Profiles feature on a media gateway. The first task names the voice ports or DS1 groups that are serving as MGCP endpoints. This task also associates the ports with an MGCP service type or application and starts the MGCP daemon.

The last two tasks allow you to configure MGCP parameters to meet your requirements. Each MGCP parameter is either a global parameter or a profile-related parameter. When you configure a global MGCP parameter value, it applies to all the MGCP endpoints on the gateway. When you configure a profile-related MGCP parameter value, it applies only to the endpoints associated with the MGCP profile that you are configuring at that moment (an MGCP profile is a user-defined subset of all the MGCP endpoints on the gateway). There is also a predefined MGCP profile named *default* that you can use to configure profile-related parameters for endpoints that do not belong to a user-defined MGCP profile.

See the following sections for configuration tasks for the MGCP 1.0 including NCS 1.0 and TGCP 1.0 Profiles feature. Each task in the list is identified as either required or optional:

Identifying Endpoints and Configuring the MGCP Application

This task is required. Voice ports or DS0 groups that are acting as MGCP endpoints must be identified and associated with the MGCP application. The commands to identify MGCP endpoints depend on the type of endpoint that you are configuring.

To identify endpoints and configure the MGCP application, use the commands in the appropriate table, beginning in global configuration mode:

Analog CAS and POTS Lines

To identify endpoints and configure the MGCP application for use with analog CAS and POTS lines, use these commands, beginning in global configuration mode:

SUMMARY STEPS

1. **dial-peer voice** *tag* **pots**
2. **application mgcpapp**
3. **port** *port-number*
4. **exit**
5. **mgcp** [*gw-port*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**dial-peer voice** *tag* **pots** **Example:** `Router(config)# dial-peer voice tag pots`	Enters dial-peer configuration mode and specifies the method of voice encapsulation.
Step 2	**application mgcpapp** **Example:** `Router(config-dial-peer)# application mgcpapp`	Enables the MGCP application on this dial peer.
Step 3	**port** *port-number* **Example:** `Router(config-dial-peer)# port port-number`	Associates a dial peer with a specific voice port.
Step 4	**exit** **Example:** `Router(config-dial-peer)# exit`	Exits the current mode.
Step 5	**mgcp** [*gw-port*] **Example:** `Router(config)# mgcp [gw-port]`	Initiates the MGCP daemon. The optional argument is the UDP port over which the gateway receives messages from the call agent (the gateway MGCP port number). Default is 2427.

Digital CAS Trunks

To identify endpoints and configure the MGCP application for use with digital CAS trunks, use these commands, beginning in global configuration mode:

SUMMARY STEPS

1. **controller** {**t1** | **e1**} *cntlr-number*
2. **mode cas**
3. Do one of the following:
   - **framing** {**sf** | **esf**}
   - for T1 lines
   - or for E1 lines
   - **framing** {**crc4** | **no-crc4**} [**australia**]
4. Do one of the following:
   - **linecode** {**ami** | **b8zs**}
   - for T1 lines
   - or for E1 lines
   - **linecode** {**ami** | **hdb3**}
5. **ds0-group** *channel-number* **timeslots** *range* **type** *type*
6. **exit**
7. Do one of the following:
   - **voice-port** *slot/port:ds0-group-no*
   - for Cisco 2600 and Cisco 3600 series
   - or for Cisco MC3810
   - **voice-port** *slot:ds0-group-no*
8. **dial-type** {**dtmf** | **mf** | **pulse**}
9. **exit**
10. **dial peer voice** *tag* **pots**
11. **application mgcpapp**
12. **port** *port-number*
13. **exit**
14. **mgcp** [*gw-port*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**controller** {**t1** | **e1**} *cntlr-number* **Example:** `Router(config)# controller {t1 | e1} cntlr-number`	Configures a T1 or E1 controller and enters controller configuration mode for the digital CAS port.
Step 2	**mode cas** **Example:** `Router(config-controller)# mode cas`	(Required for Cisco MC3810 only) Configures the T1 or E1 controller to support CAS mode.
Step 3	Do one of the following:	Selects frame type for T1 or E1 line.

	Command or Action	Purpose

	• **framing** {**sf** | **esf**}
	• for T1 lines
	• or for E1 lines
	• **framing** {**crc4** | **no-crc4**} [**australia**]
	Example:
	`Router(config-controller)# framing {sf | esf}`
	Example:
	Example:
	`Router(config-controller)# framing {crc4 | no-crc4} [australia]`
		T1 default is **sf**. E1 default is **crc4**.

Step 4	Do one of the following:
	• **linecode** {**ami** | **b8zs**}
	• for T1 lines
	• or for E1 lines
	• **linecode** {**ami** | **hdb3**}
	Example:
	`Router(config-controller)# linecode {ami | b8zs}`
	Example:
	Example:
	`Router(config-controller)# linecode {ami | hdb3}`
		Specifies the line encoding to use.
		T1 default is **ami**. E1 default is **hdb3**.

Step 5	**ds0-group** *channel-number* **timeslots** *range* **type** *type* **Example:** `Router(config-controller)# ds0-group channel-number timeslots range type type`	Specifies the DS0 time slots that make up a logical voice port on a T1 or E1 controller and specifies the signaling type by which the router connects to the PBX or PSTN. Use command-line interface (CLI) help (enter **?** after **type**) for valid signaling types.
Step 6	**exit** **Example:** `Router(config-controller)# exit`	Exits the current mode.
Step 7	Do one of the following: • **voice-port** *slot/port:ds0-group-no*	Enters voice-port configuration mode.

	Command or Action	Purpose

	• for Cisco 2600 and Cisco 3600 series
	• or for Cisco MC3810
	• **voice-port** *slot:ds0-group-no*
	Example:
	`Router(config)# voice-port slot /port :ds0-group-no`
	Example:
	Example:
	`Router(config)# voice-port slot :ds0-group-no`	

Step 8	**dial-type** {**dtmf** | **mf** | **pulse**} **Example:** `Router(config-voiceport)# dial-type {dtmf | mf | pulse}`	(Required for MF trunks) Specifies the type of out-dialing for voice port interfaces. Default is **dtmf**.
Step 9	**exit** **Example:** `Router(config-voiceport)# exit`	Exits the current mode.
Step 10	**dial peer voice** *tag* **pots** **Example:** `Router(config)# dial peer voice tag pots`	Enters dial-peer configuration mode and specifies the method of voice encapsulation.
Step 11	**application mgcpapp** **Example:** `Router(config-dial-peer)# application mgcpapp`	Enables the MGCP application on this dial peer.
Step 12	**port** *port-number* **Example:** `Router(config-dial-peer)# port port-number`	Associates a dial peer with a specific voice port.
Step 13	**exit** **Example:** `Router(config-dial-peer)# exit`	Exits the current mode.

	Command or Action	Purpose
Step 14	**mgcp** [*gw-port*] **Example:** `Router(config)# mgcp [gw-port ]`	Initiates the MGCP daemon. The optional port-number argument is the UDP port over which the gateway receives messages from the call agent (the gateway MGCP port number). Default is 2427.

ISUP Signaling Trunks

To identify endpoints and configure the MGCP application for use with Integrated Services Digital Network Upper Part (ISUP) signaling trunks, use these commands, beginning in global configuration mode:

SUMMARY STEPS

1. **controller** {**t1** | **e1**} *cntlr-number*
2. **ds0-group** *channel-number* **timeslots** *range* **type none service mgcp**
3. **exit**
4. **mgcp** [*gw-port*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**controller** {**t1**	**e1**} *cntlr-number* **Example:** `Router(config)# controller {t1 | e1} cntlr-number`	Configures a T1 or E1 controller and enters controller configuration mode for the ISUP trunk port.
Step 2	**ds0-group** *channel-number* **timeslots** *range* **type none service mgcp** **Example:** `Router(config-controller)# ds0-group channel-number timeslots range type none service mgcp`	Specifies the DS0 time slots that make up a logical voice port on a T1 or E1 controller and specifies the signaling type by which the router connects to the PBX or PSTN. Specify the **type none** and **service mgcp** options to identify this voice port as an MGCP endpoint.
Step 3	**exit** **Example:** `Router(config-controller)# exit`	Exits the current mode.
Step 4	**mgcp** [*gw-port*] **Example:** `Router(config)# mgcp [gw-port ]`	Initiates the MGCP daemon. The optional port number argument allows you to specify the UDP port over which the gateway receives messages from the call agent (the gateway MGCP port number). Default UDP port number for gateways is 2427.

FGD-OS Trunks

To identify endpoints and configure the MGCP application for use with Feature Group D Operator Services (FGD-OS) signaling over T1 or E1 trunks, use these commands, beginning in global configuration mode:

SUMMARY STEPS

1. **controller** {**t1** | **e1**} *cntlr-number*
2. **ds0-group** *channel-number* **timeslots** *range* **type fgd-os service mgcp**
3. **exit**
4. **mgcp** [*gw-port*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**controller** {**t1** | **e1**} *cntlr-number* **Example:** `Router(config)# controller {t1 | e1} cntlr-number`	Configures a T1 or E1 controller and enters controller configuration mode for the FGD-OS trunk port.
Step 2	**ds0-group** *channel-number* **timeslots** *range* **type fgd-os service mgcp** **Example:** `Router(config-controller)# ds0-group channel-number timeslots range type fgd-os service mgcp`	Specifies the DS0 time slots that make up a logical voice port on a T1 or E1 controller and specifies the signaling type by which the router connects to the PBX or PSTN. Specify the **type fgd-os** option for FGD-OS signaling, and the **service mgcp** option to identify this voice port as an MGCP endpoint.
Step 3	**exit** **Example:** `Router(config-controller)# exit`	Exits the current mode.
Step 4	**mgcp** [*gw-port*] **Example:** `Router(config)# mgcp [gw-port ]`	Initiates the MGCP daemon. The optional argument is the UDP port over which the gateway receives messages from the call agent (the gateway MGCP port number). Default is 2427.

Digital VoATM with AAL2 PVC

To identify endpoints and configure the MGCP application for use with digital Voice over Asynchronous Transfer Mode (VoATM) with ATM Adaptation Layer 2 (AAL2) Permanent Virtual Circuit (PVC), use these commands, beginning in global configuration mode:

SUMMARY STEPS

1. **controller** {**t1** | **e1**} *cntlr-number*
2. **mode atm**

3. Do one of the following:
   - **framing** {**sf** | **esf**}
   - for T1 lines
   - or for E1 lines
   - **framing** {**crc4** | **no-crc4**} [**australia**]
4. Do one of the following:
   - **linecode** {**ami** | **b8zs**}
   - for T1 lines
   - or for E1 lines
   - **linecode** {**ami** | **hdb3**}
5. **exit**
6. **dial peer voice** *tag* **pots**
7. **application mgcpapp**
8. **port** *port-number*
9. **exit**
10. **mgcp** [*gw-port*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**controller** {**t1** | **e1**} *cntlr-number* **Example:** `Router(config)# controller {t1 | e1} cntlr-number`	Enters dial-peer configuration mode and specifies the method of voice encapsulation.
Step 2	**mode atm** **Example:** `Router(config-controller)# mode atm`	Specifies that the controller supports ATM encapsulation and create ATM interface 0. When the controller is set to ATM mode, the following takes place: • Controller framing is automatically set to Extended Superframe (ESF). • The line code is automatically set to B8ZS.
Step 3	Do one of the following: • **framing** {**sf** | **esf**} • for T1 lines • or for E1 lines • **framing** {**crc4** | **no-crc4**} [**australia**] **Example:** `Router(config-controller)# framing {sf | esf}` **Example:**	Selects frame type for T1 or E1 line. T1 default is **sf**. E1 default is **crc4**.

	Command or Action	Purpose
	Example: `Router(config-controller)# framing {crc4 | no-crc4} [australia]`	

Step 4	Do one of the following:
	• **linecode** {**ami** | **b8zs**}
	• for T1 lines
	• or for E1 lines
	• **linecode** {**ami** | **hdb3**}
	Example:
	`Router(config-controller)# linecode {ami | b8zs}`
	Example:
	Example:
	`Router(config-controller)# linecode {ami | hdb3}`
		Specifies the line encoding to use.
		T1 default is **ami**. E1 default is **hdb3**.

Step 5	**exit** **Example:** `Router(config-controller)# exit`	Exits the current mode.
Step 6	**dial peer voice** *tag* **pots** **Example:** `Router(config)# dial peer voice tag pots`	Enters dial-peer configuration mode and specifies the method of voice encapsulation.
Step 7	**application mgcpapp** **Example:** `Router(config-dial-peer)# application mgcpapp`	Enables the MGCP application on this dial peer.
Step 8	**port** *port-number* **Example:** `Router(config-dial-peer)# port port-number`	Associates a dial peer with a specific voice port.
Step 9	**exit** **Example:** `Router(config-dial-peer)# exit`	Exits the current mode.

	Command or Action	Purpose
Step 10	**mgcp** [*gw-port*] **Example:** `Router(config)# mgcp [gw-port ]`	Initiates the MGCP daemon. The optional argument is the UDP port over which the gateway receives messages from the call agent (the gateway MGCP port number). Default is 2427.

Configuring Global MGCP Parameters

This optional task configures global MGCP parameters on the gateway so that you can set these values to conform to the requirements of the call agent, trunks, or lines that are being used with this gateway. The global parameter values that you configure are associated with every MGCP endpoint that you have identified on this gateway.

In addition to the global MGCP parameters, there are other MGCP parameters that apply only to MGCP profiles on the gateway. For configuration of profile-related parameters, see the Configuring an MGCP Profile and Profile-Related MGCP Parameters, on page 42.

Note The only parameter that is common to both profile and global configurations is the call-agent parameter, which is configured with the **call-agent** command for MGCP profile configuration and with the **mgcp call-agent** command for the global configuration. These commands are mutually exclusive; whichever command you configure first blocks configuration of the other. For example, if the MGCP profile **call-agent** command is configured on an endpoint, then you are not allowed to configure the global **mgcp call-agent**command.

To configure global MGCP parameters, complete these steps as needed, beginning in global configuration mode:

SUMMARY STEPS

1. **mgcp call-agent** {*dns-name* | *ip-address*} [*port*] [**service-type** *type*] [**version** *protocol-version*]
2. **mgcp behavior** {**auep** | **signal**} **v0.1**
3. **mgcp sdp simple**
4. **mgcp sdp xpc-codec**
5. **mgcp codec** *type* [**packetization-period** *value*]
6. **no mgcp timer receive-rtcp**
7. **no mgcp piggyback message**
8. **mgcp endpoint offset**
9. **mgcp persistent** {**hookflash** | **offhook** | **onhook**}
10. **mgcp request timeout** {*timeout-value* | **max** *maxtimeout-value*}
11. **mgcp dtmf-relay voip codec** {**all** | **low-bit-rate**} **mode** {**cisco** | **nse** | **out-of-band**}
12. **mgcp max-waiting-delay** *value*
13. **mgcp restart-delay** *value*
14. **mgcp vad**
15. **mgcp ip-tos** {**high-reliability** | **high-throughput** | **low-cost** | **low-delay** | **rtp precedence** *value* | **signaling precedence** *value*}

16. **mgcp quality-threshold** {**hwm-cell-loss** *value* | **hwm-jitter-buffer** *value* | **hwm-latency** *value* | **hwm-packet-loss** *value* | **lwm-cell-loss** *value* | **lwm-jitter-buffer** *value* | **lwm-latency** *value* | **lwm-packet-loss** *value*}
17. **mgcp playout** { **adaptive** *init-value min-value max-value* | **fax** *value* | **fixed** *init-value*
18. **mgcp package-capability** [*package-type*]
19. **mgcp default package** [*package-type*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**mgcp call-agent** {*dns-name* | *ip-address*} [*port*] [**service-type** *type*] [**version** *protocol-version*] **Example:** `Router(config)# mgcp call-agent {dns-name	ip-address} [port] [service-type type] [version protocol-version]`	Configures parameters for communicating with the call agent (media gateway controller). **Note** You can define a call agent globally with the **mgcp call-agent** command, or locally for each MGCP profile with the **call-agent** command, but not both. Whichever command you configure first blocks configuration of the other.
Step 2	**mgcp behavior** {**auep** | **signal**} **v0.1** **Example:** `Router(config)# mgcp behavior {auep	signal} v0.1`	(Optional) Forces a gateway to follow the MGCP Version 0.1 protocol for a specified behavior. All other MGCP functionality continues to behave according to the version of MGCP that is specified in the **mgcp call-agent** command. • **auep** --Forces the gateway to reply to an Audit Endpoint (AUEP) command according to the MGCP Version 0.1 specification. If this keyword is used, an AUEP command on an out-of-service endpoint results in a return code of 501. Use this keyword with Cisco IOS Release 12.3(2)T1 or a later release. • **signal** --Forces the gateway to handle signaling tones according to the MGCP Version 0.1 specification. The MGCP 0.1 specification treats call signaling tones as on-off tones, which terminate only after a specific MGCP message has been sent to stop the signal. The specifications for MGCP 1.0 and later versions treat call signaling tones as timeout tones, which terminate when the appropriate timeout timer expires. Use this keyword with Cisco IOS Release 12.3(4)T or a later release. • **v0.1** --Selects MGCP Version 0.1.
Step 3	**mgcp sdp simple** **Example:** `Router(config)# mgcp sdp simple`	Specifies that a subset of the SDP fields should be used.

	Command or Action	Purpose
Step 4	**mgcp sdp xpc-codec** **Example:** `Router(config)# mgcp sdp xpc-codec`	Enables codec negotiation in the SDP.
Step 5	**mgcp codec** *type* [**packetization-period** *value*] **Example:** `Router(config)# mgcp codec type [packetization-period value]`	Selects the default codec type and its optional packetization period value.
Step 6	**no mgcp timer receive-rtcp** **Example:** `Router(config)# no mgcp timer receive-rtcp`	Disables the timer used by a gateway to disconnect a VoIP call when the IP connectivity is lost with the remote gateway. The timer is known as the RTP Control Protocol (RTCP) transmission interval timer.
Step 7	**no mgcp piggyback message** **Example:** `Router(config)# no mgcp piggyback message`	Disables piggyback messages.
Step 8	**mgcp endpoint offset** **Example:** `Router(config)# mgcp endpoint offset`	Increments the voice-port or DS0-group portion of the endpoint name for NCS 1.0.
Step 9	**mgcp persistent** {**hookflash** | **offhook** | **onhook**} **Example:** `Router(config)# mgcp persistent {hookflash | offhook | onhook}`	Enables call-agent notification of the specified type of event.
Step 10	**mgcp request timeout** {*timeout-value* | **max** *maxtimeout-value*} **Example:** `Router(config)# mgcp request timeout {timeout-value | max maxtimeout-value }`	Specifies how long the gateway waits for a call-agent response to a request before retransmitting the request.
Step 11	**mgcp dtmf-relay voip codec** {**all** | **low-bit-rate**} **mode** {**cisco** | **nse** | **out-of-band**} **Example:** `Router(config)# mgcp dtmf-relay voip codec {all | low-bit-rate} mode {cisco | nse | out-of-band}`	Ensures accurate forwarding of digits with a compressed codec.

	Command or Action	Purpose
Step 12	**mgcp max-waiting-delay** *value* **Example:** `Router(config)# mgcp max-waiting-delay value`	Specifies the number of milliseconds to wait after a restart before connecting with the call agent. Range is from 0 to 600,000 (600 seconds). Default is 3000. If used, these values should be staggered among gateways to avoid having large numbers of gateways connecting with the call agent at the same time after a mass restart.
Step 13	**mgcp restart-delay** *value* **Example:** `Router(config)# mgcp restart-delay value`	Sets the delay value sent in the RestartInProgress (RSIP) graceful teardown, in seconds. Range is from 0 to 600. Default is 0.

Step 14	**mgcp vad**
	Example:
	`Router(config)#`
	`mgcp vad`
		Enables voice activity detection (VAD) as a default for MGCP calls. Default is disabled.

Step 15	**mgcp ip-tos** {**high-reliability** | **high-throughput** | **low-cost** | **low-delay** | **rtp precedence** *value* | **signaling precedence** *value*} **Example:** `Router(config)# mgcp ip-tos {high-reliability | high-throughput | low-cost | low-delay | rtp precedence value | signaling precedence value }`	Enables the IP type of service (ToS) for MGCP-controlled connections.
Step 16	**mgcp quality-threshold** {**hwm-cell-loss** *value* | **hwm-jitter-buffer** *value* | **hwm-latency** *value* | **hwm-packet-loss** *value* | **lwm-cell-loss** *value* | **lwm-jitter-buffer** *value* | **lwm-latency** *value* | **lwm-packet-loss** *value*} **Example:** `Router(config)# mgcp quality-threshold {hwm-cell-loss value	hwm-jitter-buffer value	hwm-latency value	hwm-packet-loss value	lwm-cell-loss value	lwm-jitter-buffer value	lwm-latency value	lwm-packet-loss value }`	Sets the jitter buffer size threshold, latency threshold, and packet-loss threshold parameters.
Step 17	**mgcp playout** { **adaptive** *init-value min-value max-value* | **fax** *value* | **fixed** *init-value* **Example:**	Configures the jitter buffer packet size in milliseconds for MGCP calls. The default is **adaptive** 60 4 200 • **adaptive** *init-value min-value max-value* --Defines the range for the jitter-buffer packet size. The range

	Command or Action	Purpose
	`Router(config)# mgcp playout {adaptive init-value min-value max-value | fax value | fixed init-value }`	for each value is 4 to 250. Default is 60 4 200. Note that *init-value* must be between *min-value*and *max-value*. • **fax** *value* --Defines the fax playout buffer size. The range is 0 to 700. The default value is 300. The range and default value might vary with different platforms. See the platform digital signal processor (DSP) specifications before setting this value. • **fixed** *init-value* --Defines the fixed size for the jitter-buffer packet size. The range is 4 to 250. There is no default value.

Step 18	**mgcp package-capability** [*package-type*]
	Example:
	`Router(config)#`
	`mgcp package-capability`
	`[package-type ]`
		Specifies an MGCP package to be supported on this gateway. Configure one package at a time and repeat this command to configure support for more than one package. Available package types vary with the type of gateway.

Step 19	**mgcp default package** [*package-type*]
	Example:
	`Router(config)#`
	`mgcp default package [package-type ]`
		Defines the package to be used as the default when no package is named with an event. Available package types vary with the type of gateway.

Configuring an MGCP Profile and Profile-Related MGCP Parameters

This optional task creates a named, user-defined MGCP profile that consists of a subset of all the MGCP endpoints on this gateway. More than one MGCP profile can be configured on a gateway. Each MGCP profile is associated with a call agent and one or more endpoints. When multiple MGCP profiles are configured, endpoints on a single media gateway can be controlled by different call agents. When each endpoint comes on line, an RSIP (RestartInProgress) message notifies the appropriate call agent of the endpoint's presence.

Note When partitioning a gateway for multiple call-agent control, the call agents must be coordinated so that there are no overlapping transaction identification numbers.

In addition, this task allows you to configure profile-related MGCP parameters to conform to the requirements of the call agent, trunks, or lines that are being used with the profile's endpoints. These parameters are called profile-related MGCP parameters because they are associated with a particular MGCP profile, or subset of endpoints, and they are configured in MGCP profile configuration mode. Other parameters are considered

global MGCP parameters; when they are configured, they apply to all the endpoints on a gateway. Global MGCP parameters are discussed in the Configuring Global MGCP Parameters, on page 38.

The parameters for an MGCP profile are configured in a special MGCP profile configuration mode that you enter with the **mgcp profile** command. One or more endpoints are associated with the profile by using the **voice-port** command in MGCP profile configuration mode.

Note The only parameter that can be configured in both profile configuration mode and in global configuration mode is call agent, which is configured with the **call-agent** command for MGCP profiles, and with the **mgcp call-agent** command for global configurations. These commands are mutually exclusive; whichever command you configure first blocks configuration of the other. For example, if the MGCP profile **call-agent** command is configured on an endpoint, then you are not allowed to configure the global **mgcp call-agent** command.

You do not have to define MGCP profiles to configure profile-related parameters. For endpoints that are not associated with a user-defined MGCP profile, the values for profile-related parameters are provided by a predefined profile with the name *default* . The default profile is configured in the same way that a user-defined MGCP profile is configured, except that the keyword **default** is used in place of a profile name in the **mgcp profile** command. The default profile has no association with voice ports or a call agent (the call agent for these endpoints is defined by the global **mgcp call-agent** command).

In the excerpt below from a **show running-config** command output, two MGCP profiles are defined: MAX1 and MAX2. Each profile is associated with a different call agent and a different voice port. The MAX1 profile is configured with a value of 3 for the max1 retries parameter and 5 for max2 retries. The MAX2 profile uses the values in the default profile for those parameters. In the MAX2 profile, the MT package is configured as a persistent package. The max1 retries parameter for the default profile is configured with a value of 2. The max2 retries parameter is not configured, so the value used is the default value, which is 7. The MAX2 profile has a value of 2 for the max1 retries parameter and 7 for max2 retries.

```
!
mgcp profile MAX1
 call agent ca1.example.com 4022 service-type mgcp version 1.0
 max1 retries 3
 max2 retries 5
 voice-port 2/1:1
!
mgcp profile MAX2
 call-agent ca2.example.com 50031 service-type mgcp version 0.1
 package persistent mt-package
 voice-port 2/0:1
!
mgcp profile default
 max1 retries 2
```

To configure parameters for a user-defined MGCP profile or for the default profile, use the following commands as appropriate, beginning in global configuration mode:

SUMMARY STEPS

1. **mgcp profile** {*profile-name* | **default**}
2. **description** *text*
3. **call-agent** {*dns-name* | *ip-address*} [*port*] [**service-type** *type*] [**version** *protocol-version*]
4. **voice-port** *port-number*
5. **default** *command*

6. **package persistent** *package-name*
7. **timeout tsmax** *tsmax-value*
8. **timeout tdmax** *tdmax-value*
9. **timeout tdinit** *tdinit-value*
10. **timeout tcrit** *tcrit-value*
11. **timeout tpar** *tpar-value*
12. **timeout thist** *thist-value*
13. **timeout tone mwi** *mwitone-value*
14. **timeout tone ringback** *ringbacktone-value*
15. **timeout tone ringback connection** *connectiontone-value*
16. **timeout tone network congestion** *congestiontone-value*
17. **timeout tone busy** *busytone-value*
18. **timeout tone dial** *dialtone-value*
19. **timeout tone dial stutter** *stuttertone-value*
20. **timeout tone ringing** *ringingtone-value*
21. **timeout tone ringing distinctive** *distinctivetone-value*
22. **timeout tone reorder** *reordertone-value*
23. **timeout tone cot1** *continuity1tone-value*
24. **timeout tone cot2** *continuity2tone-value*
25. **max1 lookup**
26. **max1 retries** *value*
27. **max2 lookup**
28. **max2 retries** *value*
29. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**mgcp profile** {*profile-name* | **default**} **Example:** `Router(config)# mgcp profile {profile-name | default}`	Initiates MGCP profile mode, in which you create and configure a named MGCP profile associated with one or more endpoints, or configure the default profile. Effective with Cisco IOS Release 12.4(24)T3, the maximum number of MGCP profiles that can be configured is increased from 13 (12 plus 1 default) to 29 (28 plus 1 default).
Step 2	**description** *text* **Example:** `Router(config-mgcp-profile)# description text`	Provides a description for the profile.
Step 3	**call-agent** {*dns-name* | *ip-address*} [*port*] [**service-type** *type*] [**version** *protocol-version*] **Example:**	Defines the call agent's DNS name or IP address, UDP port number, service type, and protocol version. (Not used when configuring the default profile.)

	Command or Action	Purpose
	`Router(config-mgcp-profile)# call-agent {dns-name	ip-address } [port] [service-type type] [version protocol-version]`	**Note** You can define a call agent globally with the **mgcp call-agent**command, or locally for each MGCP profile with the **call-agent**command, but not both. Whichever command you configure first blocks configuration of the other.
Step 4	**voice-port** *port-number* **Example:** `Router(config-mgcp-profile)# voice-port port-number`	Provides the voice port number or DS0 group number for the endpoint to be associated with this MGCP profile. Repeat this command to add more than one endpoint to the profile. (Not used when configuring the default profile.)
Step 5	**default** *command* **Example:** `Router(config-mgcp-profile)# default command`	Restores the parameter represented by *command* to its default value.
Step 6	**package persistent** *package-name* **Example:** `Router(config-mgcp-profile)# package persistent package-name`	Configures the package type used when reporting persistent events for an MF CAS endpoint type. Valid types are **ms-package** and **mt-package.**Default is **ms-package**.
Step 7	**timeout tsmax** *tsmax-value* **Example:** **Example:** `Router(config-mgcp-profile)# timeout tsmax tsmax-value`	Configures the maximum timeout value after which MGCP messages are removed from the retransmission queue, in seconds. Range is from 1 to 1000. Default is 20.
Step 8	**timeout tdmax** *tdmax-value* **Example:** `Router(config-mgcp-profile)# timeout tdmax tdmax-value`	Configures the maximum timeout value for the disconnected procedure (Tdmax), in seconds. Range is from 300 to 600. Default is 600.
Step 9	**timeout tdinit** *tdinit-value* **Example:** `Router(config-mgcp-profile)# timeout tdinit tdinit-value`	Configures the initial waiting delay value (Tdinit) used as the timer for the disconnect procedure, in seconds. Range is from 1 to 30. Default is 15.

	Command or Action	Purpose
Step 10	**timeout tcrit** *tcrit-value* **Example:** `Router(config-mgcp-profile)# timeout tcrit tcrit-value`	Configures the critical timeout value (Tcritical) for the interdigit timer used in digit map matching, in seconds. Range is from 1 to 600. Default is 4.
Step 11	**timeout tpar** *tpar-value* **Example:** `Router(config-mgcp-profile)# timeout tpar tpar-value`	Configures the partial timeout value (Tpartial) for the interdigit timer used in digit map matching, in seconds. Range is from 1 to 60. Default is 16.
Step 12	**timeout thist** *thist-value* **Example:** `Router(config-mgcp-profile)# timeout thist thist-value`	Configures the packet storage timeout value, in seconds. Range is from 1 to 1100. Default is 30.
Step 13	**timeout tone mwi** *mwitone-value* **Example:** `Router(config-mgcp-profile)# timeout tone mwi mwitone-value`	Configures the message waiting indicator timeout value, in seconds. Range is from 1 to 600. Default is 16.
Step 14	**timeout tone ringback** *ringbacktone-value* **Example:** `Router(config-mgcp-profile)# timeout tone ringback ringbacktone-value`	Configures the ringback tone timeout value, in seconds. Range is from 1 to 600. Default is 180.
Step 15	**timeout tone ringback connection** *connectiontone-value* **Example:** `Router(config-mgcp-profile)# timeout tone ringback connection connectiontone-value`	Configures the timeout value for ringback tone on connection, in seconds. Range is from 1 to 600. Default is 180.
Step 16	**timeout tone network congestion** *congestiontone-value* **Example:** `Router(config-mgcp-profile)# timeout tone network congestion congestiontone-value`	Configures the network congestion tone timeout value, in seconds. Range is from 1 to 600. Default is 180.
Step 17	**timeout tone busy** *busytone-value* **Example:** `Router(config-mgcp-profile)# timeout tone busy busytone-value`	Configures the busy tone timeout value, in seconds. Range is from 1 to 600. Default is 3.

	Command or Action	Purpose
Step 18	**timeout tone dial** *dialtone-value* **Example:** `Router(config-mgcp-profile)# timeout tone dial dialtone-value`	Configures the dial tone timeout value, in seconds. Range is from 1 to 600. Default is 16.
Step 19	**timeout tone dial stutter** *stuttertone-value* **Example:** `Router(config-mgcp-profile)# timeout tone dial stutter stuttertone-value`	Configures the stutter dial tone timeout value, in seconds. Range is from 1 to 600. Default is 16.
Step 20	**timeout tone ringing** *ringingtone-value* **Example:** `Router(config-mgcp-profile)# timeout tone ringing ringingtone-value`	Configures the ringing tone timeout value, in seconds. Range is from 1 to 600. Default is 180.
Step 21	**timeout tone ringing distinctive** *distinctivetone-value* **Example:** `Router(config-mgcp-profile)# timeout tone ringing distinctive distinctivetone-value`	Configures the distinctive ringing tone timeout value, in seconds. Range is from 1 to 600. Default is 180.
Step 22	**timeout tone reorder** *reordertone-value* **Example:** `Router(config-mgcp-profile)# timeout tone reorder reordertone-value`	Configures the reorder tone timeout value, in seconds. Range is from 1 to 600. Default is 30.
Step 23	**timeout tone cot1** *continuity1tone-value* **Example:** `Router(config-mgcp-profile)# timeout tone cot1 continuity1tone-value`	Configures the continuity1 tone timeout value, in seconds. Range is from 1 to 600. Default is 3.
Step 24	**timeout tone cot2** *continuity2tone-value* **Example:** `Router(config-mgcp-profile)# timeout tone cot2 continuity2tone-value`	Configures the continuity2 tone timeout value, in seconds. Range is from 1 to 600. Default is 3.
Step 25	**max1 lookup** **Example:** `Router(config-mgcp-profile)# max1 lookup`	Enables the DNS lookup procedure after the suspicion threshold is reached. Default is enabled.

	Command or Action	Purpose
Step 26	**max1 retries** *value* **Example:** `Router(config-mgcp-profile)# max1 retries value`	Sets the suspicion threshold number of retries. Range is from 3 to 30. Default is 5.
Step 27	**max2 lookup** **Example:** `Router(config-mgcp-profile)# max2 lookup`	Enables the DNS lookup procedure after the disconnect threshold is reached. Default is enabled.
Step 28	**max2 retries** *value* **Example:** `Router(config-mgcp-profile)# max2 retries value`	Sets the disconnect threshold number of retries. Range is from 3 to 30. Default is 7.
Step 29	**exit** **Example:** `Router(config-mgcp-profile)# exit`	Exits the current mode.

Verifying the Configuration

SUMMARY STEPS

1. **show running-configuration**
2. **show mgcp** [**connection** | **endpoint** | **profile** [*profile-name*] | **statistics**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show running-configuration** **Example:** `Router# show running-configuration`	Displays the current configuration settings.
Step 2	**show mgcp** [**connection**	**endpoint**	**profile** [*profile-name*]	**statistics** **Example:** `Router# show mgcp [connection	endpoint	profile [profile-name]	statistics]`	Displays the current MGCP settings.

Troubleshooting Tips

The following suggestions help with troubleshooting:

- Use the **show running-config** command to verify that the following are properly configured:
  - For CAS and POTS endpoints, POTS dial peers are configured with the **mgcpapp** application.
  - The correct packages are enabled in the **mgcp package-capability** command.
  - The **mgcp call-agent** or **call-agent** command defines the call agent and service type correctly.
- Reset the MGCP statistical counters with the **clear mgcp statistics**command.
- If RTP traffic is not getting through, make sure that IP routing is enabled. Use the **show rtp statistics**command, then use the **debug ip udp** command and track down the MGCP RTP packets.

```
Router# show rtp statistics
RTP Statistics info:
No. CallId Xmit-pkts Xmit-bytes Rcvd-pkts  Rcvd-bytes Lost pkts  Jitter Latenc
1   17492  0x8A      0x5640     0x8A       0x5640     0x0        0x0      0x0
Router# show rtp statistics
RTP Statistics info:
No. CallId Xmit-pkts Xmit-bytes Rcvd-pkts  Rcvd-bytes Lost pkts  Jitter Latenc
1   17492  0xDA      0x8840     0xDB       0x88E0     0x0        0x160    0x0
```

- If an RSIP message is not received by the call agent, make sure that the **mgcp call-agent**command or the MGCP profile **call-agent** command is configured with the correct call agent name or IP address and UDP port. Use the **show mgcp** command or the **show mgcp profile** command to display this information:

```
Router# show mgcp
MGCP Admin State ACTIVE, Oper State ACTIVE - Cause Code NONE
MGCP call-agent: 172.29.248.51  Initial protocol service is MGCP, v. 1.0
...
MGCP gateway port: 2727, MGCP maximum waiting delay 3000
...
Router# show mgcp profile
MGCP Profile nycprofile
Description: NY branch office configuration
Call-agent: 10.14.2.200 Initial protocol service is MGCP, v. 1.0
```

- To verify connections and endpoints, use the **show mgcp** command:

```
Router# show mgcp connection
Endpoint  Call_ID(C) Conn_ID(I) (P)ort (M)ode (S)tate (C)odec (E)vent[SIFL] (R)esult[EA]
1. S0/DS1-1/5      C=F123AB,5,6  I=0x3  P=16506,16602  M=3  S=4  C=1 E=2,0,0,2  R=0,0
2. S0/DS1-1/6      C=F123AB,7,8  I=0x4  P=16602,16506  M=3  S=4  C=1 E=0,0,0,0  R=0,0
Router# show mgcp endpoint
T1/0 ds0-group 0 timeslots 1-24
T1/1 ds0-group 0 timeslots 1-24
T1/2 ds0-group 0 timeslots 1-24
T1/3 ds0-group 0 timeslots 1-24
```

- If an MGCP message is rejected, it may be because the remote media gateway does not support SDP mandatory parameters (the *o*= , *s*= , and *t*= lines). If this is the case, configure the **mgcp sdp simple** command to send SDP messages without those parameters.
- If you notice problems with voice quality, make sure that the **cptone** (voice-port configuration) command is set for the correct country code. Capturing RTP packets from the sniffer may help to debug the problem, such as whether the payload type or timestamps are set correctly, and so forth.

- To check operation of interfaces, use the **show interface**command.
- To view information about activity on the T1 or E1 line, use the **show controllers** command. Alarms, line conditions, and other errors are displayed. The data is updated every 10 seconds; and every 15 minutes, the cumulative data is stored and retained for 24 hours.
- When necessary, you can enable debug traces for errors, events, media, packets, and parser. The command **debug mgcp packets** can be used to verify that your packets are arriving at the gateway and to monitor message flow in general. Note that there is always a performance penalty when using debug commands. The sample output below shows the use of the optional **input-hex** keyword to enable display of hexadecimal values.

```
Router# debug mgcp packets input-hex
Media Gateway Control Protocol input packets in hex value debugging is on
MGCP Packet received -
DLCX 49993 * MGCP 0.1
MGCP Packet received in hex -
44 4C 43 58 20 34 39 39 39 33 20 2A 20 4D 47 43 50 20 30 2E 31 A
send_mgcp_msg, MGCP Packet sent --->
250 49993
```

Configuration Examples for MGCP 1.0

Cisco uBR925 Using Radio Frequency Interface Example

This example shows how to set up a Cisco uBR925 as an MGCP residential gateway. The call agent is specified to the cable router (Cisco uBR925, Cisco CVA122, or Cisco CVA122E) by a Dynamic Host Configuration Protocol (DHCP) offer on a cable radio frequency (RF) network. On completion of the DHCP offer, the call agent is set in the MGCP profile on the cable modem. This setting is displayed with the **show mgcp profile** command. The router does not show the call agent in the CLI.

```
version 12.2
no service single-slot-reload-enable
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname hydepark
!
logging rate-limit console 10 except errors
!
clock timezone - 0 6
ip subnet-zero
no ip routing
ip domain-name example.com
ip name-server 10.0.0.229
!
ip ssh time-out 120
ip ssh authentication-retries 3
no ip dhcp-client network-discovery
!
interface Ethernet0
 ip address 192.168.0.11 255.255.0.0
 no ip route-cache
```

```
 no ip mroute-cache
 bridge-group 59
 bridge-group 59 spanning-disabled
!
interface cable-modem0
 no ip route-cache
 no ip mroute-cache
 cable-modem boot admin 2
 cable-modem boot oper 5
 bridge-group 59
 bridge-group 59 spanning-disabled
!
ip classless
no ip http server
no ip http cable-monitor
!
snmp-server manager
!
voice-port 0
 input gain -2
 output attenuation 0
!
voice-port 1
 input gain -2
 output attenuation 0
!
mgcp
! Use this CLI with NCS 1.0
mgcp endpoint offset
!
mgcp profile default
!
dial-peer voice 100 pots
 application MGCPAPP
 port 0
!
dial-peer voice 101 pots
 application MGCPAPP
 port 1
!
line con 0
line vty 0 4
 login
!
end
```

Cisco uBR925 Using Ethernet0 Interface Example

This example shows how to set up a Cisco uBR925 as a residential gateway:

```
version 12.2
no service single-slot-reload-enable
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname monticello
!
logging rate-limit console 10 except errors
!
clock timezone - 0 6
```

```
ip subnet-zero
ip domain-name example.com
ip name-server 10.0.0.229
!
ip ssh time-out 120
ip ssh authentication-retries 3
no ip dhcp-client network-discovery
!
interface Ethernet0
 ip address 192.168.0.11 255.255.0.0
 no ip route-cache
 no ip mroute-cache
 bridge-group 59
 bridge-group 59 spanning-disabled
!
interface cable-modem0
 no ip route-cache
 no ip mroute-cache
 shutdown
 cable-modem boot admin 2
 cable-modem boot oper 5
 no cable-modem compliant bridge
 cable-modem voip clock-internal
 bridge-group 59
 bridge-group 59 spanning-disabled
!
ip classless
no ip http server
no ip http cable-monitor
!
ip default-gateway 172.16.1.1
!
! We are using the cable modem without its RF interface. So
! route IP traffic out the Ethernet0 interface.
!
ip route 0.0.0.0 0.0.0.0 Ethernet0
!
snmp-server manager
!
voice-port 0
 input gain -2
 output attenuation 0
!
voice-port 1
 input gain -2
 output attenuation 0
!
mgcp
!
! The ip address of call agent below can be a FQDN as well.
mgcp call-agent 10.0.0.224 service-type ncs version 1.0
! Use this CLI with NCS 1.0
mgcp endpoint offset
!
mgcp profile default
!
dial-peer voice 100 pots
 application MGCPAPP
 port 0
!
dial-peer voice 101 pots
 application MGCPAPP
 port 1
!
```

```
line con 0
line vty 0 4
 login
!
end
```

Cisco CVA122 Using Radio Frequency Interface Example

The call agent is specified to the cable router (Cisco uBR925, Cisco CVA122, or Cisco CVA122E) by a DHCP offer on a cable RF network. On completion of the DHCP offer, the call agent is set in the MGCP profile on the cable modem. This setting is displayed with the **show mgcp profile** command. The router does not show the call agent in the CLI.

```
version 12.2
no service single-slot-reload-enable
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service internal
!
hostname mtvernon
!
no logging buffered
logging rate-limit console 10 except errors
!
clock timezone - -5
ip subnet-zero
no ip routing
ip domain-name example.com
ip name-server 10.0.0.229
!
no ip dhcp-client network-discovery
!
interface Ethernet0
 ip address 10.20.0.59 255.255.0.0
 no ip route-cache
 no ip mroute-cache
 shutdown
 bridge-group 59
 bridge-group 59 spanning-disabled
!
interface cable-modem0
 no ip route-cache
 no ip mroute-cache
 cable-modem boot admin 2
 cable-modem boot oper 5
 bridge-group 59
 bridge-group 59 spanning-disabled
!
interface usb0
 ip address 10.20.0.59 255.255.0.0
 no ip route-cache
 no ip mroute-cache
 arp timeout 0
 bridge-group 59
 bridge-group 59 spanning-disabled
!
ip classless
no ip http server
no ip http cable-monitor
```

```
!
access-list 1 deny   10.0.0.254
access-list 1 permit any
snmp-server packetsize 4096
snmp-server manager
call rsvp-sync
!
voice-port 0
 input gain -2
 output attenuation 0
 timeouts interdigit 2
!
voice-port 1
 input gain -2
 output attenuation 0
 timeouts interdigit 2
!
mgcp
!
mgcp profile default
!
mgcp profile test
 call-agent test service-type ncs version 1.0
!
dial-peer voice 100 pots
 application MGCPAPP
 port 0
!
dial-peer voice 101 pots
 application MGCPAPP
 port 1
!
line con 0
 exec-timeout 0 0
line vty 0 4
 exec-timeout 0 0
 login
!
end
```

Cisco 2600 Series as a Residential Gateway Example

This example shows a Cisco 2620 router being configured as an analog residential gateway:

```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname betty-2620
!
voice-port 1/0/0
!
voice-port 1/0/1
!
dial-peer voice 1 pots
application mgcpapp
destination-pattern 100
port 1/0/0
!
dial-peer voice 2 pots
application mgcpapp
```

```
destination-pattern 101
port 1/0/1
!
process-max-time 200
!
mgcp 4000
mgcp call-agent 10.14.2.200 4000 service-type mgcp version 1.0
mgcp sdp simple
no mgcp timer receive-rtcp
mgcp sdp xpc-codec
no mgcp piggyback message
mgcp endpoint offset
no mgcp persistent hook on
no mgcp persistent hook flash
mgcp request timeout 1000
mgcp dtmf-relay codec all mode cisco
mgcp max-waiting-delay 600000
mgcp restart-delay 500
mgcp codec g711ulaw packetization-period 10
mgcp ip-tos rtp precedence 7
mgcp quality-threshold lwm-jitter-buffer 59
mgcp quality-threshold lwm-latency 199
mgcp quality-threshold lwm-packet-loss 2
mgcp playout adaptive 100 50 150
mgcp package-capability dtmf-package
mgcp package-capability mf-package
mgcp package-capability rtp-package
mgcp package-capability as-package
isdn voice-call-failure 0
srcp 2428
cns event-service server
!
mgcp profile cisco
 call-agent 10.14.2.200 4000 service-type mgcp version 1.0
 voice-port 0:1
 package persistent mt-package
 timeout tsmax 100
 timeout tdinit 30
 timeout tcrit 600
 timeout tpar 600
 timeout thist 60
 timeout tone mwi 600
 timeout tone ringback 600
 timeout tone ringback connection 600
 timeout tone network congestion 600
 timeout tone busy 600
 timeout tone dial 600
 timeout tone dial stutter 600
 timeout tone ringing 600
 timeout tone ringing distinctive 600
 timeout tone reorder 600
 timeout tone cot1 600
 timeout tone cot2 600
 max1 retries 10
 no max2 lookup
 max2 retries 10
!
interface Ethernet0/0
 ip address 10.14.12.9 255.0.0.0
!
interface Ethernet0/1
 no ip address
 shutdown
!
```

```
ip classless
ip route 0.0.0.0 0.0.0.0 10.14.0.1
no cdp run
!
line con 0
exec-timeout 0 0
line aux 0
line vty 0 4
exec-timeout 0 0
 password test
 login
!
end
```

Cisco 3660 Platform as a Trunking Gateway Example

This example shows a Cisco 3660 that is being configured for CAS trunks. The association of endpoints with the MGCP application is made in the dial-peer configuration.

```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname charley-3660
!
controller t1 1/0
 linecode b8zs
 clock source line secondary 1
 ds0-group 0 timeslots 1-24 type e&m-winkstart
!
controller t1 1/1
 linecode b8zs
 clock source line secondary 1
 ds0-group 0 timeslots 1-24 type e&m-winkstart
!
ip subnet-zero
!
voice-port 1/0:0
 dial-type mf
!
voice-port 1/1:0
 dial-type mf
!
dial-peer voice 1 pots
 application mgcpapp
 destination-pattern 100
 port 1/0:0
!
dial-peer voice 2 pots
 application mgcpapp
 destination-pattern 101
 port 1/1:0
!
mgcp 4000
mgcp call-agent 10.14.2.200 4000 service-type mgcp version 1.0
mgcp sdp simple
no mgcp timer receive-rtcp
mgcp sdp xpc-codec
no mgcp piggyback message
mgcp endpoint offset
mgcp persistent hook on
```

```
mgcp persistent hook flash
mgcp request timeout 1000
mgcp dtmf-relay codec all mode cisco
mgcp max-waiting-delay 600000
mgcp restart-delay 500
mgcp codec g711ulaw packetization-period 10
mgcp ip-tos rtp precedence 7
mgcp quality-threshold lwm-jitter-buffer 59
mgcp quality-threshold lwm-latency 199
mgcp quality-threshold lwm-packet-loss 2
mgcp playout adaptive 100 50 150
mgcp package-capability dtmf-package
mgcp package-capability mf-package
mgcp package-capability rtp-package
mgcp package-capability as-package
isdn voice-call-failure 0
srcp 2428
cns event-service server
!
mgcp profile cisco
 call-agent 10.14.2.200 4000 service-type mgcp version 1.0
 voice-port 1/0:0
 package persistent mt-package
 timeout tsmax 100
 timeout tdinit 30
 timeout tcrit 600
 timeout tpar 600
 timeout thist 60
 timeout tone mwi 600
 timeout tone ringback 600
 timeout tone ringback connection 600
 timeout tone network congestion 600
 timeout tone busy 600
 timeout tone dial 600
 timeout tone dial stutter 600
 timeout tone ringing 600
 timeout tone ringing distinctive 600
 timeout tone reorder 600
 timeout tone cot1 600
 timeout tone cot2 600
 max1 retries 10
 no max2 lookup
 max2 retries 10
!
interface FastEthernet0/0
 ip address 10.14.12.12 255.0.0.0
 speed auto
 duplex auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.14.0.1
no ip http server
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
line vty 0 4
```

```
 exec-timeout 0 0
 password trial
 login
!
end
```

Cisco MC3810 as a Residential Gateway Example

The following example shows a Cisco MC3810 being configured as a residential gateway:

```
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log uptime
!
hostname harry
!
logging buffered
!
ip subnet-zero
ip host buffalo 192.168.254.254
!
mgcp
mgcp call-agent 10.14.90.1
!
voice-card 0
 codec complexity high
!
controller T1 0
 framing esf
 linecode b8zs
!
interface Ethernet0
 ip address 10.14.92.3 255.255.0.0
!
interface Serial0
 shutdown
!
interface Serial1
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
!
interface FR-ATM20
 no ip address
 shutdown
!
ip default-gateway 10.14.0.1
ip route 192.168.254.0 255.255.255.0 10.14.0.1
!
voice-port 1/1
!
dial-peer voice 1 pots
 application mgcpapp
 port 1/1
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
line 2 3
```

```
line vty 0 4
login
!
end
```

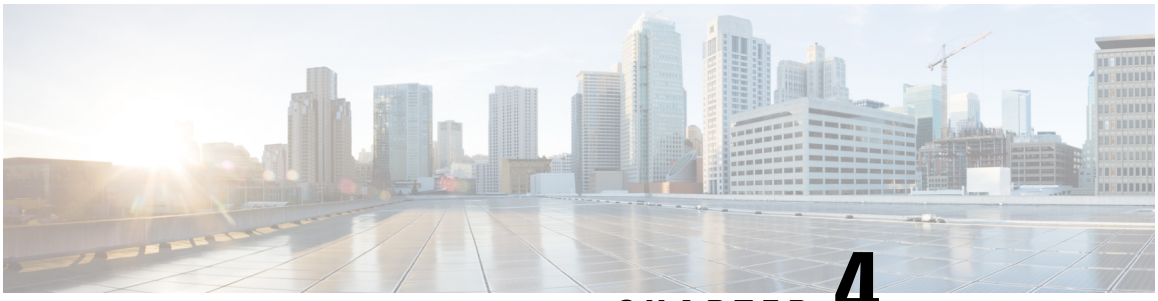
Cisco MC3810 as a VoAAL2 Gateway using AAL2 PVCs Example

This example shows a Cisco MC3810 being configured as a VoAAL2 gateway using AAL2 PVCs:

```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname stella-mc3810
!
network-clock base-rate 56k
ip subnet-zero
no ip domain-lookup
ip host camel 192.168.254.254
ip host buffalo 192.168.254.253
!
mgcp
mgcp call-agent 10.14.117.4 service-type mgcp version 0.1
mgcp dtmf-relay voip codec all mode nse
mgcp dtmf-relay voaal2 codec all
mgcp modem passthrough nse
mgcp package-capability rtp-package
mgcp tse payload 100
mgcp timer receive-rtcp 100
mgcp timer net-cont-test 3000
isdn voice-call-failure 0
!
voice-card 0
!
controller T1 0
    mode atm
    framing esf
    linecode b8zs
!
interface Ethernet0
    ip address 10.14.121.1 255.255.0.0
!
interface Serial0
    no ip address
    no ip mroute-cache
    shutdown
    no fair-queue
!
interface Serial1
    no ip address
    shutdown
!
interface ATM0
    no ip address
    ip mroute-cache
    no atm ilmi-keepalive
!
interface ATM0.2 point-to-point
   pvc 2/200
      vbr-rt 760 760 100
      encapsulation aal2
```

```
      vcci 2
!
interface FR-ATM20
     no ip address
     shutdown
!
router igrp 1
    redistribute connected
    network 1.0.0.0
!
ip default-gateway 10.14.0.1
no ip http server
ip classless
ip route 192.168.254.0 255.255.255.0 10.14.0.1
!
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
voice-port 1/1
!
voice-port 1/2
     shutdown
!
voice-port 1/6
     shutdown
!
dial-peer voice 1 pots
    application mgcpapp
    port 1/1
!
line con 0
    transport input none
line aux 0
   line 2 3
 line vty 0 4
    password lab
    login
!
end
```

Note See the "Additional References for MGCP and SGCP" section in the Preface for related documents, standards, and MIBs. See " Glossary " for definitions of terms in this guide.



CHAPTER 4

Configuring MGCP Basic CLASS and Operator Services

This chapter provides information on configuring and troubleshooting the MGCP Basic (CLASS) and Operation Services feature. The feature provides xGCP support for three-way calling on residential and trunking gateways.

Feature benefits include the following:

- The merged SGCP/MGCP software for RGWs, BGWs, and TGWs enables easier development and growth of Cisco and customer solutions.
- MGCP BCOS satisfies the requirements for providing basic CLASS services on Cisco IOS gateways that enable multiple xGCP solutions, particularly residential gateway and IP Centrex.

For more information about this and related Cisco IOS voice features, see the following:

- "Overview of MGCP and Related Protocols" on page 3
- Entire Cisco IOS Voice Configuration Library--including library preface and glossary, other feature documents, and troubleshooting documentation--at http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/cisco_ios_voice_configuration_library_glossary/vcl.htm

Feature History for MGCP Basic (CLASS) and Operation Services

Release	Modification
12.2(2)T	This feature was introduced.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for MGCP Basic CLASS and Operator Services

Prerequisites are described in the "Prerequisites for Configuring MGCP and Related Protocols" section on page 3 .

Restrictions for MGCP Basic CLASS and Operator Services

- For the Cisco MC3810 series platform, the MGCP BCOS software is supported on an HCM version of an DSP card; it is not supported on an VCM version.

To check the type of DSP card in your Cisco MC3810 series platform, enter a **show version** command at the EXEC prompt.

- • If you have an HCM card, the following line appears as part of the **show version** information:

1 6-DSP (slot 2) High Performance Compression Module(v01.A0)

- • If you have an VCM card, the following line appears as part of the **show version** information:

1 6-DSP (slot 2) Voice Compression Module(v255.V7)

If you have an HCM card, the MGCP BCOS features will function properly. If you have an VCM card, the feature is not supported.

- The G.728 and G.723 codecs do not support three-way calling.

Information About MGCP Basic CLASS and Operator Services

The MGCP BCOS are a set of calling features, sometimes called "custom calling" features, that use MGCP to transmit voice, video, and data over the IP network. These features are usually found in circuit-based networks. MGCP BCOS brings them to the Cisco IOS gateways on packet-based networks.

The MGCP BCOS software is built on the MGCP CAS PBX and AAL2 software package, and supports MGCP 0.1 and the earlier protocol version Simple Gateway Control Protocol (SGCP) 1.1 and 1.5.

The following MGCP BCOS features are available on residential gateways (RGWs) and business gateways (BGWs):

The following two features can be run as residential gateway (RGW) or trunking gateway (TGW) features:

Distinctive Power Ring

A telephone rings in a distinctive pattern when a call comes in from a predefined telephone number. The following patterns are available:

- R1: One long ring
- R2: Long ring -long ring
- R3: Short ring-short ring-long ring
- R4: Short ring - long ring - short ring
- R5: One short ring

Visual Message Waiting Indicator

A light goes on when a message is waiting for the line.

Caller ID

The calling party's telephone number, date, and time of the call appear on the receiving telephone's display between the first and second rings. A maximum of 18 digits are shown., and private and unlisted numbers are displayed. If the called party answers the phone on the first ring, the calling party's number does not appear.

If the called party has an appropriate name display unit, the calling party's name and telephone number appear on the display. The name and number appear between the first and second rings.

If the calling party has blocked Caller ID from displaying the telephone number, the called party sees "P" for private or "Anonymous" on the display unit.

Caller ID with Call Waiting

If the called party has Caller ID and has enabled the Call Waiting feature, then the calling party's name (if an appropriate display unit is available) and telephone number appear while the called party is on the line with another call.

If the calling party has blocked Caller ID from displaying the name and telephone number, the called party will see "P" for private or "Anonymous" on the display unit.

Call Forwarding

The following scenarios are available:

- The call agent transfers all incoming calls to a designated telephone number when the called number does not answer after a predetermined interval.
- The call agent transfers all incoming calls to a designated telephone number when the called number is busy.
- The call agent transfers all incoming calls to a specific destination when the user enters a code and a destination telephone number that receives the calls. The user is responsible for all charges between the original called number and the receiving telephone number.

- A user can activate Call Forwarding remotely using a touch-tone telephone and a user-defined personal identification number (PIN), which, by default, is the last four digits of the user's telephone number. The original destination telephone emits a Ring Splash when a call is forwarded.

Ring Splash

Also known as Reminder Ring, Ring Splash is activated when the user enables Call Forwarding on the telephone. The user hears Distinctive Power Ring R5 when the line is idle and a call has been forwarded. This reminds the user that Call Forwarding is active.

Distinctive Call-Waiting Tone

The called party hears four audible tone patterns (waiting tones, or WTs) when a call is waiting on the called party's line. The call agent provides the following tone patterns in sequence as the incoming call continues to wait:

- WT1: One short tone
- WT2: Short tone-short tone
- WT3: Short tone-short tone-short tone
- WT4: Short tone-long tone-short tone

Message-Waiting Tone

For users with an active voice mail system, a special dial tone is heard when the user goes off-hook and a message is waiting. The dial tone is a sequence of 10 short tones followed by a steady tone. If the user has a telephone with a visual message indicator, the indicator light goes on when a message is waiting.

Stutter Dial Tone

This tone is used in place of the dial tone to indicate that a message is waiting. When the user goes off-hook, a sequence of three short tones followed by a steady tone is heard.

Off-Hook Warning Tone

The user hears this tone when the telephone is off-hook. The tone is repeated bursts of sound of rising pitch.

911 Calls

The user can make a 911 call to an Emergency Service Bureau (ESB), and the call is maintained as long as the ESB does not hang up. If the user hangs up, the call is maintained. If the user hangs up and picks up the phone again, the call resumes. If the user hangs up and does not pick up the phone again, the ESB can ring the user and resume the call.

This feature is available in SGCP mode on the Cisco 3660 platforms and in MGCP mode on all supported platforms.

Three-Way Calling

The user can create a 3-way call by pressing the switchhook quickly to put the first call on hold, dial a third party, and press the switchhook again quickly to join all parties to the call. This feature is supported on all five platforms.

Considerations for Three-way Calling

- The user who sets up the 3-way call must be connected to a residential gateway, which handles the call setup. TWC is transparent to a trunking gateway.
- Only the G.711u and G.711a codecs support TWC. If any part of a 3-way call is made on a codec other than the G.711u, that codec must be switched to G.711u mode before the second switchhook flash in order for the 3-way call to be set up.
- TWC supports calls originating as Voice over IP or Voice over AAL2 calls, not Voice over ATM or Voice over Frame Relay calls. However, if the network has ATM or Frame Relay as a transport protocol, the VoIP call is completed.
- The user originating the 3-way call is the controller. Each of the two other users on the call can add another person onto the call, which is referred to as call chaining. Those new users can also add another person to the call. However, when five people in total are on the call, adding more users causes voice quality to degrade.
- If the controller of the call hangs up, all the users are disconnected from the call. If one of the non-controller users hangs up, the remaining users are still connected to the call.
- If the controller presses the switchhook quickly for a third time, the last user connected to the call is dropped from the call.
- If two users are on a call and a third user calls one of them, that third user cannot be joined (bridged) into the two-party call.

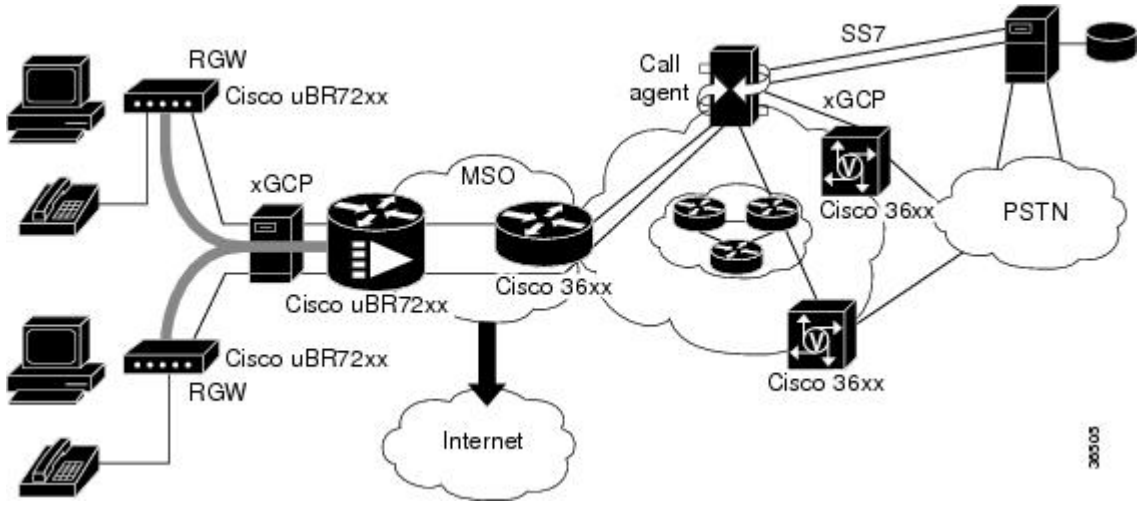
Examples of Service-Provider Solutions

The Basic CLASS and Operator Services features support MGCP solutions in the following areas:

- Residential cable access

A CLEC can use residential cable access to provide residential customers with basic telephony and data services. CLASS features and Three-way calling, Caller ID with Call Waiting, and Distinctive Call Waiting Tone are features that support these customers. The figure below illustrates a possible residential cable access solution.

Figure 4: Residential Cable Access Solution

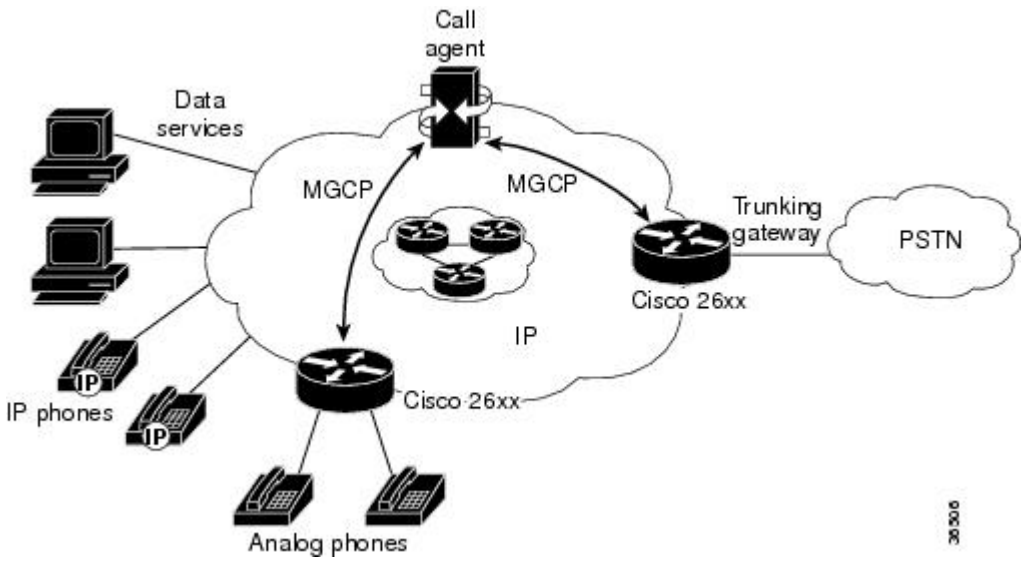


Note that, in the figure above, the residential gateway must support the CLASS features and 911 capability.

- IP Centrex and IP PBX

In these solutions, a call agent provides business voice services that are traditionally offered by a circuit-based PBX. CLASS features and Three-way calling, Caller ID with Call Waiting, Distinctive Call Waiting Tone, and Visual Message Waiting Indicator are features suitable for these customers. The figure below illustrates an IP Centrex solution:

Figure 5: IP Centrex Solution



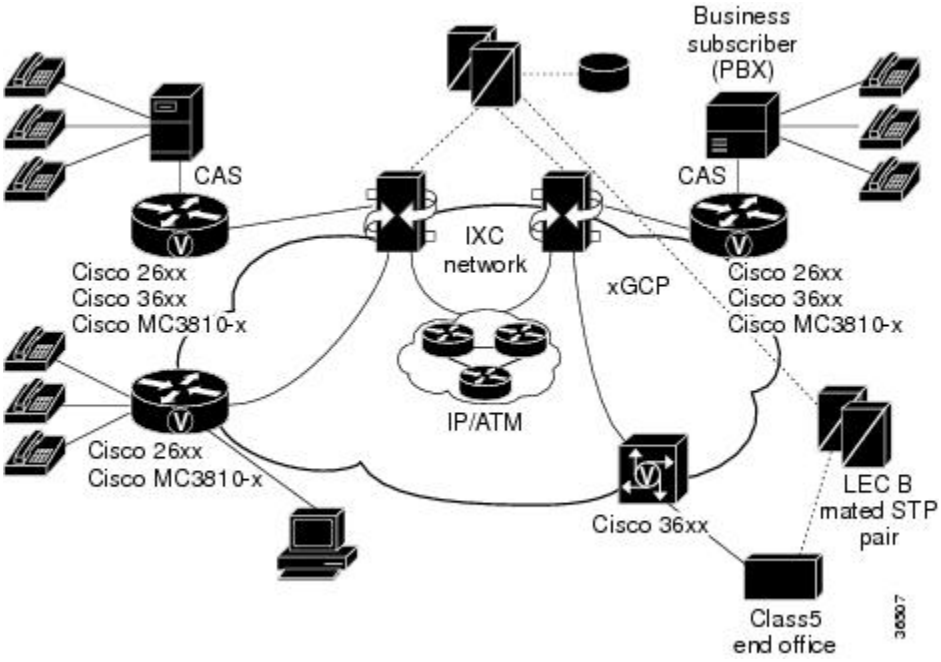
In the figure above, the residential gateway (the Cisco 2600 series platforms) must support the CLASS features.

- Integrated access

A CLEC or IXC can provide small, medium, and large businesses with integrated voice and data access services. The integrated access device can be located at the central office or on the customer's premises.

Access to the subscriber can be analog or digital, and transport of voice and data can be over IP, Frame Relay, or ATM. CLASS features and Three-way calling, Caller ID with Call Waiting, Distinctive Call Waiting Tone, and Visual Message Waiting Indicator are features suitable for these customers. The figure below illustrates an integrated access solution.

Figure 6: Integrated Access Solution

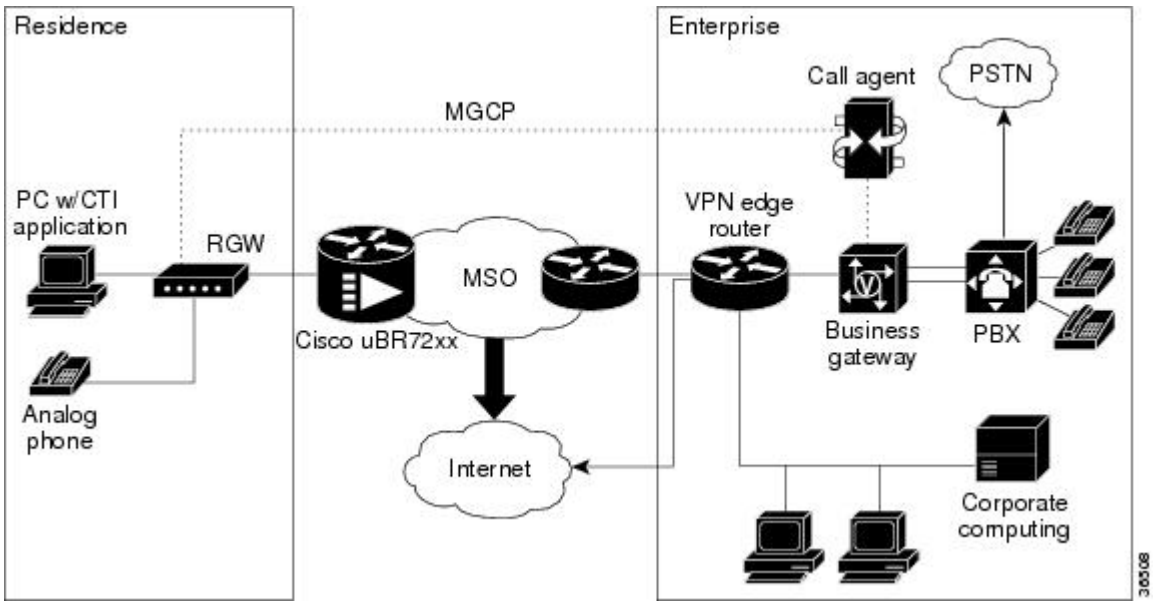


In the figure above, the residential gateway (the Cisco 2600 series and Cisco MC3810 series platforms) must support the CLASS features.

- Telecommuter or small-office-home-office solution

The figure below illustrates a telecommuter or small-office-home-office solution:

Figure 7: Telecommuter or Small Office-Home Office Solution



In the figure above, the residential gateway must support the CLASS features.

Other solutions are possible using the MGCP open protocol.

Troubleshooting MGCP Basic CLASS and Operator Services

No new or modified configuration tasks are required to initiate MGCP Basic CLASS and Operator Services. MGCP BCOS co resides with MGCP CAS PBX and AAL2 PVC software, for which configuration activities are required. These are discussed in " Appendix A: Configuring MGCP CAS PBX and AAL2 PVC .

The following MGCP BCOS features do not work on telephones from all manufacturers when the telephones are connected to a Cisco MC3810 series platform:

- CID - Caller ID
- VMWI - Visual Message Waiting Indicator
- CIDCW - Caller ID with Call Waiting

The table below summarizes the findings for the models tested.

Table 4: Telephones and Feature Capabilities

Telephone	CID	VMWI	CIDCW
Casio TI-345	Y	--	N
Casio TI-360	Y	--	N
Dial Digital CP-2892C	Y	Y	Y
GE 29299GE1-A	Y	--	Y

Telephone	CID	VMWI	CIDCW
Panasonic KX-TSC7	Y	N	N
Panasonic KX-TSC55-b	Y	Y	Y
Sony IT-ID80	Y	--	Y

To correct this operation, change the idle voltage in the voice port from low to high.

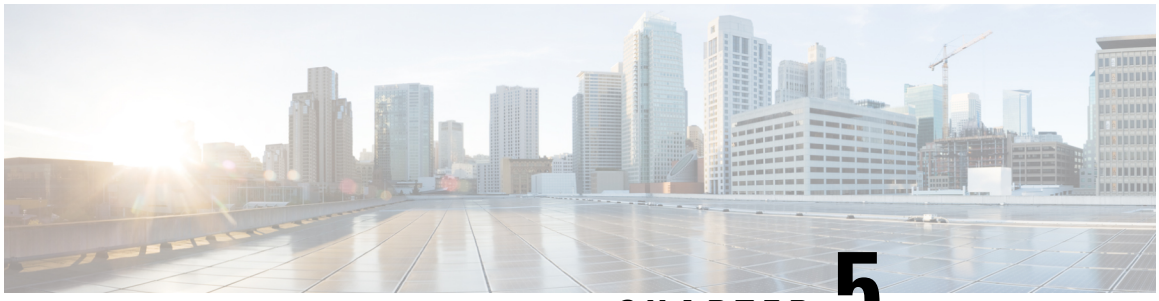
To change the voice port idle voltage, perform these additional steps:

- If the phone is already connected to the voice port, lift the phone's handset.
- If the phone is not connected to the voice port, do the following:
  1. Attach the phone to the voice port.
  2. Do a "shut" to the voice port.
  3. Do a "no shut" to the voice port.
  4. Lift the phone's handset.

Configuration Examples for MGCP Basic CLASS and Operator Services

No new or modified configuration settings are needed to implement MGCP Basic CLASS and Operator Services. See the MGCP CAS PBX and AAl2 PVC setup in "Appendix A: Configuring MGCP CAS PBX and AAL2 PVC" for sample configurations.

Tip See the "Additional References for MGCP and SGCP" section on page x for related documents, standards, and MIBs and the " Glossary " for definitions of terms in this guide.



CHAPTER 5

Configuring NAS Package for MGCP

This chapter provides information on configuring the Network Access Server (NAS) Package for MGCP feature. The feature adds support for the MGCP NAS package on universal gateways. Data calls can be terminated on a trunking media gateway that is serving as a NAS. Trunks on the NAS are controlled and managed by a call agent supporting MGCP for both voice and data calls. The call agent must support the MGCP NAS package.

Key feature benefits derive from the presence of universal ports that are able to terminate both voice and data calls under control of the MGCP call agent. These benefits include the following:

- Cost savings
  - Sharing of trunks (T1 or E1) for dial and voice services
  - Collapsed IP backbone infrastructure
  - Simplified operations and management
- Increased revenue
  - Optimized utilization of trunk (T1 or E1) resources
- Flexibility in deploying new services
- Flexibility in access network engineering

For more information about this and related Cisco IOS voice features, see the following:

- "Overview of MGCP and Related Protocols" on page 3
- Entire Cisco IOS Voice Configuration Library--including library preface and glossary, other feature documents, and troubleshooting documentation--at http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/cisco_ios_voice_configuration_library_glossary/vcl.htm

Feature History for NAS Package for MGCP

Release	Modification
12.2(2)XB	This feature was introduced on the Cisco AS5350 and Cisco AS5400.
12.2(11)T	This feature was implemented on the Cisco AS5850.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for NAS Package for MGCP

Prerequisites are described in the "Prerequisites for Configuring MGCP and Related Protocols" section on page 3 . In addition, the following apply:

- Configure a data network.
- Configure MGCP.

Information About NAS Package for MGCP

This feature adds support for the Network Access Server Package for Media Gateway Control Protocol package on the Cisco AS5350, Cisco AS5400, and Cisco AS5850 universal gateways. With this implementation, data calls can be terminated on a trunking media gateway that is serving as a network access server (NAS). Trunks on the NAS are controlled and managed by a call agent that supports Media Gateway Control Protocol (MGCP) for both voice and data calls. The call agent must support the MGCP NAS package.

These capabilities are enabled by the universal port functionality of the Cisco AS5350, Cisco AS5400, and Cisco AS5850, which allows these platforms to operate simultaneously as network access servers and voice gateways to deliver universal services on any port at any time. These universal services include dial access, real-time voice and fax, wireless data access, and unified communications.

The MGCP NAS package implements signals and events to create, modify, and tear down data calls. The events include signaling the arrival of an outbound call (IP to Public Switched Telephone Network [PSTN]) to the media gateway controller (call agent), reporting carrier loss and call authorization status, and receiving callback requests. The following types of calls can be terminated as data calls:

- Data within the voice band (analog modem)
- ISDN data (digital modem)
- Data over voice when using a call agent that recognizes this call type and delivers these calls as digital data to the NAS

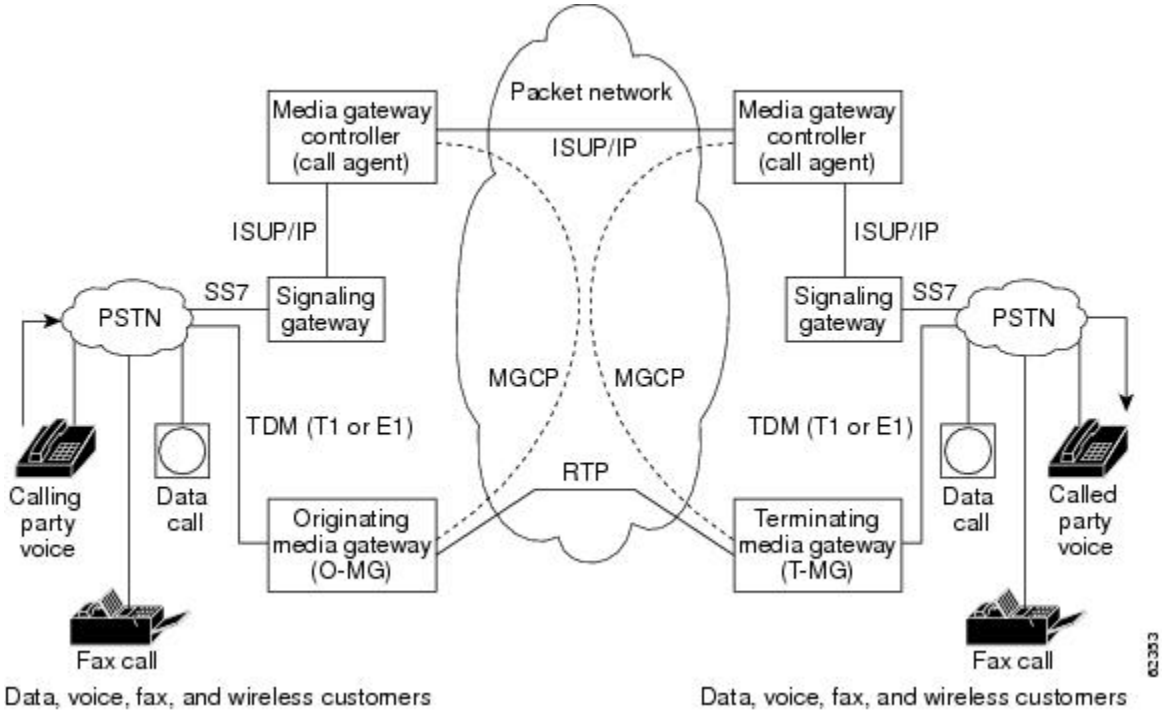
The NAS package provides MGCP capabilities for data calls on the Cisco AS5350, Cisco AS5400, and Cisco AS5850 that support all the dial-in and dial-out services, including the following:

- Virtual Private Network (VPN) with Layer 2 Tunneling Protocol (L2TP)
- Scalable Multichassis Multilink PPP (MMP) across multiple channels
- MGCP 1.0 and MGCP 0.1
- Call preauthentication with MGCP dial calls

Resource pool management can be used to manage dial ports when dialed number identification service (DNIS) preauthentication is enabled. The NAS returns an error with a preauthentication failure code to the call agent, which releases the call gracefully with a busy cause. Refer to the Cisco IOS Release 12.3 Configuration Guides and Command References , for more information about dial-pool management, and for more information about authentication, authorization, and accounting (AAA) preauthentication services.

The figure below shows a typical network topology for universal port media gateways.

Figure 8: Media Gateways Operating As Network Access Servers



How to Configure NAS Package for MGCP

With the Network Access Server Package for Media Gateway Control Protocol feature, the NAS supports both data and voice calls, which can be managed from a single call agent that supports MGCP with the NAS package. The NAS package provides the interface to a call agent (media gateway controller) for handling modem calls that terminate on the NAS and that originate from the PSTN, including callback requests. Results of AAA authorization and preauthorization requests from the NAS are reported to the call agent as notifications.

See the following sections for configuration tasks for the Network Access Server Package for Media Gateway Control Protocol feature. Each task in the list is identified as either required or optional.

Configuring the NAS for MGCP

In this task, MGCP is configured on the trunking gateway (NAS), and the NAS package is set as the default package. The steps that are listed are the minimum needed to configure MGCP on the NAS. For more commands and optional settings for MGCP, see the documents listed in the "Related Documents" section on page xi .

To configure the NAS Package for MGCP feature, use the following commands in global configuration mode:

SUMMARY STEPS

1. **mgcp** [*gw-port*]
2. **mgcp call-agent** {*dns-name* | *ip-address*} [*ca-port*] [**service-type** *type*] [**version** *protocol-version*]
3. **mgcp default-package nas-package**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**mgcp** [*gw-port*] **Example:** `Router(config)# mgcp [gw-port ]`	Allocates resources for MGCP and starts the MGCP daemon. If no port is specified, the command defaults to port 2427.
Step 2	**mgcp call-agent** {*dns-name* | *ip-address*} [*ca-port*] [**service-type** *type*] [**version** *protocol-version*] **Example:** `Router(config)# mgcp call-agent {dns-name	ip-address } [ca-port] [service-type type] [version protocol-version]`	Configures the gateway with the address and protocol of the call agent (media gateway controller). Make sure to specify a call agent that supports the NAS package.
Step 3	**mgcp default-package nas-package** **Example:** `Router(config)# mgcp default-package nas-package`	(Optional) Defines the default package to be used for MGCP signaling. For this feature, specify the NAS-Package. Default generally used on trunking gateways is Trunk-Package and can be left unchanged.

Configuring Controllers

In this task, in addition to the standard controller commands, you configure a T1 or E1 controller for external signaling control by MGCP. You can also set the AAA preauthentication timer to expire after a certain number of milliseconds have elapsed without a response from the AAA server and indicate whether the call should be accepted or rejected if no response occurs before the timer expires.

To configure a controller to use the Network Access Server Package for Media Gateway Control Protocol feature, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. **controller** {**t1** | **e1**} *slot/port*
2. Do one of the following:
   - **framing** {**sf** | **esf**}
   - for TI lines
   - or for E1 lines
   - **framing** {**crc4** | **no-crc4**} [**australia**]
3. **extsig mgcp**
4. **guard-timer** *milliseconds* [**on-expiry** {**accept** | **reject**}]
5. Do one of the following:
   - **linecode** {**ami** | **b8zs**}
   - for T1 lines
   - or for E1 lines
   - **linecode** {**ami** | **hdb3**}
6. **ds0-group** *channel-number* **timeslots** *range* **type none service mgcp**
7. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**controller** {**t1**	**e1**} *slot/port* **Example:** `Router(config)# controller {t1 | e1} slot/port`	Configures a T1 or E1 controller and enters controller configuration mode.

Step 2	Do one of the following:
	• **framing** {**sf**
		esf}
		• for TI lines
		• or for E1 lines
		• **framing** {**crc4**
			no-crc4} [**australia**]
			Example:
			`Router(config-controller)# framing {sf | esf}`
			Example:
			Example:
			`Router(config-controller)# framing {crc4 | no-crc4} [australia]`
				Selects the frame type for the T1 or E1 trunk.
				T1 default is **sf**. E1 default is **crc4**.

	Command or Action	Purpose
Step 3	**extsig mgcp** **Example:** `Router(config-controller)# extsig mgcp`	Configures external signaling control by MGCP for this controller. For T3 trunks, each logical T1 must be configured with the **extsig mgcp**command.
Step 4	**guard-timer** *milliseconds* [**on-expiry** {**accept** | **reject**}] **Example:** `Router(config-controller)# guard-timer milliseconds [on-expiry {accept | reject}]`	(Optional) Sets a guard timer for the number of milliseconds to wait for a AAA server to respond to a preauthentication request before expiring. Also specifies the default action to take when the timer expires without a response from AAA.

Step 5	Do one of the following:
	• **linecode** {**ami** | **b8zs**}
	• for T1 lines
	• or for E1 lines
	• **linecode** {**ami** | **hdb3**}
	Example:
	`Router(config-controller)# linecode {ami | b8zs}`
	Example:
	Example:
	`Router(config-controller)# linecode {ami | hdb3}`
		Specifies the line encoding to use.
		T1 default is **ami**. E1 default is **hdb3**.

Step 6	**ds0-group** *channel-number* **timeslots** *range* **type none service mgcp**
	Example:
	`Router(config-controller)# ds0-group channel-number`
	Example:
	`timeslots range type none service mgcp`
		Specifies the DS0 time slots that make up a logical voice port on a T1 or E1 controller and specifies the signaling type by which the router connects to the PBX or PSTN.

Step 7	**exit**
	Example:
	`Router(config-controller)#`
	`exit`
		Exits the current mode.

Configuring Dialer Interfaces and Routing

This set of tasks configures dial-on-demand routing (DDR) on a dialer interface that is under external call control by MGCP.

DDR refers to a collection of Cisco features that allows two or more Cisco routers to establish a dynamic connection over simple dial-up facilities to route packets and exchange routing updates on an as-needed basis. DDR is used for low-volume, periodic network connections over the PSTN or an ISDN. A connection is automatically established whenever interesting traffic is detected; during configuration you define what constitutes interesting traffic.

ISDN B channels, synchronous serial interfaces, and asynchronous interfaces can all be converted to dialer interfaces using dialer interface configuration commands.

DDR provides several functions. First, DDR spoofs, or pretends, that there are established configured routes to provide the image of full-time connectivity using the dialer interfaces. When the routing table forwards a packet to a dialer interface, DDR filters out the interesting packets for establishing, maintaining, and releasing switched connections. Internetworking is achieved over the DDR-maintained connection using PPP or other WAN encapsulation techniques.

The encapsulation methods available depend on the physical interface being used. Cisco supports PPP, High-Level Data Link Control (HDLC), Serial Line Internet Protocol (SLIP), and X.25 data-link encapsulations for DDR. PPP is the recommended encapsulation method because it supports multiple protocols and is used for synchronous, asynchronous, or ISDN connections. In addition, PPP performs address negotiation and authentication, and it is interoperable with different vendors.

There are two ways of setting up addressing on dialer interfaces:

- Applying a subnet to the dialer interfaces--Each site with a dialer interface is given a unique node address on a shared subnet for use on its dialer interface. This method is similar to numbering a LAN or multipoint WAN, and it simplifies the addressing scheme and creation of static routes.
- Using unnumbered interfaces--Similar to using unnumbered addressing on leased-line point-to-point interfaces, the address of another interface on the router is borrowed for use on the dialer interface. Unnumbered addressing takes advantage of the fact that there are only two devices on the point-to-point link.

DDR uses manually entered static network protocol routes. This eliminates the use of a routing protocol that broadcasts routing updates across the DDR connection, causing unnecessary connections.

Similar to the function provided by an Address Resolution Protocol (ARP) table, dialer map statements translate next-hop protocol addresses to telephone numbers. Without statically configured dialer maps, DDR call initiation cannot occur. When the routing table points at a dialer interface, and the next-hop address is not found in a dialer map, the packet is dropped.

Authentication in DDR network design provides two functions: security and dialer state. As most DDR networks connect to the PSTN, it is imperative that a strong security model be implemented to prevent unauthorized access to sensitive resources. Authentication also allows the DDR code to keep track of what sites are currently connected and provides for building of Multilink PPP bundles.

In summary, the following main tasks are involved in configuring the dialer interface and routing:

- Specification of interesting traffic--What traffic type should enable the link?
- Definition of static routes--What route do you take to get to the destination?

- Configuration of dialer information--What number do you call to get to the next-hop router, and what service parameters do you use for the call?

For MGCP NAS, configuration of dialer interfaces entails the use of the **dialer extsig** command in interface configuration mode, which enables the External Call Service Provider (XCSP) subsystem to provide an interface between the Cisco IOS software and the MGCP protocol. The XCSP subsystem enables services such as modem call setup and teardown for the dialer interface.

To configure the dialer interface and routing, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. **interface** *dialer-name*
2. Do one of the following:
   - **ip unnumbered** *interface-number*
   -
   - **ip address** *ip-address subnet-mask* [**secondary**]
3. **encapsulation ppp**
4. **dialer in-band** [**no-parity** | **odd-parity**]
5. **dialer idle-timeout** *seconds* [**inbound** | **either**]
6. **dialer map** *protocol next-hop-address* [**name** *host-name*] [*dial-string*[**:** *isdn-subaddress*]]
7. **dialer extsig**
8. **dialer-group** *number*
9. **no cdp enable**
10. **ppp authentication chap**
11. **exit**
12. **dialer list** *number* **protocol** *protocol-name* {**permit** | **deny** [**list** *access-list-number* | *access-group*]}
13. **ip route** *prefix mask* {*ip-address* | *interface-type interface-number*} [*distance*] [**tag** *tag*] [**permanent**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**interface** *dialer-name* **Example:** `Router(config)# interface dialer-name`	Enters interface mode for the dialer interface.
Step 2	Do one of the following: • **ip unnumbered** *interface-number* • • **ip address** *ip-address subnet-mask* [**secondary**] **Example:** `Router(config-if)# ip unnumbered interface-number` **Example:**	Enables IP processing on the dialer interface, configures the dialer interface not to have an explicit IP address, and assigns the IP address of the loopback interface instead. This command helps conserve IP addresses.

	Command or Action	Purpose
	Example: `Router(config-if)# ip address ip-address subnet-mask [secondary]`	
Step 3	**encapsulation ppp** **Example:** `Router(config-if)# encapsulation ppp`	Sets encapsulation type for PPP.

Step 4	**dialer in-band** [**no-parity** | **odd-parity**]
	Example:
	`Router(config-if)#`
	`dialer in-band [no-parity | odd-parity]`
		Specifies that dial-on-demand routing (DDR) is to be supported. The **in-band** keyword specifies that the same interface that sends the data performs call setup and teardown operations between the router and an external dialing device such as a modem.
		By default, no parity is applied to the dialer string.

Step 5	**dialer idle-timeout** *seconds* [**inbound** | **either**] **Example:** `Router(config-if)# dialer idle-timeout seconds [inbound | either]`	Specifies the duration of idle time before a line is disconnected. Default direction is outbound. Default idle time is 120 seconds.
Step 6	**dialer map** *protocol next-hop-address* [**name** *host-name*] [*dial-string*[**:** *isdn-subaddress*]] **Example:** `Router(config-if)# dialer map protocol next-hop-address [name host-name] [dial-string[:isdn-subaddress]]`	Configures a serial interface to make digital calls or to accept incoming calls from a specified location and to authenticate if so configured.

Step 7	**dialer extsig**
	Example:
	`Router(config-if)#`
	`dialer extsig`
		Specifies an interface for the initiation and termination of digital calls for external signaling protocols. Only one dialer with external signaling per NAS is permitted.

Step 8	**dialer-group** *number* **Example:** `Router(config-if)# dialer-group number`	Controls access by configuring an interface to belong to a specific dialing group.

	Command or Action	Purpose
Step 9	**no cdp enable** **Example:** `Router(config-if)# no cdp enable`	Disables Cisco Discovery Protocol (CDP) on the interface.
Step 10	**ppp authentication chap** **Example:** `Router(config-if)# ppp authentication chap`	Enables Challenge Handshake Authentication Protocol (CHAP) authentication on the interface.
Step 11	**exit** **Example:** `Router(config-if)# exit`	Exits the current mode.
Step 12	**dialer list** *number* **protocol** *protocol-name* {**permit** | **deny** [**list** *access-list-number* | *access-group*]} **Example:** `Router(config)# dialer list number protocol protocol-name {permit | deny [list access-list-number | access-group ]}`	Defines a DDR dialer list for dialing by protocol or by a combination of a protocol and a previously defined access list. Each dialer interface can have only one dialer group, but the same dialer list can be assigned to multiple interfaces (using the **dialer-group** command).
Step 13	**ip route** *prefix mask* {*ip-address* | *interface-type interface-number*} [*distance*] [**tag** *tag*] [**permanent**] **Example:** `Router(config)# ip route prefix mask {ip-address | interface-type interface-number } [distance ] [tag tag ] [permanent]`	Establishes a static route. Because you do not want dynamic routing protocols running across the DDR links, you manually configure static routes.

Verifying the NAS Package for MGCP

To verify configuration, use the following commands.

SUMMARY STEPS

1. Use the following command to display the running configuration to verify configured parameters for MGCP, controllers, dialer interfaces, and routing:
2. Use the following command to display MGCP configurations for NAS:

DETAILED STEPS

Step 1 Use the following command to display the running configuration to verify configured parameters for MGCP, controllers, dialer interfaces, and routing:

Example:

```
Router# show running-configuration
```

The following example shows the configuration for serial interface 1:

Example:

```
Router# show running-configuration interface serial 1
Building configuration...
Current configuration:
!
interface Serial1
no ip address
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
shutdown
!
end
```

Step 2 Use the following command to display MGCP configurations for NAS:

Example:

```
Router# show mgcp nas
 {dump
 slot
 port
 channel |
info
```

The following is sample output from the **show mgcp nas dump** command:

Example:

```
Router# show mgcp nas dump 7 0 23
Slot 7 state= Up
Port 0 state= Up
State  Idle  PortCb=0x630DE864 ss_id=0x0 handle=0x0
bearer cap=Modem call_id= conn_id=
Events req-
4d21h:
 callp=0x62D137D4 - state=MGCP_CALL_IDLE - data_call No
Endpt name=S7/DS1-0/23
```

The following is sample output from the **show mgcp nas info** command:

Example:

```
Router# show mgcp nas info
Slot 7 state= Up
Port 0 state= Up
ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID XX XX XX
XX XX XX XX XX
Channel State Legend
```

```
NP=Not Present, OO=Out Of Service, ID=Idle, US=In Use
CI=Connection in progress, RI=In Release in progress
RO=Out Release in progress, DN=Down, SH=Shutdown
XX=Unconfigurable
```

Troubleshooting Tips

In addition, a number of **show** and **debug** commands are useful for troubleshooting the Network Access Server Package for Media Gateway Control Protocol feature. These commands are listed in the following sections:

MGCP Troubleshooting

To display detailed information on the MGCP application and operations, use the following commands in privileged EXEC mode:

Command	Purpose
show mgcp nas info `Router# show mgcp nas info`	Displays status of the MGCP data channels. See Example Output for show mgcp nas info Command, on page 83.
show mgcp nas dump *slot port chan* `Router# show mgcp nas dump slot port chan`	Displays status and details about the specified MGCP data slot, port, and channel. See Example Output for show mgcp nas dump Command, on page 83.
show mgcp connection `Router# show mgcp connection`	Displays active MGCP connections on the router. See Example Output for show mgcp connection Command, on page 83.
show xcsp slot *slot-num* `Router# show xcsp slot slot-num`	Displays the status of a router slot under the control of the External Call Service Provider (XCSP) subsystem. See Example Output for show xcsp slot Command, on page 84.

Command	Purpose
show xcsp port *slot port* `Router# show xcsp port slot port`	Displays the status of a port under the control of the External Call Service Provider (XCSP) subsystem. See Example Output for show xcsp port Command, on page 84.
show cdapi `Router# show cdapi`	Displays information about the call distributor application programming interface (CDAPI), which is the internal API that provides an interface between the MGCP signaling stacks and applications. See Example Output for show cdapi Command, on page 84.

Example Output for show mgcp nas info Command

The following is sample output from the **show mgcp nas info** command:

```
Router# show mgcp nas info
Slot 7 state= Up
Port 0 state= Up
ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID ID XX XX XX
XX XX XX XX XX
Channel State Legend
NP=Not Present, OO=Out Of Service, ID=Idle, US=In Use
CI=Connection in progress, RI=In Release in progress
RO=Out Release in progress, DN=Down, SH=Shutdown
XX=Unconfigurable
```

Example Output for show mgcp nas dump Command

The following is sample output from the **show mgcp nas dump** command:

```
Router# show mgcp nas dump 7 0 23
Slot 7 state= Up
Port 0 state= Up
State  Idle  PortCb=0x630DE864 ss_id=0x0 handle=0x0
bearer cap=Modem call_id= conn_id=
Events req-
4d21h:
 callp=0x62D137D4 - state=MGCP_CALL_IDLE - data_call No
Endpt name=S7/DS1-0/23
```

Example Output for show mgcp connection Command

The following is sample output from the **show mgcp connection** command for Voice over IP (VoIP) connections:

```
Router# show mgcp connection
Endpoint   Call_ID(C) Conn_ID(I) (P)ort (M)ode (S)tate (C)odec (E)vent[SIFL] (R)esult[EA]
1. S0/DS1-0/1 C=103,23,24 I=0x8 P=16586,16634 M=3 S=4,4 C=5 E=2,0,0,2 R=0,0
2. S0/DS1-0/2 C=103,25,26 I=0x9 P=16634,16586 M=3 S=4,4 C=5 E=0,0,0,0 R=0,0
3. S0/DS1-0/3 C=101,15,16 I=0x4 P=16506,16544 M=3 S=4,4 C=5 E=2,0,0,2 R=0,0
4. S0/DS1-0/4 C=101,17,18 I=0x5 P=16544,16506 M=3 S=4,4 C=5 E=0,0,0,0 R=0,0
5. S0/DS1-0/5 C=102,19,20 I=0,6 P=16572,16600 M=3 S=4,4 C=5 E=2,0,0,2 R=0,0
```

```
6. S0/DS1-0/6 C=102,21,22 I=0x7 P=16600,16572 M=3 S=4,4 C=5 E=0,0,0,0 R=0,0
Total number of active calls 6
```

The following is sample output from the **show mgcp connection** command for VoAAL2 connections:

```
Router# show mgcp connection
Endpoint  Call_ID(C) Conn_ID(I)(V)cci/cid (M)ode (S)tate (C)odec (E)vent[SIFL] (R)esult[EA]
1.aaln/S1/1   C=1,11,12    I=0x2    V=2/10     M=3    S=4,4    C=1    E=3,0,0,3     R=0,0
Total number of active calls 1
```

Example Output for show xcsp slot Command

The following is sample output from the **show xcsp slot** command:

```
Router# show xcsp slot 1
Slot 1 configured
Number of ports configured=1 slot state= Up
```

Example Output for show xcsp port Command

The following is sample output for the **show xcsp port** command:

```
Router# show xcsp port 1 0
Slot 1 configured
Number of ports configured=1 slot state= Up
================================================
Port 0 State= Up type = 5850 24 port T1
Channel states
  0  Idle
  1  Idle
  2  Idle
  3  Idle
  4  Idle
  5  Idle
  6  Idle
  7  Idle
  8  Idle
  9  Idle
  10  Idle
  11  Idle
  12  Idle
  13  Idle
  14  Idle
  15  Idle
  16  Idle
  17  Idle
  18  Idle
  19  Idle
  20  Idle
  21  Idle
  22  Idle
  23  Idle
```

Example Output for show cdapi Command

The following is output for the **show cdapi** command:

```
Router# show cdapi
Registered CDAPI Applications/Stacks
====================================
Application TSP CDAPI Application
```

```
Application Type(s) Voice Facility Signaling
Application Level Tunnel
Application Mode Enbloc
Signaling Stack ISDN
Interface Se023
Signaling Stack ISDN
Interface Se123
Active CDAPI Calls
==================
Interface Se023
No active calls.
Interface Se123
Call ID = 0x39, Call Type = VOICE, Application = TSP CDAPI Application
CDAPI Message Buffers
=====================
Used Msg Buffers 0, Free Msg Buffers 1600
Used Raw Buffers 1, Free Raw Buffers 799
Used Large-Raw Buffers 0, Free Large-Raw Buffers 80
scarlatti1#
```

MGCP Debugging

To debug MGCP calls, events, and operations, use the following commands in privileged EXEC mode:

Command	Purpose
debug mgcp all `Router# debug mgcp all`	Enables all MGCP debugs. See Example Output for debug mgcp all Command, on page 86.
debug mgcp events `Router# debug mgcp events`	Enables MGCP events debugging, which shows information such as the following: whether the router is detected, the MGCP event that initiates a call, and the reset of an controller that is being serviced by MGCP. See Example Output for debug mgcp events Command, on page 86.
debug mgcp packets `Router# debug mgcp packets`	Enables debugging of MGCP packets. Useful for displaying contents of NTFY, CRCX, DLCX, and other packets. See Example Output for debug mgcp packets Command, on page 86.
debug mgcp parser `Router# debug mgcp parser`	Enables debugging of MGCP parser and builder. Useful to determine whether NTFY, CRCX, and other packets have the format that the router expects. See Example Output for debug mgcp parser Command, on page 87.

Command	Purpose
debug mgcp nas `Router# debug mgcp nas`	Enables debugging for MGCP data channels and events. See Example Output for debug mgcp nas Command, on page 87.
debug xcsp {**all** | **cot** | **event** } `Router# debug xcsp {all | cot | event}`	Enables reporting of the exchange of signaling information between the MGCP protocol stack and end applications, such as call switching module (CSM) and dialer. See Example Output for debug xcsp Command, on page 87.
debug cdapi {**detail** | **events**} `Router# debug cdapi {detail | events}`	Displays real-time information about the call distributor application programming interface (CDAPI). See Example Output for debug cdapi Command, on page 89.

Example Output for debug mgcp all Command

The **debug mgcp all** command and keyword would show a compilation of all this output, including the **debug mgcp voipcac** command and keyword output. Note that using the **debug mgcp all** command and keyword may severely impact network performance.

Example Output for debug mgcp events Command

The following example illustrates the output from the **debug mgcp events** command and keyword:

```
Router# debug mgcp events
Media Gateway Control Protocol events debugging is on
Router#
1w1d: MGC stat - 172.19.184.65, total=44, succ=7, failed=21
1w1d: MGCP msg 1
1w1d: remove_old_under_specified_ack:
1w1d: MGC stat - 172.19.184.65, total=44, succ=8, failed=21
1w1d: updating lport with 2427setup_ipsocket: laddr=172.29.248.193, lport=2427,
faddr=172.19.184.65, fport=2427
1w1d: enqueue_ack: ackqhead=0, ackqtail=0, ackp=1DC1D38, msg=21A037C
```

Example Output for debug mgcp packets Command

The following example illustrates the output from the **debug mgcp packets**command and keyword:

```
Router# debug mgcp packets
Media Gateway Control Protocol packets debugging is on
Router#
1w1d: MGCP Packet received -
DLCX 408631346 * MGCP 0.1
1w1d: send_mgcp_msg, MGCP Packet sent --->
1w1d: 250 408631346
<---
```

Example Output for debug mgcp parser Command

The following example illustrates the output from the **debug mgcp parser** command and keyword:

```
Router# debug mgcp parser
Media Gateway Control Protocol parser debugging is on
Router#
1w1d: -- mgcp_parse_packet() - call mgcp_parse_header
- mgcp_parse_header()- Request Verb FOUND DLCX
- mgcp_parse_packet() - out mgcp_parse_header
- SUCCESS: mgcp_parse_packet()- MGCP Header parsing was OK
- mgcp_val_mandatory_parms()
- SUCCESS: mgcp_parse_packet()- END of Parsing
1w1d: -- mgcp_build_packet()-
1w1d: - mgcp_estimate_msg_buf_length() - 87 bytes needed for header
- mgcp_estimate_msg_buf_length() - 87 bytes needed after checking parameter lines
- mgcp_estimate_msg_buf_length() - 87 bytes needed after checking SDP lines
- SUCCESS: MGCP message building OK
- SUCCESS: END of building
```

Example Output for debug mgcp nas Command

The following example displays output for the **debug mgcp nas** command and keyword, with the **debug mgcp packets**command and keyword enabled as well:

```
Router# debug mgcp nas
Media Gateway Control Protocol nas pkg events debugging is on
Router# debug mgcp packets
Media Gateway Control Protocol packets debugging is on
Router#
01:49:14:MGCP Packet received -
CRCX 58 S7/DS1-0/23 MGCP 1.0
X:57
 M:nas/data
 C:3
 L:b:64, nas/bt:modem, nas/cdn:3000, nas/cgn:1000
mgcp_parse_conn_mode :string past nas = data
mgcp_chq_nas_pkg:Full string:nas/bt:modem
mgcp_chq_nas_pkg:string past slash:bt
mgcp_chq_nas_pkg:string past colon:modem
mgcp_chq_nas_pkg:Full string:nas/cdn:3000
mgcp_chq_nas_pkg:string past slash:cdn
mgcp_chq_nas_pkg:string past colon:3000
mgcp_chq_nas_pkg:Full string:nas/cgn:1000
c5400#
mgcp_chq_nas_pkg:string past slash:cgn
mgcp_chq_nas_pkg:string past colon:1000
CHECK DATA CALL for S7/DS1-0/23
 mgcpapp_xcsp_get_chan_cb -Found - Channel state  Idle
 CRCX Recv
mgcpapp_endpt_is_data:endpt S7/DS1-0/23, slot 7, port 0 chan 23
 mgcpapp_data_call_hnd:mgcpapp_xcsp_get_chan_cb -Found - Channel state  Idle
bw=64, bearer=E1,cdn=3000,cgn=1000
```

Example Output for debug xcsp Command

The following examples show output for the **debug xcsp all** command and keyword and the **debug xcsp event** command and keyword:

```
Router# debug xcsp all
xcsp all debugging is on
```

```
Router# debug xcsp event
xcsp events debugging is on
01:49:14:xcsp_call_msg:Event  Call Indication , channel state =  Idle  for slot port channel
 7
c5400# 0 23
01:49:14:xcsp_process_sig_fsm:state/event  Idle / Call Indication
01:49:14:xcsp_incall:
01:49:14:xcsp_incall CONNECT_IND:cdn=3000 cgn=1000
01:49:14:xcsp:START guard TIMER
01:49:14:xcsp_fsm:slot 7 port 0 chan 23 oldstate =  Idle  newstate= Connection
in progress mgcpapp_process_mgcp_msg PROCESSED NAS PACKAGE EVENT
01:49:14:Received message on XCSP_CDAPI
01:49:14:process_cdapi_msg :slot/port/channel 7/0/23
01:49:14: process_cdapi_msg:new  slot/port/channel 7/0/23
01:49:14:
c5400#Received CONN_RESP:callid=0x7016
01:49:14:process_cdapi:Event CONN_RESP, channel state = 8 for slot port channel 7 0 23
01:49:14:xcsp_process_sig_fsm:state/event  Connection in progress / In Call accept
 mgcpapp_xcsp_alert:
 mgcpapp_xcsp_get_chan_cb -Found - Channel state  Connection in progress
200 58  Alert
I:630AED90
<---:Ack send SUCCESSFUL
01:49:14:xcsp_fsm:slot 7 p
c5400#ort 0 chan 23 oldstate =  Connection in progress  newstate= Connection in progress
01:49:14:Received message on XCSP_CDAPI
01:49:14:process_cdapi_msg :slot/port/channel 7/0/23
01:49:14: process_cdapi_msg:new  slot/port/channel 7/0/23
01:49:14: Received CALL_CONN:callid=0x7016
01:49:14:process_cdapi:Event CONN_, channel state = 8 for slot port channel 7
0 23
01:49:14:xcsp_process_sig_fsm:state/event  Connection in progress / in call connect
 mgcpapp_xcsp_connect:
 mgcpapp_xc
c5400#sp_get_chan_cb -Found - Channel state In Use
01:49:14:STOP TIMER
01:49:14:xcsp_fsm:slot 7 port 0 chan 23 oldstate =  Connection in progress
newstate=In Use
c5400#
01:50:23:Received message on XCSP_CDAPI
01:50:23:process_cdapi_msg :slot/port/channel 7/0/23
01:50:23: process_cdapi_msg:new  slot/port/channel 7/0/23
01:50:23: Received CALL_DISC_REQ:callid=0x7016
01:50:23:process_cdapi:Event DISC_CONN_REQ, channel state = 7 for slot port
channel 7 0 23
01:50:23:xcsp_process_sig_fsm:state/event In Use / release Request
 mgcpapp_xcsp_disconnect
 mgcpapp_xcsp_get_chan_cb -Fou
c5400#nd - Channel state In Use
01:50:23:send_mgcp_msg, MGCP Packet sent --->
01:50:23:RSIP 1 *@c5400 MGCP 1.0
RM:restart
.
DLCX 4 S7/DS1-0/23 MGCP 1.0
C:3
I:630AED90
E:801 /NAS User request
<---
01:50:23:xcsp_fsm:slot 7 port 0 chan 23 oldstate = In Use  newstate=Out
Release in progress
 xcsp_restart Serial7/0:22 vc = 22
 xcsp_restart Put idb Serial7/0:22 in down state
01:50:23:MGCP Packet received -
200 4 bye
```

```
 Data call ack received callp=0x62AEEA70mgcpapp_xcsp
c5400#_ack_recv:mgcpapp_xcsp_get_chan_cb -Found - Channel state Out Release in progress
mgcpapp_xcsp_ack_recv ACK 200 rcvd:transaction id = 4 endpt=S7/DS1-0/23
01:50:23:xcsp_call_msg:Event  Release confirm , channel state = Out Release in progress for
 slot port channel 7 0 23
01:50:23:xcsp_process_sig_fsm:state/event Out Release in progress/ Release confirm
01:50:23:STOP TIMER
01:50:23:xcsp_fsm:slot 7 port 0 chan 23 oldstate = Out Release in progress
newstate= Idle
```

Example Output for debug cdapi Command

The following example shows output for the **debug cdapi** command:

```
003909 ISDN Se123 RX <- SETUP pd = 8 callref = 0x06BB
003909 Bearer Capability i = 0x9090A2
003909 Channel ID i = 0xA18381
003909 Facility i =
0x9FAA068001008201008B0100A1180202274C020100800F534341524C415454492D3530303733
003909 Progress Ind i = 0x8183 - Origination address is non-ISDN
003909 Calling Party Number i = 0xA1, '50073'
003909 Called Party Number i = 0xC1, '3450070'
003909 CDAPI Se123 TX -> CDAPI_MSG_CONNECT_IND to TSP CDAPI Application call = 0x24
003909 From Appl/Stack = ISDN
003909 Call Type = VOICE
003909 B Channel = 0
003909 Cause = 0
003909 Calling Party Number = 50073
003909 Called Party Number = 3450070
003909 CDAPI Se123 TX -> CDAPI_MSG_CONNECT_RESP to ISDN call = 0x24
003909 From Appl/Stack = TSP CDAPI Application
003909 Call Type = VOICE
003909 B Channel = 0
003909 Cause = 0
003909 CDAPI-ISDN Se123 RX <- CDAPI_MSG_CONNECT_RESP from TSP CDAPI Application call = 0x24
003909 Call Type = VOICE
003909 B Channel = 0
003909 Cause = 0
003909 CDAPI Se123 TX -> CDAPI_MSG_SUBTYPE_CALL_PROC_REQ to ISDN call = 0x24
003909 From Appl/Stack = TSP CDAPI Application
003909 Call Type = VOICE
003909 B Channel = 0
003909 Cause = 0
003909 CDAPI-ISDN Se123 RX <- CDAPI_MSG_SUBTYPE_CALL_PROC_REQ from TSP CDAPI Application
call = 0x24
003909 Call Type = VOICE
003909 B Channel = 0
003909 Cause = 0
003909 ISDN Se123 TX -> CALL_PROC pd = 8 callref = 0x86BB
003909 Channel ID i = 0xA98381
```

Controller Troubleshooting

The commands in this section can be helpful in finding sources of problems with call connections and switching. The call switching module (CSM) associated with a controller contains digit collection logic that processes incoming calls for automatic number information (ANI) and dialed number identification service (DNIS) digits.

To display information on controller and CSM configuration and operation, use the following commands in privileged EXEC mode.

Command	Purpose
show controllers t1 | e1 [*slot* **/** *port*] Router# show controllers t1 | e1 [*slot*/*port*]	Displays whether the T1 or E1 connection between the router and switch (central office [CO] or PBX) is up or down and whether the connection is functioning properly. See Example Output for show controllers e1 or t1 Command, on page 90.
show voice port [*slot* **/** *port*] Router# show voice port [*slot* */port*]	Displays the port state and the parameters configured on the voice ports of Cisco voice interface cards. Voice-port defaults, like all command-line interface default parameters, do not display in the output for the **show running-config**command, but they can be seen with the **show voice port** command. See Example Output for show voice port Command, on page 92.
show csm modem [*slot/port* | *modem-group-number*] Router# show csm modem [*slot* */port* | *modem-group-number*]	Displays the CSM call statistics for a specific modem, for a group of modems, or for all modems.
debug csm modem [*slot/port* | **group** *modem-group-number*] Router# debug csm modem [*slot* */port* | group *modem-group-number*]	Traces the complete sequence of switching of incoming and outgoing modem call.

Example Output for show controllers e1 or t1 Command

The following is an output example from the **show controllers e1** command on the Cisco 7500 series:

```
Router# show controllers e1
e1 0/0 is up.
Applique type is Channelized E1 - unbalanced
Framing is CRC4, Line Code is HDB3
No alarms detected.
Data in current interval (725 seconds elapsed):
0 Line Code Violations, 0 Path Code Violations
0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
Total Data (last 24 hours)
0 Line Code Violations, 0 Path Code Violations,
```

```
0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins,
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
```

The following is an example of the **show controllers e1** display including the board identifier type:

```
Router# show controllers e1
E1 4/1 is up.
No alarms detected.
  Framing is CRC4, Line Code is hdb3
Data in current interval (0 seconds elapsed):
0 Line Code Violations, 0 Path Code Violations 0 Slip Secs, 0 Fr Loss Secs,
0 Line Err Secs, 0 Degraded Mins 0 Errored Secs, 0 Bursty Err Secs,
0 Severely Err Secs, 0 Unavail Secs
Total Data (last 79 15 minute intervals):
0 Line Code Violations, 0 Path Code Violations, 0 Slip Secs, 0 Fr Loss Secs,
0 Line Err Secs, 0 Degraded Mins, 0 Errored Secs, 0 Bursty Err Secs,
0 Severely Err Secs, 0 Unavail Secs
```

The following is an example from the **show controllers t1** command on the Cisco 7500 series routers:

```
Router# show controllers t1
T1 4/1 is up.
No alarms detected.
  Framing is ESF, Line Code is AMI, Clock Source is line
Data in current interval (0 seconds elapsed):
0 Line Code Violations, 0 Path Code Violations 0 Slip Secs, 0 Fr Loss Secs,
0 Line Err Secs, 0 Degraded Mins 0 Errored Secs, 0 Bursty Err Secs,
0 Severely Err Secs, 0 Unavail Secs
Total Data (last 79 15 minute intervals):
0 Line Code Violations, 0 Path Code Violations, 0 Slip Secs, 0 Fr Loss Secs,
0 Line Err Secs, 0 Degraded Mins, 0 Errored Secs, 0 Bursty Err Secs,
0 Severely Err Secs, 0 Unavail Secs
```

The following example shows the status of the T1 controllers connected to the Cisco AS5800 access servers:

```
Router# show controller T1
T1 1/0/0:1 is up.
No alarms detected.
Framing is ESF, Line Code is AMI, Clock Source is Line.
Data in current interval (770 seconds elapsed):
5 Line Code Violations, 8 Path Code Violations
0 Slip Secs, 0 Fr Loss Secs, 7 Line Err Secs, 0 Degraded Mins
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 7 Unavail Secs
Total Data (last 81 15 minute intervals):
7 Line Code Violations, 4 Path Code Violations,
6 Slip Secs, 20 Fr Loss Secs, 2 Line Err Secs, 0 Degraded Mins,
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 2 Unavail Secs
T1 1/0/1:5 is down.
Transmitter is sending remote alarm.
Receiver has loss of frame.
Framing is SF, Line Code is AMI, Clock Source is Line.
Data in current interval (770 seconds elapsed):
50 Line Code Violations, 5 Path Code Violations
0 Slip Secs, 7 Fr Loss Secs, 7 Line Err Secs, 0 Degraded Mins
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 7 Unavail Secs
Total Data (last 81 15 minute intervals):
27 Line Code Violations, 22 Path Code Violations,
0 Slip Secs, 13 Fr Loss Secs, 13 Line Err Secs, 0 Degraded Mins,
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 13 Unavail Secs
Router#
```

Example Output for show voice port Command

The following is sample output from the Cisco AS5800 for the **show voice port** command:

```
ISDN 1/0/0:D
Type of VoicePort is ISDN
Operation State is DORMANT
Administrative State is UP
No Interface Down Failure
Description is ""
Noise Regeneration is enabled
Non Linear Processing is enabled
Music On Hold Threshold is Set to -38 dBm
In Gain is Set to 0 dB
Out Attenuation is Set to 0 dB
Echo Cancellation is enabled
Echo Cancel Coverage is set to 16 ms
Connection Mode is normal
Connection Number is not set
Initial Time Out is set to 10 s
Interdigit Time Out is set to 10 s
Region Tone is set for US
```

The following example displays voice port configuration information for the digital voice port 0 located in slot 1, DS0 group 1:

```
receEive and transMit Slot is 1, Sub-unit is 0, Port is 1
Type of VoicePort is E&M
Operation State is DORMANT
Administrative State is UP
No Interface Down Failure
Description is not set
Noise Regeneration is enabled
Non Linear Processing is enabled
Music On Hold Threshold is Set to -38 DBMS
In Gain is Set to 0 dBm
Out Attenuation is Set to 0 dB
Echo Cancellation is enabled
Echo Cancel Coverage is set to 8 ms
Connection Mode is normal
Connection Number is not set
Initial Time Out is set to 10 s
Interdigit Time Out is set to 10 s
Region Tone is set for US
```

The following is sample output from the show voice port command for an E&M digital voice port on a Cisco 3600 series:

```
receEive and transMit Slot is 1, Sub-unit is 0, Port is 1
Type of VoicePort is E&M
Operation State is DORMANT
Administrative State is UP
No Interface Down Failure
Description is not set
Noise Regeneration is enabled
Non Linear Processing is enabled
Music On Hold Threshold is Set to -38 dBm
In Gain is Set to 0 dB
Out Attenuation is Set to 0 dB
Echo Cancellation is enabled
Echo Cancel Coverage is set to 8 ms
Connection Mode is normal
```

```
Connection Number is not set
Initial Time Out is set to 10 s
Interdigit Time Out is set to 10 s
Region Tone is set for US
```

The following is sample output from the show voice port command for an FXS analog voice port on a Cisco MC3810 multiservice concentrator:

```
Voice port 1/2 Slot is 1, Port is 2
Type of VoicePort is FXS
Operation State is UP
Administrative State is UP
No Interface Down Failure
Description is not set
Noise Regeneration is enabled
Non Linear Processing is enabled
In Gain is Set to 0 dB
Out Attenuation is Set to 0 dB
Echo Cancellation is enabled
Echo Cancel Coverage is set to 8 ms
Connection Mode is normal
Connection Number is not set
Initial Time Out is set to 10 s
Interdigit Time Out is set to 10 s
Coder Type is g729ar8
Companding Type is u-law
Voice Activity Detection is disabled
Ringing Time Out is 180 s
Wait Release Time Out is 30 s
Nominal Playout Delay is 80 milliseconds
Maximum Playout Delay is 160 milliseconds
Analog Info Follows:
Region Tone is set for northamerica
Currently processing Voice
Maintenance Mode Set to None (not in mtc mode)
Number of signaling protocol errors are 0
Impedance is set to 600r Ohm
Analog interface A-D gain offset = -3 dB
Analog interface D-A gain offset = -3 dB
Voice card specific Info Follows:
Signal Type is loopStart
Ring Frequency is 20 Hz
Hook Status is On Hook
Ring Active Status is inactive
Ring Ground Status is inactive
Tip Ground Status is active
Digit Duration Timing is set to 100 ms
InterDigit Duration Timing is set to 100 ms
Ring Cadence are [20 40] * 100 msec
InterDigit Pulse Duration Timing is set to 500 ms
```

The following is sample output from the show voice port command for a Foreign Exchange Station (FXS) analog voice port on a Cisco 3600 series:

```
Foreign Exchange Station 1/0/0 Slot is 1, Sub-unit is 0, Port is 0
Type of VoicePort is FXS
Operation State is DORMANT
Administrative State is UP
The Interface Down Failure Cause is 0
Alias is NULL
Noise Regeneration is enabled
Non Linear Processing is enabled
Music On Hold Threshold is Set to 0 dBm
```

```
In Gain is Set to 0 dB
Out Attenuation is Set to 0 dB
Echo Cancellation is enabled
Echo Cancel Coverage is set to 16ms
Connection Mode is Normal
Connection Number is
Initial Time Out is set to 10 s
Interdigit Time Out is set to 10 s
Analog Info Follows:
Region Tone is set for northamerica
Currently processing none
Maintenance Mode Set to None (not in mtc mode)
Number of signaling protocol errors are 0
Voice card specific Info Follows:
Signal Type is loopStart
Ring Frequency is 25 Hz
Hook Status is On Hook
Ring Active Status is inactive
Ring Ground Status is inactive
Tip Ground Status is inactive
Digit Duration Timing is set to 100 ms
InterDigit Duration Timing is set to 100 ms
Hook Flash Duration Timing is set to 600 ms
```

The following is sample output from the show voice port command for an E&M analog voice port on a Cisco 3600 series:

```
E&M Slot is 1, Sub-unit is 0, Port is 0
Type of VoicePort is E&M
Operation State is unknown
Administrative State is unknown
The Interface Down Failure Cause is 0
Alias is NULL
Noise Regeneration is disabled
Non Linear Processing is disabled
Music On Hold Threshold is Set to 0 dBm
In Gain is Set to 0 dB
Out Attenuation is Set to 0 dB
Echo Cancellation is disabled
Echo Cancel Coverage is set to 16ms
Connection Mode is Normal
Connection Number is
Initial Time Out is set to 0 s
Interdigit Time Out is set to 0 s
Analog Info Follows:
Region Tone is set for northamerica
Currently processing none
Maintenance Mode Set to None (not in mtc mode)
Number of signaling protocol errors are 0
Voice card specific Info Follows:
Signal Type is wink-start
Operation Type is 2-wire
Impedance is set to 600r Ohm
E&M Type is unknown
Dial Type is dtmf
In Seizure is inactive
Out Seizure is inactive
Digit Duration Timing is set to 0 ms
InterDigit Duration Timing is set to 0 ms
Pulse Rate Timing is set to 0 pulses/second
InterDigit Pulse Duration Timing is set to 0 ms
Clear Wait Duration Timing is set to 0 ms
Wink Wait Duration Timing is set to 0 ms
Wink Duration Timing is set to 0 ms
```

```
Delay Start Timing is set to 0 ms
Delay Duration Timing is set to 0 ms
```

Dialer Interface and Routing Troubleshooting

To obtain information on dialer interfaces, routing configuration, and routing operations, use the following commands in privileged EXEC mode.

Command	Purpose
show dialer map `Router# show dialer map`	Displays configured dynamic and static dialer maps. See Example Output for show dialer map Command, on page 95.
show dialer `Router# show dialer`	Displays general diagnostic information about an interface configured for DDR, such as the number of times the dialer string has been successfully reached, and the idle timer and the fast idle timer values for each B channel. Current call-specific information is also provided, such as the length of a call and the number and name of the device to which the interface is currently connected. When external signaling is configured, the output also displays the CDAPI state. See Example Output for show dialer Command, on page 96.
show interface *Dialer-num* `Router# show interface Dialer-num`	Shows whether the interface and protocol are up (spoofing), a state in which the dialer interface pretends to be up/up so that associated routes remain in force and packets can be routed to the interface. See Example Output for show interface Command, on page 97.
show ip route `Router# show ip route`	Displays the routes known to the router, including static and dynamically learned routes. See Example Output for show ip route Command, on page 97.

Example Output for show dialer map Command

The following is sample output from the **show dialer map** command.

```
Router# show dialer map
Static dialer map ip 10.1.1.1 name peer_1 on Dialer1
Static dialer map ip 10.1.1.2 name peer_2 on Dialer1
BAP dialer map ip 10.1.1.2 name peer_2 on Dialer1
Dynamic dialer map ip 10.1.1.3 name peer_3 on Dialer1
BAP dialer map ip 10.1.1.3 name peer_3 on Dialer1
```

Example Output for show dialer Command

The following is sample output from the **show dialer** command for a BRI interface when dialer profiles are configured:

```
Router# show dialer interface bri 0
BRI0 - dialer type = ISDN
Dial String Successes Failures Last called Last status
0 incoming call(s) have been screened.
BRI0: B-Channel 1
Idle timer (120 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is data link layer up
Dial reason: ip (s=10.1.1.8, d=10.1.1.1)
Interface bound to profile Dialer0
Time until disconnect 102 secs
Current call connected 00:00:19
Connected to 5773872 (wolfman)
BRI0: B-Channel 2
Idle timer (120 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is idle
```

The following is sample output from the **show dialer** command for a dialer under external signaling control:

```
Router# show dialer
Se7/0:0 - dialer type = IN-BAND SYNC NO-PARITY
Rotary group 1, priority 0
Idle timer (222222 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is idle
Dialer cdapi state is idle <<<<<<<<<==================
Se7/0:1 - dialer type = IN-BAND SYNC NO-PARITY
Rotary group 1, priority 0
Idle timer (222222 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is idle
Dialer cdapi state is idle <<<<<<<<<==================
```

The following is sample output from the **show dialer** command for an asynchronous interface:

```
Router# show dialer interface async 1
Async1 - dialer type = IN-BAND NO-PARITY
Idle timer (900 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Time until disconnect 838 secs
Current call connected 0:02:16
Connected to 8986
Dial String Successes Failures Last called Last status
8986 0 0 never Defaults
8986 8 3 0:02:16 Success Defaults
```

When the show dialer EXEC command is issued for a synchronous serial interface configured for DTR dialing, output similar to the following is displayed:

```
Serial 0 - dialer type = DTR SYNC
Idle timer (120 secs), Fst idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dial String Successes Failures Last called Last status
---- 1 0 1:04:47 Success DTR dialer
8986 0 0 never Defaults
```

Example Output for show interface Command

The following is sample output from the **show interface Dialer0**command:

```
Router# show interface Dialer0
Dialer0 is up (spoofing), line protocol is up (spoofing)
  Hardware is Unknown
  Internet address is 60.0.0.2/24
  MTU 1500 bytes, BW 56 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, loopback not set
  DTR is pulsed for 1 seconds on reset
  Last input never, output never, output hang never
  Last clearing of "show interface" counters 1d17h
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/0/16 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 42 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes
     0 packets output, 0 bytes
```

Example Output for show ip route Command

The following examples display all downloaded static routes. A P designates which route was installed using AAA route download.

```
Router# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
U - per-user static route, o - ODR, P - periodic downloaded static route
T - traffic engineered route
Gateway of last resort is 172.21.17.1 to network 0.0.0.0
172.31.0.0/32 is subnetted, 1 subnets
P 172.31.229.41 is directly connected, Dialer1 20.0.0.0/24 is subnetted, 3 subnets
P 10.1.1.0 [200/0] via 172.31.229.41, Dialer1
P 10.1.3.0 [200/0] via 172.31.229.41, Dialer1
P 10.1.2.0 [200/0] via 172.31.229.41, Dialer1
Router# show ip route static
172.27.4.0/8 is variably subnetted, 2 subnets, 2 masks
P 172.1.1.1/32 is directly connected, BRI0
P 172.27.4.0/8 [1/0] via 103.1.1.1, BRI0
S 172.31.0.0/16 [1/0] via 172.21.114.65, Ethernet0
S 10.0.0.0/8 is directly connected, BRI0
P 10.0.0.0/8 is directly connected, BRI0
172.21.0.0/16 is variably subnetted, 5 subnets, 2 masks
S 172.21.114.201/32 is directly connected, BRI0
S 172.21.114.205/32 is directly connected, BRI0
S 172.21.114.174/32 is directly connected, BRI0
S 172.21.114.12/32 is directly connected, BRI0
P 10.0.0.0/8 is directly connected, BRI0
P 10.1.0.0/8 is directly connected, BRI0
P 10.2.2.0/8 is directly connected, BRI0
S* 0.0.0.0/0 [1/0] via 172.21.114.65, Ethernet0
S 172.29.0.0/16 [1/0] via 172.21.114.65, Ethernet0
```

To debug dialer and authorization or to clear in-progress calls, use the following commands in privileged EXEC mode.

Command	Purpose
debug dialer Router# debug dialer	Displays the activity that triggers a dial attempt. See Example Output for show dialer Command, on page 96.
clear interface Router# clear interface	Clears a call that is in progress. In a troubleshooting situation, it is sometimes useful to clear historical statistics to track the current number of successful calls relative to failures. Use this command with care. It sometimes requires that you clear both the local and remote routers. See Example Output for clear interface Command, on page 98.
debug ppp negotiation Router# debug ppp negotiation	Displays negotiation of PPP options and Network Control Protocol (NCP) parameters. See Example Output for debug ppp negotiation Command, on page 99.
debug ppp authentication Router# debug ppp authentication	Displays exchange of Challenge Handshake Authentication Protocol (CHAP) and Password Authentication Protocol (PAP) packets. See Example Output for debug ppp authentication Command, on page 99.

Example Output for debug dialer Command

Displays the activity that triggers a dial attempt.

```
Dialing cause: Async1: ip (s=172.16.1.111 d=172.16.2.22)
```

Example Output for clear interface Command

The following example demonstrates the use of the **clear interface** command with the RLM feature:

```
Router# clear interface loopback 1
02:48:52: rlm 1: [State_Up, rx ACTIVE_LINK_BROKEN] over link [10.1.1.1(Loopback1), 10.1.4.1]
02:48:52: rlm 1: link [10.1.1.2(Loopback2), 10.1.4.2] requests activation
02:48:52: rlm 1: link [10.1.1.1(Loopback1), 10.1.4.1] is deactivated
02:48:52: rlm 1: link [10.1.1.1(Loopback1), 10.1.4.1] = socket[10.1.1.1, 10.1.4.1]
02:48:52: rlm 1: [State_Recover, rx USER_SOCKET_OPENED] over link [10.1.1.1(Loopback1),
10.1.4.1] for user RLM_MGR
02:48:52: rlm 1: link [10.1.1.1(Loopback1), 10.1.4.1] is opened
02:48:52: rlm 1: link [10.1.1.1(Loopback1), 10.1.5.1] = socket[10.1.1.1, 10.1.5.1]
```

```
02:48:52: rlm 1: [State_Recover, rx USER_SOCKET_OPENED] over link [10.1.1.1(Loopback1),
10.1.5.1] for user RLM_MGR
02:48:52: rlm 1: link [10.1.1.1(Loopback1), 10.1.5.1] is opened
02:48:52: rlm 1: [State_Recover, rx START_ACK] over link [10.1.1.2(Loopback2), 10.1.4.2]
02:48:52: rlm 1: link [10.1.1.2(Loopback2), 10.1.4.2] is activated
02:48:52: rlm 1: [State_Up, rx LINK_OPENED] over link [10.1.1.1(Loopback1), 10.1.4.1]
```

Example Output for debug ppp negotiation Command

The following is sample output from the **debug ppp negotiation** command. This is a normal negotiation, where both sides agree on Network Control Program (NCP) parameters. In this case, protocol type IP is proposed and acknowledged.

```
Router# debug ppp negotiation
ppp: sending CONFREQ, type = 4 (CI_QUALITYTYPE), value = C025/3E8
ppp: sending CONFREQ, type = 5 (CI_MAGICNUMBER), value = 3D56CAC
ppp: received config for type = 4 (QUALITYTYPE) acked
ppp: received config for type = 5 (MAGICNUMBER) value = 3D567F8 acked (ok)
PPP Serial4: state = ACKSENT fsm_rconfack(C021): rcvd id 5
ppp: config ACK received, type = 4 (CI_QUALITYTYPE), value = C025
ppp: config ACK received, type = 5 (CI_MAGICNUMBER), value = 3D56CAC
ppp: ipcp_reqci: returning CONFACK.
(ok)
PPP Serial4: state = ACKSENT fsm_rconfack(8021): rcvd id 4
```

The following is sample output from the debug ppp negotiation command when the remote side of the connection is unable to respond to LQM requests:

```
Router# debug ppp negotiation
ppp: sending CONFREQ, type = 4 (CI_QUALITYTYPE), value = C025/3E8
ppp: sending CONFREQ, type = 5 (CI_MAGICNUMBER), value = 44B7010
ppp: sending CONFREQ, type = 4 (CI_QUALITYTYPE), value = C025/3E8
ppp: sending CONFREQ, type = 5 (CI_MAGICNUMBER), value = 44B7010
ppp: sending CONFREQ, type = 4 (CI_QUALITYTYPE), value = C025/3E8
ppp: sending CONFREQ, type = 5 (CI_MAGICNUMBER), value = 44B7010
ppp: sending CONFREQ, type = 4 (CI_QUALITYTYPE), value = C025/3E8
ppp: sending CONFREQ, type = 5 (CI_MAGICNUMBER), value = 44B7010
ppp: sending CONFREQ, type = 4 (CI_QUALITYTYPE), value = C025/3E8
ppp: sending CONFREQ, type = 5 (CI_MAGICNUMBER), value = 44B7010
ppp: sending CONFREQ, type = 4 (CI_QUALITYTYPE), value = C025/3E8
ppp: sending CONFREQ, type = 5 (CI_MAGICNUMBER), value = 44B7010
ppp: sending CONFREQ, type = 4 (CI_QUALITYTYPE), value = C025/3E8
ppp: sending CONFREQ, type = 5 (CI_MAGICNUMBER), value = 44B7010
ppp: sending CONFREQ, type = 4 (CI_QUALITYTYPE), value = C025/3E8
ppp: sending CONFREQ, type = 5 (CI_MAGICNUMBER), value = 44B7010
ppp: sending CONFREQ, type = 4 (CI_QUALITYTYPE), value = C025/3E8
ppp: sending CONFREQ, type = 5 (CI_MAGICNUMBER), value = 44B7010
ppp: sending CONFREQ, type = 4 (CI_QUALITYTYPE), value = C025/3E8
ppp: sending CONFREQ, type = 5 (CI_MAGICNUMBER), value = 44B7010
ppp: sending CONFREQ, type = 4 (CI_QUALITYTYPE), value = C025/3E8
ppp: sending CONFREQ, type = 5 (CI_MAGICNUMBER), value = 44B7010
ppp: sending CONFREQ, type = 4 (CI_QUALITYTYPE), value = C025/3E8
ppp: sending CONFREQ, type = 5 (CI_MAGICNUMBER), value = 44C1488
```

Example Output for debug ppp authentication Command

The following is sample output from the **debug ppp authentication** command. Use this debug command to determine why an authentication fails.

```
Router# debug ppp authentication
Serial0: Unable to authenticate. No name received from peer
```

```
Serial0: Unable to validate CHAP response. USERNAME pioneer not found.
Serial0: Unable to validate CHAP response. No password defined for USERNAME pioneer
Serial0: Failed CHAP authentication with remote.
Remote message is Unknown name
Serial0: remote passed CHAP authentication.
Serial0: Passed CHAP authentication with remote.
Serial0: CHAP input code = 4 id = 3 len = 48
```

Configuration Examples for NAC Package for MGCP

NAS Package for MGCP Example

This example configures the Network Access Server Package for Media Gateway Control Protocol Feature on a Cisco AS5400:

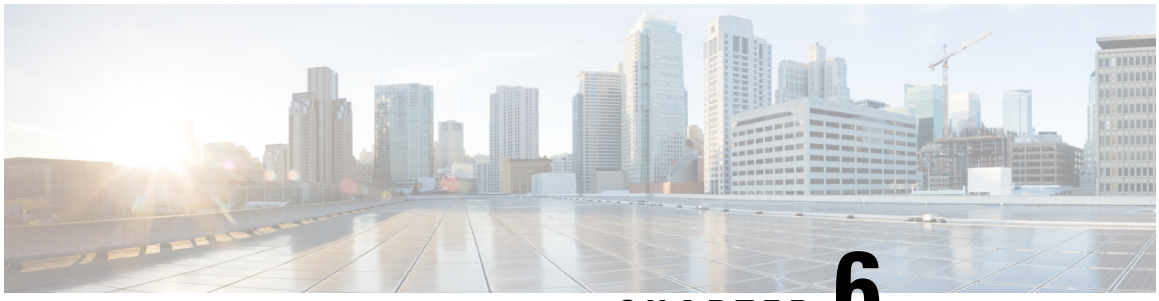
```
version 12.2
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 54iwo
!
no boot startup-test
logging rate-limit console 10 except errors
!
resource-pool disable
!
resource-pool profile service user1sample
!
voice-fastpath enable
ip subnet-zero
ip host 54ccxv 172.18.16.25
!
no ip dhcp-client network-discovery
isdn switch-type primary-ni
!
fax interface-type modem
mta receive maximum-recipients 0
!
controller T1 7/0
 framing esf
 extsig mgcp
 guard-timer 10 on-expiry reject
 linecode b8zs
 ds0-group 1 timeslots 1-24 type none service mgcp
!
controller T1 7/1
 framing esf
 linecode ami
 pri-group timeslots 1-24
!
controller T1 7/2
 framing sf
 linecode ami
!
controller T1 7/3
 framing sf
 linecode ami
```

```
!
controller T1 7/4
 framing sf
 linecode ami
!
controller T1 7/5
 framing sf
 linecode ami
!
controller T1 7/6
 framing sf
 linecode ami
!
controller T1 7/7
 framing sf
 linecode ami
!
interface Loopback0
 ip address 172.16.0.3 255.255.255.0
!
interface FastEthernet0/0
 ip address 172.18.184.183 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0
 no ip address
 shutdown
 clockrate 2000000
!
interface Serial0/1
 no ip address
 shutdown
 clockrate 2000000
!
interface Serial7/1:23
 no ip address
 encapsulation ppp
 dialer rotary-group 9
 dialer-group 1
 isdn switch-type primary-ni
 isdn incoming-voice modem
 no cdp enable
!
interface Async1/00
 ip unnumbered Loopback0
 dialer in-band
 dialer map ip 172.23.0.1 234567
 dialer-group 1
!
interface Async1/01
 ip address 10.17.1.1 255.255.255.0
 encapsulation ppp
 dialer in-band
 dialer map ip 10.17.1.2 22222
 dialer-group 1
!
interface Async1/02
```

```
 no ip address
!
interface Async1/03
 no ip address
!
interface Async1/04
 no ip address
!
interface Async1/05
 no ip address
!
interface Async3/102
 no ip address
!
interface Async3/103
 no ip address
!
interface Async3/104
 no ip address
!
interface Async3/105
 no ip address
!
interface Async3/106
 no ip address
!
interface Async3/107
 no ip address
!
interface Group-Async0
 no ip address
 no group-range
!
interface Dialer1
 ip unnumbered Loopback0
 encapsulation ppp
 dialer in-band
 dialer idle-timeout 222222
 dialer map ip 172.16.0.1 name 53bxbv 1000
 dialer extsig
 dialer-group 1
 no cdp enable
 ppp authentication chap
 ppp direction dedicated
!
interface Dialer9
 ip address 10.1.1.1 255.255.255.0
 encapsulation ppp
 dialer in-band
 dialer map ip 10.1.1.2 23456
 dialer-group 1
 no cdp enable
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.18.184.1
ip route 172.16.0.1 255.255.255.255 Dialer1
ip route 172.23.0.1 255.255.255.255 Async1/00
no ip http server
!
dialer-list 1 protocol ip permit
!
call rsvp-sync
!
voice-port 7/0:1
```

```
!
voice-port 7/1:D
!
mgcp
mgcp call-agent 172.18.64.242 service-type mgcp version 1.0
no mgcp timer receive-rtcp
!
mgcp profile default
 max2 retries 5
!
line con 0
 exec-timeout 0 0
 logging synchronous
line aux 0
 logging synchronous
line vty 0 4
 password mango
 login
line 1/00 1/107
 no flush-at-activation
 modem InOut
line 3/00 3/107
 no flush-at-activation
 modem InOut
!
scheduler allocate 10000 400
end
```

Note See the "Additional References for MGCP and SGCP" section on page x for related documents, standards, and MIBs and see the " Glossary " for definitions of terms in this guide.



CHAPTER 6

Configuring SGCP RSIP and AUEP Enhancements

This section provides information on configuring the Simple Gateway Control Protocol (SGCP) Restart In Progress (RSIP) and Audit Endpoint (AUEP) Enhancements feature. The feature provides enhancements to SGCP for disconnected RSIP and audit endpoints requested by call agents.

Feature benefits include the following:

- Provides SGCP 1.5 gateways with the ability to synchronize endpoints with call agents after the disconnected procedure has occurred.

For more information about this and related Cisco IOS voice features, see the following:

- "Overview of MGCP and Related Protocols" on page 3
- Entire Cisco IOS Voice Configuration Library--including library preface and glossary, other feature documents, and troubleshooting documentation--at http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/cisco_ios_voice_configuration_library_glossary/vcl.htm

Feature History for SGCP RSIP and AUEP Enhancements

Release	Modification
12.2(11)T	This feature was introduced on the following platforms: Cisco IAD2420 series, Cisco 2600 series, and Cisco MC3810.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for SGCP RSIP and AUEP Enhancements

- Configure SGCP 1.5 on the gateway.

Restrictions for SGCP RSIP and AUEP Enhancements

- This feature applies only to SGCP 1.5 gateways.
- This feature does not apply to MGCP gateways.

Information About SGCP RSIP and AUEP Enhancements

The SGCP RSIP and AUEP Enhancements feature provides additional messaging capabilities that allow an endpoint on a Simple Gateway Control Protocol (SGCP) 1.5 gateway to synchronize with a call agent after the endpoint returns to service from the disconnected procedure. The additional messaging capabilities provide the following:

- A special disconnected Restart In Progress (RSIP) message that the gateway sends to the call agent as a result of the disconnected procedure.
- Additional fields in the Audit Endpoint (AUEP) command that the call agent uses to query the endpoint's status when contact is reestablished.

Media Gateway Control Protocol (MGCP) provides this ability automatically, but it must be explicitly configured for SGCP networks, as described in the How to Configure SGCP RSIP and AUEP Enhancements, on page 107.

An endpoint may lose contact with its call agent because the call agent is temporarily off line or because of faults in the network. When a gateway recognizes that an endpoint has lost its communication with the call agent, it initiates the disconnected procedure. The disconnected procedure requires the endpoint to send RSIPs to the call agent and also to guarantee that the first message that the call agent sees from the endpoint is an RSIP command. The endpoint continues to attempt to send RSIPs at the intervals prescribed by the disconnected procedure until an attempt is successful. The RSIP identifies itself as an RSIP that was generated from a disconnected procedure rather than from a restart. The following output is seen on the gateway:

```
Disconnected RSIP sent from gateway
00:04:27:RSIP 7 ds1-3/2@RouterA SGCP 1.5
RM:disconnected
```

On receipt of a disconnected RSIP message, the call agent may decide to send an AUEP command to query the status of endpoints and synchronize endpoints. The SGCP RSIP and AUEP Enhancements feature provides the following additional fields of information in the AUEP:

- I--List of connection identifiers for current connections on the endpoint
- ES--Event state of the endpoint (off-hook or on-hook)

- RM--Restart method for the endpoint, which is one of the following:
  - Graceful--Endpoints are being taken out of service after a delay; the call agent should not make new connections.
  - Forced--Endpoints were abruptly taken out of service; connections were lost.
  - Restart--Endpoints with no connections will be returned to service after a delay.
  - Disconnected--Endpoints are being returned to service after the disconnected procedure.

How to Configure SGCP RSIP and AUEP Enhancements

Configuring SGCP RSIP and AUEP Enhancements

To configure enhanced restart and endpoint audit messaging capabilities on an SGCP gateway, use the following command in global configuration mode:

Command	Purpose
`Router(config)# mgcp sgcp disconnect notify`	Enables enhanced endpoint synchronization with a call agent after a disconnected procedure. The command is disabled by default.

Verifying SGCP RSIP Configuration

To verify your configuration, enter the **show mgcp** command. The following example shows that disconnected RSIP is enabled.

```
Router# show mgcp
MGCP Admin State ACTIVE, Oper State ACTIVE - Cause Code NONE
MGCP call-agent:172.16.193.148 Initial protocol service is SGCP 1.5
MGCP block-newcalls DISABLED
MGCP send SGCP RSIP:forced/restart/graceful DISABLED, disconnected ENABLED
MGCP quarantine mode discard/step
MGCP quarantine of persistent events is ENABLED
MGCP dtmf-relay for VoIP disabled for all codec types
MGCP dtmf-relay for VoAAL2 disabled for all codec types
MGCP voip modem passthrough mode:NSE, codec:g711ulaw, redundancy:DISABLED,
MGCP voaal2 modem passthrough mode:NSE, codec:g711ulaw
MGCP TSE payload:0
MGCP Named Signalling Event (NSE) response timer:200
MGCP Network (IP/AAL2) Continuity Test timer:200
MGCP 'RTP stream loss' timer:5
MGCP request timeout 500
MGCP maximum exponential request timeout 4000
MGCP gateway port:2427, MGCP maximum waiting delay 3000
MGCP restart delay 0, MGCP vad DISABLED
MGCP rtrcac DISABLED
MGCP system resource check DISABLED
MGCP xpc-codec:DISABLED, MGCP persistent hookflash:DISABLED
MGCP persistent offhook:ENABLED, MGCP persistent onhook:DISABLED
MGCP piggyback msg ENABLED, MGCP endpoint offset DISABLED
MGCP simple-sdp DISABLED
MGCP undotted-notation DISABLED
MGCP codec type g711ulaw, MGCP packetization period 20
```

```
MGCP JB threshold lwm 30, MGCP JB threshold hwm 150
MGCP LAT threshold lmw 150, MGCP LAT threshold hwm 300
MGCP PL threshold lwm 1000, MGCP PL threshold hwm 10000
MGCP CL threshold lwm 1000, MGCP CL threshold hwm 10000
MGCP playout mode is adaptive 60, 4, 200 in msec
MGCP IP ToS low delay disabled, MGCP IP ToS high throughput disabled
MGCP IP ToS high reliability disabled, MGCP IP ToS low cost disabled
MGCP IP RTP precedence 5, MGCP signaling precedence:3
MGCP default package:line-package
MGCP supported packages:gm-package dtmf-package trunk-package line-package
   hs-package atm-package ms-package dt-package res-package
   mt-package
MGCP Digit Map matching order:shortest match
SGCP Digit Map matching order:always left-to-right
MGCP VoAAL2 ignore-lco-codec DISABLED
```

Configuration Examples for SGCP RSIP and AUEP Enhancements

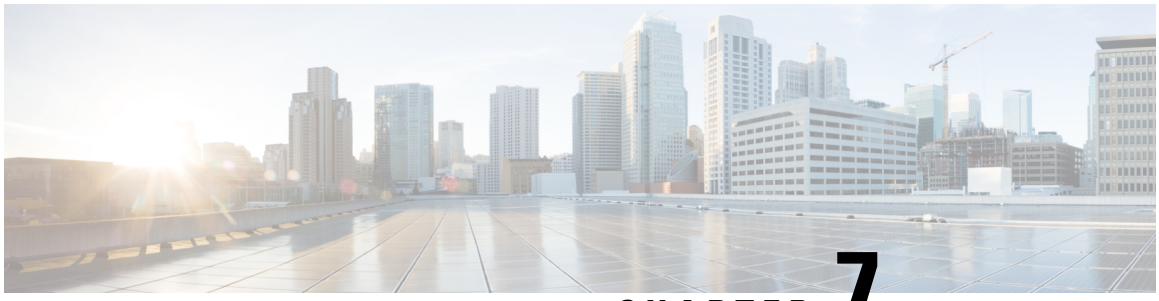
Disconnected RSIP Messaging Example

The following example shows the configuration of disconnected RSIP messaging on a Cisco MC3810.

```
version 12.2
no parser cache
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router2
!
boot system tftp smithj/mc3810-r3jj1 172.16.206.10
logging buffered 2000000 debugging
no logging console
enable password lab
!
network-clock base-rate 56k
ip subnet-zero
!
no ip domain-lookup
ip host corona 172.16.206.10
ip host redlands 172.31.140.33
ip host rialto 172.16.193.147
!
voice service voip
 fax protocol t38 ls-redundancy 0 hs-redundancy 0
!
no voice confirmation-tone
voice-card 0
!
controller T1 0
 mode cas
 framing esf
 clock source internal
 linecode ami
 ds0-group 0 timeslots 1-24 type fxs-ground-start
!
interface Ethernet0
 ip address 172.16.193.162 255.255.255.0
```

```
 no ip mroute-cache
!
interface Serial0
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
!
interface Serial1
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
!
interface FR-ATM20
 no ip address
 shutdown
ip classless
ip route 10.0.0.0 10.0.0.0 172.16.193.1
ip route 172.16.0.0 255.255.0.0 172.16.193.1
no ip http server
!
!
call rsvp-sync
!
voice-port 0:0
!
voice-port 1/1
!
voice-port 1/2
 description package
!
mgcp
mgcp call-agent 172.16.193.148 service-type sgcp version 1.5
mgcp sgcp disconnect notify
!
mgcp profile default
!
dial-peer cor custom
!
dial-peer voice 1 pots
 application mgcpapp
 port 1/1
!
dial-peer voice 2 pots
 application mgcpapp
 port 1/2
!
dial-peer voice 3 pots
 application mgcpapp
 port 0:0
!
gatekeeper
 shutdown
!
line con 0
 exec-timeout 0 0
line aux 0
line 2 3
line vty 0 4
 exec-timeout 0 0
 password hemet
 login
```

```
!
end
```



CHAPTER 7

Configuring MGCP Gateway Support

This section provides information on configuring the MGCP Gateway Support for the **mgcp bind** command feature.

Feature benefits include the following:

- Media gateway controller-to-media gateway (MGC-to-MG) signaling and identification

The command allows you to use a loopback interface IP address for sourcing MGCP packets, which is transparent to any interface failure.

- Security of the media gateway

The command allows you to obtain a predefined interface for both MGCP and media control, which can be used for security configuration.

- Possible clash of voice and dial addressing

This feature allows you to assign a media bind interface other than loopback 0, which allows dial calls to conserve IP addresses.

- No interface diversity using routing and reduced MGCP voice diversity

You can use routing capability more efficiently if you configure the loopback interface for control. Using the command to configure the loopback interface helps in creating redundant MGCP control or media interface.

- MGCP backward compatibility

This feature is backward compatible with earlier MGCP features.

For more information about this and related Cisco IOS voice features, see the following:

- "Overview of MGCP and Related Protocols" on page 3
- Entire Cisco IOS Voice Configuration Library--including library preface and glossary, other feature documents, and troubleshooting documentation--at http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/cisco_ios_voice_configuration_library_glossary/vcl.htm

Feature History for MGCP Gateway Support for the mgcp bind Command

Release	Modification
12.2(13)T	This feature was introduced.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring MGCP Gateway Support

The current Media Gateway Control Protocol (MGCP) implementation does not allow the assignment of particular IP addresses for sourcing MGCP commands and media packets, which can cause firewall and security problems. This feature allows you to configure interfaces on which control and media packets can be exchanged. This new functionality allows you to separate signaling from voice by binding control (MGCP signaling) and media (Real-Time Transport Protocol, or RTP voice, fax, and modem) to specific gateway interfaces.

This feature includes new commands that can be used to configure the required interface for MGCP control and control of the required media packets.

Information About MGCP Gateway Support

If the media gateway (MG) uses an IP address, which is the outgoing interface of the MG, the media gateway controller (MGC) identifies the MG entity with that address. If that interface fails, MG sources MGCP from another interface, which is not known to the MGC. Some form of name lookup (host or Domain Name System, or DNS) needs to occur on the MGC at this time. Using the **mgcp bind**command, a loopback interface IP address can be used for sourcing MGCP packets, which is transparent to any interface failure.

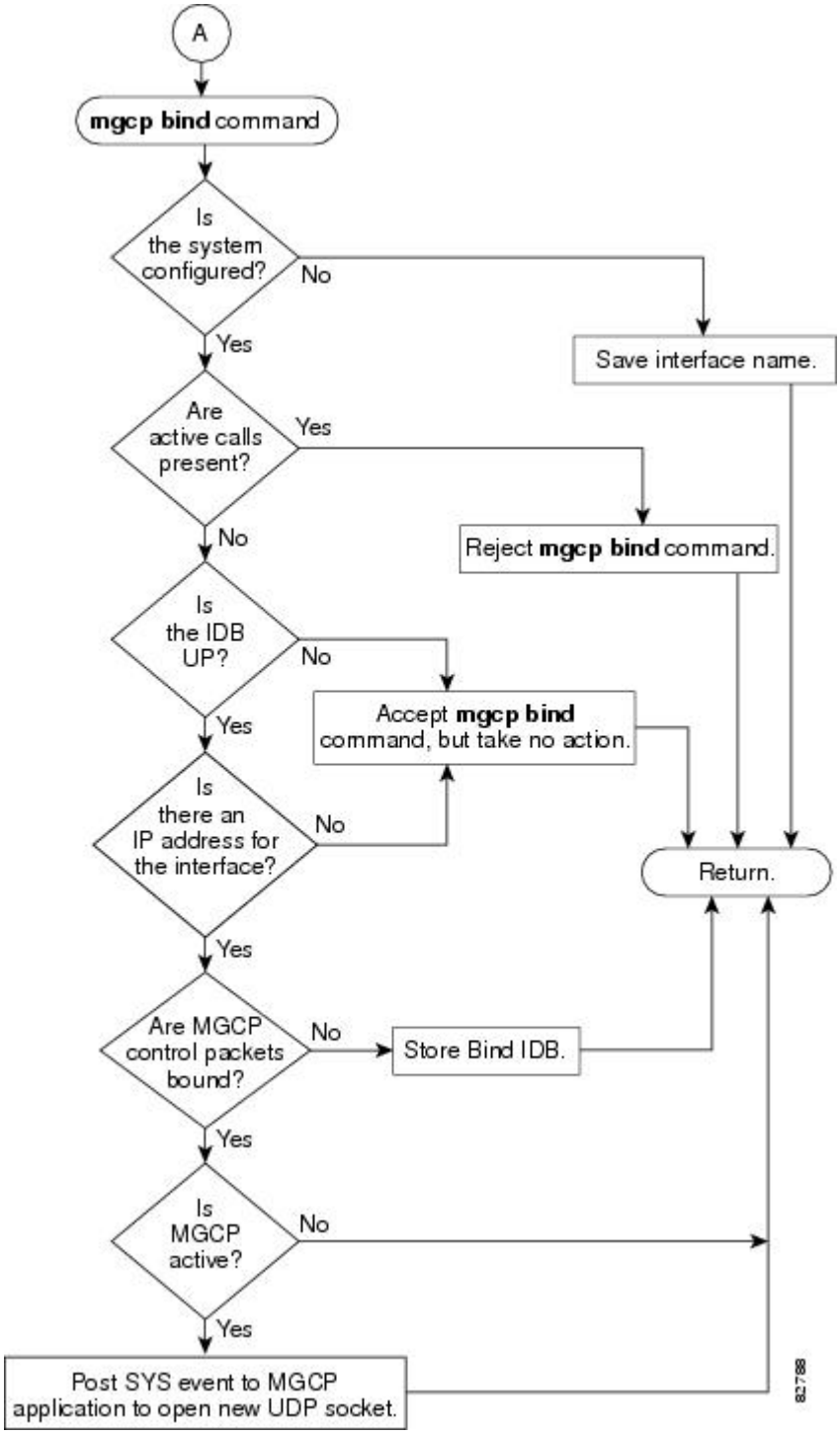
Present implementation of MGCP media uses the "loopback 0" or best available IP address in the order indicated for media. A fixed default loopback 0 address for media streams breaks the dial address pool convention used for most configurations, where dial IP addresses are assigned from the loopback 0 address range. With this feature, it is possible to assign a media bind interface other than loopback 0, which helps dial calls conserve IP addresses.

If you configure the loopback interface for control, you can use routing capability more efficiently. Using the**mgcp bind** command to configure the loopback interface helps in creating redundant MGCP control or media interface.

In the current implementation of MGCP, the source address of MGCP and media control is given by the IP layer. Because of this inconsistency, it is not possible to include a reliable access list or firewall configuration. Using the **mgcp bind** command for both MGCP and media control, you can get a predefined interface or IP address that can be used for security configuration.

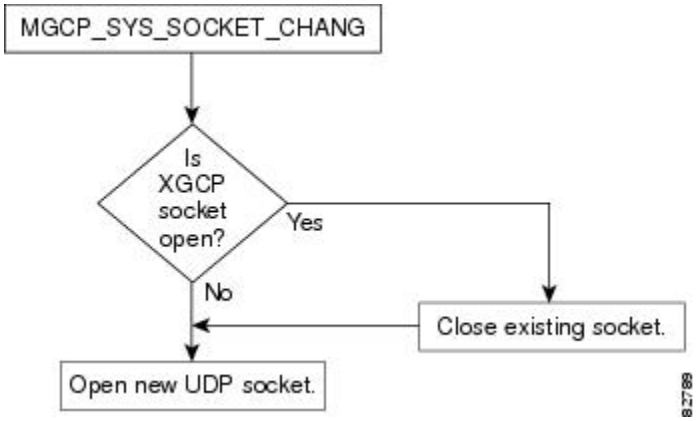
The figure below shows a typical configuration flow using the**mgcp bind** command.

Figure 9: Bind Configuration Flowchart



The figure below shows how the **mgcp bind** command takes effect for MGCP control. When the**mgcp bind** command is configured for MGCP control, the MGCP_SYS_SOCKET_CHANG system event is posted to MGCPAPP. This event is processed by opening a new socket based on the configured interface.

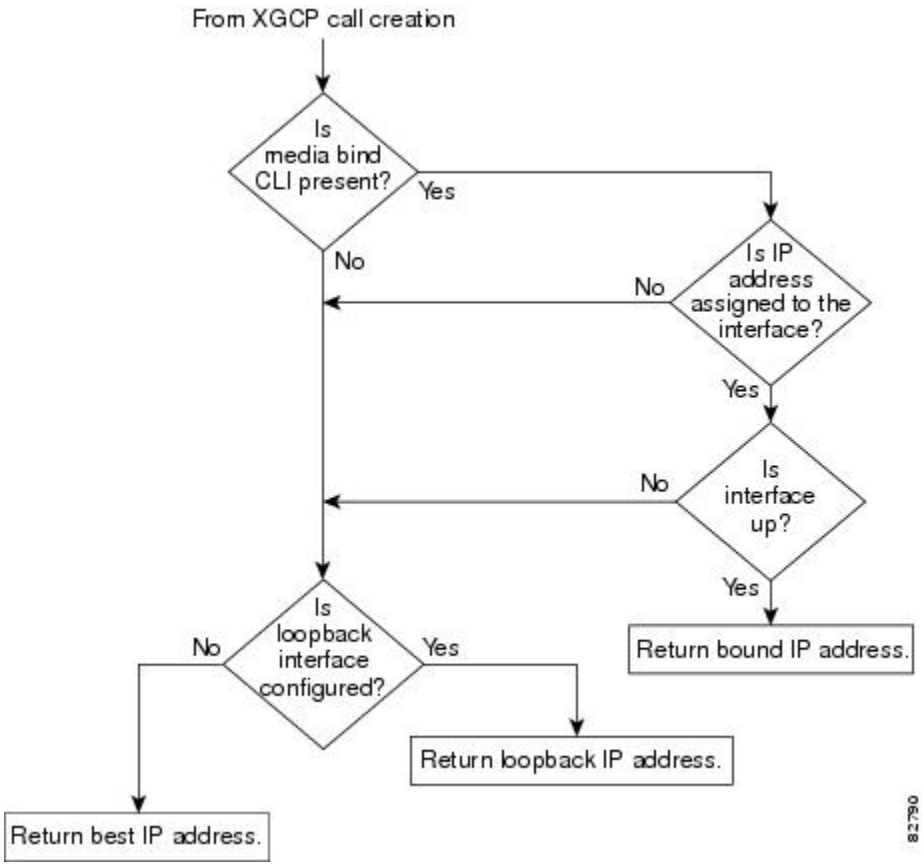
Figure 10: Bind Configuration for Control Flowchart



The time frame for execution of the**mgcp bind** command for media is different from that for control. The figure below shows how the**mgcp bind**command is used for media. In this case, the IP address used for media Session Description Protocol (SDP) negotiation is taken from the configured interface. This flow is not active until an MGCP call is created.

The function call to get an IP address for the media returns a configured interface IP address, a loopback interface IP address, or a best available IP address in the order specified in the figure.

Figure 11: Bind Configuration for Media Flowchart



How to Configure MGCP Gateway Support

Note If more than 72 end points are configured with MGCP in a single voice gateway, we recommend you to increase the hold-queue size on the interface of the gateway to 300.

Configuring the MGCP Application

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mgcp call-agent** {*dns-name* | *ip-address*} [*port*] [**service-type** *type*] [**version** *protocol-version*]
4. **mgcp**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**mgcp call-agent** {*dns-name* | *ip-address*} [*port*] [**service-type** *type*] [**version** *protocol-version*] **Example:** `Router(config)# mgcp call-agent 209.165.200.225 service-type mgcp version 1.0`	Configures the MGCP protocol and corresponding call agent.
Step 4	**mgcp** **Example:** `Router(config)# mgcp`	Enables MGCP on the gateway.
Step 5	**exit** **Example:** `Router(config)# exit`	Exits the current mode.

Configuring the bind Command

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mgcp bind** {**control** | **media**} **source-interface** *interface-id*
4. **mgcp**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**mgcp bind** {**control**	**media**} **source-interface** *interface-id* **Example:** `Router(config)# mgcp bind {control} source-interface FastEthernet`	Sets a source interface for signaling and media packets.
Step 4	**mgcp** **Example:** `Router(config)# mgcp`	Enables MGCP on the gateway.
Step 5	**exit** **Example:** `Router(config)# exit`	Exits the current mode.

Troubleshooting Tips

To troubleshoot the MGCP Gateway Support for the Bind Command feature, use the **debug mgcp** command to enable debug traces for MGCP errors, events, media, packets, parser, and call admission control (CAC).

The following example illustrates the output for the **debug mgcp** command with the all keyword:

```
Router# debug mgcp all
20:54:13: MGC stat - 192.168.10.10, total=37, succ=28, failed=8
20:54:13: MGCP Packet received -
```

```
CRCX 55560 s0/ds1-0/1 SGCP 1.1
C: 78980
M: sendrecv
L: a:G.726-16
20:54:13: -- mgcp_parse_packet() - call mgcp_parse_header
- mgcp_parse_header()- Request Verb FOUND CRCX
- mgcp_parse_packet() - out mgcp_parse_header
- SUCCESS: mgcp_parse_packet()-MGCP Header parsing was OK
- mgcp_parse_parameter_lines(), code_str:: 78980, code_len:2, str:1640150312
- mgcp_parse_parameter_lines(str:C: 78980) -num_toks: 19
- mgcp_parse_parameter_lines() check NULL str(78980), in_ptr(C: 78980)
- mgcp_parse_parameter_lines() return Parse function in
mgcp_parm_rules_array[1]
- mgcp_parse_call_id(in_ptr: 78980)
- SUCCESS: mgcp_parse_call_id()-Call ID string(78980) parsing is OK
- mgcp_parse_parameter_lines(), code_str:: sendrecv, code_len:2, str:1640150312
- mgcp_parse_parameter_lines(str:M: sendrecv) -num_toks: 19
- mgcp_parse_parameter_lines() check NULL str(sendrecv), in_ptr(M: sendrecv)
- mgcp_parse_parameter_lines() return Parse function in
mgcp_parm_rules_array[6]
- mgcp_parse_conn_mode(in_ptr: sendrecv)
- mgcp_parse_conn_mode()- tmp_ptr:(sendrecv)
- mgcp_parse_conn_mode(match sendrecv sendrecv
- mgcp_parse_conn_mode(case MODE_SENDRECV)
- SUCCESS: Connection Mode parsing is OK
- mgcp_parse_parameter_lines(), code_str:: a:G.726-16, code_len:2,
str:1640150312
- mgcp_parse_parameter_lines(str:L: a:G.726-16) -num_toks: 19
- mgcp_parse_parameter_lines() check NULL str(a:G.726-16), in_ptr(L:
a:G.726-16)
- mgcp_parse_parameter_lines() return Parse function in mgcp_parm_rules_array[5]
- mgcp_parse_con_opts()
- mgcp_parse_codecs()
- SUCCESS: CODEC strings parsing is OK- SUCCESS: Local Connection option
parsing is OK- mgcp_val_mandatory_parms()
20:54:13: - SUCCESS: mgcp_parse_packet()- END of Parsing
20:54:13: MGCP msg 1
20:54:13: mgcp_search_call_by_endpt: endpt = s0/ds1-0/1, new_call = 1
20:54:13: slot=0,ds1=0,ds0=1
20:54:13: search endpoint - New call=1, callp 61C28130
20:54:13: callp: 61C28130, vdbptr: 0, state: 0
20:54:13: mgcp_remove_old_ack:
20:54:13: mgcp_idle_crcx: get capability
passthru is 3
20:54:13: process_request_ev- callp 61C28130, voice_if 61C281A4
20:54:13: process_detect_ev- callp 61C28130, voice_if 61C281A4
process_signal_ev- callp 61C28130, voice_ifp 61C281A4
20:54:13: mgcp_process_quarantine_mode- callp 61C28130, voice_if 61C281A4
20:54:13: mgcp_process_quarantine_mode- new q mode: process=0, loop=0
20:54:13: mgcp_xlat_ccapi_error_code - ack_code_tab_index = 0,
20:54:13: No SDP connection info
20:54:13: mgcp_select_codec - LC option, num codec=1, 1st codec=5
20:54:13: mgcp_select_codec - num supprt codec=11
20:54:13: mgcp_select_codec - LC codec list only
20:54:13: codec index=0, bw=16000, codec=5
20:54:13: selected codec=5mgcp_get_pkt_period: voip_codec=2, pkt_period=0, call
adjust_packetization_period
mgcp_get_pkt_period: voip_codec=2, pkt_period=10, after calling
adjust_packetization_period
20:54:13: selected codec 5
20:54:13: IP Precedence=60
20:54:13: MGCP msg qos value=0mgcp_get_pkt_period: voip_codec=2, pkt_period=0,
call adjust_packetization_period
mgcp_get_pkt_period: voip_codec=2, pkt_period=10, after calling
```

```
adjust_packetization_period
mgcp_new_codec_bytes: voip_codec=2, pkt_period=10, codec_bytes=20
20:54:13: callp : 61C28AE8, state : 2, call ID : 40, event : 5, minor evt:
1640137008
20:54:13: MGCPAPP state machine: state = 2, event = 5
20:54:13: mgcp_call_connect: call_id=40, ack will be sent later.
20:54:13: callp : 61C28AE8, new state : 3, call ID : 40
20:54:14: xlate_ccapi_ev - Protocol is SGCP, change pkg=2
20:54:14: MGCP Session Appl: ignore CCAPI event 22, callp 61C28130
20:54:14: xlate_ccapi_ev - Protocol is SGCP, change pkg=2
20:54:14: callp : 61C28130, state : 2, call ID : 39, event : 5, minor evt: 20
20:54:14: MGCPAPP state machine: state = 2, event = 5
20:54:14: callp : 61C28130, new state : 3, call ID : 39
20:54:14: xlate_ccapi_ev - Protocol is SGCP, change pkg=2
20:54:14: callp : 61C28130, state : 3, call ID : 39, event : 6, minor evt: 20
20:54:14: MGCPAPP state machine: state = 3, event = 6
20:54:14: call_id=39, mgcp_ignore_ccapi_ev: ignore 6 for state 3
20:54:14: callp : 61C28130, new state : 3, call ID : 39
20:54:14: MGCP voice mode event
20:54:14: xlate_ccapi_ev - Protocol is SGCP, change pkg=2
20:54:14: callp : 61C28130, state : 3, call ID : 39, event : 17, minor evt: 0
20:54:14: MGCPAPP state machine: state = 3, event = 17
20:54:14: mgcp_voice_mode_done(): callp 61C28130, major ev 17,
minor ev 0mgcp_start_ld_timer: timer already initialized
20:54:14: send_mgcp_create_ack
20:54:14: map_mgcp_error_code_to_string error_tab_index = 0, protocol version:
2
20:54:14: MGC stat - 1.13.89.3, total=37, succ=29, failed=8
20:54:14: Codec Cnt, 1, first codec 5
20:54:14: First Audio codec, 5, local encoding, 96
20:54:14: -- mgcp_build_packet()-
20:54:14: - mgcp_estimate_msg_buf_length() - 87 bytes needed for header
- mgcp_estimate_msg_buf_length() - 125 bytes needed after checking parameter lines
- mgcp_estimate_msg_buf_length() - 505 bytes needed after cheking SDP lines
20:54:14: --- mgcp_build_parameter_lines() ---
- mgcp_build_conn_id()
- SUCCESS: Conn ID string building is OK
- SUCCESS: Building MGCP Parameter lines is OK
- SUCCESS: building sdp owner id (o=) line
- SUCCESS: building sdp session name (s=) line
- SUCCESS: MGCP message building OK
- SUCCESS: END of building
updating lport with 2427
20:54:14: send_mgcp_msg, MGCP Packet sent --->
200 55560
I: 10
v=0
o=- 78980 0 IN IP4 192.168.10.9
s=Cisco SDP 0
c=IN IP4 192.168.10.9
t=0 0
m=audio 16444 RTP/AVP 96
a=rtpmap:96 G.726-16/8000/1
<---
20:54:14: enqueue_ack: voice_if=61C281A4, ackqhead=0, ackqtail=0,
ackp=61D753E8, msg=61D00010
20:54:14:
mgcp_process_quarantine_after_ack:ack_code=200mgcp_delete_qb_evt_q:cleanup QB
evt q
20:54:14: callp : 61C28130, new state : 4, call ID : 39
```

Verifying MGCP Gateway Support

SUMMARY STEPS

1. Router# **show mgcp**
2. Router# **show ip socket**
3. Router# **show running-configuration**

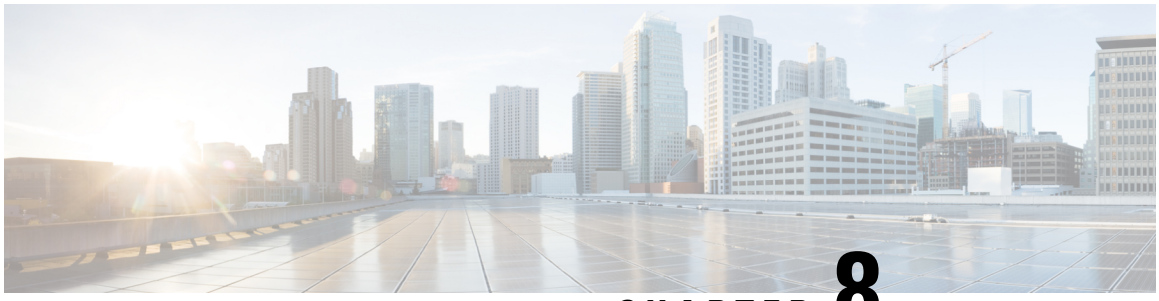
DETAILED STEPS

	Command or Action	Purpose
Step 1	Router# **show mgcp**	Checks your configuration.
Step 2	Router# **show ip socket**	Displays IP socket information.
Step 3	Router# **show running-configuration**	Verifies bind functionality.

Configuration Examples for MGCP Gateway Support

The following is partial output from the**show running-configuration** command indicating that bind is functional on receiving router 172.18.192.204. Updated output for MGCP binding is highlighted under the voice service VoIP indicator.

```
ip subnet-zero
ip ftp source-interface Ethernet0
!
voice service voip
mgcp bind control source-interface FastEthernet0
mgcp bind media source-interface FastEthernet0
!
interface FastEthernet0
 ip address 172.18.192.204 255.255.255.0
 duplex auto
 speed auto
 fair-queue 64 256 1000
 ip rsvp bandwidth 75000 100
!
```



CHAPTER 8

Configuring MGCP CAS MD Package

This chapter provides information on configuring the MGCP channel-associated signaling (CAS) MD Package feature. This feature introduces support for Feature Group D (FGD) Exchange Access North American (EANA) protocol signaling. The CAS MD package adds support for the reporting of automatic number identification (ANI) and dialed number identification service (DNIS) digits to enable the MGCP call agent to better handle customer billing.

For more information about this and related Cisco IOS voice features, see the following:

- "Overview of MGCP and Related Protocols" on page 3
- Entire Cisco IOS Voice Configuration Library--including library preface and glossary, other feature documents, and troubleshooting documentation--at http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/voice_c/vcl.htm .

Feature History for MGCP CAS MD Package

Release	Modification
12.4(4)T	This feature was introduced on the Cisco AS5850.
12.4(15)T	Support was added for the Cisco AS5350, Cisco AS5350XM, Cisco AS5400XM, and Cisco AS5400HPX platforms.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for MGCP CAS MD Package

Prerequisites are described in "Prerequisites for Configuring MGCP and Related Protocols" on page 3.

Restrictions for MGCP CAS MD Package

FGD Exchange Access International (EAIN) signaling is not supported.

Information About MGCP CAS MD Package

MD Package

The MD package supports the FGD EANA protocol for T1 CAS interfaces as defined in RFC 3064. It includes support for ANI and DNIS reporting that enables the MGCP call agent to improve its handling of customer billing. The MD package is enabled automatically when a T1 interface is configured using the **ds0-group** command with the **fgd-eana** keyword. The order in which the voice gateway sends the ANI and DNIS digits can be controlled by using the **notify** command in the MGCP profile.

How to Configure the MGCP CAS MD Package

Note You do not have to enable the CAS MD package with the **mgcp package-capability** command. The CAS MD package is enabled automatically when a T1 controller is configured for FGD EANA signaling using the **ds0-group** command.

Configuring the Incoming Called Number in the MGCP Dial Peer

Perform this procedure to specify the dial string to use for matching incoming calls to the MGCP dial peer.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *tag* **pots**
4. **service mgcpapp**
5. **incoming called number** *string*
6. **port** *port*
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**dial-peer voice** *tag* **pots** **Example:** `Router(config)# dial-peer voice 1003 pots`	Defines a dial peer as a POTS device and enters dial-peer configuration mode.
Step 4	**service mgcpapp** **Example:** `Router(config-dial-peer)# service mgcpapp`	Enables MGCP on the dial peer. **Note** Do not use this command in dial peers that support PRI backhaul or BRI backhaul.
Step 5	**incoming called number** *string* **Example:** `Router(config-dial-peer)# incoming called number .`	Specifies the digit string that is used to match incoming calls to the dial peer.
Step 6	**port** *port* **Example:** `Router(config-dial-peer)# port 0/0:3:0`	Binds the MGCP application to the specified voice port.
Step 7	**end** **Example:** `Router(config-dial-peer)# end`	Exits to privileged EXEC mode.

Modifying ANI and DNIS Order when Using CAS MD Package

Perform this procedure to specify the order in which ANI and DNIS digits are sent in notify messages to the call agent when using the CAS MD package.

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **mgcp profile** {*profile-name* | **default**}
4. **notify** {**ani-dnis** | **dnis-ani**}
5. **end**
6. **show mgcp profile** [*profile-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**mgcp profile** {*profile-name*	**default**} **Example:** `Router(config)# mgcp profile default`	Defines an MGCP profile to be associated with one or more MGCP endpoints.
Step 4	**notify** {**ani-dnis**	**dnis-ani**} **Example:** `Router(config-mgcp-profile)# notify dnis-ani`	Specifies the order in which ANI and DNIS digits are reported to the MGCP call agent. • **ani-dnis** --ANI digits are sent in the first notify message. This is the default order. • **dnis-ani** --DNIS digits are sent in the first notify message.
Step 5	**end** **Example:** `Router(config-mgcp-profile)# end`	Exits to privileged EXEC mode.
Step 6	**show mgcp profile** [*profile-name*] **Example:** `Router# show mgcp profile default`	Displays configuration information for MGCP profiles including the setting of the **notify** command.

Configuration Examples for MGCP CAS MD Package

CAS MD Package Configuration Example

The following example shows the significant portions of a configuration for the CAS MD package.

```
...
controller T1 0/0:3
 framing esf
 ds0-group 0 timeslots 1 type fgd-eana mf ani-dnis
!
controller T1 0/0:4
 framing esf
 ds0-group 0 timeslots 1 type fgd-eana mf ani-dnis
...
mgcp profile default
 notify dnis-ani
!
!
dial-peer voice 1003 pots
 service mgcpapp
 incoming called-number .
 port 0/0:3:0
!
dial-peer voice 1004 pots
 service mgcpapp
 incoming called-number .
 port 0/0:4:0
...
```

Cisco AS5850 Configuration Example

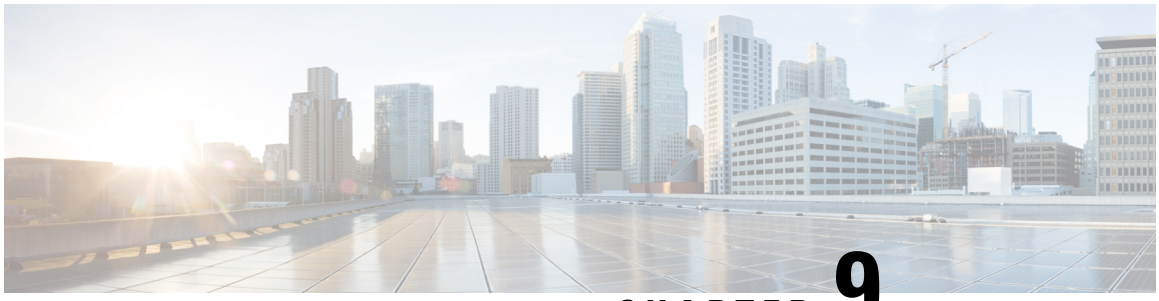
The following example shows a complete running configuration for a Cisco AS5850 universal gateway that is using the CAS MD package.

```
Current configuration : 2636 bytes
!
version 12.4
no service pad
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
service internal
!
hostname Sample
!
boot-start-marker
boot system flash:c5850-p9-mz
boot-end-marker
!
!
redundancy
 mode classic-split
logging buffered 20000000 debugging
no logging console
enable password temp
```

```
!
no aaa new-model
!
resource policy
!
!
!
resource-pool disable
dial-tdm-clock priority 1 external t1 120ohm
spe default-firmware spe-firmware-1
!
!
!
!
ip subnet-zero
ip cef distributed
!
!
!
isdn switch-type primary-5ess
!
!
!
!
!
!
controller T3 0/0
 framing c-bit
 cablelength 224
 t1 1-7 controller
!
controller T1 0/0:1
 shutdown
 framing sf
 ds0-group 0 timeslots 1 type fgd-eana mf ani-dnis
!
controller T1 0/0:2
 shutdown
 framing sf
 ds0-group 0 timeslots 1 type fgd-eana mf ani-dnis
!
controller T1 0/0:3
 framing esf
 ds0-group 0 timeslots 1 type fgd-eana mf ani-dnis
!
controller T1 0/0:4
 framing esf
 ds0-group 0 timeslots 1 type fgd-eana mf ani-dnis
!
controller T1 0/0:5
 framing esf
!
controller T1 0/0:6
 shutdown
 framing esf
!
controller T1 0/0:7
 framing esf
!
!
!
interface Loopback0
 no ip address
 no ip route-cache cef
```

```
 no ip route-cache distributed
 no ip route-cache
!
interface FastEthernet6/0
 ip address 172.16.0.46 255.255.255.0
 no ip proxy-arp
 logging event link-status
 speed 100
 full-duplex
 no keepalive
!
interface GigabitEthernet6/0
 no ip address
 logging event link-status
 shutdown
 negotiation auto
!
interface GigabitEthernet6/1
 no ip address
 logging event link-status
 shutdown
 negotiation auto
!
interface Group-Async0
 no ip address
 encapsulation ppp
 group-range 0/00 3/323
!
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.0.200
no ip http server
!
!
!
!
!
!
voice-port 0/0:1:0
!
voice-port 0/0:2:0
!
voice-port 0/0:3:0
!
voice-port 0/0:4:0
!
mgcp
mgcp call-agent 172.16.0.200 18384 service-type mgcp version 0.1
mgcp package-capability dtmf-package
mgcp package-capability mf-package
mgcp package-capability rtp-package
no mgcp piggyback message
mgcp persistent onhook
mgcp fax t38 inhibit
!
mgcp profile default
!
!
dial-peer voice 1003 pots
 service mgcpapp
 incoming called-number .
 port 0/0:3:0
!
dial-peer voice 1004 pots
```

```
 service mgcpapp
 incoming called-number .
 port 0/0:4:0
!
!
!
line con 0
 exec-timeout 0 0
 transport output all
line aux 0
 exec-timeout 0 0
 transport output all
line vty 0 4
 exec-timeout 0 0
 privilege level 15
 no login
 transport input all
 transport output all
line 0/00 0/215
 modem InOut
 transport input all
line 3/00 3/323
 modem InOut
 transport input all
!
end
```



CHAPTER 9

Media and Signaling Authentication and Encryption

The Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways feature provides support for Cisco Secure Survivable Remote Site Telephony (SRST) and voice security features that include authentication, integrity, and encryption of voice media and related call control signaling.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Media and Signaling Authentication and Encryption

Make sure that the following tasks have been completed before configuring the Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways feature:

- Cisco IOS Media Gateway Control Protocol (MGCP) is configured.
- Cisco Unified Communications Manager 4.1(2) or a later release is running.

- Cisco Secure SRST is configured on the router. For more information on configuring secure SRST on the router, refer to the document Setting up Secure SRST.
- Cisco IOS gateways have the prerequisite Cisco IOS images installed. Voice security features are delivered on Advanced IP Services or Advanced Enterprise Services images.

It is recommended that IP security (IPsec) be configured on the Cisco IOS gateway. Both software and hardware-based IPsec connections are supported.

For more information on configuring Cisco IOS-based (software) IPsec, refer to the following:

- *Cisco IOS Security Configuration Guide*, Release 12.3
- *Cisco IOS Security Command Reference*, Release 12.3

For more information on configuring hardware-based IPsec on the gateway, refer to the following books:

- *Cisco 2621 Modular Access Router with AIM-VPN/BP Security Policy*
- *Cisco 2651 Modular Access Router with AIM-VPN/BP Security Policy*
- *Cisco 3640 Modular Access Router with AIM-VPN/BP Security Policy*
- *Cisco 3660 Modular Access Router with AIM-VPN/BP Security Policy*

It is recommended that IPsec be configured on the Cisco CallManager. For more information, refer to the Microsoft Knowledge Base article " Configuring IPsec Between a Microsoft Windows 2000 Server and a Cisco Device. "

If you want to interoperate with Cisco IP phones, make sure that the following tasks have been completed before configuring the Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways feature:

- Cisco CallManager is set up for secure mode operation, and a certificate trust list (CTL) client is installed. For more information on CTL client setup, refer to Cisco IP Phone Authentication and Encryption for Cisco CallManager 4.0(1), "Authentication, Integrity and Encryption" chapter.
- The phones are configured to support secure calls if the gateways will interoperate with Cisco IP phones. For more information on Cisco IP phone configuration, refer to the following:
  - Cisco IP Phone Model 7960G and 7940G Administration Guide for Cisco CallManager Release 4.2, "Security Configuration Menu" section.
  - *Cisco IP Phone 7970 Administration Guide for Cisco CallManager, Release 4.x and later*, "Understanding Security Features for Cisco IP Phones" section.

Restrictions for Media and Signaling Authentication and Encryption

The Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways feature is supported on Cisco IOS MGCP 0.1 and Cisco IOS MGCP 1.0.

Cisco IOS MGCP SRTP support on the Cisco AS5400XM gateway is limited to the c5510 digital signal processors (DSP) series.

Cisco IOS MGCP gateways support voice security features on the following endpoints only: T1, E1, FXS, and FXO.

When a Cisco IOS MGCP voice gateway is used in conjunction with the Cisco CallManager, the automatic download feature that allows you to complete the gateway configuration on the Cisco CallManager server by downloading the configuration to that gateway through a TFTP server is not supported with voice security features.

Voice security during conferencing, transcoding, and music-on-hold is not supported.

Note If one component in the voice gateway path is not secure, the entire call falls back to nonsecure mode.

The table below provides a list of supported IP phones, gateways and network modules for voice security features.

Table 5: Supported Products for Voice Security Features

Supported Cisco IP Phones	Supported Gateways	Supported Network Modules
• Cisco IP Phone 7940 • Cisco IP Phone 7960 • Cisco IP Phone 7970	• Cisco 2600XM • Cisco 2691 • Cisco 2811 • Cisco 2821 • Cisco 2851 • Cisco 3640A • Cisco 3660 • Cisco 3700 • Cisco 3825 • Cisco 3845 • Cisco VG224 • Cisco AS5400XM	• EVM-HD • NM-HDV2 • NM-HDV2-1T1/E1 • NM-HDV2-2T1/E1 • NM-HD-1V • NM-HD-2V • NM-HD-2VE • PVDM2

Voice security features impact quality of service (QoS) as follows:

- The Secure Real-Time Transport Protocol Control Protocol (SRTCP) packet size increases by an 80-bit authentication tag, a 31-bit index field, and a 1-bit encryption flag.
- The bandwidth of Real-Time Transport Protocol (RTP) streams increases slightly with the introduction of the 32-bit authentication tag on every SRTP packet sent. Additional bandwidth is required for supported SRTP codecs as shown in the table below.

Table 6: SRTP Codec Bandwith Requirements

Codec	Packetization Period (milliseconds)	RTP Bandwidth (kbps)	SRTP Bandwidth (kbps)
G.711 mu-law, G.711 A-law	10-20	96-80	99.2-81.6
G.729, G.729A	10-220	40-9.454	43.2-9.6

Only Clear Channel, G.711, and G.729 codecs support voice security features.

Voice security features support channel density on the TI-5510 DSP as shown in the table below.

Table 7: TI -5510 DSP Channel Density

Codec	Number of Nonsecure Calls	Number of Secure Calls
Clear Channel, G.711	16	10
G.729	6	6
G.729A	8	8

Use the **codec complexity** command in voice-card configuration mode to specify secure codec complexity and call density per DSP.

Information About Media and Signaling Authentication and Encryption

Benefits of Media and Signaling Authentication and Encryption

- Provides privacy and confidentiality for voice calls
- Protects against voice security violations

Feature Design

The Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways feature implements voice security features that include signaling authentication along with media and signaling encryption on MGCP gateways.

The feature provides secure VoIP calls by addressing security requirements for privacy, integrity, and confidentiality of voice conversations. The Cisco IP telephony network establishes and maintains authenticated communications using authentication and encryption technology. Signaling authentication validates that no tampering has occurred to signaling packets during transmission.

Encryption, the process of converting clear-text data into enciphered data, provides data integrity and authentication. IPsec, a standards-based set of security protocols and algorithms, ensures that signaling information (that is, Dual Tone Multi-Frequency (DTMF) digits, passwords, personal identification numbers

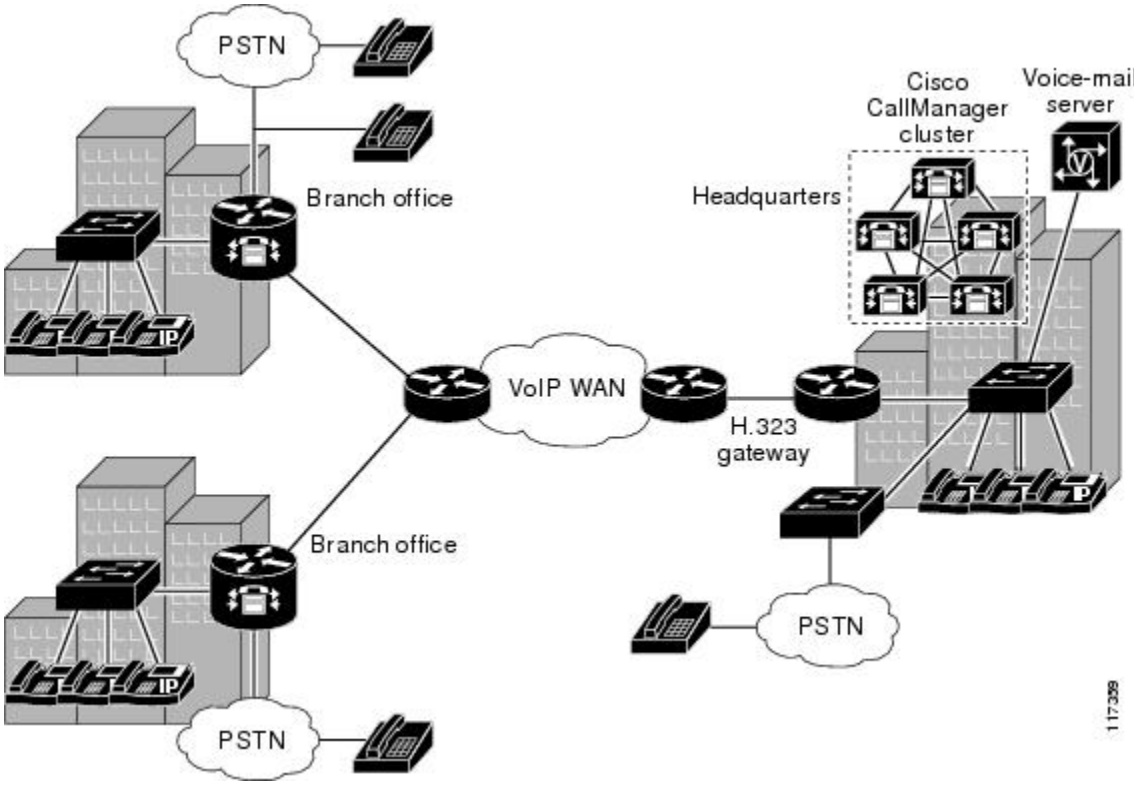
(PINs), and encryption keys) that is sent between the gateway and Cisco CallManager is encrypted. Media encryption using standards-based SRTP ensures that media streams between supported devices are secure.

Voice security features support the following capabilities between gateways and from gateways to IP phones that support the encryption feature:

- Gateway to Cisco CallManager call control authentication and encryption using IPsec
- Media encryption and authentication of voice RTP streams using SRTP
- Exchange of RTP Control Protocol (RTCP) information using SRTCP
- SRTP to RTP fallback for calls between secure and nonsecure endpoints
- Secure to clear-text fallback for new calls during SRST operation

The figure below shows a typical topology where voice security features are deployed.

Figure 12: Voice Security Features in the Telephony Network



MGCP Gateway Behavior and Voice Security Features

To implement voice security features in Cisco CallManager networks, the MGCP gateway communicates with Cisco CallManager over a secure IPsec connection that provides encryption of IP packets. To ensure that your signaling information is secure, estacblish an IPsec connection between the CallManager and the gateways, as described in the Prerequisites for Media and Signaling Authentication and Encryption, on page 129 section. You can verify that the IPsec tunnel is secure using the commands listed in the Verifying Voice Security Features, on page 141 section.

Note Although you may enable media authentication and encryption without signaling encryption, this practice is discouraged. If the gateway to Cisco CallManager connection is not secure, media keys will be sent in clear-text and your voice call will not be considered secure.

After the IPsec tunnel is established, all call control and signaling of MGCP packets between the gateway and Cisco CallManager go through the secured IPsec tunnel, with the Cisco CallManager directing the MGCP gateway to set up and tear down SRTP streams. SRTP media keys are distributed by Cisco CallManager through the secured IPsec tunnel.

Cisco implements voice security features on MGCP gateways by supporting the SRTP package and SRTP Session Description Protocol (SDP) extensions, as defined in the Internet Engineering Task Force (IETF) specifications draft-ietf-mmusic-sdescriptions-02.txt (*Security Descriptions for Media Streams* and RFC 4568, *Session Description Protocol (SDP) Security Descriptions for Media Streams*).

SRTP package capability is disabled by default. Use the Cisco IOS command-line interface (CLI) to enable the feature. For more information, see theConfiguring Voice Security Features, on page 139 section.

Cisco uses the Internet Key Exchange (IKE) standard to implement IPsec. IKE provides authentication of the IPsec peers and negotiates IPsec keys and IPsec security associations (SAs). An IPsec SA describes how two or more entities will use security services to communicate securely. For example, an IPsec SA defines the encryption algorithm, the authentication algorithm, and the shared session key to be used during the IPsec connection. Both IPsec and IKE require and use SAs to identify the parameters of their connections. IKE can negotiate and establish its own SA. The IPsec SA is established either by IKE or by manual user configuration. IKE has two phases of key negotiation: phase 1 and phase 2. Phase 1 negotiates a security association (a key) between two IKE peers. The key negotiated in phase 1 enables IKE peers to communicate securely in phase 2. During phase 2 negotiation, IKE establishes keys (security associations) for other applications, such as IPsec.

The Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways feature also implements an extended codec selection algorithm that combines selection of a codec with selection of a cryptographic suite to be used to encrypt the RTP stream. Cisco IOS Release 12.3(11)T supports the AES_CM_128_HMAC_SHA1_32 cryptographic suite, which includes the AES-128-countermode encryption algorithm and the Hashed Message Authentication Codes (HMAC) Secure Hash Algorithm1 (SHA1) authentication algorithm.

Note MGCP for SRTP on Cisco IOS gateways can be configured to use either MGCP 1.0 signaling support with the Cisco public switched telephone network (PSTN) Gateway (PGW) 2200 carrier-class call agent, or MGCP 0.1 signaling support with Cisco Unified Communications Manager.

Voice Security Features Interoperability with Endpoints

Cisco IOS MGCP gateways support voice security features on T1, E1, FXS, and FXO endpoints supported by network modules listed in *Voice Security Features Interoperability with Endpoints*, thereby enabling secure calls from analog phone to analog phone, or fax machine to fax machine. Similarly, secure calls are enabled from time- division multiplexing (TDM) endpoints or analog phones to Cisco IP phones. For a Cisco IP Phone to make and receive secure calls, all endpoints, that is, phones of all call participants, must support voice security features. If a call is nonsecure, no special icon displays on the phone. If a call is secure, the phone displays either the authenticated or encrypted call icons. For more information on secure call icons, refer to

Cisco IP Phone 7970 Administration Guide for Cisco CallManager, Release 4.x or later, "Identifying Encrypted and Authenticated Phone Calls" section.

How to Configure Media and Signaling Authentication and Encryption Feature

Installing Cisco CallManager

This task installs Cisco CallManager and configures it to work with IPsec and the Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways feature.

SUMMARY STEPS

1. Install Cisco CallManager on the server.
2. Determine the Windows OS version by going to C:\utils and double-clicking MCSVer.exe program. If you have Windows 2000.2.6sr3, no additional Windows upgrade is required. If you have Windows 2000.2.5 or a prior version, you must upgrade to Windows 2000.2.6. If you have Windows 2000.2.6, you must upgrade to Windows 2000.2.6sr3.
3. Upgrade from Windows 2000.2.5 or a prior version.
4. Upgrade from Windows 2000.2.6 to Windows 2000.2.6.sr3.
5. Upgrade Cisco CallManager to version 4.1.
6. Use the **ping** command on both the gateway and Cisco CallManager to test the connection between the gateway and Cisco CallManager. See the section, 'Configuring IPsec on Cisco CallManger'.

DETAILED STEPS

Step 1 Install Cisco CallManager on the server.

- Insert Cisco CallManager HW Detection CD version 2000.2.6, Disk1.
- When prompted, insert Cisco CallManager Base OS CD , Disk3 or 4.

Step 2 Determine the Windows OS version by going to C:\utils and double-clicking MCSVer.exe program. If you have Windows 2000.2.6sr3, no additional Windows upgrade is required. If you have Windows 2000.2.5 or a prior version, you must upgrade to Windows 2000.2.6. If you have Windows 2000.2.6, you must upgrade to Windows 2000.2.6sr3.

Step 3 Upgrade from Windows 2000.2.5 or a prior version.

- Go to 'http://www.cisco.com/cgi-bin/tablebuild.pl/cmva-3des', to download the following files:
  - win-OS-Upgrade-K9.2000-2-6.exe.
  - win-OS-Upgrade-K9.2000-2-6-Readme.htm

Follow the steps listed in the ReadMe file.

Step 4 Upgrade from Windows 2000.2.6 to Windows 2000.2.6.sr3.

- Go to 'http://www.cisco.com/cgi-bin/tablebuild.pl/cmva-3des', to download the following files:

- win-OS-Upgrade-K9.2000-2-6sr3.exe
- win-OS-Upgrade-K9.2000-2-6sr3-Readme.htm.

Follow the steps listed in the ReadMe file.

Step 5 Upgrade Cisco CallManager to version 4.1.

- Go to 'http://www.cisco.com/cgi-bin/tablebuild.pl/cmva-3des'.
- Copy CiscoCallManagerUpgrade.exe to the local system.
- Run the upgrade.

Step 6 Use the **ping** command on both the gateway and Cisco CallManager to test the connection between the gateway and Cisco CallManager. See the section, 'Configuring IPsec on Cisco CallManger'.

Configuring IPsec on Cisco CallManager

This task configures the IPsec connection between the MGCP gateway and the Cisco CallManager.

SUMMARY STEPS

1. Create an IPsec policy on the Windows 2000 server.
2. Build a filter from the Cisco CallManager to the gateway.
3. Build a filter from the gateway to the Cisco CallManager.
4. Configure a rule to negotiate tunnel security.
5. Set key exchange security methods.
6. Assign the new IPsec policy to the Windows 2000 gateway.
7. Use the **ping** command on both the gateway and Cisco CallManager to test the connection between the gateway and Cisco CallManager.
8. Run **ipsecmon.exe** on the Cisco CallManager to verify the configuration.
9. Use the **show crypto isakmp sa** command on the gateway to verify the IPsec configuration.

DETAILED STEPS

Step 1 Create an IPsec policy on the Windows 2000 server.

- Use the Microsoft Management Console (MMC) to work on the IP Security Policy Management snap-in. Click **Start**, click **Run**, and then enter **secpol.msc**.
- Right-click **IP Security Policies on Local Machine**, and then click **Create IP Security Policy**.
- Click **Next**, and then type a name for your policy.
- Clear the **Activate the default response rule** check box, and then click **Next**.
- Click **Finish**, while keeping the **Edit**check box chosen.

Step 2 Build a filter from the Cisco CallManager to the gateway.

- In the properties for the new policy created in *Configuring IPsec on Cisco CallManager*, clear the **Use Add Wizard** check box, and then click **Add** to create a new rule.
- On the IP Filter List tab, click **Add**.
- Enter an appropriate name for the filter list, clear the **Use Add Wizard** check box, and then click **Add**.
- In the Source address area, choose the option **My IP Address**from the drop-down arrow. Enter the Cisco CallManager IP address.
- In the Destination address area, click **A specific IP Subnet**from the drop-down arrow. Enter the IP address of the router interface in the same subnet as the Cisco CallManager.
- Clear the **Mirrored**check box.
- On the Protocol tab, make sure the protocol type is set to Any. (IPsec tunnels do not support protocol-specific or port-specific filters.)
- (Optional) If you want to enter a description for your filter, click the **Description**tab. It is recommended that you give the filter the same name you used for the filter list. The filter name is displayed in the IPsec monitor when the tunnel is active.
- Click **OK**, and then click **Close**.

Step 3 Build a filter from the gateway to the Cisco CallManager.

- On the IP Filter List tab, click **Add**.
- Type an appropriate name for the filter list, clear the **Use Add Wizard** check box, and then click **Add**.
- In the Source address area, click **A specific IP Subnet**from the dropdown arrow. Enter the IP address of the router interface in the same subnet as the Cisco CallManager.
- In the Destination address area, choose the option **My IP Address**from the dropdown arrow.
- Clear the **Mirrored**check box.
- (Optional) If you want to enter a description for your filter, click the **Description** tab.
- Click **OK**, and then click **Close**.

Step 4 Configure a rule to negotiate tunnel security.

- On the IP Filter List tab, click the filter list you created in *Configuring IPsec on Cisco CallManager*.
- On the Tunnel Setting tab, choose the option **Tunnel Setting - encryption peers**. For Cisco-Microsoft and for Microsoft-Cisco, configure the setting according to: http://www.cisco.com/en/US/tech/tk583/tk372/technologies_configuration_example09186a00800b12b5.shtml
- On the Connection Type tab, click **All network connections**.
- On the Filter Action tab, clear the **Use Add Wizard** check box, and then click **Add** to create a new filter action.

Note You must create a new filter; otherwise the default filter action allows incoming traffic in the clear.

- Keep the Negotiate security option enabled, and click the **Accept unsecured communication**, but clear the **always respond using IPsec** check box.

Note You must perform this step to ensure secure operation.

- Choose the **Custom** option to add a security method. Click the **Data integrity and encryption** box for Encapsulating Security Payload (ESP). Click **MD5** for the Integrity algorithm. Click **DES**for the Encryption algorithm. Check the **Generate a new Key every 3600 seconds** box.
- Click **OK**. On the General tab, enter a name for the new filter action and then click **OK**.
- Choose the filter action you created in *Configuring IPsec on Cisco CallManager*.
- On the Authentication Methods tab, perform the steps to configure a preshared key.

Note The preshared key must match the key configured on the router.

- Click **Close**.

Step 5 Set key exchange security methods.

- Right-click the IP Security Policy created in *Configuring IPsec on Cisco CallManager* and choose **Properties**.
- Click the **General** tab.
- Click the **Advanced**button.
- Click the **Methods** button.
- Ensure that the security Method with the following settings is at the top of the preference order: Type--IKE, Encryption--DES, Integrity--SHA1, Diffie-Hellman--Low(1)
- Save the configuration.

Step 6 Assign the new IPsec policy to the Windows 2000 gateway.

- In the IP Security Policies on Local Machine MMC snap-in, right-click the new policy, and then click **Assign**. A green arrow appears in the folder icon next to the new policy.

Step 7 Use the **ping** command on both the gateway and Cisco CallManager to test the connection between the gateway and Cisco CallManager.

Step 8 Run **ipsecmon.exe** on the Cisco CallManager to verify the configuration.

Step 9 Use the **show crypto isakmp sa** command on the gateway to verify the IPsec configuration.

Configuring the Cisco PGW

MGCP for SRTP on Cisco IOS gateways can be configured for use with the Cisco PSTN gateway (PGW) 2200 carrier-class call agent.

To configure this feature, you must first tell the Cisco PGW 2200 Softswitch that the media gateways support SRTP. Then you specify that SIP and TDM trunk groups support SRTP.

For a detailed description of the configuration tasks, see the "Secure Real-time Transport Protocol Support" feature guide.

Configuring Voice Security Features

This task configures voice security features on the Cisco IOS MGCP gateway.

Before you begin

We strongly recommend that you first establish an IPsec connection between the Cisco CallManager and the MGCP gateway before you use the MGCP SRTP package. Otherwise, media keys will be sent in clear text and your voice call will not be considered secure. For more information, see the "Installing Cisco CallManager, on page 135" and "Configuring IPsec on Cisco CallManager, on page 136" sections.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mgcp package-capability srtp-package**
4. **mgcp validate call-agent source-ipaddr**
5. **mgcp crypto rfc-preferred**
6. **voice-card** *slot*
7. **codec complexity secure**
8. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**mgcp package-capability srtp-package** **Example:** `Router(config)# mgcp package-capability srtp-package`	Enables the MGCP gateway capability to process SRTP packages.
Step 4	**mgcp validate call-agent source-ipaddr** **Example:** `Router(config)# mgcp validate call-agent source-ipaddr`	(Optional) Enables MGCP application validation that packets received are sent by a configured call agent.
Step 5	**mgcp crypto rfc-preferred** **Example:**	(Optional) Enables support for the media-level SDP a=crypto attribute on the Cisco IOS MGCP gateway.

	Command or Action	Purpose
	`Router(config)# mgcp crypto rfc-preferred`	
Step 6	**voice-card** *slot* **Example:** `Router(config)# voice-card 1`	Enters voice-card configuration mode and configures the voice card in the specified network module slot.
Step 7	**codec complexity secure** **Example:** `Router(config-voice-card)# codec complexity secure`	Restricts the number of channels per NM-HDV network module from four to two, enabling SRTP support on the TI-549 DSP. **Note** You need not specify secure codec complexity for TI-5510 DSPs, which support SRTP capability in all complexity modes.
Step 8	**exit** **Example:** `Router(config-voice-card)# exit`	Exits the current configuration mode.

Configuring Secure IP Telephony Calls

This task enables secure IP telephony calls from gateway to IP phone.

Voice security features use digital certificates contained in eTokens for device authentication. This process validates the identity of a device and ensures that the entity is who it claims to be. Device authentication occurs between the Cisco CallManager server and supported IP phones when each entity accepts the certificate of the other entity. Cisco implements device authentication using the CTL feature on the Cisco CallManager. The CTL Client creates a certificate on each server in the cluster and generates a CTL file in the TFTP Path of the server for the phones to download. This file provides the IP phone with a list of certified hosts that it can trust. For more information, refer to *Cisco IP Phone Authentication and Encryption for Cisco CallManager 4.0(1)*, "Signaling Authentication" chapter .

Before you begin

- CTL Provider service must be running on the Cisco CallManager server.
- Smart Card service must be running on the Cisco CallManager server.
- Two USB eTokens are required.

SUMMARY STEPS

1. Install CiscoCTLClient.exe from c:\CiscoPlugins\Client\.
2. Launch Cisco CTL Client from the desktop shortcut.
3. Enter the Cisco CallManager IP address and password, then click **Next**.
4. Choose **Set CallManager Cluster to Secure Mode**, then click **Next**.
5. Click **Add** for Security Token Information.

6. Click **Add Tokens**for CTL Entries.
7. When prompted, insert the first USB eToken, then click **OK**.
8. Repeat and *Configuring Secure IP Telephoney Calls* for the second eToken.
9. Click **Finish** for CTL Entries, then enter your eToken Password when prompted and click **OK**.
10. Verify that voice security features are enabled.

DETAILED STEPS

Step 1 Install CiscoCTLClient.exe from c:\CiscoPlugins\Client\.

Step 2 Launch Cisco CTL Client from the desktop shortcut.

Step 3 Enter the Cisco CallManager IP address and password, then click **Next**.

Step 4 Choose **Set CallManager Cluster to Secure Mode**, then click **Next**.

Step 5 Click **Add** for Security Token Information.

Step 6 Click **Add Tokens**for CTL Entries.

Step 7 When prompted, insert the first USB eToken, then click **OK**.

Step 8 Repeat and *Configuring Secure IP Telephoney Calls* for the second eToken.

Step 9 Click **Finish** for CTL Entries, then enter your eToken Password when prompted and click **OK**.

Step 10 Verify that voice security features are enabled.

- Open Cisco CallManager Administration, choose **Access System**, then **Enterprise Parameters**. Scroll down to Security Parameters, and verify that Cluster Security is set to 1.
- Set the Cisco CallManager Enterprise Parameter to **Encrypted**to force all devices in the cluster to run encrypted mode. You can also set each IP phone individually to encrypted mode by choosing **Device**, then **Phone**, then **Find**, then **Security Mode = Encrypted**. Reboot the IP phones and verify that the Security Mode displays Encrypted under Security Settings.

Verifying Voice Security Features

This task verifies voice security feature configuration and MGCP gateway to Cisco CallManager IPsec connections.

SUMMARY STEPS

1. **show mgcp**
2. **show mgcp connection**
3. **show mgcp srtp** {**summary**| **detail** [*endpoint*]}
4. **show mgcp statistics**
5. **show call active voice**
6. **show voice call** *port*
7. **show voice call status**
8. **show voice call status** *call-id*
9. **show voice dsp**
10. **show rtpspi call**

11. **show rtpspi statistics**
12. **show ccm-manager**
13. **show crypto engine accelerator statistic**
14. **show crypto ipsec sa**
15. **show crypto isakmp sa**
16. **show crypto session**
17. **show crypto session detail**

DETAILED STEPS

Step 1 show mgcp

Use this command to display the state of the **mgcp package-capability srtp-package** and **mgcp validate call-agent source-ipaddr** commands.

Example:

```
Router# show mgcp
MGCP Admin State ACTIVE, Oper State ACTIVE - Cause Code NONE
MGCP call-agent: 10.7.0.200 Initial protocol service is MGCP 0.1
```

The following line shows that call-agent validation is enabled:

Example:

```
MGCP validate call-agent source-ipaddr ENABLED
MGCP block-newcalls DISABLED
MGCP send SGCP RSIP: forced/restart/graceful/disconnected DISABLED
MGCP quarantine mode discard/step
MGCP quarantine of persistent events is ENABLED
MGCP dtmf-relay for VoIP disabled for all codec types
MGCP dtmf-relay for VoAAL2 disabled for all codec types
MGCP voip modem passthrough disabled
MGCP voaal2 modem passthrough disabled
MGCP voip modem relay: Disabled.
MGCP TSE payload: 100
MGCP T.38 Named Signalling Event (NSE) response timer: 200
MGCP Network (IP/AAL2) Continuity Test timer: 200
MGCP 'RTP stream loss' timer disabled
MGCP request timeout 500
MGCP maximum exponential request timeout 4000
MGCP gateway port: 2427, MGCP maximum waiting delay 3000
MGCP restart delay 0, MGCP vad DISABLED
MGCP rtrcac DISABLED
MGCP system resource check DISABLED
MGCP xpc-codec: DISABLED, MGCP persistent hookflash: DISABLED
MGCP persistent offhook: ENABLED, MGCP persistent onhook: ENABLED
MGCP piggyback msg DISABLED, MGCP endpoint offset DISABLED
MGCP simple-sdp ENABLED
MGCP undotted-notation DISABLED
MGCP codec type g711ulaw, MGCP packetization period 20
MGCP JB threshold lwm 30, MGCP JB threshold hwm 150
MGCP LAT threshold lwm 150, MGCP LAT threshold hwm 300
MGCP PL threshold lwm 1000, MGCP PL threshold hwm 10000
MGCP CL threshold lwm 1000, MGCP CL threshold hwm 10000
MGCP playout mode is adaptive 60, 4, 200 in msec
MGCP Fax Playout Buffer is 300 in msec
```

```
MGCP media (RTP) dscp: ef, MGCP signaling dscp: af31
MGCP default package: line-package
```

The following lines show that the **srtp-package**command is enabled:

Example:

```
MGCP supported packages: gm-package dtmf-package mf-package trunk-package
         line-package ms-package dt-package mo-package mt-package
         sst-package fxr-package srtp-package
MGCP Digit Map matching order: shortest match
SGCP Digit Map matching order: always left-to-right
MGCP VoAAL2 ignore-lco-codec DISABLED
MGCP T.38 Fax is ENABLED
MGCP T.38 Fax ECM is ENABLED
MGCP T.38 Fax NSF Override is DISABLED
MGCP T.38 Fax Low Speed Redundancy: 0MGCP T.38 Fax High Speed Redundancy: 0
MGCP control bound to interface FastEthernet0/0
MGCP media bind :DISABLED
MGCP Upspeed payload type for G711ulaw: 0,  G711alaw: 8
MGCP Dynamic payload type for G.726-16K codec
MGCP Dynamic payload type for G.726-24K codec
MGCP Dynamic payload type for G.Clear codec
```

Step 2 **show mgcp connection**

Use this command to display information on active connections, including the encryption suite.

Example:

```
Router# show mgcp connection
Endpoint        Call_ID(C) Conn_ID(I) (P)ort (M)ode (S)tate (CO)dec (E)vent[SIFL] (R)esult[EA]
Encryption(K)
```

The following line shows that encryption status is enabled, K=1.

Example:

```
1. S1/DS1-0/1   C=2,1,2  I=0x2  P=18204,0  M=2  S=4,4 CO=1 E=0,0,0,0  R=0,0 K=1
```

Step 3 **show mgcp srtp** {**summary**| **detail** [*endpoint*]}

Use this command to display SRTP connections and validate master keys and salts for endpoints.

Example:

```
Router# show mgcp srtp summary
MGCP SRTP Connection Summary
Endpoint             Conn Id    Crypto Suite
aaln/S3/SU0/0        8          AES_CM_128_HMAC_SHA1_32
aaln/S3/SU0/1        9          AES_CM_128_HMAC_SHA1_32
S3/DS1-0/1           6          AES_CM_128_HMAC_SHA1_32
S3/DS1-0/2           7          AES_CM_128_HMAC_SHA1_32
4 SRTP connections active
Router# show mgcp srtp detail
MGCP SRTP Connection Detail for Endpoint *
Definitions: CS=Crypto Suite, KS=HASHED Master Key/Salt, SSRC=Syncronization Source, ROC=Rollover
Counter, KDR=Key Derivation Rate, SEQ=Sequence Number, FEC=FEC Order, MLT=Master Key Lifetime,
MKI=Master Key Index:MKI Size
Endpoint aaln/S3/SU0/0 Call ID 2 Conn ID 8
  Tx:CS=AES_CM_128_HMAC_SHA1_32 KS=3NaOYXS9dLoYDaBHpzRejREfhf0= SSRC=Random ROC=0 KDR=1 SEQ=Random
 FEC=FEC->SRTP MLT=0x80000000 MKI=0:0
  Rx:CS=AES_CM_128_HMAC_SHA1_32 KS=llYCQoqxtxtdf7ECe+x+DK+G9v4= SSRC=Random ROC=0 KDR=1 SEQ=Random
```

```
 FEC=FEC->SRTP MLT=0x80000000 MKI=0:0
Endpoint aaln/S3/SU0/1 Call ID 101 Conn ID 9
  Tx:CS=AES_CM_128_HMAC_SHA1_32 KS=llYCQoqxtxtdf7ECe+x+DK+G9v4= SSRC=Random ROC=0 KDR=1 SEQ=Random
 FEC=FEC->SRTP MLT=0x80000000 MKI=0:0
  Rx:Not Configured
Endpoint S3/DS1-0/1 Call ID 1 Conn ID 6
  Tx:CS=AES_CM_128_HMAC_SHA1_32 KS=3NaOYXS9dLoYDaBHpzRejREfhf0= SSRC=Random ROC=0 KDR=1 SEQ=Random
 FEC=FEC->SRTP MLT=0x80000000 MKI=0:0
  Rx:CS=AES_CM_128_HMAC_SHA1_32 KS=llYCQoqxtxtdf7ECe+x+DK+G9v4= SSRC=Random ROC=0 KDR=1 SEQ=Random
 FEC=FEC->SRTP MLT=0x80000000 MKI=0:0
Endpoint S3/DS1-0/2 Call ID 100 Conn ID 7
  Tx:CS=AES_CM_128_HMAC_SHA1_32 KS=llYCQoqxtxtdf7ECe+x+DK+G9v4= SSRC=Random ROC=0 KDR=1 SEQ=Random
 FEC=FEC->SRTP MLT=0x80000000 MKI=0:0
  Rx:Not Configured
4 SRTP connections displayed
Router# show mgcp srtp detail S3/DS1-0/*
MGCP SRTP Connection Detail for Endpoint S3/DS1-0/*
Definitions: CS=Crypto Suite, KS=HASHED Master Key/Salt, SSRC=Syncronization Source, ROC=Rollover
Counter, KDR=Key Derivation Rate, SEQ=Sequence Number, FEC=FEC Order, MLT=Master Key Lifetime,
MKI=Master Key Index:MKI Size
```

The following lines allow you to compare and validate a hashed version of the master key and salt, as indicated by the KS field, without the display revealing the actual master key and salt.

Example:

```
Endpoint S3/DS1-0/1 Call ID 1 Conn ID 6
  Tx:CS=AES_CM_128_HMAC_SHA1_32 KS=3NaOYXS9dLoYDaBHpzRejREfhf0= SSRC=Random ROC=0 KDR=1 SEQ=Random
 FEC=FEC->SRTP MLT=0x80000000 MKI=0:0
  Rx:CS=AES_CM_128_HMAC_SHA1_32 KS=llYCQoqxtxtdf7ECe+x+DK+G9v4= SSRC=Random ROC=0 KDR=1 SEQ=Random
 FEC=FEC->SRTP MLT=0x80000000 MKI=0:0
Endpoint S3/DS1-0/2 Call ID 100 Conn ID 7
  Tx:CS=AES_CM_128_HMAC_SHA1_32 KS=llYCQoqxtxtdf7ECe+x+DK+G9v4= SSRC=Random ROC=0 KDR=1 SEQ=Random
 FEC=FEC->SRTP MLT=0x80000000 MKI=0:0
  Rx:Not Configured
2 SRTP connections displayed
```

Step 4 **show mgcp statistics**

Use this command to display statistics, including dropped packets from unconfigured call agents.

Example:

```
Router# show mgcp statistics
 UDP pkts rx 0, tx 0
 Unrecognized rx pkts 0, MGCP message parsing errors 0
 Duplicate MGCP ack tx 0, Invalid versions count 0
```

The following line shows the number of dropped packets from unconfigured call agents.

Example:

```
 rx pkts from unknown Call Agent 0
 CreateConn rx 0, successful 0, failed 0
 DeleteConn rx 0, successful 0, failed 0
 ModifyConn rx 0, successful 0, failed 0
 DeleteConn tx 0, successful 0, failed 0
 NotifyRequest rx 0, successful 0, failed 0
 AuditConnection rx 0, successful 0, failed 0
 AuditEndpoint rx 0, successful 0, failed 0
 RestartInProgress tx 0, successful 0, failed 0
 Notify tx 0, successful 0, failed 0
 ACK tx 0, NACK tx 0
```

```
ACK rx 0, NACK rx 0
IP address based Call Agents statistics:
No Call Agent message.
System resource check is DISABLED. No available statistic
```

Step 5 **show call active voice**

Use this command to display encryption statistics.

Example:

```
Router# show call active voice
GENERIC: SetupTime=21072 Index=0 PeerAddress= PeerSubAddress= PeerId=0
PeerIfIndex=0 LogicalIfIndex=0 ConnectTime=0 CallState=3 CallSecurity = On CallOrigin=2 ChargedUnits=0

InfoType=0 TransmitPackets=375413 TransmitBytes=7508260 ReceivePackets=377734
ReceiveBytes=7554680
VOIP: ConnectionId[0x19BDF910 0xAF500007 0x0 0x58ED0] RemoteIPAddress=17635075
RemoteUDPPort=16394 RoundTripDelay=0 SelectedQoS=0 SessionProtocol=1
SessionTarget= OnTimeRvPlayout=0 GapFillWithSilence=0 GapFillWithPrediction=600
GapFillWithInterpolation=0 GapFillWithRedundancy=0 HiWaterPlayoutDelay=110
LoWaterPlayoutDelay=64 ReceiveDelay=94 VADEnable=0 CoderTypeRate=0
GENERIC: SetupTime=21072 Index=1 PeerAddress=+14085271001 PeerSubAddress=
PeerId=0 PeerIfIndex=0 LogicalIfIndex=5 ConnectTime=21115 CallState=4 CallOrigin=1
ChargedUnits=0 InfoType=1 TransmitPackets=377915 TransmitBytes=7558300
ReceivePackets=375594 ReceiveBytes=7511880 TotalPacketsEncrypted=375594
```

The following lines show statistics for encrypted and decrypted packets.

Example:

```
TotalPacketsDecrypted=375594 DecryptionFailurePacketCount=0 TotalPacketsAuthenticated=375594
AuthenticationFailurePacketCount=0 DuplicateReplayPacketCount=0 OutsideWindowReplayPacketCount=0
TELE: ConnectionId=[0x19BDF910 0xAF500007 0x0 0x58ED0] TxDuration=16640
VoiceTxDuration=16640 FaxTxDuration=0 CoderTypeRate=0 NoiseLevel=0 ACOMLevel=4
OutSignalLevel=-440 InSignalLevel=-440 InfoActivity=2 ERLLevel=227
SessionTarget=
```

Step 6 **show voice call** *port*

Use this command to display SRTP statistics.

Example:

```
Router# show voice call 1/0/0
1/0/0
      vtsp level 0 state = S_CONNECTvpm level 1 state = FXSLS_CONNECT
vpm level 0 state = S_UP
calling number , calling name unavailable, calling time 01/08 03:44
c3745_13#       ***DSP VOICE TX STATISTICS***
Tx Vox/Fax Pkts: 108616, Tx Sig Pkts: 0, Tx Comfort Pkts: 0
Tx Dur(ms): 2172320, Tx Vox Dur(ms): 2172320, Tx Fax Dur(ms): 0
        ***DSP VOICE RX STATISTICS***
Rx Vox/Fax Pkts: 108602, Rx Signal Pkts: 0, Rx Comfort Pkts: 0
Rx Dur(ms): 2172320, Rx Vox Dur(ms): 2171990, Rx Fax Dur(ms): 0
Rx Non-seq Pkts: 3, Rx Bad Hdr Pkts: 0
Rx Early Pkts: 0, Rx Late Pkts: 0
        ***DSP VOICE VP_DELAY STATISTICS***
Clk Offset(ms): -2819596, Rx Delay Est(ms): 65
Rx Delay Lo Water Mark(ms): 65, Rx Delay Hi Water Mark(ms): 65
        ***DSP VOICE VP_ERROR STATISTICS***
Predict Conceal(ms): 250, Interpolate Conceal(ms): 0
Silence Conceal(ms): 0, Retroact Mem Update(ms): 0
```

```
Buf Overflow Discard(ms): 0, Talkspurt Endpoint Detect Err: 0
        ***DSP LEVELS***
TDM Bus Levels(dBm0): Rx -37.7 from PBX/Phone, Tx -35.5 to PBX/Phone
TDM ACOM Levels(dBm0): +5.0, TDM ERL Level(dBm0): +5.0
TDM Bgd Levels(dBm0): -35.9, with activity being silence
        ***DSP VOICE ERROR STATISTICS***
Rx Pkt Drops(Invalid Header): 0, Tx Pkt Drops(HPI SAM Overflow): 0
        ***DSP VOICE SRTP STATISTICS***
```

The following lines show voice SRTP statistics.

Example:

```
*Jan  8 2004 04:21:01.743 PAT: TotalPacketsEncrypted: 108616  TotalPacketsDecrypted: 108602
DecryptionFailurePacketCount: 0  TotalPacketsAuthenticated: 108602
AuthenticationFailurePacketCount: 0 DuplicateReplayPacketCount: 0
OutsideWindowReplayPacketCount: 0  packetsBadReceivedSSRC: 0
```

Note When a T.38 fax call (nonsecure) is attempted and the fax call goes through, then switches back to secure voice (SRTP) mode, output for the **show voice call** *port* command displays an authentication failure packet count of 20. This is a normal occurrence and should not affect voice quality. The authentication failure packet count occurs because the gateways do not switch back to secure voice at the same time; that is, one side of the call is in SRTP voice mode for a short period of time while the other side is in T.38 fax mode.

Example:

Step 7 **show voice call status**

Use this command to display status of all voice ports.

Example:

```
Router# show voice call status
CallID     CID  ccVdb      Port      DSP/Ch  Called #   Codec    Dial-peers
0x5        11DE 0x660B24D0 1/0/0     1/1                g711ulaw 999100/0
0x7        11E1 0x665031A8 1/0:23.-1 1/2    *           g729ar8  0/999
0x11       11E4 0x6652B3B4 1/1:1.1   1/3     232222     g729ar8  999/0
3 active calls found
```

Step 8 **show voice call status** *call-id*

Use this command to display status of a specific call.

Example:

```
Router# show voice call status 5
Gathering information (10 seconds)...
CallID     Port      DSP/Ch  Codec    Rx/Tx     En/De     ERL/Reflctr Jitter
0x5        1/0/0     1/1     g711ulaw 500/500   500/500   5.0/3       65/0
Router# show voice call status 7
Gathering information (10 seconds)...
CallID     Port      DSP/Ch  Codec    Rx/Tx     En/De     ERL/Reflctr Jitter
0x7        1/0:23.-1 1/2     g729ar8  500/500   500/500   6.0/4       70/0
Router# show voice call status 11
Gathering information (10 seconds)...
CallID     Port      DSP/Ch  Codec    Rx/Tx     En/De     ERL/Reflctr Jitter
0x11       1/1:1.1   1/3     g729ar8  500/500   500/500   7.0/4       70/0
```

Step 9 **show voice dsp**

Use this command to display the status of DSP voice channels.

Example:

```
Router# show voice dsp
DSP   DSP         DSPWARE  CURR   BOOT                    PAK TX/RX
TYPE NUM CH CODEC     VERSION  STATE STATE   RST AI VOICEPORT TS ABORT PACK COUNT
==== === == ======== ======= ===== ======= === == ======== === ==== ===========
C549 1   01 {medium} 4.4.3   IDLE   idle       0   0   1/0:0       1       0     9357/9775
C549 1   02 {medium} 4.4.3   IDLE   idle             0   1/0:0       2     0     0/0
C549 2   01 {medium} 4.4.3   IDLE   idle         0   0   1/0:0       3       0     0/0
C549 2   02 {medium} 4.4.3   IDLE   idle             0    1/0:0       4   0     0/0
C549 3   01 {medium} 4.4.3   IDLE   idle       0   0   1/0:0       5       0         0/13
C549 3   02 {medium} 4.4.3   IDLE   idle             0   1/0:0       6       0     0/13
```

Step 10 **show rtpspi call**

Use this command to display active SRTP call details.

Example:

```
Router# show rtpspi call
RTP Service Provider info:
No. CallId dstCallId Mode      LocalRTP RmtRTP LocalIP    RemoteIP   SRTP
1   6      5         Snd-Rcv   18662    19392  0xA0A0A0D  0xA0A0A0B    1
2   8      7         Snd-Rcv   18940    16994  0xA0A0A0D  0xA0A0A0B    1
3   16     17        Snd-Rcv   19038    17198  0xA0A0A0D  0xA0A0A0B    1
```

Step 11 **show rtpspi statistics**

Use this command to display RTP statistics.

Example:

```
Router# show rtpspi statistics
RTP Statistics info:
No. CallId     Xmit-pkts Xmit-bytes Rcvd-pkts  Rcvd-bytes Lost pkts  Jitter Late
nc
1   6          0x842C    0x54AC30   0x842A     0x54AAE8   0x0        0x41     0x2
2   8          0x52B8    0x7C140    0x52B5     0x7C0F8    0x0        0x46     0x2
3   16         0x2EB0    0x46080    0x2EAF     0x46068    0x0        0x46     0x2
```

Step 12 **show ccm-manager**

Use this command to display the status and availability of Cisco CallManager.

Example:

```
Router# show ccm-manager
MGCP Domain Name: router
Priority        Status                  Host
============================================================
Primary         Registered              10.10.10.130
First Backup    Duplicate of Primary    10.10.10.130
Second Backup   None
Current active Call Manager:    10.10.10.130
Backhaul/Redundant link port:   2428
Failover Interval:              30 seconds
Keepalive Interval:             15 seconds
Last keepalive sent:            04:06:40 PAT Jan 8 2004 (elapsed time: 00:00:04)
Last MGCP traffic time:         04:06:40 PAT Jan 8 2004 (elapsed time: 00:00:04)
Last failover time:             None
```

```
Last switchback time:           None
Switchback mode:                Graceful
MGCP Fallback mode:             Enabled/OFF
Last MGCP Fallback start time:  03:42:25 PAT Jan 8 2004
Last MGCP Fallback end time:    03:42:44 PAT Jan 8 2004
MGCP Download Tones:            Disabled
Backhaul Link info:
    Link Protocol:      TCP
    Remote Port Number: 2428
    Remote IP Address:  10.10.10.130
    Current Link State: OPEN
    Statistics:
        Packets recvd:   7
        Recv failures:   0
        Packets xmitted: 13
        Xmit failures:   0
    PRI Ports being backhauled:
        Slot 1, port 0
Configuration Error History:
FAX mode: cisco
```

Step 13 show crypto engine accelerator statistic

Use this command to display statistics and error counters for the onboard hardware accelerator of the router for IPsec encryption.

Example:

```
Router# show crypto engine accelerator statistic
Virtual Private Network (VPN) Module in slot : 0
        Statistics for Hardware VPN Module since the last clear
         of counters 1814 seconds ago
                    638 packets in                        638 packets out
                  88640 bytes in                        87601 bytes out
                      0 paks/sec in                         0 paks/sec out
                      0 Kbits/sec in                        0 Kbits/sec out
                    315 packets decrypted                 323 packets encrypted
                  37680 bytes before decrypt            49921 bytes encrypted
                  21104 bytes decrypted                 67536 bytes after encrypt
                      0 packets decompressed                0 packets compressed
                      0 bytes before decomp                 0 bytes before comp
                      0 bytes after decomp                  0 bytes after comp
                      0 packets bypass decompr              0 packets bypass compres
                      0 bytes bypass decompres              0 bytes bypass compressi
                      0 packets not decompress              0 packets not compressed
                      0 bytes not decompressed              0 bytes not compressed
                  1.0:1 compression ratio               1.0:1 overall
                     33 commands out                       33 commands acknowledged
                Last 5 minutes:
                     60 packets in                         60 packets out
                      0 paks/sec in                         0 paks/sec out
                    121 bits/sec in                       120 bits/sec out
                   1720 bytes decrypted                  1140 bytes encrypted
                     46 Kbits/sec decrypted                30 Kbits/sec encrypted
                  1.0:1 compression ratio               1.0:1 overall
        Errors:
           ppq full errors         :        0   ppq rx errors           : 0
           cmdq full errors        :        0   cmdq rx errors          : 0
           no buffer               :        0   replay errors           : 0
           dest overflow           :        0   authentication errors   : 0
           Other error             :        0   RNG self test fail      : 0
           DF Bit set              :        0   Hash Miscompare         : 0
           Unwrappable object      :        0   Missing attribute       : 0
           Invalid attrribute value:        0   Bad Attribute           : 0
```

```
           Verification Fail       :        0   Decrypt Failure         : 0
           Invalid Packet          :        0   Invalid Key             : 0
           Input Overrun           :        0   Input Underrun          : 0
           Output buffer overrun   :        0   Bad handle value        : 0
           Invalid parameter       :        0   Bad function code       : 0
           Out of handles          :        0   Access denied           : 0
Warnings:
           sessions_expired        :        0   packets_fragmented      : 0
           general:                :        0
        HSP details:
           hsp_operations          :        0   hsp_sessions            : 0
```

Step 14 **show crypto ipsec sa**

Use this command to display the settings used by current SAs.

Example:

```
Router# show crypto ipsec sa

interface: FastEthernet0/0
    Crypto map tag: Gateway, local addr. 10.10.10.13
   protected vrf:
   local  ident (addr/mask/port/port): (10.10.10.13/255.255.255.255/0/0)
   remote ident (addr/mask/port/port): (10.10.10.130/255.255.255.255/0/0)
   current_peer: 10.10.10.130:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 324, #pkts encrypt: 324, #pkts digest: 324
    #pkts decaps: 316, #pkts decrypt: 316, #pkts verify: 316
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 71, #recv errors 0
     local crypto endpt.: 10.10.10.13, remote crypto endpt.: 10.10.10.130
     path mtu 1500, media mtu 1500
     current outbound spi: 9073D35
     inbound esp sas:
      spi: 0x9FCB508(167556360)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5121, flow_id: 1, crypto map: gateway
        crypto engine type: Hardware, engine_id: 2
        sa timing: remaining key lifetime (k/sec): (4446388/1913)
        ike_cookies: 6A391EE1 E57F3670 D4D78758 2F5C8E7C
        IV size: 8 bytes
        replay detection support: Y
      spi: 0xD132AE54(3509759572)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5123, flow_id: 3, crypto map: gateway
        crypto engine type: Hardware, engine_id: 2
        sa timing: remaining key lifetime (k/sec): (4402107/1913)
        ike_cookies: 6A391EE1 E57F3670 D4D78758 2F5C8E7C
        IV size: 8 bytes
        replay detection support: Y
     inbound ah sas:
     inbound pcp sas:
     outbound esp sas:
      spi: 0x7D078A45(2097646149)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5122, flow_id: 2, crypto map: gateway
        crypto engine type: Hardware, engine_id: 2
        sa timing: remaining key lifetime (k/sec): (4446388/1911)
```

```
      ike_cookies: 6A391EE1 E57F3670 D4D78758 2F5C8E7C
      IV size: 8 bytes
      replay detection support: Y
    spi: 0x9073D35(151469365)
      transform: esp-3des esp-sha-hmac ,
      in use settings ={Tunnel, }
      slot: 0, conn id: 5124, flow_id: 4, crypto map: gateway
      crypto engine type: Hardware, engine_id: 2
      sa timing: remaining key lifetime (k/sec): (4402077/1911)
      ike_cookies: 6A391EE1 E57F3670 D4D78758 2F5C8E7C
      IV size: 8 bytes
      replay detection support: Y
  outbound ah sas:
  outbound pcp sas:
protected vrf:
local  ident (addr/mask/prot/port): (10.10.10.13/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (10.10.10.131/255.255.255.255/0/0)
current_peer: 10.10.10.131:500
  PERMIT, flags={origin_is_acl,}
 #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
 #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
 #pkts compressed: 0, #pkts decompressed: 0
 #pkts not compressed: 0, #pkts compr. failed: 0
 #pkts not decompressed: 0, #pkts decompress failed: 0
 #send errors 0, #recv errors 0
  local crypto endpt.: 10.10.10.13, remote crypto endpt.: 10.10.10.131
  path mtu 1500, media mtu 1500
  current outbound spi: 0
  inbound esp sas:
  inbound ah sas:
  inbound pcp sas:
  outbound esp sas:
  outbound ah sas:
  outbound pcp sas:
```

Step 15 **show crypto isakmp sa**

Use this command to display current IKE SAs at a peer.

Example:

```
Router# show crypto isakmp sa
dst             src             state          conn-id slot
10.10.10.130    10.10.10.13     QM_IDLE              1    0
```

Step 16 **show crypto session**

Use this command to display the status of the current crypto session.

Example:

```
Router# show crypto session
Crypto session current status
Interface: FastEthernet0/0
Session status: UP-ACTIVE
Peer: 10.10.10.130/500
  IKE SA: local 10.10.10.13/500 remote 10.10.10.130/500 Active
  IPSEC FLOW: permit ip host 10.10.10.13 host 10.10.10.130
        Active SAs: 4, origin: crypto map
```

Step 17 **show crypto session detail**

Use this command to display IPsec details and statistics of the current crypto session.

Example:

```
Router# show crypto session detail
Crypto session current status
Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, X - IKE Extended Authentication
Interface: FastEthernet0/0
Session status: UP-ACTIVE
Peer: 10.10.10.130/500 fvrf: (none) ivrf: (none)
      Phase1_id: 10.10.10.130
      Desc: (none)
  IKE SA: local 10.10.10.13/500 remote 10.10.10.130/500 Active
         Capabilities:(none) connid:1 lifetime:07:30:00
  IPSEC FLOW: permit ip host 10.10.10.13 host 10.10.10.130
        Active SAs: 4, origin: crypto map
        Inbound:  #pkts dec'ed 335 drop 0 life (KB/Sec) 4402106/1800
        Outbound: #pkts enc'ed 327 drop 71 life (KB/Sec) 4402076/180
```

Configuration Examples for Media and Signaling Authentication and Encryption

Voice Security Features Example

The following example shows voice security features enabled:

```
Router# show running-config
Building configuration...
Current configuration : 2304 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname router
!
boot-start-marker
boot-end-marker
!
voice-card 1
 no dspfarm
!
voice-card 2
 no dspfarm
!
```

The following lines show secure codec complexity enabled:

```
voice-card 4
 codec complexity secure
 dspfarm
!
!
no aaa new-model
```

```
ip subnet-zero
!
ip cef
no ip domain lookup
!
ip domain name cisco.com
```

The IP domain name should match the domain name configured on Cisco CallManager.

```
!
Cisco CallManager-manager mgcp
!
crypto isakmp policy 1
 authentication pre-share
 lifetime 28800
crypto isakmp key cisco123 address 10.1.1.12
```

The crypto key should match the key configured on Cisco CallManager. This method and encapsulation mode should also match the method and encapsulation mode configured on Cisco CallManager. Other methods of key exchange are also supported. For more information refer to *Cisco IOS Security Configuration Guide*, Release 12.3 .

```
!
crypto ipsec transform-set rtpset esp-des esp-md5-hmac
mode transport
```

The crypto IPsec configuration should match the Cisco CallManager configuration.

```
!
crypto map rtp 1 ipsec-isakmp
 set peer 10.1.1.12
 set transform-set rtpset
 match address 115
!
interface FastEthernet0/1
 ip address 10.1.1.212 255.255.255.0
 load-interval 30
 duplex auto
 speed auto
 crypto map rtp
!
```

The following line shows the IPsec access list.

```
access-list 115 permit ip host 10.1.1.212 host 10.1.1.12
!
voice-port 1/0/0
!
voice-port 2/0/0
!
mgcp
mgcp call-agent 10.1.1.12 service-type mgcp version 0.1
```

The **mgcp package-capability** command enables the MGCP application ability to manage SRTP calls and advertise SRTP capability in SDP sent to remote gateways.

```
mgcp package-capability srtp-package
!
mgcp profile default
!
dial-peer voice 100 pots
```

```
 application mgcpapp
 port 1/0/0
!
dial-peer voice 200 pots
 application mgcpapp
 port 2/0/0
!
dial-peer voice 201 pots
 application mgcpapp
 port 2/0/1
!
dial-peer voice 202 pots
 application mgcpapp
 port 2/0/2
!
dial-peer voice 203 pots
 application mgcpapp
 port 2/0/3
!
dial-peer voice 101 pots
 application mgcpapp
 port 1/0/1
!
dial-peer voice 110 pots
 application mgcpapp
 port 1/1/0
!
dial-peer voice 111 pots
 application mgcpapp
 port 1/1/1
!
!
alias exec k show mgcp conn | inc K=
alias exec sr sh call active voi | inc SRTP
alias exec rs sh rtpspi call | inc Snd-Rcv
alias exec vc sh voi call
alias exec m sh mgcp conn
alias exec cav sh call active voi
alias exec rsa sh rtpspi call
alias exec cc clear counters
alias exec sta sh int fa0/1 stat
alias exec cef sh ip cef
!
line con 0
 exec-timeout 0 0
 logging synchronous
line aux 0
line vty 0 4
 login
!
!
end
```

Additional References

The following sections provide references related to the Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways feature.

Related Documents

Related Topic	Document Title
Cisco CallManager configuration	Cisco IP Phone Authentication and Encryption for Cisco CallManager 4.0(1)
Cisco CallManager and IPsec configuration	• " How to Configure IPsec Tunneling in Windows 2000 ," Microsoft Knowledge Base article • " Step-by-Step Guide to Internet Protocol Security (IPsec) ," "Building A Custom IPsec Policy" section, Microsoft Knowledge Base article
Cisco IP Phone 7940 and 7960 administration	Cisco IP Phone Model 7960G and 7940G Administration Guide for Cisco CallManager
Cisco IP Phone 7970 administration	*Cisco IP Phone 7970 Administration Guide for Cisco CallManager*
Cisco 2621 configuration	*Cisco 2621 Modular Access Router with AIM-VPN/BP Security Policy*
Cisco 2651 configuration	*Cisco 2651 Modular Access Router with AIM-VPN/BP Security Policy*
Cisco 3640 configuration	*Cisco 3640 Modular Access Router with AIM-VPN/BP Security Policy*
Cisco 3660 configuration	*Cisco 3660 Modular Access Router with AIM-VPN/BP Security Policy*
Secure SRST router configuration	Setting Up Secure SRST
Advanced Encryption Standard (AES) feature	*Advanced Encryption Standard*
IPsec configuration	*Cisco IOS Security Configuration Guide*, Release 12.3
IPsec commands	*Cisco IOS Security Command Reference,* Release 12.3
Cisco IOS voice configuration	*Cisco IOS Voice Configuration Library*
Cisco IOS voice command reference	*Cisco IOS Voice Command Reference*
Configuring IPsec Between a Microsoft Windows 2000 Server and a Cisco Device	Configuring IPsec Between a Microsoft Windows 2000 Server and a Cisco Device
Secure Real-time Transport Protocol Support	Secure Real-time Transport Protocol Support

Standards

Standards	Title
IETF draft draft-ietf-mmusic-sdescriptions-02.txt	Security Descriptions for Media Streams

MIBs

MIB	MIBs Link
CISCO-VOICE-DIAL-CONTROL-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 3711	*Secure Real-time Transport Protocol*
RFC 4040	RTP Payload Format for a 64 kbit/s Transparent Call
RFC 4568	Session Description Protocol (SDP) Security Descriptions for Media Streams

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for Media and Signaling Authentication and Encryption

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 8: Feature Information for Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways

Feature Name	Releases	Feature Information
Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways	12.3(11)T2 12.3(14)T	In 12.3(11)T2, this feature was introduced. In 12.3(14)T support was added for the Cisco Secure SRST feature and the NM-HDV network module.
Support for MGCP 1.0 Call Control for SRTP on Cisco IOS Gateways	15.0(1)XA	This feature provides support for MGCP 1.0 call control for SRTP on Cisco IOS gateways, and for fax pass-through and the Clear Channel codec at the media level under MGCP 1.0 and 0.1. The following command was introduced: **mgcp crypto rfc-preferred**.

Glossary

CCM --Cisco Call Manager.

CLI --command-line interface.

CTL --Certificate Trust List.

DTMF --dual-tone multifrequency

HMAC --Hashed Message Authentication Codes.

IETF --Internet Engineering Task Force. Standards body for Internet standards.

IKE --Internet Key Exchange.

IPsec --IP security.

MGCP --Multimedia Gateway Control Protocol.

PIN --Personal identification number.

RTCP --Real-Time Transport Protocol Control Protocol.

RTP --Real-Time Transport Protocol

SDP --Session Description Protocol.

SHA1 --Secure Hash Algorithm1.

SRST --Survivable Remote Site Telephony.

SRTP --Secure RTP.

SRTCP --Secure RTCP.

VoIP --Voice over IP.

CHAPTER 10

Configuring MGCP CAS PBX and AAL2 PVC

This section provides information on configuring the MGCP Channel-Associated Signaling (CAS) Private-Branch-Exchange (PBX) and ATM Adaptation Layer 2 (AAL2) Permanent Virtual Circuit (PVC) feature.

Feature benefits include the following:

- The merged Simple Gateway Control Protocol/Media Gateway Control Protocol (SGCP/MGCP) software for residential gateways (RGWs), business gateways (BGWs), and trunking gateways (TGWs) enables easier development and growth of Cisco and customer solutions.
- MGCP CAS PBX and AAL2 PVC software meets customer requirements for CAS connectivity to traditional PBXs and regulatory requirements for support of 911, Barge In, and Busy Line Verify features.

For more information about this and related Cisco IOS voice features, see the following:

- "Overview of MGCP and Related Protocols" on page 3
- Entire Cisco IOS Voice Configuration Library--including library preface and glossary, other feature documents, and troubleshooting documentation--at http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/cisco_ios_voice_configuration_library_glossary/vcl.htm

Feature History for MGCP CAS PBX and AAL2 PVC

Release	Modification
12.1(5)XM	This feature was introduced on the following platforms: Cisco 1750, Cisco 2600 series, Cisco 3600 series, Cisco AS5300, Cisco MC3810, and Cisco uBR924.
12.2(2)T	This feature was integrated into this release on all previously supported platforms except the Cisco AS5300. A new command was added (mgcp rtp unreachable timeout) and an existing command was modified (mgcp sdp).
12.2(11)T	This feature was implemented on the Cisco AS5300 and Cisco AS5850. **Note** AAL2 PVC is not supported on the Cisco AS5850.

- Finding Feature Information, on page 158
- Prerequisites for MGCP CAS PBX and AAL2 PVC, on page 158
- Restrictions for MGCP CAS PBX and AAL2 PVC, on page 158

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for MGCP CAS PBX and AAL2 PVC

Prerequisites are described in the "Prerequisites for Configuring MGCP and Related Protocols" section on page 3 .

Restrictions for MGCP CAS PBX and AAL2 PVC

MGCP CAS PBX and AAL2 PVC Software Caveats

- Only the Cisco MC3810 series platform supports MGCP 0.1 control of AAL2 voice transport in this Cisco IOS release.
- For the Cisco MC3810 series platform, the AAL2 PVC functionality is supported on an high-performance compression module (HCM) version of an digital signal processor (DSP) card; it is not supported on an voice compression module (VCM) version.

To check the type of DSP card, enter a **show version** command at the EXEC prompt.

- • If you have an HCM card, the following line appears as part of the **show version**information:

```
1 6-DSP (slot 2) High Performance Compression Module(v01.A0)
```

- • If you have an VCM card, the following line appears as part of the **show version**information:

```
1 6-DSP (slot 2) Voice Compression Module(v255.V7)
```

If you have an HCM card, the MGCP Basic CLASS and Operator Services (BCOS) features will function correctly. If you have an VCM card, the AAL2 PVC feature is not supported.

- The Cisco AS5300 multiservice platform supports only the Feature Group-D Operator Services (FGD-OS) Barge-In/Busy Line Verify and 911 features of the MGCP CAS PBX and AAL2 PVC software.

Features Not Supported

- Basic CLASS and Operator features are covered in the MGCP Basic CLASS and Operator Services software. For more information on these capabilities, see Configuring MGCP Basic CLASS and Operator Services .
- The MGCP CAS PBX and AAL2 PVC software has not implemented DSP clock slotting changes, Comfort Noise Indication, ATM SVCs, TGCP, AAL1, FXO support in SGCP, ATM on the Cisco 3660 platform, and VoIP Call Admission Control (CAC). These capabilities are part of other Cisco development efforts.

Information About MGCP CAS PBX and AAL2 PVC

The MGCP CAS PBX and AAL2 PVC features extend the earlier Simple Gateway Control Protocol (SGCP) Channel Associated Signaling (CAS) and AAL2 support onto the merged SGCP/MGCP software base to enable various service provider solutions.

MGCP CAS PBX and AAL2 PVC Features

- CAS termination and translation to MGCP on Business Gateways (BGWs) and Trunking Gateways (TGWs).

Digital CAS (E&M) interfaces are supported in addition to the analog (FXO, FXS, and E&M) interfaces.

For this feature release, the BGWs are the Cisco 3810 series and Cisco 2600 series routers. The TGWs are the Cisco 3600 series multiservice platforms.

- Support for CAS PBX and Feature Group D CAS Functions.

MGCP 0.1 has been expanded to support CAS packages that handle CAS PBX and Feature Group D CAS functions, including Barge-In/Busy Line Verify, and 911 capabilities on the TGW.

- Expanding MGCP 0.1 to control AAL2 voice transport.

The earlier version of the merged SGCP/MGCP stack supported only Voice over IP. The merged stack will now support both VoIP and VoAAL2.

Only the Cisco MC3810 series platforms supports this feature in this release.

- Addition of SGCP CAS PBX support to the existing merged SGCP/MGCP software stack.

The CAS PBX gateway features include CAS PBX trunks, digit maps, CAS events, and quarantine buffer software. These features were available in the existing standalone SGCP software; now they are supported in the merged stack.

- Consolidation of various SGCP and MGCP feature sets onto one software image for Residential Gateways (RGWs), BGWs, and TGWs.

For this feature release, the RGWs are the Cisco uBR924 cable router and Cisco 1750 access router.

The essential difference for current SGCP users is that support for the SGCP application has been replaced with the MGCP application. The MGCP application supports both SGCP commands and MGCP commands, permitting access to a larger feature set than with the SGCP application alone. The MGCP CAS PBX and AAL2 PVC software assumes the MGCP mode as the default environment. This allows the gateway to

recognize both MGCP and SGCP messages sent by the call agent. However, the user can specify SGCP mode for certain messages that will be sent by the gateway (by using the **sgcp** option as the service type in the **mgcp call-agent** command).

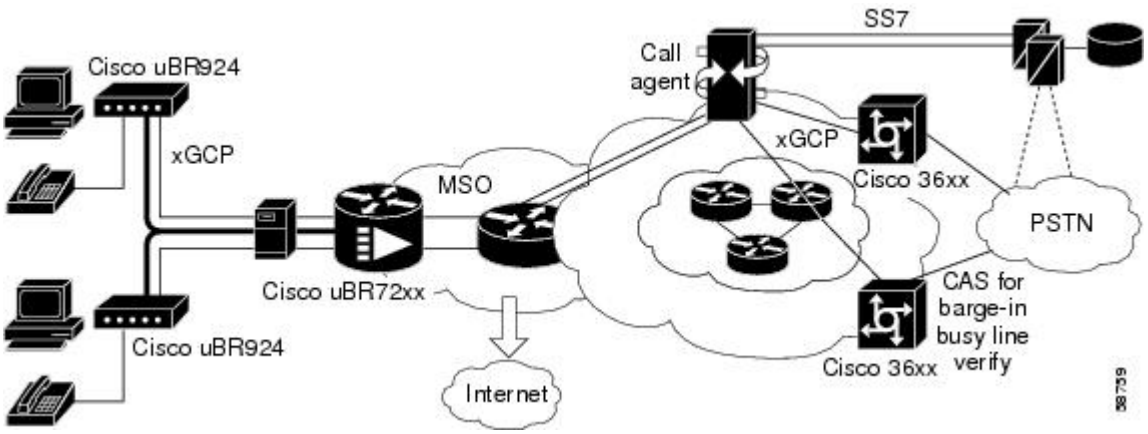
Examples of Service Provider Solutions

MGCP CAS PBX and AAL2 PVC features support several types of service provider solutions:

- Residential cable access

A CLEC can use residential cable access to provide residential customers with basic telephony and data services. The figure below illustrates a possible residential cable access solution:

Figure 13: Residential Cable Access Solution

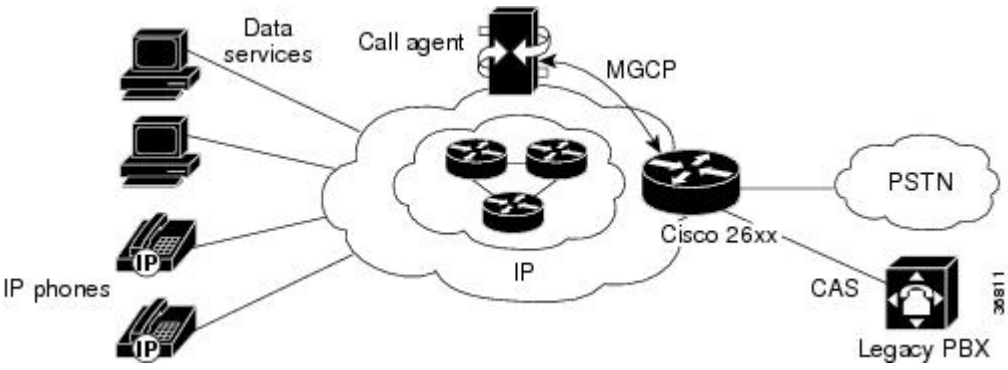


Note that in the figure above, the trunking gateway (the Cisco 3660 platform) requires support of incoming and outgoing MF signaling for the Barge-In and Busy-Line Verify features. The residential gateway (the Cisco uBR924 cable access router) must support the CLASS features and 911 capability.

- IP Centrex and IP PBX

In these solutions, a call agent provides business voice services traditionally offered by a circuit-based PBX. The figure below illustrates an IP Centrex solution:

Figure 14: IP Centrex Solution

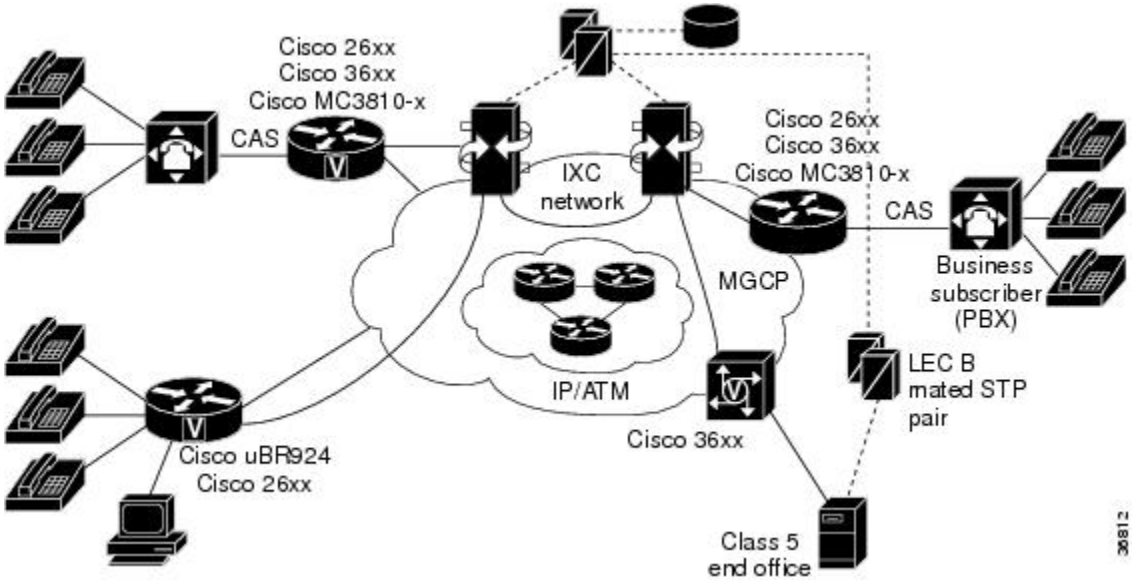


In the figure above, the BGW (the Cisco 2600 platform) requires PBX connectivity to interface with the legacy PBX.

- Integrated Access

A CLEC or IXC can provide small, medium, and large businesses with integrated voice and data access services. The integrated access device can be located at the central office or on the customer's premises. Access to the subscriber can be analog or digital T1 interfaces in addition to DSL. Transport of voice and data can be over IP, Frame Relay, or ATM. The figure below illustrates an integrated access solution:

Figure 15: Integrated Access Solution

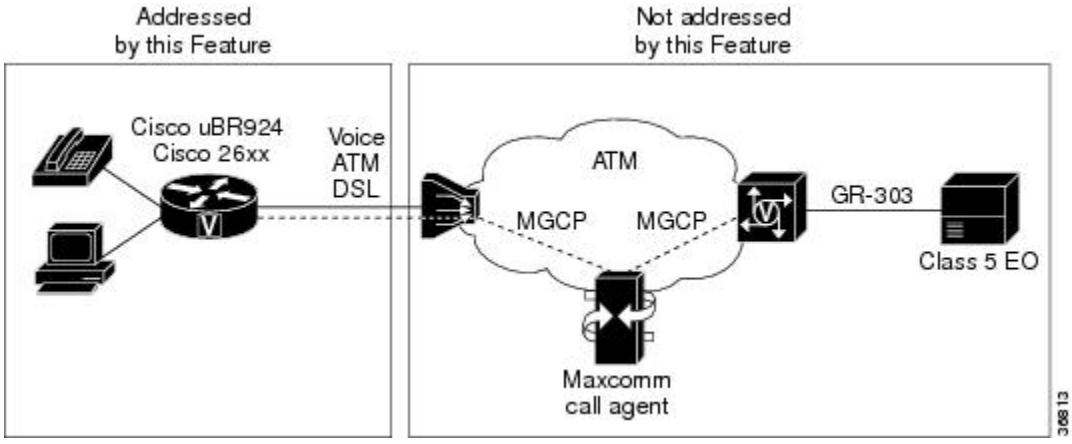


In the figure above, MGCP control of calls over the AAL2 PVCs is required on the BGWs (the Cisco 2600 series, Cisco 3600, and Cisco 3810 series platforms) to connect into the ATM network for VToA.

- Telecommuter or Small Office-Home Office

The figure below illustrates a telecommuter/small office-home office solution:

Figure 16: Telecommuter or Small Office-Home Office Solution



In the figure above, MGCP must control the calls over AAL2 PVCs, and an analog FXS interface is required.

How to Configure MGCP CAS PBX and AAL2 PVC

Some tasks indicate one or more configuration examples affected by the command. See the specific configuration example listing for the parameter values.

Configuring the Gateway

SUMMARY STEPS

1. **mgcp**
2. **mgcp call-agent** {*ipaddr* | *hostname*} [*port*] [**service-type** *type*] **version** v*ersion-number*
3. **mgcp dtmf-relay voip codec** {**all** | **low-bit-rate**} **mode** {**cisco** | **nse** | **out-of-band**}
4. **mgcp package-capability** {**as-package** | **atm-package** | **dtmf-package** | **gm-package** | **hs-package** | **nas-package** | **rtp-package** | **script-package** | **trunk-package**}
5. **mgcp sgcp restart notify**
6. **mgcp modem passthrough** [**voip** | **voaal2**] **mode** [**cisco** | **nse**]
7. **mgcp tse payload** *type*
8. **mgcp rtp unreachable timeout** *timer-value*
9. **no mgcp timer receive-rtcp**
10. **mgcp timer net-cont-test** *timer*
11. **controller T1 0**
12. **mode atm**
13. **no shutdown**
14. **exit**
15. **mgcp quarantine mode process**
16. **controller T1 1**
17. **mode cas**
18. **ds0-group** *channel-number* **timeslots** *range* **type** *signaling-type* **tone** *type addr info* **service** *service-type*
19. **exit**
20. **interface atm0** [*subinterface-number* [**multipoint** | **point-to-point**]]
21. **pvc** [*name*] *vpi/vci*
22. **encapsulation** *aal-encap*
23. **vbr-rt** *peak-rate average-rate* [*burst*]
24. **vcci** *pvc-identifier*
25. **exit**
26. **exit**
27. **dial-peer voice** *number* **pots**
28. **application MGCPAPP**
29. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**mgcp** **Example:** `Router(config)# mgcp`	Starts the MGCP daemon.
Step 2	**mgcp call-agent** {*ipaddr* | *hostname*} [*port*] [**service-type** *type*] **version** v*ersion-number* **Example:** `Router(config)# mgcp call-agent {ipaddr	hostname} [port] [service-type type] version version-number`	Configures the MGCP call agent and service type. If you want SGCP mode, use sgcp as the service type.
Step 3	**mgcp dtmf-relay voip codec** {**all** | **low-bit-rate**} **mode** {**cisco** | **nse** | **out-of-band**} **Example:** `Router(config)# mgcp dtmf-relay voip codec {all	low-bit-rate} mode {cisco	nse	out-of-band}`	(Optional. See Configuration Example 2.) Specifies compressed codecs for digit forwarding.
Step 4	**mgcp package-capability** {**as-package** | **atm-package** | **dtmf-package** | **gm-package** | **hs-package** | **nas-package** | **rtp-package** | **script-package** | **trunk-package**} **Example:** `Router(config)# mgcp package-capability {as-package	atm-package	dtmf-package	gm-package	hs-package	nas-package	rtp-package	script-package	trunk-package}`	(Optional. See Configuration Example 2.) Assigns packages to the gateway. Also refer to the **mgcp default-package** command.
Step 5	**mgcp sgcp restart notify** **Example:** `Router(config-if)# mgcp sgcp restart notify`	(Required only for SGCP mode with a call agent supporting RSIP. See Configuration Examples 4 through 9.) Causes MGCP to send SGCP RSIP messages.
Step 6	**mgcp modem passthrough** [**voip** | **voaal2**] **mode** [**cisco** | **nse**] **Example:** `Router(config-if)# mgcp modem passthrough [voip	voaal2] mode [cisco	nse]`	(Optional for **nse** mode) Enables the gateway to process fax or modem messages. VoAAL2 does not support **cisco**.
Step 7	**mgcp tse payload** *type* **Example:** `Router(config)# mgcp tse payload type`	(Required for **nse**mode. See Step 6.) Enables the TSE payload for fax and modem messages.

	Command or Action	Purpose
Step 8	**mgcp rtp unreachable timeout** *timer-value* **Example:** `Router(config)# mgcp rtp unreachable timeout timer-value`	(Optional) Enables detection of unreachable remote VoIP endpoints.
Step 9	**no mgcp timer receive-rtcp** **Example:** `Router(config)# no mgcp timer receive-rtcp`	(Required for non-RGWs. See Configuration Examples 2 through 9.) Turns off the RTP RTCP receive timeout interval at the gateway.
Step 10	**mgcp timer net-cont-test** *timer* **Example:** `Router(config)# mgcp timer net-cont-test timer`	(Optional for non-RGWs. See Configuration Examples 2 through 9.) Turns on the continuity test timeout interval at the gateway.
Step 11	**controller T1 0** **Example:** `Router(config)# controller T1 0`	(Required for ATM mode. See Configuration Examples 2 through 9.) Select s the T1 controller 0.
Step 12	**mode atm** **Example:** `Router(config-controller)# mode atm`	(Required for ATM mode. See Configuration Examples 2 through 9.) Specifies that the controller will support ATM encapsulation and create ATM interface 0. When the controller is set to ATM mode, the following takes place: • Controller framing is automatically set to Extended SuperFrame (ESF). • The linecode is automatically set to B8ZS.
Step 13	**no shutdown** **Example:** `Router(config-controller)# no shutdown`	(Optional for ATM mode. See Configuration Examples 2 through 9.) Ensures that the controller is activated.
Step 14	**exit** **Example:** `Router(config-controller)# exit`	(Required for ATM mode. See Configuration Examples 2 through 9.) Exits the current mode.
Step 15	**mgcp quarantine mode process** **Example:** `Router(config)# mgcp quarantine mode process`	(Optional) Turns on processing for SGCP quarantine mode.

	Command or Action	Purpose
Step 16	**controller T1 1** **Example:** `Router(config)# controller T1 1`	(Required for CAS PBX. See Configuration Examples 3, 4, and 5.) Select the T1 controller 1.
Step 17	**mode cas** **Example:** `Router(config-controller)# mode cas`	(Required for CAS PBX. See Configuration Examples 3, 4, and 5.) Specify that the controller will support CAS.
Step 18	**ds0-group** *channel-number* **timeslots** *range* **type** *signaling-type* **tone** *type addr info* **service** *service-type* **Example:** `Router(config-controller)# ds0-group channel-number timeslots range type signaling-type tone type addr info service service-type`	(Required for CAS PBX. See Configuration Examples 3, 4, and 5.) Configure the T1 timeslots for CAS calls.
Step 19	**exit** **Example:** `Router(config-controller)# exit`	(Required for CAS PBX. See Configuration Examples 3, 4, and 5.) Exit controller configuration mode.
Step 20	**interface atm0** [*subinterface-number* [**multipoint** | **point-to-point**]] **Example:** `Router(config)# interface atm0 [subinterface-number [multipoint | point-to-point]]`	(Required for ATM mode. See Configuration Examples 2 through 9.) Enter interface configuration mode to configure ATM interface 0 or an ATM subinterface. Default for subinterfaces is **multipoint.** For all scenarios: Set up three subinterfaces for point-to-point.
Step 21	**pvc** [*name*] *vpi/vci* **Example:** `Router(config-if)# pvc [name ] vpi/vci`	(Required for ATM mode. See Configuration Examples 2 through 9.) Create an ATM PVC for voice traffic and enter ATM virtual circuit configuration mode. **Note** The **ilmi** and **qsaal**options are not supported for AAL2.
Step 22	**encapsulation** *aal-encap* **Example:** `Router(config-if-atm-vc)# encapsulation aal-encap`	(Required for ATM mode. See Configuration Examples 2 through 9.) Set the encapsulation of the PVC for voice traffic. **aal2** automatically creates channel identifiers (CIDs) 1 through 255. Some of the Scenarios use **aal5snap** for ATM0.1 and ATM0.3. Use **aal2** for ATM0.2.

	Command or Action	Purpose
Step 23	**vbr-rt** *peak-rate average-rate* [*burst*] **Example:** `Router(config-if-atm-vc)# vbr-rt peak-rate average-rate [burst]`	(Required for ATM mode. See Configuration Examples 2 through 9.) Configures the PVC for the variable-bit-rate real-time (voice) traffic.
Step 24	**vcci** *pvc-identifier* **Example:** `Router(config-if-atm-vc)# vcci pvc-identifier`	(Optional for ATM mode. See Configuration Examples 2 through 9.) Assigns a unique identifier to the PVC.
Step 25	**exit** **Example:** `Router(config-if-atm-vc)# exit`	(Required for ATM mode. See Configuration Examples 2 through 9.) Exits the current mode.
Step 26	**exit** **Example:** `Router(config-if)# exit`	(Required for ATM mode. See Configuration Examples 2 through 9.) Exits the current mode.
Step 27	**dial-peer voice** *number* **pots** **Example:** `Router(config)# dial-peer voice number pots`	Enter dial peer configuration mode for the POTS dial peer.
Step 28	**application MGCPAPP** **Example:** `Router(config-dial-peer)# application MGCPAPP`	Initiates the MGCP protocol for the voice ports.
Step 29	**exit** **Example:** `Router(config-dial-peer)# exit`	Exits the current mode.

Configuring Subcell Multiplexing for AAL2 Voice

This section describes the configuration tasks necessary to enable AAL2 common part sublayer (CPS) subcell multiplexing when the Cisco MC3810 series platform interoperates with a voice interface service module (VISM) in an MGX switch.

SUMMARY STEPS

1. **voice service voatm**

2. **session protocol aal2**
3. **subcell-mux**
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**voice service voatm** **Example:** `Router(config)# voice service voatm`	(Required) Enters voice-service configuration mode.
Step 2	**session protocol aal2** **Example:** `Router(config-voice-service)# session protocol aal2`	(Required) Enters voice-service-session configuration mode and specifies AAL2 trunking.
Step 3	**subcell-mux** **Example:** `Router(config-voice-service-session)# subcell-mux`	(Required) Enables subcell multiplexing. By default, subcell multiplexing is not enabled.
Step 4	**end** **Example:** `Router(config-voice-service-session)# end`	(Required) Exits the current mode.

Configuring the Cable Access Router for SGCP and MGCP

The Cisco uBR924 cable access router requires standard per-port provisioning to work with MGCP CAS PBX and AAL2 PVC:

To access SGCP functionality, use the command:

```
S|0|ca1@call-agent.abc.com:2427|S|1|ca2@call-agent.abc.com:2427
```

To access MGCP functionality, use the command:

```
M|0|ca1@call-agent.abc.com:2427|M|1|ca2@call-agent.abc.com:2427
```

For either functionality type, port 0 points to call agent 1 and port 1 points to call agent 2. If needed, both ports can point to the same call agent.

Verifying the MGCP CAS PBX and AAL2 PVC Configurations

To verify configuration, use the following commands.

SUMMARY STEPS

1. **show dial-peer voice sum**
2. **show running-configuration**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show dial-peer voice sum** **Example:** `Router# show dial-peer voice sum`	Displays the status of the dial peer. The dial peer should be active. If it is not, use the **no shut** command to make it so.
Step 2	**show running-configuration** **Example:** `Router# show running-configuration`	Displays the current configuration settings.

Configuration Examples for MGCP CAS PBX and AAL2 PVC

Example 1 MGCP Residential Gateway

The following example illustrates the configuration for a Cisco MC3810 series platform with CAS running the MGCP application:

```
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log uptime
!
hostname Router
!
logging buffered
!
ip subnet-zero
ip host first 192.168.254.254
!
mgcp
mgcp call-agent 172.16.90.1
!
voice-card 0
  codec complexity high
!
controller T1 0
  framing esf
  linecode b8zs
!
interface Ethernet0
  ip address 172.16.92.3 255.255.0.0
!
interface Serial0
  shutdown
!
```

```
interface Serial1
  no ip address
  no ip route-cache
  no ip mroute-cache
  shutdown
!
interface FR-ATM20
  no ip address
  shutdown
!
ip default-gateway 172.16.0.1
ip route 198.168.254.0 255.255.255.0 172.16.0.1
!
voice-port 1/1
!
dial-peer voice 1 pots
  application MGCPAPP
  port 1/1
!
line con 0
  exec-timeout 0 0
  transport input none
line aux 0
line 2 3
line vty 0 4
  login
!
end
```

Example 2 MGCP Gateway using Voice over ATM AAL2

The following configuration illustrates a Cisco MC3810 series platform running the MGCP application using ATM AAL2 to carry voice traffic:

```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname main.office
!
network-clock base-rate 56k
ip subnet-zero
no ip domain-lookup
ip host second 192.168.254.254
ip host first 192.168.254.253
!
mgcp
mgcp call-agent 172.16.117.4 service-type mgcp version 0.1
mgcp dtmf-relay voip codec all mode nse
mgcp dtmf-relay voaal2 codec all
mgcp package-capability rtp-package
mgcp tse payload 100
mgcp timer receive-rtcp 100
mgcp timer net-cont-test 3000
isdn voice-call-failure 0
!
voice-card 0
!
controller T1 0
  mode atm
  framing esf
```

```
  linecode b8zs
!
interface Ethernet0
  ip address 171.16.121.1 255.255.0.0
!
interface Serial0
  no ip address
  no ip mroute-cache
  shutdown
  no fair-queue
!
interface Serial1
  no ip address
  shutdown
!
interface ATM0
  no ip address
  ip mroute-cache
  no atm ilmi-keepalive
interface ATM0.2 point-to-point
  pvc 2/200
   vbr-rt 760 760 100
   encapsulation aal2
vcci 2
!
interface FR-ATM20
  no ip address
  shutdown
!
router group1 1
  redistribute connected
  network 172.0.0.0
!
ip default-gateway 172.16.0.1
no ip http server
ip classless
ip route 192.168.254.0 255.255.255.0 172.16.0.1
!
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
voice-port 1/1
  codec g711ulaw
!
voice-port 1/2
  shutdown
!
voice-port 1/6
  shutdown
!
dial-peer voice 1 pots
  application MGCPAPP
  destination-pattern 2220001
  port 1/1
!
line con 0
  transport input none
line aux 0
  line 2 3
line vty 0 4
login
!
end
```

Example 3 MGCP and SGCP EM Wink-Start

The following example illustrates an E&M wink-start configuration on the Cisco MC3810 series platform that can be defined for either the SGCP or MGCP modes:

```
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname sales
!
network-clock base-rate 56k
ip subnet-zero
!
mgcp
no mgcp timer receive-rtcp
call rsvp-sync
!
voice service voatm
!
 session protocol aal2
  subcell-mux
!
voice-card 0
!
controller T1 0
 mode atm
 framing esf
 clock source internal
 linecode b8zs
!
controller T1 1
 mode cas
 framing esf
 linecode b8zs
 ds0-group 1 timeslots 1-24 type e&m-wink-start
!
interface Ethernet0
 ip address 172.29.248.199 255.255.255.0
 no ip route-cache
 no ip mroute-cache
!
interface Serial0
 no ip address
 no ip route-cache
 no ip mroute-cache
!
interface Serial1
 no ip address
 no ip route-cache
 no ip mroute-cache
 shutdown
!
interface ATM0
 no ip address
 ip mroute-cache
 no atm ilmi-keepalive
!
interface ATM0.2 point-to-point
 pvc 2/200
```

```
  vbr-rt 1536 1536 100
  encapsulation aal2
  vcci 10
!
interface FR-ATM20
 no ip address
 no ip route-cache
 shutdown
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.29.248.1
no ip http server
!
voice-port 1:1
 dial-type mf
!
dial-peer cor custom
!
dial-peer voice 1 pots
 application mgcpapp
 destination-pattern 1
 port 1:1
!
gatekeeper
 shutdown
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
line 2 3
line vty 0 4
login
 length 0
!
ntp clock-period 17248569
ntp server 172.29.1.129
end
```

Example 4 SGCP 1.5 CAS PBX using Voice over ATM AAL2

The following figure and configuration illustrate the network connections for a Cisco MC3810 series platform with CAS running the MGCP application in SGCP 1.5 mode. ATM AAL2 carries voice traffic.

- T1/0 is configured to run ATM with three permanent virtual circuits (PVCs):
  - 1 PVC with encapsulation AAL5 carries SGCP messages (signaling VC)
  - 1 PVC with encapsulation AAL5 carries data traffic (data VC)
  - 1 PVC with encapsulation AAL2 carries voice traffic (bearer VC)

This bearer VC has a **vcci** of 2 assigned to it. The service manager uses this **vcci** value and a selected channel identifier (CID) value for a voice call on this router.

For AAL2, allocate 200 ATM cells/sec (84.8K bits/sec) for each G711u no vad call, 100 ATM cells/sec (42.4K bits/sec) for each G726-32 no vad or G729a no vad call.

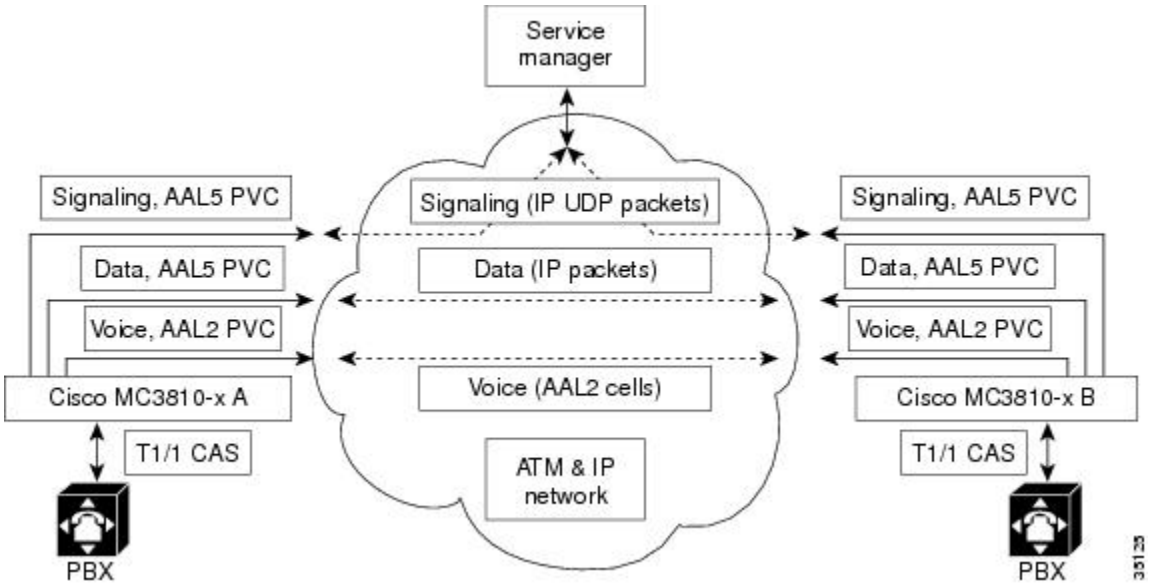
- In this configuration, T1/1 is configured as three DS-0 groups:
  - 1 FXS ground start group
  - 1 E&M immediate start group

- 1 E&M wink start group

For these voice ports, the dial type is set to **mf**to support mf dialing.

- **mgcp sdp** is configured to enable SGCP RSIP messages notification.
- **mgcp modem passthrough mode** is configured to allow **nse** processing of fax or modem calls.

Figure 17: SGCP 1.5 CAS PBX using Voice over ATM AAL2 Configuration



Router A Configuration

```
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname A
!
network-clock base-rate 56K
ip subnet-zero
!
mgcp
mgcp call-agent 10.0.0.1 service-type sgcp version 1.5
mgcp sgcp restart notify
mgcp tse payload 100
no mgcp timer receive-rtcp
mgcp timer net-cont-test 3000
isdn voice-call-failure 0
!
cns event-service server
voice-card 0
!
controller T1 0
  mode atm
  framing esf
  clock source line
```

```
  linecode b8zs
!
controller T1 1
  mode cas
  framing esf
  clock source line
  linecode b8zs
  ds0-group 1 timeslots 1-8 type e&m-immediate-start
  ds0-group 2 timeslots 9-16 type e&m-wink-start
  ds0-group 3 timeslots 17-24 type fxs-ground-start
!
interface Ethernet0
  ip address 172.16.24.103 255.255.0.0
!
interface Serial0
  no ip address
  no ip route-cache
  no ip mroute-cache
  shutdown
!
interface Serial1
  no ip address
  no ip route-cache
  no ip mroute-cache
  shutdown
  no cdp enable
!
interface ATM0
  no ip address
  ip mroute-cache
  no atm ilmi-keepalive
!
interface ATM0.1 point-to-point
  description signaling vc
  ip address 10.0.0.2 255.0.0.0
  pvc 1/1
   vbr-rt 1536 64
   encapsulation aal5snap
!
interface ATM0.2 point-to-point
  description bearer vc
  pvc 2/200
   vbr-rt 1536 1400 100
   encapsulation aal2
   vcci 2
!
interface ATM0.3 point-to-point
  description data vc
  ip address 10.0.0.5 255.0.0.0
  pvc 1/100
   encapsulation aal5snap
!
interface FR-ATM20
  no ip address
  no ip route-cache
  shutdown
!
ip classless
no ip http server
!
voice-port 1:1
!
voice-port 1:2
  dial-type mf
```

```
!
voice-port 1:3
!
dial-peer voice 1 pots
  application MGCPAPP
  port 1:1
!
dial-peer voice 2 pots
  application MGCPAPP
  port 1:2
!
dial-peer voice 3 pots
  application MGCPAPP
  port 1:3
!
line con 0
  exec-timeout 0 0
  privilege level 15
  transport input none
line aux 0
line 2 3
line vty 0 4
  login
!
end
```

Router B Configuration

```
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname B
!
network-clock base-rate 56K
ip subnet-zero
!
mgcp
mgcp call-agent 10.0.0.1 service-type sgcp version 1.5
mgcp sgcp restart notify
mgcp tse payload 100
no mgcp timer receive-rtcp
mgcp timer net-cont-test 3000
isdn voice-call-failure 0
!
cns event-service server
voice-card 0
!
controller T1 0
  mode atm
  framing esf
  clock source line
  linecode b8zs
!
controller T1 1
  mode cas
  framing esf
  clock source line
  linecode b8zs
  ds0-group 1 timeslots 1-8 type e&m-immediate-start
  ds0-group 2 timeslots 9-16 type e&m-wink-start
```

```
  ds0-group3 timeslots 17-24 type fxs-ground-start
!
interface Ethernet0
  ip address 172.17.24.103 255.255.0.0
!
interface Serial0
  no ip address
  no ip route-cache
  no ip mroute-cache
  shutdown
!
interface Serial1
  no ip address
  no ip route-cache
  no ip mroute-cache
  shutdown
  no cdp enable
!
interface ATM0
  no ip address
  ip mroute-cache
  no atm ilmi-keepalive
!
interface ATM0.1 point-to-point
  description signaling vc
  ip address 10.0.0.3 255.0.0.0
  pvc 1/1
   vbr-rt 1536 64
   encapsulation aal5snap
!
interface ATM0.2 point-to-point
  description bearer vc
  pvc 2/200
   vbr-rt 1536 1400 100
   encapsulation aal2
   vcci 2
!
interface ATM0.3 point-to-point
  description data vc
  ip address 10.0.0.8 255.0.0.0
  pvc 1/100
   encapsulation aal5snap
!
interface FR-ATM20
  no ip address
  no ip route-cache
  shutdown
!
ip classless
no ip http server
!
voice-port 1:1
!
voice-port 1:2
  dial-type mf
!
voice-port 1:3
!
dial-peer voice 1 pots
  application MGCPAPP
  port 1:1
!
dial-peer voice 2 pots
  application MGCPAPP
```

```
  port 1:2
!
dial-peer voice 3 pots
  application MGCPAPP
  port 1:3
!
line con 0
  exec-timeout 0 0
  privilege level 15
  transport input none
line aux 0
line 2 3
line vty 0 4
  login
!
end
```

Example 5 SGCP 1.5 CAS PBX using Voice over IP over ATM AAL5

The following figure and configuration illustrate the network connections for a Cisco MC3810 series platform with CAS running the MGCP application in SGCP 1.5 mode. Voice over IP over ATM AAL5 carries voice traffic.

This configuration is very similar to the AAL2 example in the previous section except that an AAL5 PVC is the bearer PVC for voice traffic.

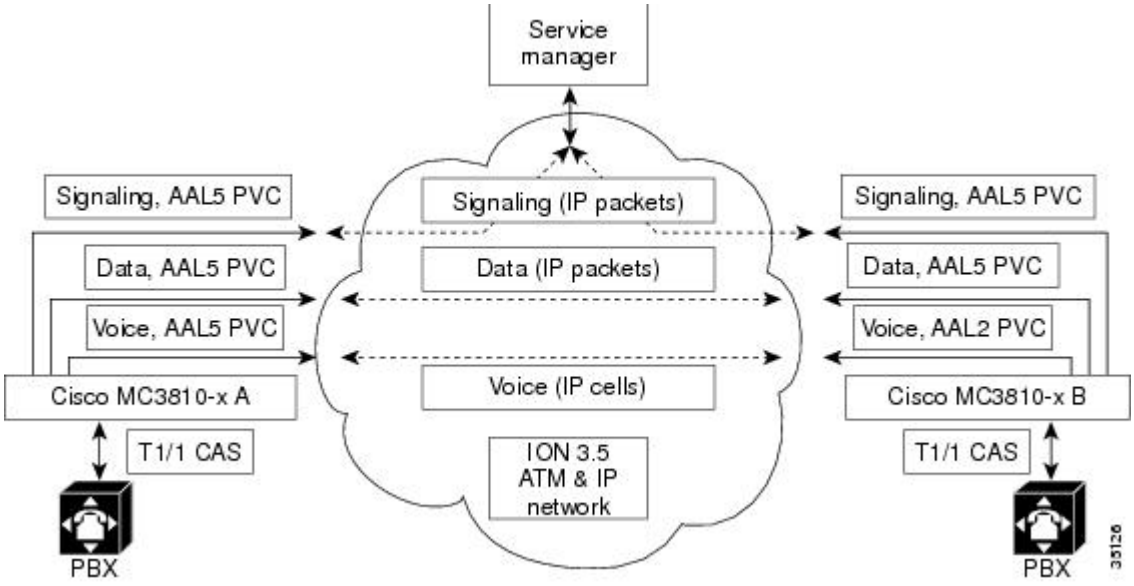
This configuration has a loopback interface with an IP address assigned to it. During voice calls, the gateway gives this IP address to the service manager as the address for the other gateway of the voice connection to use as the destination IP address.

In the example below, Router A's loopback address is 192.168.1.0 and Router B's address is 192.168.5.0. If Router A originated a call to Router B, A would give 192.168.1.0 to the Service Manager and B would give 192.168.5.0. The IP route configuration commands of both routers direct the IP traffic into the voice bearer PVC since the loopback addresses are on different IP subnets.

For Voice over IP, allocate 300 ATM cells/sec (127.2K bits/sec) for each G711u no vad call, and 200 ATM cells/sec (84.8K bits/sec) for each G726-32 no vad or G729a no vad call.

Note For G711u no vad calls, a T1 running ATM does not have enough bandwidth to carry 24 voice calls.

Figure 18: SGCP 1.5 CAS PBX using Voice over IP over ATM AAL5 Configuration



Router A Configuration

```
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname A
!
network-clock base-rate 56K
ip subnet-zero
!
mgcp
mgcp call-agent 10.0.0.1 service-type sgcp version 1.5
mgcp modem passthrough nse
mgcp sgcp restart notify
mgcp tse payload 100
no mgcp timer receive-rtcp
mgcp timer net-cont-test 3000
isdn voice-call-failure 0
!
cns event-service server
voice-card 0
!
controller T1 0
  mode atm
  framing esf
  linecode b8zs
!
controller T1 1
  mode cas
  framing esf
  clock source line
  linecode b8zs
  ds0-group 1 timeslots 1-8 type e&m-immediate-start
  ds0-group 2 timeslots 9-16 type e&m-wink-start
```

```
  ds0-group 3 timeslots 17-24 type fxs-ground-start
  framing esf
  linecode b8zs
!
interface Loopback0
  ip address 192.168.1.0 255.255.255.0
!
interface Ethernet0
  ip address 172.16.24.103 255.255.0.0
!
interface Serial0
  no ip address
  no ip route-cache
  no ip mroute-cache
  shutdown
!
interface Serial1
  no ip address
  no ip route-cache
  no ip mroute-cache
  shutdown
  no cdp enable
!
interface ATM0
  no ip address
  ip mroute-cache
  no atm ilmi-keepalive
!
interface ATM0.1 point-to-point
  description signaling vc
  ip address 10.0.0.2 255.0.0.0
  pvc 1/1
   vbr-rt 1536 64
   encapsulation aal5snap
!
interface ATM0.2 point-to-point
  description bearer vc
  ip address 10.0.0.5 255.0.0.0
  pvc 1/2
   vbr-rt 1536 1400 100
   encapsulation aal5mux ip
!
interface ATM0.3 point-to-point
  description data vc
  ip address 10.0.0.8 255.0.0.0
  pvc 1/100
   encapsulation aal5snap
!
interface FR-ATM20
  no ip address
  no ip route-cache
  shutdown
!
ip classless
ip route 10.0.0.15 255.0.0.0 ATM0.2
no ip http server
!
!
voice-port 1:1
!
voice-port 1:2
  dial-type mf
!
voice-port 1:3
```

```
!
dial-peer voice 1 pots
  application MGCPAPP
  port 1:1
!
dial-peer voice 2 pots
  application MGCPAPP
  port 1:2
!
dial-peer voice 3 pots
  application MGCPAPP
  port 1:3
!
line con 0
  exec-timeout 0 0
  privilege level 15
  transport input none
line aux 0
line 2 3
line vty 0 4
  login
!
end
```

Router B Configuration

```
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname B
!
network-clock base-rate 56K
ip subnet-zero
!
mgcp
mgcp call-agent 10.0.0.1 service-type sgcp version 1.5
mgcp modem passthrough nse
mgcp sgcp restart notify
mgcp tse payload 100
no mgcp timer receive-rtcp
mgcp timer net-cont-test 3000
isdn voice-call-failure 0
!
cns event-service server
voice-card 0
!
controller T1 0
  mode atm
  framing esf
  linecode b8zs
!
controller T1 1
  mode cas
  ds0-group 1 timeslots 1-8 type e&m-immediate-start
  ds0-group 2 timeslots 9-16 type e&m-wink-start
  ds0-group3 timeslots 17-24 type fxs-ground-start
  framing esf
  linecode b8zs
!
interface Loopback 0
```

```
  ip address 192.168.5.0 255.255.255.0
!
interface Ethernet0
  ip address 172.17.24.103 255.255.0.0
!
interface Serial0
  no ip address
  no ip route-cache
  no ip mroute-cache
  shutdown
!
interface Serial1
  no ip address
  no ip route-cache
  no ip mroute-cache
  shutdown
  no cdp enable
!
interface ATM0
  no ip address
  ip mroute-cache
  no atm ilmi-keepalive
!
interface ATM0.1 point-to-point
  description signaling vc
  ip address 10.0.0.3 255.0.0.0
  pvc 1/1
   vbr-rt 1536 64
   encapsulation aal5snap
!
interface ATM0.2 point-to-point
  description bearer vc
  ip address 10.0.0.6 255.0.0.0
  pvc 1/2
   vbr-rt 1536 1400 100
   encapsulation aal5mux ip
!
interface ATM0.3 point-to-point
  description data vc
  ip address 10.0.0.9 255.0.0.0
  pvc 1/100
   encapsulation aal5snap
!
interface FR-ATM20
  no ip address
  no ip route-cache
  shutdown
!
ip classless
ip route 10.0.0.16 255.0.0.0 ATM0.2
no ip http server
!
!
voice-port 1:1
!
voice-port 1:2
  dial-type mf
!
voice-port 1:3
!
dial-peer voice 1 pots
  application MGCPAPP
  port 1:1
!
```

```
dial-peer voice 2 pots
  application MGCPAPP
  port 1:2
!
dial-peer voice 3 pots
  application MGCPAPP
  port 1:3
!
!
line con 0
  exec-timeout 0 0
  privilege level 15
  transport input none
line aux 0
line 2 3
line vty 0 4
  login
!
end
```

Example 6 SGCP 1.5 Analog EM PBX using Voice over ATM AAL2

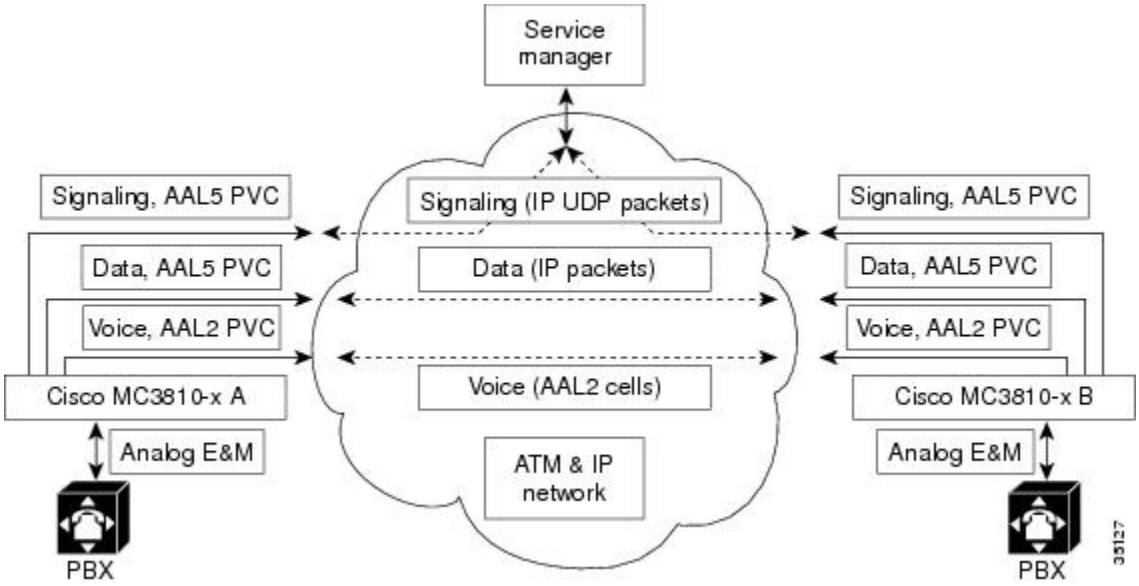
The following figure and configuration illustrate the network connections for a Cisco MC3810 series platform with Analog E&M running the MGCP application in SGCP 1.5 mode. ATM AAL2 carries voice traffic.

This configuration is similar to the SGCP 1.5 CAS PBX using Voice over ATM AAL2 configuration, with these exceptions:

- No DS-0 groups are configured for T1/1 because the slot is used by analog voice.
- The E&M port must be configured to match the type of analog PBX to which the port is connected.
- E&M protocol is set to either E&M immediate or wink start. For wink start, set the dial-type to **mf**.
- Operation must be set to 2-w (for 2-wire) or 4-w (for 4-wire).
- Type is set to I, II, IV, or V.

In this example, the bearer PVC has enough bandwidth for two G711u no vad calls because the router has only two voice ports.

Figure 19: SGCP 1.5 Analog EandM PBX using Voice over ATM AAL2 Configuration



Router A Configuration

```
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname A
!
network-clock base-rate 56K
ip subnet-zero
!
mgcp
mgcp call-agent 10.0.0.1 service-type sgcp version 1.5
mgcp tse payload 100
no mgcp timer receive-rtcp
mgcp timer net-cont-test 3000
mgcp sgcp restart notify
isdn voice-call-failure 0
!
!
cns event-service server
voice-card 0
!
controller T1 0
  mode atm
  framing esf
  linecode b8zs
!
interface Ethernet0
  ip address 172.16.24.101 255.255.0.0
!
interface Serial0
  no ip address
  no ip route-cache
  no ip mroute-cache
```

```
  shutdown
!
interface Serial1
  no ip address
  no ip route-cache
  no ip mroute-cache
  shutdown
  no cdp enable
!
interface ATM0
  no ip address
  ip mroute-cache
  no atm ilmi-keepalive
!
interface ATM0.1 point-to-point
  description signaling vc
  ip address 10.0.0.2 255.0.0.0
  pvc 1/1
   vbr-rt 1536 64
   encapsulation aal5snap
!
interface ATM0.2 point-to-point
  description bearer vc
  pvc 1/2
   vbr-rt 1536 170 8
   encapsulation aal2
   vcci 2
!
interface ATM0.3 point-to-point
  description data vc
  ip address 10.0.0.5 255.0.0.0
  pvc 1/100
   encapsulation aal5snap
!
interface FR-ATM20
  no ip address
  no ip route-cache
  shutdown
!
ip classless
no ip http server
!
voice-port 1/3
  operation 4-wire
  type 2
  signal immediate
!
voice-port 1/4
  operation 4-wire
  type 2
  dial-type mf
!
!
dial-peer voice 3 pots
  application MGCPAPP
  port 1/3
!
dial-peer voice 4 pots
  application MGCPAPP
  port 1/4
!
line con 0
  exec-timeout 0 0
  privilege level 15
```

```
  transport input none
line aux 0
line 2 3
line vty 0 4
  login
!
end
```

Router B Configuration

```
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname B
!
network-clock base-rate 56K
ip subnet-zero
!
mgcp
mgcp call-agent 10.0.0.1 service-type sgcp version 1.5
mgcp tse payload 100
no mgcp timer receive-rtcp
mgcp timer net-cont-test 3000
mgcp sgcp restart notify
isdn voice-call-failure 0
!
cns event-service server
voice-card 0
!
controller T1 0
  mode atm
  framing esf
  linecode b8zs
!
interface Ethernet0
  ip address 172.17.24.101 255.255.0.0
!
interface Serial0
  no ip address
  no ip route-cache
  no ip mroute-cache
  shutdown
!
interface Serial1
  no ip address
  no ip route-cache
  no ip mroute-cache
  shutdown
  no cdp enable
!
interface ATM0
  no ip address
  ip mroute-cache
  no atm ilmi-keepalive
!
interface ATM0.1 point-to-point
  description signaling vc
  ip address 10.0.0.3 255.0.0.0
  pvc 1/1
   vbr-rt 1536 64
```

```
   encapsulation aal5snap
!
interface ATM0.2 point-to-point
  description bearer vc
  pvc 1/2
   vbr-rt 1536 170 8
   encapsulation aal2
   vcci 2
!
interface ATM0.3 point-to-point
  description data vc
  ip address 10.0.0.6 255.0.0.0
  pvc 1/100
   encapsulation aal5snap
!
interface FR-ATM20
  no ip address
  no ip route-cache
  shutdown
!
ip classless
no ip http server
!
voice-port 1/3
  operation 2-wire
  type 1
  signal immediate
!
voice-port 1/4
  operation 4-wire
  type 2
  dial-type mf
!
dial-peer voice 3 pots
  application MGCPAPP
  port 1/3
!
dial-peer voice 4 pots
  application MGCPAPP
  port 1/4
!
!
line con 0
  exec-timeout 0 0
  privilege level 15
  transport input none
line aux 0
line 2 3
line vty 0 4
  login
!
end
```

Example 7 SGCP 1.5 Analog EM PBX using Voice over IP over ATM AAL5

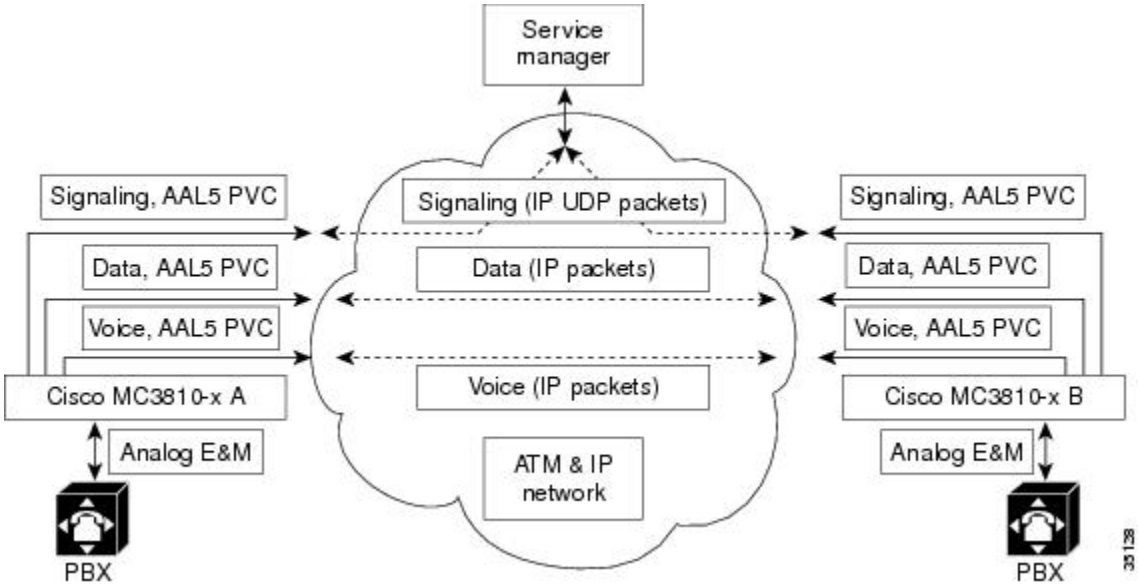
The following figure and configuration illustrate the network connections for a Cisco MC3810 series platform RGW with analog FXS loopstart ports running the MGCP application in SGCP 1.5 mode. Voice over IP over ATM AAL5 carries voice traffic.

This configuration is similar to the SGCP 1.5 CAS PBX using Voice over IP over ATM AAL5 configuration, with these exceptions:

- No DS-0 groups are configured for T1/1 because the slot is used by analog voice.
- The E&M port must be configured to match the type of analog PBX to which the port is connected.
- E&M protocol is set to either E&M immediate or wink start. For wink start, set the dial-type to **mf**.
- Operation must be set to 2-w (for 2-wire) or 4-w (for 4-wire).
- Type is set to I, II, IV, or V.

In this example, the bearer PVC has enough bandwidth for two G711u no vad calls because the router has only two voice ports.

Figure 20: SGCP 1.5 Analog EandM PBX using Voice over IP over ATM AAL5 Configuration



Router A Configuration

```
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname A
!
network-clock base-rate 56K
ip subnet-zero
!
mgcp
mgcp call-agent 10.0.0.1 service-type sgcp version 1.5
mgcp tse payload 100
no mgcp timer receive-rtcp
mgcp timer net-cont-test 3000
mgcp sgcp restart notify
isdn voice-call-failure 0
!
cns event-service server
voice-card 0
```

```
!
controller T1 0
  mode atm
  framing esf
  linecode b8zs
!
interface Loopback0
  ip address 10.0.0.2 255.0.0.
!
interface Ethernet0
  ip address 172.16.24.101 255.255.0.0
!
interface Serial0
  no ip address
  no ip route-cache
  no ip mroute-cache
  shutdown
!
interface Serial1
  no ip address
  no ip route-cache
  no ip mroute-cache
  shutdown
!
interface ATM0
  no ip address
  ip mroute-cache
  no atm ilmi-keepalive
!
interface ATM0.1 point-to-point
  description signaling vc
  ip address 10.0.0.5 255.0.0.0
  pvc 1/1
   vbr-rt 1536 64
   encapsulation aal5snap
!
interface ATM0.2 point-to-point
  description bearer vc
  ip address 10.0.0.6 255.0.0.0
  pvc 1/2
   vbr-rt 1536 260 8
   encapsulation aal5mux ip
!
interface ATM0.3 point-to-point
  description data vc
  ip address 10.0.0.8 255.0.0.0
  pvc 1/100
   encapsulation aal5snap
!
interface FR-ATM20
  no ip address
  no ip route-cache
  shutdown
!
ip classless
ip route 10.0.0.0 255.0.0.0 ATM0.2
no ip http server
!
voice-port 1/3
  operation 4-wire
  type 2
  signal immediate
!
voice-port 1/4
```

```
  operation 4-wire
  type 2
  dial-type mf
!
dial-peer voice 3 pots
  application MGCPAPP
  port 1/3
!
dial-peer voice 4 pots
  application MGCPAPP
  port 1/4
!
line con 0
  exec-timeout 0 0
  privilege level 15
  transport input none
line aux 0
line 2 3
line vty 0 4
  login
!
end
```

Router B Configuration

```
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname B
!
network-clock base-rate 56K
ip subnet-zero
!
mgcp
mgcp call-agent 10.0.0.1 service-type sgcp version 1.5
mgcp tse payload 100
no mgcp timer receive-rtcp
mgcp timer net-cont-test 3000
mgcp sgcp restart notify
isdn voice-call-failure 0
!
cns event-service server
voice-card 0
!
controller T1 0
  mode atm
  framing esf
  linecode b8zs
!
interface Loopback0
  ip address 10.0.0.3 255.0.0.0
interface Ethernet0
  ip address 172.17.24.101 255.255.0.0
!
interface Serial0
  no ip address
  no ip route-cache
  no ip mroute-cache
  shutdown
!
```

```
interface Serial1
  no ip address
  no ip route-cache
  no ip mroute-cache
  shutdown
!
interface ATM0
  no ip address
  ip mroute-cache
  no atm ilmi-keepalive
!
interface ATM0.1 point-to-point
  description signaling vc
  ip address 10.0.0.7 255.0.0.0
  pvc 1/1
   vbr-rt 1536 64
   encapsulation aal5snap
!
interface ATM0.2 point-to-point
  description bearer vc
  ip address 10.0.0.9 255.0.0.0
  pvc 1/2
   vbr-rt 1536 170 8
   encapsulation aal5mux ip
!
interface ATM0.3 point-to-point
  description data vc
  ip address 10.0.0.10 255.0.0.0
  pvc 1/100
   encapsulation aal5snap
!
interface FR-ATM20
  no ip address
  no ip route-cache
  shutdown
!
ip classless
ip route 10.0.0.20 255.0.0.0 ATM0.2
no ip http server
!
voice-port 1/3
  operation 4-wire
  type 2
  signal immediate
!
voice-port 1/4
  operation 4-wire
  type 2
  dial-type mf
!
dial-peer voice 3 pots
  application MGCPAPP
  port 1/3
!
dial-peer voice 4 pots
  application MGCPAPP
  port 1/4
!
line con 0
  exec-timeout 0 0
  privilege level 15
  transport input none
line aux 0
line 2 3
```

```
line vty 0 4
  login
!
end
```

Example 8 SGCP 1.5 RGW using Voice over ATM AAL2

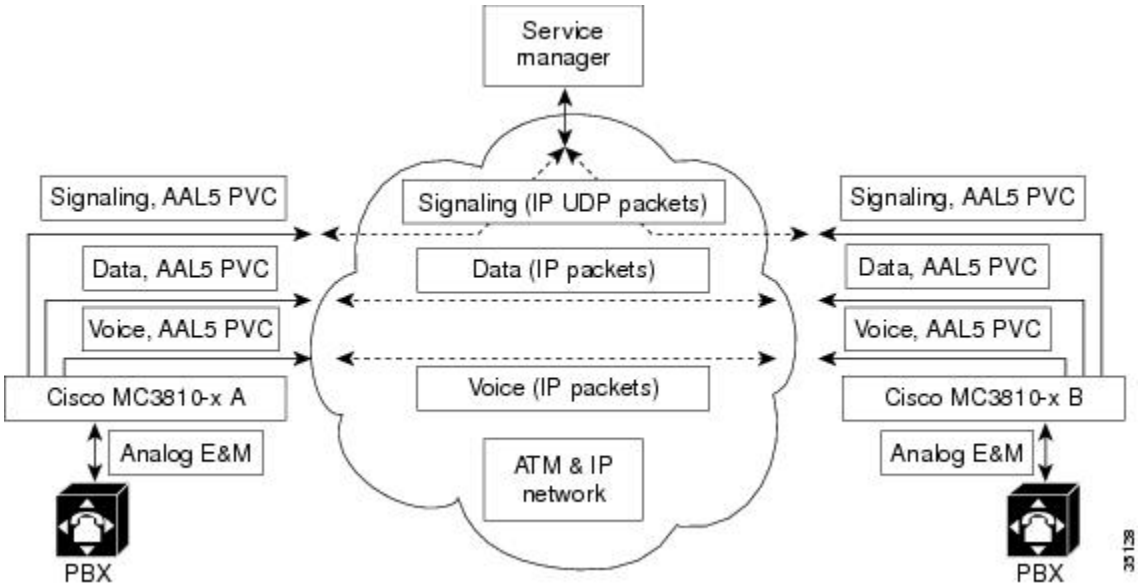
The following figure and configuration illustrate the network connections for a Cisco MC3810 series platform RGW with analog FXS port running the MGCP application in SGCP 1.5 mode. ATM AAL2 carries voice traffic.

This configuration is similar to the SGCP 1.5 CAS PBX using Voice over ATM AAL2 configuration, with these exceptions:

- No DS-0 groups are configured for T1/1 because the slot is used by analog voice.
- For RGW, the FXS ports' signaling are set to loop start, which is the default.

In this example, the bearer PVC has enough bandwidth for two G711u no vad calls because the router has only two voice ports.

Figure 21: SGCP 1.5 RGW using Voice over ATM AAL2 Configuration



Router A Configuration

```
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname A
!
network-clock base-rate 56K
ip subnet-zero
!
```

```
mgcp
mgcp call-agent 10.0.0.1 service-type sgcp version 1.5
mgcp sgcp restart notify
mgcp tse payload 100
no mgcp timer receive-rtcp
mgcp timer net-cont-test 3000
isdn voice-call-failure 0
!
!
cns event-service server
voice-card 0
!
controller T1 0
  mode atm
  framing esf
  linecode b8zs
!
interface Ethernet0
  ip address 172.16.24.101 255.255.0.0
!
interface Serial0
  no ip address
  no ip route-cache
  no ip mroute-cache
  shutdown
!
interface Serial1
  no ip address
  no ip route-cache
  no ip mroute-cache
  shutdown
  no cdp enable
!
interface ATM0
  no ip address
  ip mroute-cache
  no atm ilmi-keepalive
!
interface ATM0.1 point-to-point
  description signaling vc
  ip address 10.0.0.2 255.0.0.0
  pvc 1/1
   vbr-rt 1536 64
   encapsulation aal5snap
!
interface ATM0.2 point-to-point
  description bearer vc
  pvc 1/2
   vbr-rt 1536 170 8
   encapsulation aal2
   vcci 2
!
interface ATM0.3 point-to-point
  description data vc
  ip address 10.0.0.5 255.0.0.0
  pvc 1/100
   encapsulation aal5snap
!
interface FR-ATM20
  no ip address
  no ip route-cache
  shutdown
!
ip classless
```

```
no ip http server
!
!
voice-port 1/1
!
voice-port 1/2
!
dial-peer voice 1 pots
  application MGCPAPP
  port 1/1
!
dial-peer voice 2 pots
  application MGCPAPP
  port 1/2
!
line con 0
  exec-timeout 0 0
  privilege level 15
  transport input none
line aux 0
line 2 3
line vty 0 4
  login
!
end
```

Router B Configuration

```
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname B
!
network-clock base-rate 56K
ip subnet-zero
!
mgcp
mgcp call-agent 10.0.0.1 service-type sgcp version 1.5
mgcp sgcp restart notify
mgcp tse payload 100
no mgcp timer receive-rtcp
mgcp timer net-cont-test 3000
isdn voice-call-failure 0
!
cns event-service server
voice-card 0
!
controller T1 0
  mode atm
  framing esf
  linecode b8zs
!
interface Ethernet0
  ip address 172.17.24.101 255.255.0.0
!
interface Serial0
  no ip address
  no ip route-cache
  no ip mroute-cache
  shutdown
```

```
!
interface Serial1
  no ip address
  no ip route-cache
  no ip mroute-cache
  shutdown
  no cdp enable
!
interface ATM0
  no ip address
  ip mroute-cache
  no atm ilmi-keepalive
!
interface ATM0.1 point-to-point
  description signaling vc
  ip address 10.0.0.3 255.0.0.0
  pvc 1/1
   vbr-rt 1536 64
   encapsulation aal5snap
!
interface ATM0.2 point-to-point
  description bearer vc
  pvc 1/2
   vbr-rt 1536 170 8
   encapsulation aal2
   vcci 2
!
interface ATM0.3 point-to-point
  description data vc
  ip address 10.0.0.6 255.0.0.0
  pvc 1/100
   encapsulation aal5snap
!
interface FR-ATM20
  no ip address
  no ip route-cache
  shutdown
!
ip classless
no ip http server
!
voice-port 1/1
!
voice-port 1/2
!
dial-peer voice 1 pots
  application MGCPAPP
  port 1/1
!
dial-peer voice 2 pots
  application MGCPAPP
  port 1/2
!
line con 0
  exec-timeout 0 0
  privilege level 15
  transport input none
line aux 0
line 2 3
line vty 0 4
  login
!
end
```

Example 9 SGCP 1.5 RGW using Voice over IP over ATM AAL5

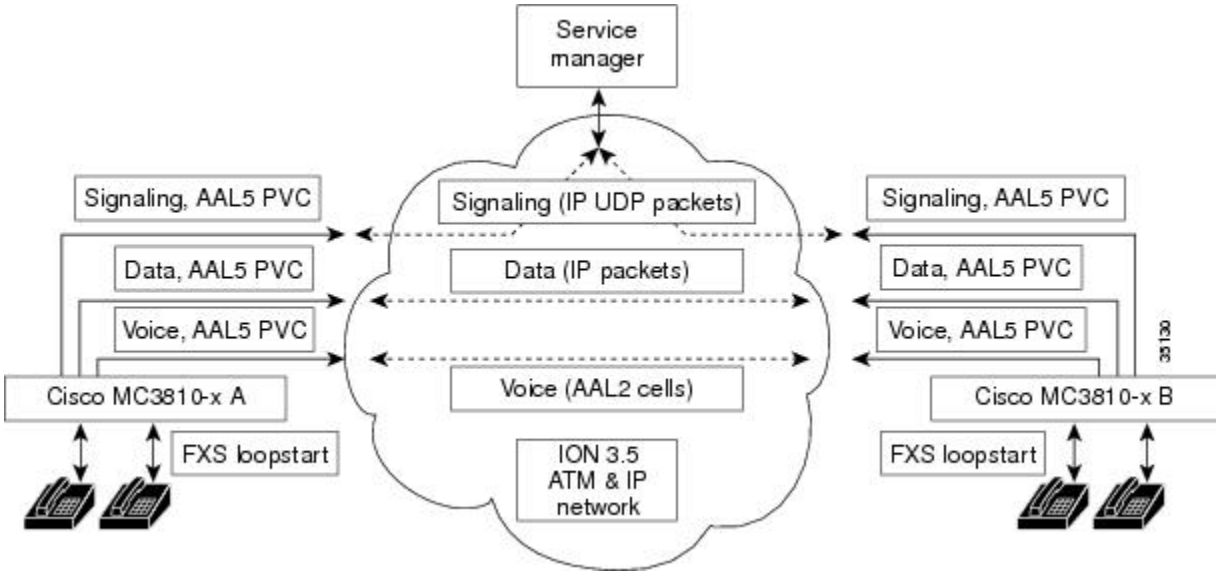
The following figure and configuration illustrate the network connections for a Cisco MC3810 series platform RGW with analog FXS port running the MGCP application in SGCP 1.5 mode. Voice over IP over ATM AAL5 carries voice traffic.

This configuration is similar to the SGCP 1.5 CAS PBX Voice Over ATM AAL5 configuration, with these exceptions:

- No DS-0 groups are configured for T1/1 because the slot is used by analog voice.
- For RGW, the FXS ports' signaling are set to loop start, which is the default.

In this example, the bearer PVC has enough bandwidth for two G711u no vad calls because the router has only two voice ports.

Figure 22: SGCP 1.5 RGW using Voice over IP over ATM AAL5 Configuration



Router A Configuration

```
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname A
!
network-clock base-rate 56K
ip subnet-zero
!
mgcp
mgcp call-agent 10.0.0.1 service-type sgcp version 1.5
mgcp sgcp restart notify
mgcp tse payload 100
no mgcp timer receive-rtcp
mgcp timer net-cont-test 3000
```

```
isdn voice-call-failure 0
!
cns event-service server
voice-card 0
!
controller T1 0
  mode atm
  framing esf
  linecode b8zs
!
interface Ethernet0
  ip address 172.16.24.101 255.255.0.0
!
interface Serial0
  no ip address
  no ip route-cache
  no ip mroute-cache
  shutdown
!
interface Serial1
  no ip address
  no ip route-cache
  no ip mroute-cache
  shutdown
!
interface ATM0
  no ip address
  ip mroute-cache
  no atm ilmi-keepalive
!
interface ATM0.1 point-to-point
  description signaling vc
  ip address 10.0.0.2 255.0.0.0
  pvc 1/1
   vbr-rt 1536 64
   encapsulation aal5snap
!
interface ATM0.2 point-to-point
  description bearer vc
  ip address 10.0.0.5 255.0.0.0
  pvc 1/2
   vbr-rt 1536 260 8
   encapsulation aal5mux ip
!
interface ATM0.3 point-to-point
  description data vc
  ip address 10.0.0.8 255.0.0.0
  pvc 1/100
   encapsulation aal5snap
!
interface FR-ATM20
  no ip address
  no ip route-cache
  shutdown
!
ip classless
ip route 10.0.0.10 255.0.0.0 ATM0.2
no ip http server
!
voice-port 1/1
!
voice-port 1/2
!
dial-peer voice 1 pots
```

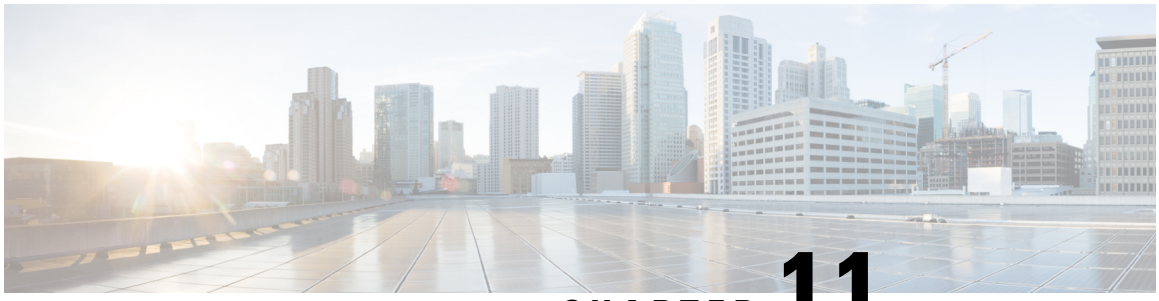
```
  application MGCPAPP
  port 1/1
!
dial-peer voice 2 pots
  application MGCPAPP
  port 1/2
!
line con 0
  exec-timeout 0 0
  privilege level 15
  transport input none
line aux 0
line 2 3
line vty 0 4
  login
!
end
```

Router B Configuration

```
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname B
!
network-clock base-rate 56K
ip subnet-zero
!
mgcp
mgcp call-agent 10.0.0.1 service-type sgcp version 1.5
mgcp sgcp restart notify
mgcp tse payload 100
no mgcp timer receive-rtcp
mgcp timer net-cont-test 3000
isdn voice-call-failure 0
!
!
cns event-service server
voice-card 0
!
controller T1 0
  mode atm
  framing esf
  linecode b8zs
!
interface Ethernet0
  ip address 172.17.24.101 255.255.0.0
!
interface Serial0
  no ip address
  no ip route-cache
  no ip mroute-cache
  shutdown
!
interface Serial1
  no ip address
  no ip route-cache
  no ip mroute-cache
  shutdown
!
```

```
interface ATM0
  no ip address
  ip mroute-cache
  no atm ilmi-keepalive
!
interface ATM0.1 point-to-point
  description signaling vc
  ip address 10.0.0.3 255.0.0.0
  pvc 1/1
   vbr-rt 1536 64
   encapsulation aal5snap
!
interface ATM0.2 point-to-point
  description bearer vc
  ip address 10.0.0.6 255.0.0.0
  pvc 1/2
   vbr-rt 1536 260 8
   encapsulation aal5mux ip
!
interface ATM0.3 point-to-point
  description data vc
  ip address 10.0.0.7 255.0.0.0
  pvc 1/100
   encapsulation aal5snap
!
interface FR-ATM20
  no ip address
  no ip route-cache
  shutdown
!
ip classless
ip route 10.0.0.12 255.0.0.0 ATM0.2
no ip http server
!
voice-port 1/1
!
voice-port 1/2
!
dial-peer voice 1 pots
  application MGCPAPP
  port 1/1
!
dial-peer voice 2 pots
  application MGCPAPP
  port 1/2
!
line con 0
  exec-timeout 0 0
  privilege level 15
  transport input none
line aux 0
line 2 3
line vty 0 4
  login
!
end
```

Tip See the "Additional References for MGCP and SGCP" section for related documents, standards, and MIBs, and the " Glossary " for definitions of terms in this guide.



CHAPTER 11

Secure Tone on MGCP TDM Gateways

The Secure Tone feature provides support for Cisco Unified Communications Manager (UCM) to play a secure or non secure tone when the secure status of the call changes.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Secure Tone on MGCP TDM Gateways

- Cisco Unified Communications Manager (UCM) 8.0(3) or a later release is running.
- Cisco IOS Media Gateway Control Protocol (MGCP) version 0.1 is configured.

Restrictions for Secure Tone on MGCP TDM Gateways

- Cisco UCM 8.0 will play the secure or non-secure indication tone to the protected device only when a two-way media connection is established.
- This feature is available only on Cisco IOS secure images.

Secure Tone on MGCP TDM Gateways

Cisco UCM not provides support for including supplementary service calls such as transfer and conferencing also changes the way in which secure and non secure indication tones are played. This new feature of playing the secure indication tone is based on the overall secure status unlike the earlier versions when it was based on end-to-end device's protected status. If the overall status is secure, the Secure Indication Tone (SIT) will be played to the protected phone. If the overall secure status is non secure, the Non-Secure Indication Tone (NSIT) will be played to the protected phone. SIT or NSIT will be played when a two-way audio media connection is first established on the protected phone.

Cisco UCM sends a Notification Request (RQNT) with the newly defined tone ID for secure or non secure status. Following is a sample message sent from Cisco UCM to the MGCP gateway to play the secure tone when the status of the call changes:

```
RQNT 199 S2/DS1-0/1@nw053b-3745.cisco.com MGCP 0.1
X: 1
R: D/[0-9ABCD*#]
S: X+TONE/st
Q: process,loop
```

How to Configure Secure Tone on MGCP TDM Gateways

Configuring Secure Tone on MGCP TDM Gateways

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mgcp package-capability tone-package**
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**mgcp package-capability tone-package** **Example:**	Configures the secure tone capability for MGCP packages.

	Command or Action	Purpose
	`Router(config)# mgcp package-capability tone-package`	
Step 4	**exit** **Example:** `Router# exit`	Exits the current mode.

Verifying and Troubleshooting Secure Tone on MGCP TDM Gateways

SUMMARY STEPS

1. **show mgcp**
2. **debug mgcp all**
3. **debug mgcp packets**

DETAILED STEPS

Step 1 **show mgcp**

This command is used for displaying the values for MGCP parameters. The parameters are displayed only when the tone package has been enabled using the **mgcp package-capability tone-package**command.

Step 2 **debug mgcp all**

This command is used to enable all debug traces for the MGCP gateway.

Step 3 **debug mgcp packets**

This command is used for enabling debug traces for the MGCP packets.

Configuration Examples for Secure Tone on MGCP TDM Gateways

Example Configuring Secure Tone for MGCP TDM Gateways

The following example shows how to enable the trunk package, DTMF package, script package, and tone package on the gateway, and then names the trunk package as the default package for the gateway:

```
Router(config)# mgcp package-capability trunk-package
Router(config)# mgcp package-capability dtmf-package
Router(config)# mgcp package-capability script-package
```

```
Router(config)# mgcp package-capability tone-package
Router(config)# mgcp default-package trunk-package
```

Example Verifying Secure Tone for MGCP TDM Gateways

The following is a partial sample output from the **show mgcp** command when the package capability has been enabled for tone package:

```
Router# show mgcp
MGCP Admin State ACTIVE, Oper State ACTIVE - Cause Code NONE
MGCP call-agent: 10.7.0.200 3460 Initial protocol service is MGCP 0.1
MGCP validate call-agent source-ipaddr DISABLED
MGCP block-newcalls DISABLED
MGCP send SGCP RSIP: forced/restart/graceful/disconnected DISABLED
MGCP quarantine mode discard/step
GCP quarantine of persistent events is ENABLED
MGCP dtmf-relay for VoIP disabled for all codec types
MGCP dtmf-relay for VoAAL2 disabled for all codec types
MGCP voip modem passthrough mode: NSE, codec: g711ulaw, redundancy: DISABLED,
MGCP voaal2 modem passthrough disabled
MGCP voip nse modem relay: Disabled
MGCP voip mdste modem relay: Enabled
        SPRT rx v14 hold time: 50 (ms), SPRT tx v14 hold count: 16,
        SPRT tx v14 hold time: 20 (ms), SPRT Retries: 12
        SSE redundancy interval: 20 (ms), SSE redundancy packet: 3,
        SSE t1 timer: 1000 (ms), SSE retries: 3
```

The following lines show that the **tone-package** keyword is enabled:

```
MGCP supported packages: gm-package dtmf-package mf-package trunk-package
                         line-package hs-package rtp-package script-package ms-package
                         dt-package mo-package mt-package sst-package mdr-package
                         fxr-package pre-package mdste-package srtp-package tone-package
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
MGCP configuration	*MGCP and Related Protocols Configuration Guide*
Cisco IOS voice configuration	*Cisco IOS Voice Configuration Library*
Cisco IOS voice commands	*Cisco IOS Voice Command Reference*
Cisco IOS debug commands	*Cisco IOS Debug Command Reference*

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

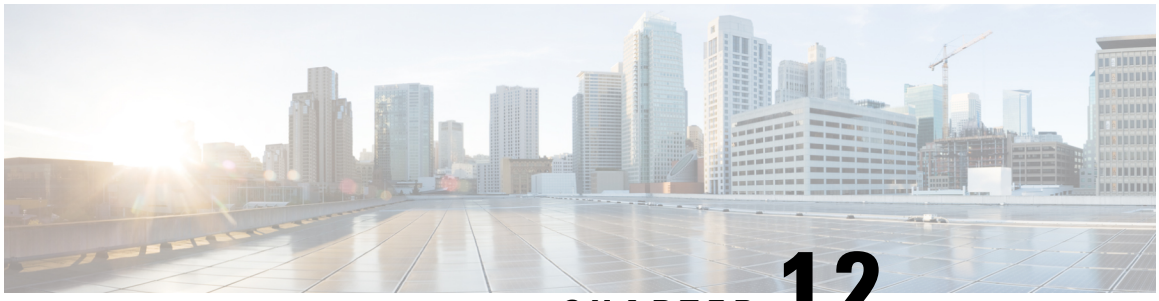
Feature Information for Secure Tone on MGCP TDM Gateways

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 9: Feature Information for Secure Tone Support on MGCP TDM Gateway

Feature Name	Releases	Feature Information
Secure Tone Support on MGCP TDM Gateway	15.1(4)M	This feature provides support for the Cisco UCM to play a secure or non secure tone when the secure status of the call changes or when the media are reconnected after the call is answered. The following command was introduced or modified: **mgcp package capability tone-package.**



CHAPTER 12

DSP Voice Quality Statistics in DLCX Messages

The DSP Voice Quality Statistics in DLCX Messages feature provides a way to trace a Media Gateway Control Protocol (MGCP) call between a Cisco PGW 2200 Softswitch and the Cisco IOS gateway by including the MGCP call ID and the DS0 and digital signal processor (DSP) channel ID in call-active and call-history records.

The voice quality statistics are sent as part of the MGCP Delete Connection (DLCX) message. By correlating an MGCP call on the Cisco PGW 2200 Softswitch with a call record on the gateway, you can understand and debug additional statistics from the DSP for problems related to voice quality.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document. Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for DSP Voice Quality Statistics in DLCX Messages

You must be using Cisco PGW 2200 version 9.4.1 or a later version with a patch level higher than CSCOgs008/CSCOnn008.

Restrictions for DSP Voice Quality Statistics in DLCX Messages

When the Secure Real-Time Transfer Protocol (SRTP) is enabled, the DLCX message will not report voice quality statistics. The following lines will be omitted for SRTP calls:

- DSP/Endpoint Configuration (EC)
- DSP/MOS K-Factor Statistics (KF)
- DSP/Concealment Statistics (CS)
- DSP/R-Factor Statistics (RF)
- DSP/User Concealment (UC)

Information About DSP Voice Quality Statistics in DLCX Messages

Cisco PGW 2200

A *call agent* (or *media gateway controller*) and *softswitch* are industry standard terms used to describe the network element that provides call control functionality to telephony and packet networks. The Cisco PGW 2200 Softswitch functions as a call agent or softswitch in "call control mode."

Note All voice quality parameters for Cisco IOS Release 12.4(4)T and later releases are supported only on the Cisco PGW 2200 call agent.

A public switched telephone network (PSTN) gateway provides an interface between traditional Signaling System No. 7 (SS7) or non-SS7 networks and networks based on MGCP, H.323, and Session Initiation Protocol (SIP), which include signaling, call control, and time-division multiplexing/IP (TDM/IP) gateway functions. The Cisco PGW 2200 Softswitch, coupled with Cisco media gateways, functions as a PSTN gateway.

Caution There is a significant performance degradation on the Cisco PGW 2200 if all connected gateways have the DSP Voice Quality Statistics in DLCX Messages feature enabled. Enabling voice quality statistics on the gateway should only be performed by Cisco personnel.

The Cisco PGW 2200 Softswitch, in either signaling or call control mode, provides a robust, carrier-class interface between PSTN and IP-based networks. Interworking with Cisco media gateways, the Cisco PGW 2200 Softswitch supports a multitude of applications and networks, including the following:

- Application service provider (ASP) termination
- Centralized routing and billing for clearinghouse of IP-based networks
- Dial access

- International and national transit networks
- Managed business voice applications
- Managed voice VPNs
- Network clearinghouse applications
- PSTN access for hosted and managed IP telephony
- PSTN access for voice over broadband networks
- Residential voice applications

MGCP

MGCP defines the call control relationship between call agents (CAs) and VoIP gateways that translate audio signals to and from the packet network. CAs are responsible for processing the calls.

An MGCP gateway handles the translation between audio signals and the packet network. The gateways interact with a CA, also called a media gateway controller (MGC), which performs signal and call processing on gateway calls. MGCP uses endpoints and connections to construct a call.

Endpoints are sources of or destinations for data and can be physical or logical locations in a device. Connections can be either point-to-point or multipoint. The gateway can be a Cisco router, an access server, or a cable modem, and the CA is a server from a third-party vendor.

Voice Quality Statistics

The Cisco PGW 2200 Softswitch can capture voice quality statistics sent from MGCP-controlled media gateways and can propagate the statistics into call detail records (CDRs) at the end of each call. The Cisco AS5x00 media gateways send voice quality statistics to the Cisco PGW 2200 Softswitch.

Most voice quality statistics are available from the DSP and are controlled using RTP Control Protocol (RTCP) report interval statistics polling. The mean and maximum values are calculated by Cisco IOS software-based polling, which results in additional CPU load for each call. The additional CPU load can be controlled by configuring polling interval by using the **ip rtcp report interval** command.

The playout delay, playout error, and DSP receive and transmit statistics are automatically polled periodically. Polling for the voice quality statistics, level, and error parameters can be added. For logging the voice quality statistics using syslog, the existing VoIP gateway accounting has been extended. For more information about statistics polling, see the **ip rtcp report interval** command in the http://www.cisco.com/en/US/partner/docs/ios-xml/ios/voice/vcr2/vcr2-cr-book.html .

Table 10: Voice Quality Statistics for Cisco IOS Release 12.4(4)T and Later Releases

DSP Technology	Platform	Voice Quality Statistics
MSA V6	Cisco AS5350, Cisco AS5350XM, Cisco AS5400, Cisco AS5400HPX, Cisco 5400XM, and Cisco AS5850 with an NPE60 or NPE108 universal port feature card.	DSP/TX DSP/RX DSP/PD DSP/PE DSP/LE DSP/ER DSP/IC
TIC5510	• Cisco 2800 series and Cisco 3800 series integrated services routers with PVDM2 modules. • Cisco VG224 voice gateway • Cisco IAD2430 series integrated access devices. • Cisco 2600XM, Cisco 2691, Cisco 3700 series access routers, and Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3800 series integrated services routers with the following network modules: NM-HDV2, NM-HDV2-1T1/E1, NM-HD-1V, NM-HD-2V, NM-HD-2VE. • Cisco 2821, Cisco 2851, Cisco 3825, and Cisco 3845 with the EVM-HD-8FXS/DID module.	DSP/TX DSP/RX DSP/PD DSP/PE DSP/LE DSP/ER DSP/IC DSP/EC DSP/KF DSP/CS DSP/RF DSP/UC DSP/DL

DSP Technology	Platform	Voice Quality Statistics
SP2600	• Cisco 2901, Cisco 2911, Cisco 2921, Cisco 2951, Cisco 3925, Cisco 3945, Cisco 3925-E, and Cisco 3945-E Integrated Services Routers with PVDM3 modules.	DSP/TX DSP/RX DSP/PD DSP/PE DSP/LE DSP/ER DSP/IC DSP/EC DSP/KF DSP/CS DSP/RF DSP/UC DSP/DL

Quality of Service for Voice

The DSP Voice Quality Statistics in DLCX Messages feature is part of the Cisco quality of service (QoS) technology. QoS is the ability of a network to provide better service to selected network traffic over various technologies, including ATM, Ethernet and 802.1 networks, Frame Relay, SONET, and IP-routed networks that may use any or all of these underlying technologies.

QoS provides the following benefits:

- Control over bandwidth, equipment, and wide-area facilities—As an example, you can limit the bandwidth consumed over a backbone link by FTP or limit the queueing of an important database access.
- More efficient use of network resources—Network analysis management and accounting tools enable you to know what your network is being used for and ensure that you are servicing the most important traffic to your business.
- Ability to customize services—QoS enables ISPs to offer carefully customized grades of service differentiation to their customers.
- Coexistence of mission-critical applications—Cisco QoS technologies ensure that bandwidth and minimum delays required by time-sensitive multimedia and voice applications are available and that other applications using the link get their fair service without interfering with mission-critical traffic.
- Foundation for a fully integrated network—Cisco QoS technologies fully integrate a multimedia network, for example, by implementing weighted fair queueing (WFQ) to increase service predictability and by implementing IP precedence signaling to differentiate traffic. In addition, the availability of Resource Reservation Protocol (RSVP) allows you to take advantage of dynamically signaled QoS.

To deliver QoS across a network that comprises heterogeneous technologies (for example, IP, ATM, LAN switches), basic QoS architecture consists of the following three components:

- QoS within a single network element (for example, queueing, scheduling, and traffic shaping tools).
- QoS signaling techniques for coordinating end-to-end QoS between network elements.
- QoS policy, management, and accounting functions to control and administer end-to-end traffic across a network.

Voice Quality Parameters for Cisco IOS Release 12.4(4)T and Later Releases

The following voice quality parameters were introduced in Cisco IOS Release 12.4(4)T:

DSP/EC

The following parameters describe the configuration of a VoIP endpoint. You can define these parameters and they are useful for debugging and logging purposes because they capture the state of the endpoint.

- CI—Codec ID. A string or a number that identifies the voice codec which is currently used in the call.
- FM—Frame size. Native frame size, in milliseconds (ms), of the selected codec. An example of a frame size and codec combination is G.729a/30ms. For the G.711 codec, the frame size is a value that you can define in the voice dial peer. For example, G.711 at 80 bytes gives 10 ms per frame. G.711 at 240 bytes gives 30 ms per frame.
- FP—Frames per packet. Number of codec speech frames encapsulated into a single Real-time Transport Protocol (RTP) packet. Typical values are 1, 2, and 3. Packing lower number of frames per packet results in lower efficiency of IP bandwidth usage. The tradeoff is lower delays and higher robustness of the network.
- VS—Voice Activity Detection (VAD)-enabled flag. VAD is enabled when VS has a value of one. It results in compression of silent periods leading to reduced or zero packets per second. VAD is disabled when VS has a value of zero. It results in the transmission of continuous packets per second irrespective of active or silent periods on the transmission path.
- GT—Transmission gain factor (linear). Digital gain multiplier applied to the transmission on the signal path from the PSTN toward the network. GT is applied at the echo canceller *Sout* port. A gain factor of less than one indicates a loss pad.
- GR—Reception gain factor (linear). Digital gain multiplier applied to reception on the signal path from the network toward the PSTN. GR is applied at the echo canceller *Rin* port. A gain factor of less than one indicates a loss pad.
- JD—Jitter buffer mode. It consists of the following modes:
  - Adaptive mode = 1
  - Fixed mode (no timestamps) = 2
  - Fixed mode (with timestamps) = 3
  - Fixed mode (with passthrough) = 4
- JN—Jitter buffer nominal playout delay. Size of the jitter buffer in milliseconds. An adaptive jitter buffer tries to make the playout delay equal to the nominal (desired) delay when the observed jitter is small enough to allow this adjustment. For a fixed-mode jitter buffer, the nominal setting is the constant playout delay itself.

- JM—Minimum playout delay. Minimum playout delay setting for an adaptive-mode jitter buffer. The playout delay never goes below the minimum playout setting even if the observed jitter is zero. This setting is not used for a fixed-mode jitter buffer because the playout delay is fixed and constant at the nominal setting.

- JX—Maximum playout delay. Sets the limit for increasing the playout delay of an adaptive-mode jitter buffer. An adaptive buffer increases when the jitter is higher than the instantaneous playout delay value.

DSP/KF

K-factor is an endpoint mean opinion score (MOS) estimation algorithm defined in the ITU standard P.VTQ. It is a general estimator of the mean value of a perceptual evaluation of speech quality (PESQ) population for a specific impairment pattern.

The ITU standard P.862 defines and describes the PESQ as an objective method for end-to-end speech quality assessment of narrow band telephone networks and speech codecs.

Mean opinion score (MOS) is associated with the output of a well-designed listening experiment. All MOS experiments use a five-point PESQ scale as defined in the ITU standard P.862.1. The MOS estimate is inversely proportional to frame loss density. Clarity decreases as more frames are lost or discarded at the receiving end.

K-factor represents a weighted estimate of average user annoyance due to distortions caused by effective packet loss such as dropouts and warbles. It does not estimate the impact of delay-related impairments such as echo. It is an estimate of listening quality (MOS-LQO) rather than conversational quality (MOS-CQO), and measurements of average user annoyance range from 1 (poor voice quality) to 5 (very good voice quality).

K-factor is trained or conditioned by speech samples from numerous speech databases, where each training sentence or network condition associated with a P.862.1 value has a duration of eight seconds. For more accurate scores, K-factor estimates are generated for every 8 seconds of active speech.

K-factor and other MOS estimators are considered to be secondary or derived statistics because they warn a network operator of frame loss only after the problem becomes significant. Packet counts, concealment ratios, and concealment second counters are primary statistics because they alert the network operator before network impairment has an audible impact or is visible through MOS.

- KF—K-factor MOS-LQO estimate (instantaneous). Estimate of the MOS score of the last 8 seconds of speech on the reception signal path. If VAD is active, the MOS calculation is suspended during periods of received silence to avoid inflation of MOS scores for calls with higher silence fractions.

- AV—Average K-factor score. Running average of scores observed since the beginning of a call.

- MI—Minimum K-factor score. Minimum score observed since the beginning of a call, and represents the worst sounding 8-second interval.

- BS—Baseline (maximum) K-factor score. K-factor score that can be obtained for the defined codec.

- NB—Number of bursts. Number of burst loss events after a call is started. A burst loss is a contiguous run of concealment events of length greater than one.

- FL—Average frame loss count. Total number of frame losses and concealment events observed after starting a call. The ratio of FL/NB provides the mean burst length in frames. The total concealment duration of the call is provided by the parameter *DSP/CS: CT*.

- NW—Number of windows. Total number of K-factor windows observed after starting a call. The number of windows is directly proportional to the duration of a call.
- VR—Version ID. Version number that identifies a specific K-factor MOS score.

DSP/CS

DSP/CS measures packet (frame) loss and its effect on voice quality in an impaired network. The parameters for concealment statistics are as follows:

- CR—Concealment ratio (instantaneous). An interval-based average concealment rate, and is the ratio of concealment time over speech time for the last 3 seconds of active speech. When VAD is enabled, calculation of the concealment ratio is suspended during periods of speech silence. During this suspension, it may take more than 3 seconds for a new value to be generated.
- AV—Average CR. Average of all CR reports after starting a call.
- MX—Maximum CR. The maximum concealment ratio observed after starting a call.
- CS—Concealed time. The duration of time in seconds during which some concealment is observed.
- CT—Total concealment time. The total duration of time in milliseconds during which concealment is observed after starting a call.
- TT—Total speech time. The duration of time in milliseconds during which active speech is observed after starting a call.
- OK—Ok time. The duration of time in seconds during which no concealment is observed.
- SC—Severely concealed time. The duration of time in seconds during which a significant amount of concealment is observed. If the concealment observed is usually greater than 50 milliseconds or approximately five percent, it is possible that the speech is not very audible.
- TS—Concealment threshold. The threshold in milliseconds used to determine a second as severely concealed. The threshold for concealed seconds is 0 milliseconds, and for severely concealed seconds is 50 milliseconds.

DSP/RF

The R-factor helps in planning voice transmission. In ITU standards G.107 and G.113, the R-factor is defined as follows:

R = Ro - Is - Id - Ie-eff + A

The parameters for the R-Factor are as follows:

- Ro is based on the signal-to-noise ratio.
- Is is the simultaneous impairment factor and includes the overall loudness rating.
- Id is the delay impairment factor and includes talker (Idte) and listener (Idle) echos, and delays (Idd).
- Ie-eff is the equipment impairment factor and includes packet losses and the types of codecs.
- A is the advantage factor.

- ML—R-factor MOS listening quality objective. It reflects only packet loss and codec-related impairments and does not include delay effects.
- MC—R-factor MOS-CQE.
- R1—R-factor LQ profile 1.
- R2—R-factor LQ profile 2.
- IF—Effective codec impairment (Ie_eff).
- ID—Idd.
- IE—Codec baseline score (Ie). The tabulated baseline codec impairment factor.
- BL—Codec baseline (Bpl). The packet loss robustness factor for the codec being used.
- R0—R0 (default). The nominal value at which the signal-to-noise ratio is considered nominal.

DSP/UC

The parameters for user concealment are as follows:

- U1—User concealment seconds 1 count (UCS1)
- U2—User concealment seconds 2 count (UCS2)
- T1—UCS1 threshold in milliseconds
- T2—UCS2 threshold in milliseconds

DSP/DL

The parameters for delay statistics are as follows:

- RT—Round trip delay
- ED—End system delay

How to Configure DSP Voice Quality Statistics in DLCX Messages

Configuring DSP Voice Quality Statistics in DLCX Messages

To configure voice quality statistics reporting for MGCP, use the following commands beginning in user EXEC mode.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mgcp voice-quality stats** [**priority***value*] [**all**]

4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**mgcp voice-quality stats** [**priority***value*] [**all**] **Example:** `Router(config)# mgcp voice-quality-stats priority 1`	Enables voice quality statistics reporting for MGCP. The following parameters are sent by default if the **priority** or **all** keywords are not used: DSP/TX, DSP/RX, DSP/PD, DSP/PE, DSP/LE, DSP/ER, DSP/IC. **Priority 1** parameters are: DSP/TX, DSP/RX, DSP/PD, DSP/LE, DSP/EC, DSP/CS, DSP/DL. **Priority 2** parameters are: DSP/PE, DSP/ER, DSP/IC, DSP/KF, DSP/RF, DSP/UC. Using **Priority 2** is similar to using the **all** keyword when the output contains the following parameters: DSP/TX, DSP/RX, DSP/PD, DSP/PE, DSP/LE, DSP/ER, DSP/IC, DSP/EC, DSP/KF, DSP/CS, DSP/RF, DSP/UC, and DSP/DL.
Step 4	**end** **Example:** `Router(config)# end`	Exits global configuration mode and enters privileged EXEC mode.

What to Do Next

Use the following Troubleshooting Tips if you did not get the expected results after configuring voice quality statistics reporting for MGCP. See the Troubleshooting Tips section for additional guidelines.

Troubleshooting Tips

Use the **debug mgcp packets** command to display statistics reported in the DLCX message generated at the end of a call. The following is sample debug output:

```
Router# debug mgcp packets

DLCX 311216 s6/ds1-4/1@as5400a MGCP 0.1
C: 48A4B
I: 2
R:
```

```
S:
X: 4BFAF
*May 5 10:20:51.643: send_mgcp_msg, MGCP Packet sent to 19.0.2.10:2427 --->
*May 5 10:20:51.643: 250 311216 OK
P: PS=1469, OS=28943, PR=1518, OR=29923, PL=0, JI=100, LA=0
DSP/TX: PK=1448, SG=0, NS=23, DU=206450, VO=39000
DSP/RX: PK=1449, SG=0, CF=23, RX=206450, VO=38000, BS=0, BP=0, LP=0
DSP/PD: CU=100, MI=90, MA=110, CO=69352809, IJ=0
DSP/PE: PC=0, IC=0, SC=0, RM=6, BO=0, EE=0
DSP/LE: TP=-24, TX=-440, RP=-87, RM=-870, BN=0, ER=50, AC=90, TA=-24, RA=-87
DSP/ER: RD=0, TD=0, RC=0, TC=0
DSP/IC: IC=0
```

Verifying DSP Voice Quality Statistics in DLCX Messages

Use the following **show** commands to check your configuration:

SUMMARY STEPS

1. Obtain the call ID by using the **show call active voice compact** command in privileged EXEC mode.
2. Check the status of active calls using the call ID obtained from the **show call active voice brief** command.
3. Verify your configuration using the **show call history voice brief** command.

DETAILED STEPS

Step 1 Obtain the call ID by using the **show call active voice compact** command in privileged EXEC mode.

Example:

```
Router# show call active voice compact

G<id> A/O FAX T<sec> Codec type Peer Address IP R<ip>:<udp>
Total call-legs: 2
G11D6 ORG T187 g729r8 TELE P
G11D6 ORG T0 g729r8 VOIP P 192.0.2.1:19324
```

Step 2 Check the status of active calls using the call ID obtained from the **show call active voice brief** command.

Example:

```
Router# show call active voice brief id 11D6

<ID>: <CallID> <start>.<index> +<connect> pid:<peer_id> <dir> <addr> <state>
  dur hh:mm:ss tx:<packets>/<bytes> rx:<packets>/<bytes>
 IP <ip>:<udp> rtt:<time>ms pl:<play>/<gap>ms lost:<lost>/<early>/<late>
  delay:<last>/<min>/<max>ms <codec>

 media inactive detected:<y/n> media cntrl rcvd:<y/n> timestamp:<time>

 long duration call detected:<y/n> long duration call duration :<sec> timestamp:<time>
  MODEMPASS <method> buf:<fills>/<drains> loss <overall%> <multipkt>/<corrected>
   last <buf event time>s dur:<Min>/<Max>s
 FR <protocol> [int dlci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
  <codec> (payload size)
 ATM <protocol> [int vpi/vci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
  <codec> (payload size)
 Tele <int> (callID) [channel_id] tx:<tot>/<v>/<fax>ms <codec> noise:<l> acom:<l> i/o:<l>/<l> dBm
  MODEMRELAY info:<rcvd>/<sent>/<resent> xid:<rcvd>/<sent> total:<rcvd>/<sent>/<drops>
```

```
        speeds(bps): local <rx>/<tx> remote <rx>/<tx>
 Proxy <ip>:<audio udp>,<video udp>,<tcp0>,<tcp1>,<tcp2>,<tcp3> endpt: <type>/<manf>
 bw: <req>/<act> codec: <audio>/<video>
  tx: <audio pkts>/<audio bytes>,<video pkts>/<video bytes>,<t120 pkts>/<t120 bytes>
 rx: <audio pkts>/<audio bytes>,<video pkts>/<video bytes>,<t120 pkts>/<t120 bytes>


Telephony call-legs: 0
SIP call-legs: 0
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 0
```

Step 3 Verify your configuration using the **show call history voice brief** command.

Example:

```
Router# show call history voice brief

<ID>: <CallID> <start>.<index> +<connect> +<disc> pid:<peer_id> <direction> <addr>
  dur hh:mm:ss tx:<packets>/<bytes> rx:<packets>/<bytes> <disc-cause>(<text>)
 IP <ip>:<udp> rtt:<time>ms pl:<play>/<gap>ms lost:<lost>/<early>/<late>
  delay:<last>/<min>/<max>ms <codec>

 media inactive detected:<y/n> media cntrl rcvd:<y/n> timestamp:<time>

 long duration call detected:<y/n> long duration call duration :<sec> timestamp:<time>
  MODEMPASS <method> buf:<fills>/<drains> loss <overall%> <multipkt>/<corrected>
   last <buf event time>s dur:<Min>/<Max>s
 FR <protocol> [int dlci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
  <codec> (payload size)
 ATM <protocol> [int vpi/vci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
  <codec> (payload size)
 Telephony <int> (callID) [channel_id] tx:<tot>/<voice>/<fax>ms <codec> noise:<lvl>dBm acom:<lvl>dBm

  MODEMRELAY info:<rcvd>/<sent>/<resent> xid:<rcvd>/<sent> total:<rcvd>/<sent>/<drops> disc:<cause
code>
             speeds(bps): local <rx>/<tx> remote <rx>/<tx>
 Proxy <ip>:<audio udp>,<video udp>,<tcp0>,<tcp1>,<tcp2>,<tcp3> endpt: <type>/<manf>
 bw: <req>/<act> codec: <audio>/<video>
  tx: <audio pkts>/<audio bytes>,<video pkts>/<video bytes>,<t120 pkts>/<t120 bytes>
 rx: <audio pkts>/<audio bytes>,<video pkts>/<video bytes>,<t120 pkts>/<t120 bytes>



Telephony call-legs: 0
SIP call-legs: 0
H323 call-legs: 0
Call agent controlled call-legs: 0
Total call-legs: 0
```

Configuration Examples for DSP Voice Quality Statistics in DLCX Messages

Example: Configuring DSP Voice Quality Statistics in DLCX Messages

The following example shows how to enable voice quality statistics reporting for MGCP:

```
Router> enable
Router# configure terminal
Router(config)# mgcp voice-quality-stats
Router(config)# end
```

The following example shows the voice quality parameters selected for **priority** 1:

```
Router(config)# mgcp voice-quality-stats priority 1

16:38:20.461771 192.0.2.1:2427 192.0.2.4:2427 MGCP..... -> 250 1133 OK
P: PS=0, OS=0, PR=0, OR=0, PL=0, JI=65, LA=0
DSP/TX: PK=118, SG=0, NS=1, DU=28860, VO=2350
DSP/RX: PK=0, SG=0, CF=0, RX=28860, VO=0, BS=0, LP=0, BP=0
DSP/PD: CU=65, MI=65, MA=65, CO=0, IJ=0
DSP/LE: TP=0, RP=0, TM=0, RM=0, BN=0, ER=0, AC=0
DSP/IN: CI=0, FM=0, FP =0, VS=0, GT=0, GR=0, JD=0, JN=0, JM=0,
DSP/CR: CR=0, MN=0, CT=0, TT=0,
DSP/DC: DC=0,
DSP/CS: CS=0, SC=0, TS=0,
DSP/UC: U1=0, U2=0, T1=0, T2=0
```

The following example shows the voice quality parameters selected for the **all** keyword:

```
Router(config)# mgcp voice-quality-stats all

16:38:20.461771 192.0.2.1:2427 192.0.2.4:2427 MGCP..... -> 250 1133 OK
P: PS=0, OS=0, PR=0, OR=0, PL=0, JI=65, LA=0
DSP/TX: PK=118, SG=0, NS=1, DU=28860, VO=2350
DSP/RX: PK=0, SG=0, CF=0, RX=28860, VO=0, BS=0, LP=0, BP=0
DSP/PD: CU=65, MI=65, MA=65, CO=0, IJ=0
DSP/PE: PC=0, IC=0, SC=0, RM=0, BO=0, EE=0
DSP/LE: TP=0, RP=0, TM=0, RM=0, BN=0, ER=0, AC=0
DSP/ER: RD=0, TD=0, RC=0, TC=0
DSP/IC: IC=0
DSP/EC: CI=0, FM=0, FP =0, VS=0, GT=0, GR=0, JD=0, JN=0, JM=0, JX=0,
DSP/KF: KF=0, AV=0, MI=0, BS=0, NB=0, FL=0,
DSP/CS: CR=0, AV=0, MN=0, MX=0, CS=0, SC=0, TS=0, DC=0,
DSP/RF: ML=0, MC=0, R1=0, R2=0, IF=0, ID=0, IE=0, BL=0, R0=0,
DSP/UC: U1=0, U2=0, T1=0, T2=0,
DSP/DL: RT=0, ED=0
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Voice commands	• Cisco IOS Voice Command Reference-A through C • Cisco IOS Voice Command Reference-D through I • Cisco IOS Voice Command Reference-K through R • Cisco IOS Voice Command Reference-S commands • Cisco IOS Voice Command Reference-T through Z
How to configure QoS for Cisco features	Cisco IOS Quality of Service Configuration Guide
Cisco MGC documentation index	*Cisco Media Gateway Controllers*
How to configure MGCP	Configuring Media Gateway Protocol and Related Protocols
How to configure QoS for voice applications	Configuring Quality of Service for Voice
How to configure voice ports	Configuring Voice Ports
Enabling basic management protocols on Cisco access platforms	*Enabling Management Protocols: NTP, SNMP, and Syslog*
Release Notes, Cisco IOS Release 12.3	*Release Notes Index, Cisco IOS Release 12.3*

Standards and RFCs

Standard/RFC	Title
No new or modified standards or RFCs are supported by this feature, and support for existing standards or RFCs has not been modified by this feature.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for DLCP Voice Quality Statistics in DLCX Messages

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 11: Feature Information for DLCP Voice Quality in DLCX Messages

Feature Name	Releases	Feature Information
DSP Voice Quality Statistics in DLCX Messages	12.3(3) 12.4(4)T 15.1(3)T	The DSP Voice Quality Statistics in DLCX Messages feature provides a way to trace a Media Gateway Control Protocol (MGCP) call between a Cisco PGW 2200 and the Cisco IOS gateway by including the MGCP call ID and the DS0 and digital signal processor (DSP) channel ID in call-active and call-history records. In Cisco IOS Release 12.4(4)T, new voice quality parameters were introduced. The following commands were introduced or modified: **debug mgcp**, **mgcp voice-quality stats**.

INDEX