Cisco Unified Communications Manager and Interoperability Configuration Guide, Cisco IOS XE Release 3S

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

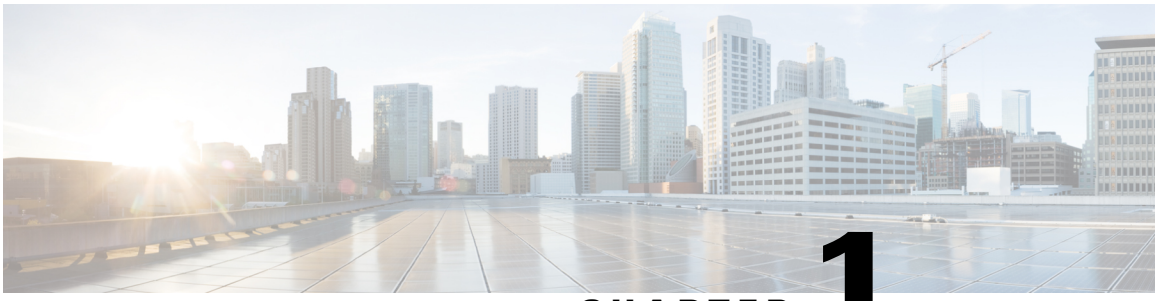
IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2015 Cisco Systems, Inc. All rights reserved.

CONTENTS



CHAPTER 1

VoIP for IPv6

This document describes VoIP in IPv6 (VoIPv6), a feature that adds IPv6 capability to existing VoIP features. This feature adds dual-stack (IPv4 and IPv6) support on voice gateways and media termination points (MTPs), IPv6 support for Session Initiation Protocol (SIP) trunks, and support for Skinny Client Control Protocol (SCCP)-controlled analog voice gateways. In addition, the Session Border Controller (SBC) functionality of connecting a SIP IPv4 or H.323 IPv4 network to a SIP IPv6 network is implemented on a Cisco UBE to facilitate migration from VoIPv4 to VoIPv6.

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 VoIP for IPv6

- Cisco Express Forwarding for IPv6 must be enabled.

- Virtual routing and forwarding (VRF) is not supported in IPv6 calls.

Cisco Unified Border Element

- Cisco IOS Release 12.4(22)T or a later release must be installed and running on your Cisco UBE.

Cisco Unified Border Element (Enterprise)

- Cisco IOS XE Release 3.3S or a later release must be installed and running on your Cisco ASR 1000 Series Router.

Restrictions for Implementing VoIP for IPv6

The following are the restrictions for Cisco UBE features:

Media Flow–Through

- Video call flows with Alternative Network Address Types (ANAT) are not supported.
- WebEx call flow with ANAT are not supported (Cisco UBE does not support ANAT on Video and Application media types).

SDP Pass-Through

- Supports only Early Offer (EO)–Early Offer (EO) and Delayed Offer (DO)–Delayed Offer (DO) call flows.
- Delayed Offer–Early Offer call flow falls back to Delayed Offer–Delayed Offer call flow.
- Supplementary services are not supported on SDP Pass-Through.
- Transcoding and DTMF interworking are not supported.

Note The above SDP Pass–Through restrictions are applicable for both IPv4 and IPv6.

- SDP Pass–Through does not support the dual-stack functionality.
- ANAT call flows does not support IPv4-to-IPv6 and IPv6-to-IPv4 Media interworking.

UDP Checksum

- CEF and process options are not supported on ASR1000 series routers.
- None option is partially supported on ISR–G2.

Media Anti–Trombone

- Media Anti–Trombone is not enabled if the initial call before tromboning is in Flow–Around (FA) mode.
- Media Anti–Trombone supports only symmetric media address type interworking (IPv4-IPv4 or IPv6-IPv6 media) with or without ANAT.

- Does not provide support for IPv4-IPv6 interworking cases with or without ANAT because Cisco UBE cannot operate in FA mode post tromboning.

Information About VoIP for IPv6

SIP Features Supported on IPv6

The Session Initiation Protocol (SIP) is an alternative protocol developed by the Internet Engineering Task Force (IETF) for multimedia conferencing over IP.

The Cisco SIP functionality enables Cisco access platforms to signal the setup of voice and multimedia calls over IP networks. SIP features also provide advantages in the following areas:

- Protocol extensibility
- System scalability
- Personal mobility services
- Interoperability with different vendors

A SIP User Agent (UA) operates in one of the following three modes:

- IPv4-only: Communication with only IPv6 UA is unavailable.
- IPv6-only: Communication with only IPv4 UA is unavailable.
- Dual-stack: Communication with only IPv4, only IPv6 and dual-stack UAs are available.

Dual-stack SIP UAs use Alternative Network Address Transport (ANAT) grouping semantics:

- Includes both IPv4 and IPv6 addresses in the Session Description Protocol (SDP).
- Is automatically enabled in dual-stack mode (can be disabled if required).
- Requires media to be bound to an interface that have both IPv4 and IPv6 addresses.
- Described in RFC 4091 and RFC 4092 (RFC 5888 describes general SDP grouping framework).

SIP UAs use “sdp-anat” option tag in the Required and Supported SIP header fields:

- Early Offer (EO) INVITE using ANAT semantics places “sdp-anat” in the Require header.
- Delayed Offer (DO) INVITE places “sdp-anat” in the Supported header.

SIP Signaling and Media Address Selection:

- Source address for SIP signaling is selected based on the destination signaling address type configured in the session-target of the outbound dial-peer:
  - If signaling bind is configured, source SIP signaling address is chosen from the bound interface.
  - If signaling bind is not configured, source SIP signaling address is chosen based on the best address in the UA to reach the destination signaling address.

SDP may or may not use ANAT semantics:

- When ANAT is used, media addresses in SDP are chosen from the interface media that is configured. When ANAT is not used, media addresses in SDP are chosen from the interface media that is configured OR based on the best address to reach the destination signaling address (when no media bind is configured).

VoIPv6 Support on Cisco UBE

Cisco UBE in VoIPv6 adds IPv6 capability to VoIP features. This feature adds dual-stack support on voice gateways, IPv6 support for SIP trunks, support for SCCP-controlled analog voice gateways, support for real-time control protocol (RTCP) pass-through, and support for T.38 fax over IPv6.

For more information on these features, refer to the following:

- "Configuring Cisco IOS Gateways" section in the Deploying IPv6 in Unified Communications Networks with Cisco Unified Communications Manager
- "Trunks" section in Deploying IPv6 in Unified Communications Networks with Cisco Unified Communications Manager
- "SCCP-controlled analog voice gateways" section in the SCCP Controlled Analog (FXS) Ports with Supplementary Features in Cisco IOS Gateways
- "RTCP Pass-Through" section in Cisco UBE RTCP Voice Pass-Through for IPv6
- "T.38 fax over IPv6" section in Fax, Modem, and Text Support over IP Configuration Guide

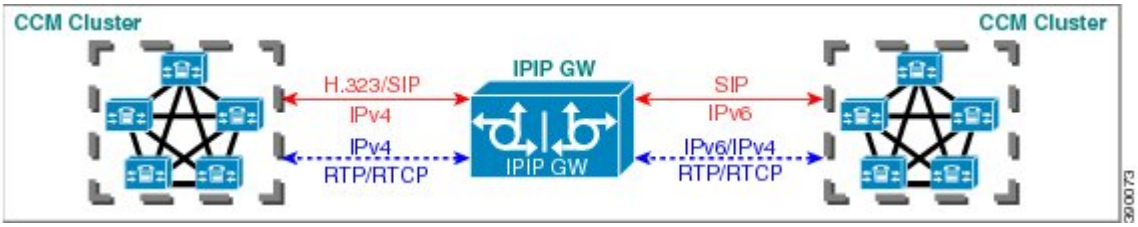
Support has been added for audio calls in media Flow–Through (FT) and Flow–Around (FA) modes, High Density (HD) transcoding, Local Transcoding Interface (LTI), along with Voice Class Codec (VCC) support, support for Hold/Resume, REFER, re-INVITE, 302 based services, and support for media anti-trombone have been added to Cisco UBE.

Cisco UBE being a signaling proxy processes all signaling messages for setting up media channels. This enables Cisco UBE to affect the flow of media packets using the media flow-through and the media flow-around modes.

- Media FT and Media FA modes support the following call flows:
  - EO–to–EO
  - DO–to–DO
  - DO–to–EO

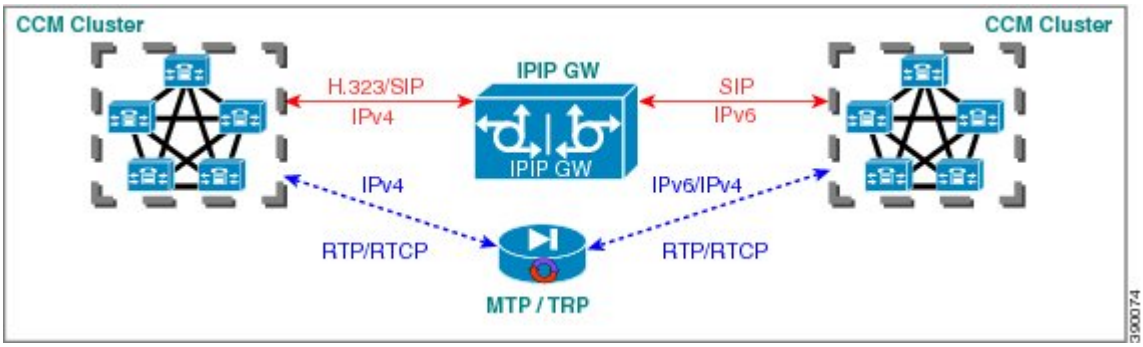
- **Media Flow-Through (FT)**: In a media flow–through mode, between two endpoints, both signaling and media flows through the IP-to-IP Gateway (IPIP GW). The IPIP GW performs both signaling and media interworking between H.323/SIP IPv4 and SIP IPv6 networks.

Figure 1: H.323/SIP IPv4 – SIP IPv6 interworking in media flow-through mode



- **Media Flow-Around (FA)**: Media flow–around provides the ability to have a SIP video call whereby signaling passes through Cisco UBE and media pass directly between endpoints bypassing the Cisco UBE.

Figure 2: H.323/SIP IPv4 - SIP IPv6 interworking in media flow-around mode



- **Assisted RTCP (RTCP Keepalive)**: Assisted Real-time Transport Control Protocol (RTCP) enables Cisco UBE to generate RTCP keepalive reports on behalf of endpoints; however, endpoints, such as second generation Cisco IP phones (7940/7960) and Nortel Media Gateways (MG 1000T) do not generate any RTCP keepalive reports. Assisted RTCPs enable customers to use Cisco UBE to interoperate between endpoints and call control agents, such as Microsoft OCS/Lync so that RTCP reports are generated to indicate session liveliness during periods of prolonged silence, such as call hold or call on mute.

  The assisted RTCP feature helps Cisco UBE to generate standard RTCP keepalive reports on behalf of endpoints. RTCP reports determine the liveliness of a media session during prolonged periods of silence, such as a call on hold or a call on mute.

- **SDP Pass–Through**: SDP is configured to pass through transparently at the Cisco UBE, so that both the remote ends can negotiate media independently of the Cisco UBE.

  SDP pass-through is addressed in two modes:

  - Flow-through—Cisco UBE plays no role in the media negotiation, it blindly terminates and re-originates the RTP packets irrespective of the content type negotiated by both the ends. This supports address hiding and NAT traversal.

- Flow-around—Cisco UBE neither plays a part in media negotiation, nor does it terminate and re-originate media. Media negotiation and media exchange is completely end-to-end.

For more information, refer to the "Configurable Pass-through of SIP INVITE Parameters" section in the Cisco Unified Border Element SIP Support Configuration Guide.

- **UDP Checksum for IPv6**: User Datagram Protocol (UDP) checksums provide data integrity for addressing different functions at the source and destination of the datagram, when a UDP packet originates from an IPv6 node.
- **IP Toll Fraud**:The IP Toll Fraud feature checks the source IP address of the call setup before routing the call. If the source IP address does not match an explicit entry in the configuration as a trusted VoIP source, the call is rejected.

  For more information, refer to the "Configuring Toll Fraud Prevention" section in the Cisco Unified Communications Manager Express System Administrator Guide.
- **RTP Port Range**: Provides the capability where the port range is managed per IP address range. This features solves the problem of limited number of rtp ports for more than 4000 calls. It enables combination of an IP address and a port as a unique identification for each call.
- **Hold/Resume**: Cisco UBE supports supplementary services such as Call Hold and Resume. An active call can be put in held state and later the call can be resumed.

  For more information, refer to the "Configuring Call Hold/Resume for Shared Lines for Analog Ports" section in Supplementary Services Features for FXS Ports on Cisco IOS Voice Gateways Configuration Guide.
- **Call Transfer (re-INVITE, REFER)**: Call transfer is used for conference calling, where calls can transition smoothly between multiple point-to-point links and IP level multicasting.

  For more information, refer to the "Configurable Pass-through of SIP INVITE Parameters" section in the Cisco Unified Border Element SIP Support Configuration Guide.
- **Call Forward (302 based)**: SIP provides a mechanism for forwarding or redirecting incoming calls. A Universal Access Servers (UAS) can redirect an incoming INVITE by responding with a 302 message (moved temporarily).

  - Consumption of 302 at stack level is supported for EO-EO, DO-DO and DO-EO calls for all combination of IPv4/IPv6/ANAT.
  - Consumption of 302 at stack level is supported for both FT and FA calls.

  For more information, refer to the " Configuring Call Transfer and Forwarding" section in Cisco Unified Communications Manager Express System Administrator Guide.
- **Media Antitrombone**: Antitromboning is a media signaling service in SIP entity to overcome the media loops. Media Trombones are media loops in a SIP entity due to call transfer or call forward. Media loops in Cisco UBE are not detected because Cisco UBE looks at both call types as individual calls and not calls related to each other.

  Antitrombone service has to be enabled only when no media interworking is required in both legs. Media antitrombone is supported only when the initial call is in IPv4 to IPv4 or IPv6 to IPv6 mode only.

  For more information, refer to the "Configuring Media Antitrombone" section in the Cisco Unified Border Element Protocol-Independent Features and Setup Configuration Guide.

- **RE-INVITE Consumption**: The Re-INVITE/UPDATE consumption feature helps to avoid interoperability issues by consuming the mid-call Re-INVITEs/UPDATEs from Cisco UBE. As Cisco UBE blocks RE-INVITE / mid-call UPDATE, remote participant is not made aware of the SDP changes, such as Call Hold, Call Resume, and Call transfer.

  For more information, refer to the "Cisco UBE Mid-call Re-INVITE/UPDATE Consumption" section in the Cisco Unified Border Element Protocol-Independent Features and Setup Configuration Guide.

- **Address Hiding**: The address hiding feature ensures that the Cisco UBE is the only point of signaling and media entry/exit in all scenarios. When you configure address-hiding, signaling and media peer addresses are also hidden from the endpoints, especially for supplementary services when the Cisco UBE passes REFER/3xx messages from one leg to the other.

  For more information, refer to the "Configuring Address Hiding" section in the SIP-to-SIP Connections on a Cisco Unified Border Element.

- **Header Passing**: Header Pass through enables header passing for SIP INVITE, SUBSCRIBE and NOTIFY messages; disabling header passing affects only incoming INVITE messages. Enabling header passing results in a slight increase in memory and CPU utilization.

  For more information, refer to the "SIP-to-SIP Connections on a Cisco Unified Border Element" section in the SIP-to-SIPConnections on Cisco Unified Border Element.

- **Refer–To Passing**: The Refer-to Passing feature is enabled when you configure refer-to-passing in Refer Pass through mode and the supplementary service SIP Refer is already configured. This enables the received refer-to header in Refer Pass through mode to move to the outbound leg without any modification. However, when refer-to-passing is configured in Refer Consumption mode without configuring the supplementary-service SIP Refer, the received Refer-to URI is used in the request-URI of the triggered invite.

  For more information, refer to the "Configuring Support for Dynamic REFER Handling on Cisco UBE" section in the Cisco Unified Border Element SIP Configuration Guide.

- **Error Pass-through**: The SIP error message pass through feature allows a received error response from one SIP leg to pass transparently over to another SIP leg. This functionality will pass SIP error responses that are not yet supported on the Cisco UBE or will preserve the Q.850 cause code across two sip call-legs.

  For more information, refer to the "Configuring SIP Error Message Passthrough" section in the Cisco Unified Border Element SIP Support Configuration Guide.

- **SIP UPDATE Interworking**: The SIP UPDATE feature allows a client to update parameters of a session (such as, a set of media streams and their codecs) but has no impact on the state of a dialog. UPDATE with SDP will support SDP Pass through, media flow around and media flow through. UPDATE with SDP support for SIP to SIP call flows is supported in the following scenarios:

  - Early Dialog SIP to SIP media changes.
  - Mid Dialog SIP to SIP media changes.

  For more information, refer to the "SIP UPDATE Message per RFC 3311" section in the Cisco Unified Border Element SIP Support Configuration Guide.

- **SIP OPTIONS Ping**: The OPTIONS ping mechanism monitors the status of a remote Session Initiation Protocol (SIP) server, proxy or endpoints. Cisco UBE monitors these endpoints periodically.

  For more information, refer to the "Cisco UBE Out-of-dialog OPTIONS Ping for Specified SIP Servers or Endpoints" section in the Configuration of SIP Trunking for PSTN Access (SIP-to-SIP) Configuration Guide.

- **Configurable Error Response Code in OPTIONS Ping**: Cisco UBE provides an option to configure the error response code when a dial peer is busied out because of an Out-of-Dialog OPTIONS ping failure.

  For more information, refer to the "Configuring an Error Response Code upon an Out-of-Dialog OPTIONS Ping Failure" section in the Cisco Unified Border Element SIP Support Configuration Guide.

- **SIP Profiles**: SIP profiles create a set of provisioning properties that you can apply to SIP trunk.

- **Dynamic Payload Type Interworking (DTMF and Codec Packets)**: The Dynamic Payload Type Interworking for DTMF and Codec Packets for SIP-to-SIP Calls feature provides dynamic payload type interworking for dual tone multifrequency (DTMF) and codec packets for Session Initiation Protocol (SIP) to SIP calls. The Cisco UBE interworks between different dynamic payload type values across the call legs for the same codec. Also, Cisco UBE supports any payload type value for audio, video, named signaling events (NSEs), and named telephone events (NTEs) in the dynamic payload type range 96 to 127.

  For more information, refer to the "Dynamic Payload Type Interworking for DTMF and Codec Packets for SIP-to-SIP Calls" section in the Cisco Unified Border Element (Enterprise) Protocol-Independent Features and Setup Configuration Guide.

- **Audio Transcoding using Local Transcoding Interface (LTI)**: Local Transcoding Interface (LTI) is an interface created to remove the requirement of SCCP client for Cisco UBE transcoding.

  For information, refer to Cisco Unified Border Element 9.0 Local Transcoding Interface (LTI).

- **Voice Class Codec (VCC) with or without Transcoding**: The Voice Class Codec feature supports basic and all Re-Invite based supplementary services like call-hold/resume, call forward, call transfer, where if any mid-call codec changes, Cisco UBE inserts/removes/modifies the transcoder as needed.

  Support for negotiation of an Audio Codec on each leg of a SIP–SIP call on the Cisco UBE feature supports negotiation of an audio codec using the Voice Class Codec (VCC) infrastructure on Cisco UBE.

  VCC supports SIP-SIP calls on Cisco UBE and allows mid-call codec change for supplementary services.

SIP Voice Gateways in VoIPv6

Session Initiation Protocol (SIP) is a simple, ASCII-based protocol that uses requests and responses to establish communication among the various components in the network and to ultimately establish a conference between two or more endpoints.

In addition to the already existing features that are supported on IPv4 and IPv6, the SIP Voice Gateways support the following features:

- **History–Info**: The SIP History–info Header Support feature provides support for the history-info header in SIP INVITE messages only. The SIP gateway generates history information in the INVITE message for all forwarded and transferred calls. The history-info header records the call or dialog history. The receiving application uses the history-info header information to determine how and why the call has reached it.

  For more information, refer to the "SIP History INFO" section in the Cisco Unified Border Element (Enterprise) SIP Support Configuration Guide.

- **Handling 181/183 Responses with/without SDP**: The Handling 181/183 Responses with/without SDP feature provides support for SIP 181 (Call is Being Forwarded) and SIP 183 (Session Progress) messages

either globally or on a specific dial-peer. Also, you can control when the specified SIP message is dropped based on either the absence or presence of SDP information.

For more information, refer to "SIP–Enhanced 180 Provisional Response Handling" section in the Cisco Unified Border Element Configuration Guide.

- **Limiting the Rate of Incoming SIP Calls per Dial-Peer (Call Spike)**: The call rate-limiting feature for incoming SIP calls starts working after a switch over in a SIP call. The rate–limiting is done for new calls received on the new Active. The IOS timers that track the call rate limits runs on active and standby mode and does not require any checkpoint. However, some statistics for calls rejected requires to be checked for the show commands to be consistent before and after the switchover.
- **PPI/PAI/Privacy and RPID Passing**: For incoming SIP requests or response messages, when the PAI or PPI privacy header is set, the SIP gateway builds the PAI or PPI header into the common SIP stack, thereby providing support to handle the call data present in the PAI or PPI header. For outgoing SIP requests or response messages, when the PAI or PPI privacy header is set, privacy information is sent using the PAI or PPI header.

  For more information, refer to the "Support for PAID PPID Privacy PCPID and PAURI Headers on Cisco UBE" section in the Cisco Unified Border Element SIP Support Configuration Guide.
- **SIP VMWI for FXS phones**: SIP provides visible message waiting indication (VMWI) on FXS phones. This feature provides users with the option to enable one message waiting indication (MWI): audible, visible, or both. The VMWI mechanism uses SIP Subscribe or Notify to get MWI updates from a virtual machine (VM) system, and then forwards updates to the FXS phone on the port.

  For more information, refer to the "Configuring SIP MWI Features" section in the SIP Configuration Guide.
- **SIP Session timer (RFC 4028)**: This feature allows for a periodic refresh of SIP sessions through a re-INVITE or UPDATE request. The refresh allows both user agents and proxies to determine whether the SIP session is still active. Two header fields can be defined: Session-Expires, which conveys the lifetime of the session, and Min-SE, which conveys the minimum allowed value for the session timer.

  For more information, refer to the "SIP Session Timer Support" section in the Cisco Unified Border Element SIP Support Configuration Guide.
- **SIP Media Inactivity Detection**: The SIP Media Inactivity Detection Timer feature enables Cisco gateways to monitor and disconnect VoIP calls if no Real-Time Control Protocol (RTCP) packets are received within a configurable time period.

  For more information, refer to the SIP Media Inactivity Timer section.

The SIP Voice Gateways feature is supported for analog endpoints that are connected to Foreign Exchange Station (FXS) ports or a Cisco VG224 Analog Phone Gateway and controlled by a Cisco call-control system, such as a Cisco Unified Communications Manager (Cisco Unified CM) or a Cisco Unified Communications Manager Express (Cisco Unified CME).

For more information on SIP Gateway features and information about configuring the SIP voice gateway for VoIPv6, see the Configuring VoIP for IPv6.

SIP Voice Gateways in VoIPv6

SIP is a simple, ASCII-based protocol that uses requests and responses to establish communication among the various components in the network and to ultimately establish a conference between two or more endpoints.

For further information about this feature and information about configuring the SIP voice gateway for VoIPv6, see the Configuring VoIP for IPv6, on page 10.

How to Configure VoIP for IPv6

Configuring VoIP for IPv6

SIP is a simple, ASCII-based protocol that uses requests and responses to establish communication among the various components in the network and to ultimately establish a conference between two or more endpoints.

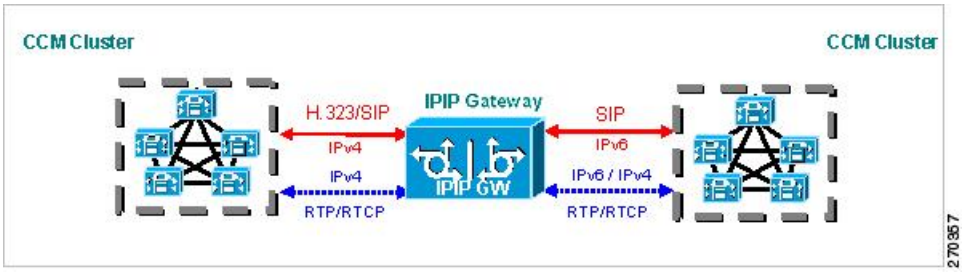
Users in a SIP network are identified by unique SIP addresses. A SIP address is similar to an e-mail address and is in the format of sip:userID@gateway.com. The user ID can be either a username or an E.164 address. The gateway can be either a domain (with or without a hostname) or a specific Internet IPv4 or IPv6 address.

A SIP trunk can operate in one of three modes: SIP trunk in IPv4-only mode, SIP trunk in IPv6-only mode, and SIP trunk in dual-stack mode, which supports both IPv4 and IPv6.

A SIP trunk uses the Alternative Network Address Transport (ANAT) mechanism to exchange multiple IPv4 and IPv6 media addresses for the endpoints in a session. ANAT is automatically enabled on SIP trunks in dual-stack mode. The ANAT Session Description Protocol (SDP) grouping framework allows user agents (UAs) to include both IPv4 and IPv6 addresses in their SDP session descriptions. The UA is then able to use any of its media addresses to establish a media session with a remote UA.

A Cisco Unified Border Element can interoperate between H.323/SIP IPv4 and SIP IPv6 networks in media flow-through mode. In media flow-through mode, both signaling and media flows through the Cisco Unified Border Element, and the Cisco Unified Border Element performs both signaling and media interoperation between H.323/SIP IPv4 and SIP IPv6 networks (see the figure below).

Figure 3: H.323/SIP IPv4--SIP IPv6 Interoperating in Media Flow-Through Mode



Shutting Down or Enabling VoIPv6 Service on Cisco Gateways

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **shutdown** [**forced**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**voice service voip** **Example:** `Device(config)# voice service voip`	Enters voice service VoIP configuration mode.
Step 4	**shutdown** [**forced**] **Example:** `Device(config-voi-serv)# shutdown forced`	Shuts down or enables VoIP call services.

Shutting Down or Enabling VoIPv6 Submodes on Cisco Gateways

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **sip**
5. **call service stop** [**forced**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Device> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**voice service voip** **Example:** `Device(config)# voice service voip`	Enters voice service VoIP configuration mode.
Step 4	**sip** **Example:** `Device(config-voi-serv)# sip`	Enters SIP configuration mode.
Step 5	**call service stop** [**forced**] **Example:** `Device(config-serv-sip)# call service stop`	Shuts down or enables VoIPv6 for the selected submode.

Configuring the Protocol Mode of the SIP Stack

Before You Begin

SIP service should be shut down before configuring the protocol mode. After configuring the protocol mode as IPv6, IPv4, or dual-stack, SIP service should be reenabled.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **sip-ua**
4. **protocol mode ipv4 | ipv6 | dual-stack** [**preference** {**ipv4** | **ipv6**}]}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**sip-ua** **Example:** `Device(config)# sip-ua`	Enters SIP user agent configuration mode.
Step 4	**protocol mode ipv4** | **ipv6** | **dual-stack** [**preference** {**ipv4** | **ipv6**}]} **Example:** `Device(config-sip-ua)# protocol mode dual-stack`	Configures the Cisco IOS SIP stack in dual-stack mode.

Example: Configuring the SIP Trunk

This example shows how to configure the SIP trunk to use dual-stack mode, with IPv6 as the preferred mode. The SIP service must be shut down before any changes are made to protocol mode configuration.

```
Device(config)# sip-ua
Device(config-sip-ua)# protocol mode dual-stack preference ipv6
```

Disabling ANAT Mode

ANAT is automatically enabled on SIP trunks in dual-stack mode. Perform this task to disable ANAT in order to use a single-stack mode.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **sip**
5. **no anat**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**voice service voip** **Example:** `Device(config)# voice service voip`	Enters voice service VoIP configuration mode.
Step 4	**sip** **Example:** `Device(config-voi-serv)# sip`	Enters SIP configuration mode.
Step 5	**no anat** **Example:** `Device(conf-serv-sip)# no anat`	Disables ANAT on a SIP trunk.

Configuring the Source IPv6 Address of Signaling and Media Packets

Users can configure the source IPv4 or IPv6 address of signaling and media packets to a specific interface's IPv4 or IPv6 address. Thus, the address that goes out on the packet is bound to the IPv4 or IPv6 address of the interface specified with the **bind** command.

The **bind** command also can be configured with one IPv6 address to force the gateway to use the configured address when the bind interface has multiple IPv6 addresses. The bind interface should have both IPv4 and IPv6 addresses to send out ANAT.

When you do not specify a bind address or if the interface is down, the IP layer still provides the best local address.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **sip**
5. **bind** {**control** | **media** | **all**} **source interface** *interface-id* [**ipv6-address** *ipv6-address*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**voice service voip** **Example:** `Device(config)# voice service voip`	Enters voice service VoIP configuration mode.
Step 4	**sip** **Example:** `Device(config-voi-serv)# sip`	Enters SIP configuration mode.
Step 5	**bind** {**control** | **media** | **all**} **source interface** *interface-id* [**ipv6-address** *ipv6-address*] **Example:** `Device(config-serv-sip)# bind control source-interface FastEthernet 0/0`	Binds the source address for signaling and media packets to the IPv6 address of a specific interface.

Example: Configuring the Source IPv6 Address of Signaling and Media Packets

```
Device(config)# voice service voip
Device(config-voi-serv)# sip
Device(config-serv-sip)# bind control source-interface fastEthernet 0/0
```

Configuring the SIP Server

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **sip-ua**
4. sip-server {**dns:** *host-name*] | **ipv4:** *ipv4–address* | **ipv6:** [**ipv6-address**] **:**[*port-nums*]}
5. **keepalive target** {{**ipv4 :** *address* | **ipv6 :** *address*}[**:** *port*] | **dns :** *hostname*} [**tcp** [**tls**]] | **udp**] [**secondary**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**sip-ua** **Example:** `Device(config)# sip-ua`	Enters SIP user agent configuration mode.
Step 4	sip-server {**dns:** *host-name*] | **ipv4:** *ipv4–address* | **ipv6:** [**ipv6-address**] **:**[*port-nums*]} **Example:** `Device(config-sip-ua)# sip-server ipv6: 2001:DB8:0:0:8:800:200C:417A`	Configures a network address for the SIP server interface.
Step 5	**keepalive target** {{**ipv4 :** *address* | **ipv6 :** *address*}[**:** *port*] | **dns :** *hostname*} [**tcp** [**tls**]] | **udp**] [**secondary**] **Example:** `Device(config-sip-ua)# keepalive target ipv6: 2001:DB8:0:0:8:800:200C:417A`	Identifies SIP servers that will receive keepalive packets from the SIP gateway.

Example: Configuring the SIP Server

```
Device(config)# sip-ua
Device(config-sip-ua)# sip-server ipv6: 2001:DB8:0:0:8:800:200C:417A
```

Configuring the Session Target

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *tag* {**mmoip** | **pots** | **vofr** | **voip**}
4. **destination pattern** [+ *string* **T**
5. **session target** {**ipv4:** *destination-address*| **ipv6: [** *destination-address* **]**| **dns : s.** | **d.** | **e.** | **u.**] *host-name* | **enum:***table -num* | **loopback:rtp** | **ras**| **sip-server**} [**:** *port*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**dial-peer voice** *tag* {**mmoip**	**pots**	**vofr**	**voip**} **Example:** `Device(config)# dial-peer voice 29 voip`	Defines a particular dial peer, specifies the method of voice encapsulation, and enters dial peer configuration mode.
Step 4	**destination pattern** [+ *string* **T** **Example:** `Device(config-dial-peer)# destination-pattern 7777`	Specifies either the prefix or the full E.164 telephone number to be used for a dial peer.
Step 5	**session target** {**ipv4:** *destination-address*| **ipv6: [** *destination-address* **]**| **dns : s.**	**d.**	**e.**	**u.**] *host-name*	**enum:***table -num*	**loopback:rtp**	**ras**| **sip-server**} [**:** *port*	Designates a network-specific address to receive calls from a VoIP or VoIPv6 dial peer.

	Command or Action	Purpose
	Example: `Device(config-dial-peer)# session target ipv6:2001:DB8:0:0:8:800:200C:417A`	

Example: Configuring the Session Target

```
Device(config)# dial-peer voice 29 voip
Device(config-dial-peer)# destination-pattern 7777
Device(config-dial-peer)# session target ipv6:2001:DB8:0:0:8:800:200C:417A
```

Configuring SIP Register Support

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **sip-ua**
4. **registrar** {**dns:** *address* | **ipv4:** *destination-address* [**:** *port*] | **ipv6:** *destination-address* **:** *port*] } **aor-domain expires** *seconds* [**tcp tls**]] **type** [**secondary**] [**scheme** *string*]
5. **retry register** *retries*
6. **timers register** *milliseconds*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**sip-ua** **Example:** `Device(config)# sip-ua`	Enters SIP user agent configuration mode.

	Command or Action	Purpose
Step 4	**registrar** {**dns:** *address* | **ipv4:** *destination-address* [**:** *port*] | **ipv6:** *destination-address* **:** *port*] } **aor-domain expires** *seconds* [**tcp tls**]] **type** [**secondary**] [**scheme** *string*] **Example:** `Device(config-sip-ua)# registrar ipv6: 2001:DB8::1:20F:F7FF:FE0B:2972 expires 3600 secondary`	Enables SIP gateways to register E.164 numbers on behalf of analog telephone voice ports, IP phone virtual voice ports, and SCCP phones with an external SIP proxy or SIP registrar.
Step 5	**retry register** *retries* **Example:** `Device(config-sip-ua)# retry register 10`	Configures the total number of SIP register messages that the gateway should send.
Step 6	**timers register** *milliseconds* **Example:** `Device(config-sip-ua)# timers register 500`	Configures how long the SIP UA waits before sending register requests.

Example: Configuring SIP Register Support

```
Device(config)# sip-ua
Device(config-sip-ua)# registrar ipv6: 2001:DB8:0:0:8:800:200C:417A expires 3600 secondary
Device(config-sip-ua)# retry register 10
Device((config-sip-ua)# timers register 500
```

Configuring Outbound Proxy Server Globally on a SIP Gateway

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **sip**
5. **outbound-proxy** {**ipv4:** *ipv4-address* \| **ipv6:** *ipv6-address* \| **dns:** *host* **:** *domain*} [**:** *port-number*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Device> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**voice service voip** **Example:** `Device(config)# voice service voip`	Enters voice service VoIP configuration mode.
Step 4	**sip** **Example:** `Device(config-voi-serv)# sip`	Enters sip configuration mode.
Step 5	**outbound-proxy** {**ipv4:** *ipv4-address* | **ipv6:** *ipv6-address* | **dns:** *host* **:** *domain*} [**:** *port-number*] **Example:** `Device(config-serv-sip)#outbound-proxy ipv6: 2001:DB8:0:0:8:800:200C:417A`	Specifies the SIP outbound proxy globally for a Cisco IOS voice gateway using an IPv6 address.

Verifying SIP Gateway Status

Before You Begin

To verify the status of SIP Gateway, use the following commands

SUMMARY STEPS

1. **show sip-ua calls**
2. **show sip-ua connections**
3. **show sip-ua status**

DETAILED STEPS

Step 1 **show sip-ua calls**

The **show sip-ua calls** command displays active user agent client (UAC) and user agent server (UAS) information on SIP calls:

```
Device# show sip-ua calls
SIP UAC CALL INFO
 Call 1
 SIP Call ID : 8368ED08-1C2A11DD-80078908-BA2972D0@2001::21B:D4FF:FED7:B000
  State of the call       : STATE_ACTIVE (7)
  Substate of the call    : SUBSTATE_NONE (0)
  Calling Number          : 2000
  Called Number           : 1000
  Bit Flags               : 0xC04018 0x100 0x0
CC Call ID              : 2
   Source IP Address (Sig ): 2001:DB8:0:ABCD::1
   Destn SIP Req Addr:Port : 2001:DB8:0:0:FFFF:5060
   Destn SIP Resp Addr:Port: 2001:DB8:0:1:FFFF:5060
   Destination Name        : 2001::21B:D5FF:FE1D:6C00
   Number of Media Streams : 1
   Number of Active Streams: 1
   RTP Fork Object         : 0x0
   Media Mode              : flow-through
   Media Stream 1
     State of the stream      : STREAM_ACTIVE
     Stream Call ID           : 2
     Stream Type              : voice-only (0)
     Stream Media Addr Type   : 1709707780
     Negotiated Codec         :  (20 bytes)
     Codec Payload Type       : 18
     Negotiated Dtmf-relay    : inband-voice
     Dtmf-relay Payload Type  : 0
     Media Source IP Addr:Port: [2001::21B:D4FF:FED7:B000]:16504
     Media Dest IP Addr:Port  : [2001::21B:D5FF:FE1D:6C00]:19548
Options-Ping    ENABLED:NO    ACTIVE:NO
   Number of SIP User Agent Client(UAC) calls: 1
SIP UAS CALL INFO
   Number of SIP User Agent Server(UAS) calls: 0
```

Step 2 **show sip-ua connections**

Use the **show sip-ua connections** command to display SIP UA transport connection tables:

Example:

```
Device# show sip-ua connections udp brief
Total active connections      : 1
No. of send failures          : 0
No. of remote closures        : 0
No. of conn. failures         : 0
No. of inactive conn. ageouts : 0
Router# show sip-ua connections udp detail

Total active connections      : 1
No. of send failures          : 0
No. of remote closures        : 0
No. of conn. failures         : 0
No. of inactive conn. ageouts : 0
---------Printing Detailed Connection Report---------
Note:
```

```
 ** Tuples with no matching socket entry
    - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port>'
      to overcome this error condition
 ++ Tuples with mismatched address/port entry
    - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port> id <connid>'
      to overcome this error condition
Remote-Agent:2001::21B:D5FF:FE1D:6C00, Connections-Count:1
  Remote-Port Conn-Id Conn-State  WriteQ-Size
  =========== ======= =========== ===========
         5060       2 Established           0
```

Step 3 **show sip-ua status**

Use the **show sip-ua status** command to display the status of the SIP UA:

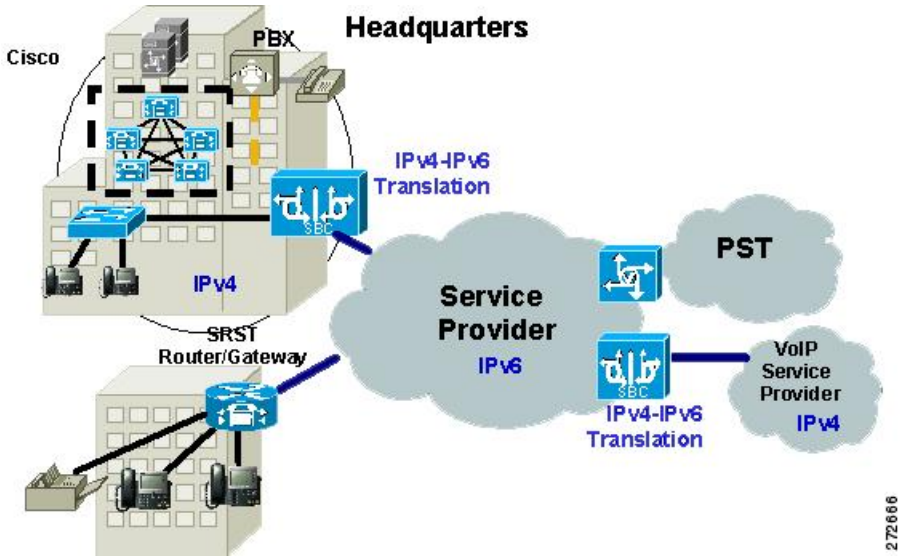
Example:

```
Device# show sip-ua status
SIP User Agent Status
SIP User Agent for UDP : ENABLED
SIP User Agent for TCP : ENABLED
SIP User Agent for TLS over TCP : ENABLED
SIP User Agent bind status(signaling): DISABLED
SIP User Agent bind status(media): DISABLED
SIP early-media for 180 responses with SDP: ENABLED
SIP max-forwards : 70
SIP DNS SRV version: 2 (rfc 2782)
NAT Settings for the SIP-UA
Role in SDP: NONE
Check media source packets: DISABLED
Maximum duration for a telephone-event in NOTIFYs: 2000 ms
SIP support for ISDN SUSPEND/RESUME: ENABLED
Redirection (3xx) message handling: ENABLED
Reason Header will override Response/Request Codes: DISABLED
Out-of-dialog Refer: DISABLED
Presence support is DISABLED
protocol mode is ipv6
SDP application configuration:
 Version line (v=) required
 Owner line (o=) required
 Timespec line (t=) required
 Media supported: audio video image
 Network types supported: IN
 Address types supported: IP4 IP6
 Transport types supported: RTP/AVP udptl
```

Configuring H.323 IPv4-to-SIPv6 Connections in a Cisco UBE

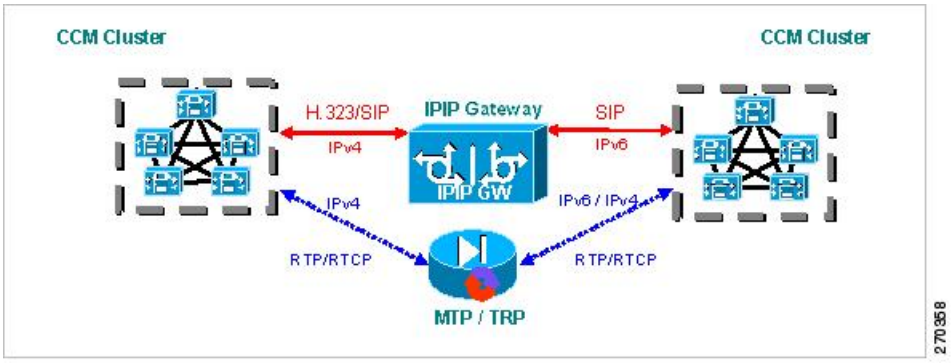
An organization with an IPv4 network can deploy a Cisco UBE on the boundary to connect with the service provider's IPv6 network (see the figure below).

Figure 4: Cisco UBE Interoperating IPv4 Networks with IPv6 Service Provider



A Cisco UBE can interoperate between H.323/SIP IPv4 and SIP IPv6 networks in media flow-through mode. In media flow-through mode, both signaling and media flows through the Cisco UBE, and the Cisco UBE performs both signaling and media interoperation between H.323/SIP IPv4 and SIP IPv6 networks (see the figure below).

Figure 5: IPv4 to IPv6 Media Interoperating Through Cisco IOS MTP



The Cisco UBE feature adds IPv6 capability to existing VoIP features. This feature adds dual-stack support on voice gateways and MTP, IPv6 support for SIP trunks, and SCCP-controlled analog voice gateways. In addition, the SBC functionality of connecting SIP IPv4 or H.323 IPv4 network to a SIP IPv6 network is implemented on an Cisco UBE to facilitate migration from VoIPv4 to VoIPv6.

Before You Begin

Cisco UBE must be configured in IPv6-only or dual-stack mode to support IPv6 calls.

Note A Cisco UBE interoperates between H.323/SIP IPv4 and SIP IPv6 networks only in media flow-through mode.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **allow-connections** *from type* **to** *to type*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**voice service voip** **Example:** `Device(config)# voice service voip`	Enters voice service VoIP configuration mode.
Step 4	**allow-connections** *from type* **to** *to type* **Example:** `Device(config-voi-serv)# allow-connections h323 to sip`	Allows connections between specific types of endpoints in a VoIPv6 network. Arguments are as follows: • *from-type* --Type of connection. Valid values: **h323**, **sip**. • *to-type* --Type of connection. Valid values: **h323**, **sip**.

Example: Configuring H.323 IPv4-to-SIPv6 Connections in a Cisco UBE

```
Device(config)# voice service voip
Device(config-voi-serv)# allow-connections h323 to sip
```

Troubleshooting Tips for VoIP for IPv6

Media Flow-Through

To enable all Session Initiation Protocol (SIP)-related debugging, use the **debug ccsip all** command in privileged EXEC mode.

To trace the execution path through the call control application programming interface (CCAPI), use the **debug voip ccapi inout** command.

Media Flow-Around

To enable all Session Initiation Protocol (SIP)-related debugging, use the **debug ccsip all** command.

To trace the execution path through the call control application programming interface (CCAPI), use the **debug voip ccapi inout** command.

SDP Pass-Through

To enable all Session Initiation Protocol (SIP)-related debugging (when the call is active in Pass through mode), use the **debug ccsip all** command.

RTP Port Range

To enable all Session Initiation Protocol (SIP)-related debugging, use the **debug ccsip all** command.

To enable debugging for Real-Time Transport Protocol (RTP) named event packets, use the **debug voip rtp** command.

VMWI SIP

To collect debug information only for signaling events, use the **debug vpm signal** command.

To show all Session Initiation Protocol (SIP) Service Provider Interface (SPI) message tracing, use the **debug ccsip messages** command.

Verifying Cisco UBE ANAT Call Flows

To verify that media settings are enabled in the media flowthrough and media flow-around feature, use the following commands:

SUMMARY STEPS

1. **show call active voice brief**
2. **show call active voice compact**
3. **show voip rtp connections**

DETAILED STEPS

Step 1 show call active voice brief

Example:

```
Device# show call active voice brief

<ID>: <CallID> <start>ms.<index> (<start>) +<connect> pid:<peer_id> <dir> <addr> <state>
  dur hh:mm:ss tx:<packets>/<bytes> rx:<packets>/<bytes> dscp:<packets violation> media:<packets
violation> audio tos:<audio tos value> video tos:<video tos value>
 IP <ip>:<udp> rtt:<time>ms pl:<play>/<gap>ms lost:<lost>/<early>/<late>
  delay:<last>/<min>/<max>ms <codec> <textrelay> <transcoded

 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>
 LostPacketRate:<%> OutOfOrderRate:<%>
  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: 2
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 2
0    : 987 361904110ms.1 (16:01:10.557 IST Tue May 14 2013) +530 pid:1 Answer 1005 connected
 dur 00:00:56 tx:1082/173120 rx:1141/182560 dscp:0 media:0 audio tos:0xB8 video tos:0x0
 IP 2001:1111:2222:3333:4444:5555:6666:1012:38356 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms
 g711ulaw TextRelay: off Transcoded: No
 media inactive detected:n media contrl rcvd:n/a timestamp:n/a
 long duration call detected:n long duration call duration:n/a timestamp:n/a
 LostPacketRate:0.00 OutOfOrderRate:0.00

0    : 988 361904120ms.1 (16:01:10.567 IST Tue May 14 2013) +510 pid:2 Originate 2005 connected
 dur 00:00:56 tx:1141/182560 rx:1082/173120 dscp:0 media:0 audio tos:0xB8 video tos:0x0
 IP 2001:1111:2222:3333:4444:5555:6666:1012:26827 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms
 g711ulaw TextRelay: off Transcoded: No
 media inactive detected:n media contrl rcvd:n/a timestamp:n/a
 long duration call detected:n long duration call duration:n/a timestamp:n/a
 LostPacketRate:0.00 OutOfOrderRate:0.00

Telephony call-legs: 0
SIP call-legs: 2
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 2

------------------------------------------------------------------------------
```

Step 2 show call active voice compact

Example:

```
Device# show call active voice compact

 <callID>  A/O FAX T<sec> Codec       type        Peer Address       IP R<ip>:<udp>
Total call-legs: 2
       987 ANS     T61    g711ulaw    VOIP        P1005 2001:......:1012:38356
       988 ORG     T61    g711ulaw    VOIP        P2005 2001:......:1012:26827
```

Step 3 **show voip rtp connections**

Example:

```
Device# show voip rtp connections

VoIP RTP Port Usage Information:
Max Ports Available: 24273, Ports Reserved: 303, Ports in Use: 2
Port range not configured, Min: 16384, Max: 32767
                                                 Ports       Ports       Ports
Media-Address Range                              Available   Reserved    In-use

Default Address-Range                            8091        101         0
2001::
2002::                                           8091        101         1
9.0.0.0             10.0.0.0                     8091        101         1
Found 2 active RTP connections
```

Feature Information for VoIP for IPv6

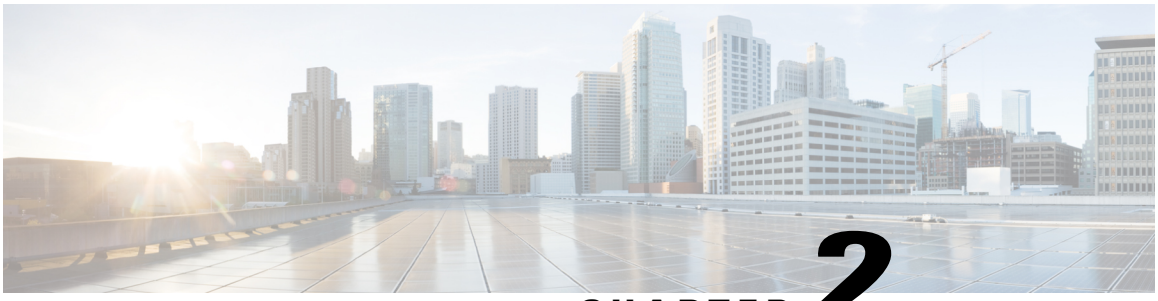
The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train 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 . An account on Cisco.com is not required.

Table 1: Feature Information for VoIP for IPv6

Feature Name	Releases	Feature Information
IPv6 Dual Stack	Cisco IOS XE Release 3.3S Cisco IOS XE Release 3.8S Cisco IOS XE Release 3.9S	Adds IPv6 capability to existing VoIP features on the Cisco Unified Border Element (Enterprise). Additionally, the SBC functionality of connecting SIP IPv4 or H.323 IPv4 network to SIP IPv6 network is implemented on a Cisco Unified Border Element to facilitate migration from VoIPv4 to VoIPv6. The following commands were introduced or modified: None

Feature Name	Releases	Feature Information
DSCP-Based QoS Support	Cisco IOS XE Release 3.9S	IPv6 supports this feature.
RTP/RTCP over IPv6	Cisco IOS Release XE 3.9S	RTP stack supports the ability to create IPv6 connections using IPv6 unicast and multicast addresses as well as IPV4 connections.



CHAPTER 2

Configuring MGCP Gateway Support

This chapter describes the basic tasks for configuring Cisco IOS MGCP gateways to interoperate with Cisco Unified Communications Manager.

Finding Support Information for Platforms and Cisco IOS Software Images

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 . You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

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

- "Overview of Cisco Unified Communications Manager and Cisco IOS Interoperability" on page 13 .
- 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 .

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

- Cisco IOS gateway is configured for VoIP.
- Voice interface card or network module is installed.
- Cisco Unified Communications Manager version 3.2 (formerly known as Cisco CallManager version 3.2) or later is used.
- Cisco Unified Communications Manager version 4.0 (formerly known as Cisco CallManager version 4.0) or later version is used.

Restrictions for Configuring MGCP Gateway Support

- Integrated access is not supported when you control voice traffic using MGCP and Cisco Unified Communications Manager. Integrated access is when the channels on a T1 or E1 interface are divided between a group used for voice and another group used for WAN access.
- T1 and E1 protocols, such as E1 R2, T1 FGD, and PRI NFAS, are not supported with MGCP.

Note Any configuration update that affects MGCP should be performed during a planned maintenance window while MGCP is disabled; otherwise, updating the configuration could disrupt MGCP functionality. Before making any configuration changes, disable MGCP using the **no mgcp** command. After all configuration changes are completed, use the **mgcp** command to enable MGCP.

Information about MGCP Gateway Support

MGCP Gateways and Cisco Unified Communications Manager

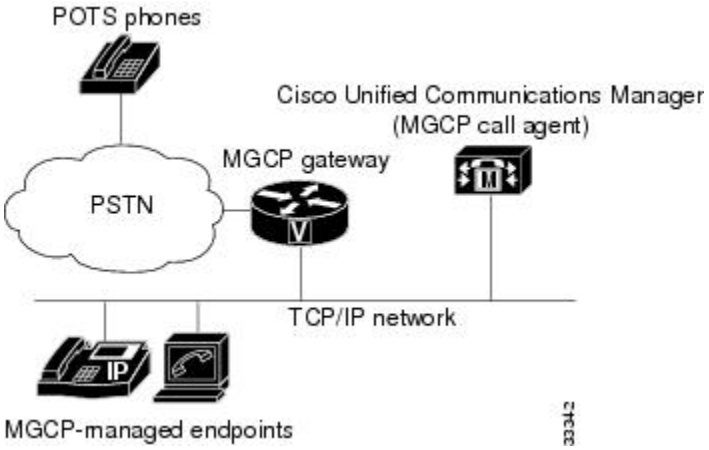
MGCP enables the remote control and management of voice and data communications devices at the edge of multiservice IP packet networks. Because of its centralized architecture, MGCP overcomes the distributed configuration and administration problems inherent in the use of protocols such as H.323. MGCP simplifies the configuration and administration of voice gateways and supports multiple (redundant) call agents, eliminating the potential for a single point of failure in controlling the Cisco IOS gateway in the network.

MGCP can be configured as a master or slave protocol to ensure that the gateway receives and executes the configuration, control, and management commands that are issued by Cisco Unified Communications Manager. The MGCP gateway is under the control of Cisco Unified Communications Manager.

MGCP uses endpoints and connections to construct a call. Endpoints are sources of or destinations for data and can be physical or logical locations identifying a device. The voice ports on the Cisco MGCP gateway are its endpoints. Connections can be point-to-point or multipoint. Cisco Unified Communications Manager acts as the MGCP call agent, managing connections between endpoints and controlling how the Cisco IOS gateway functions.

The figure below shows a typical MGCP gateway that is controlled by an MGCP call agent.

Figure 6: MGCP Gateway Controlled by Cisco Unified Communications Manager



The MGCP gateway receives most of its required configuration from the call agent. To configure an MGCP gateway, you simply identify the Cisco Unified Communications Manager server associated with the gateway and identify the gateway to the call agent. The MGCP gateway handles the translation between voice signals and the packet network and interacts with the Cisco Unified Communications Manager server. The server performs signal and call processing.

Cisco Unified Communications Manager Switchover and MGCP Gateway Fallback

This section describes how to configure Cisco Unified Communications Manager failover capabilities on the MGCP gateway.

Switchover

Cisco IOS gateways can maintain links to up to two backup Cisco Unified Communications Manager servers in addition to a primary Cisco Unified Communications Manager. This redundancy enables a voice gateway to switchover to a backup if the gateway loses communication with the primary. The backup server takes control of the devices that are registered with the primary Cisco Unified Communications Manager. The second backup takes control of the registered devices if both the primary and first backup Cisco Unified Communications Manager fail. The gateway preserves existing connections during a switchover to a backup Cisco Unified Communications Manager.

When the primary Cisco Unified Communications Manager server becomes available again, control reverts to that server. Reverting to the primary server can occur immediately, after a configurable amount of time, or only when all connected sessions are released.

Switchback

Switchback is the process a voice gateway uses to reestablish communication with the primary Cisco Unified Communications Manager server when the server becomes available again. Switchback can occur immediately, at a specified time after the last active call ends, or after a specified length of time.

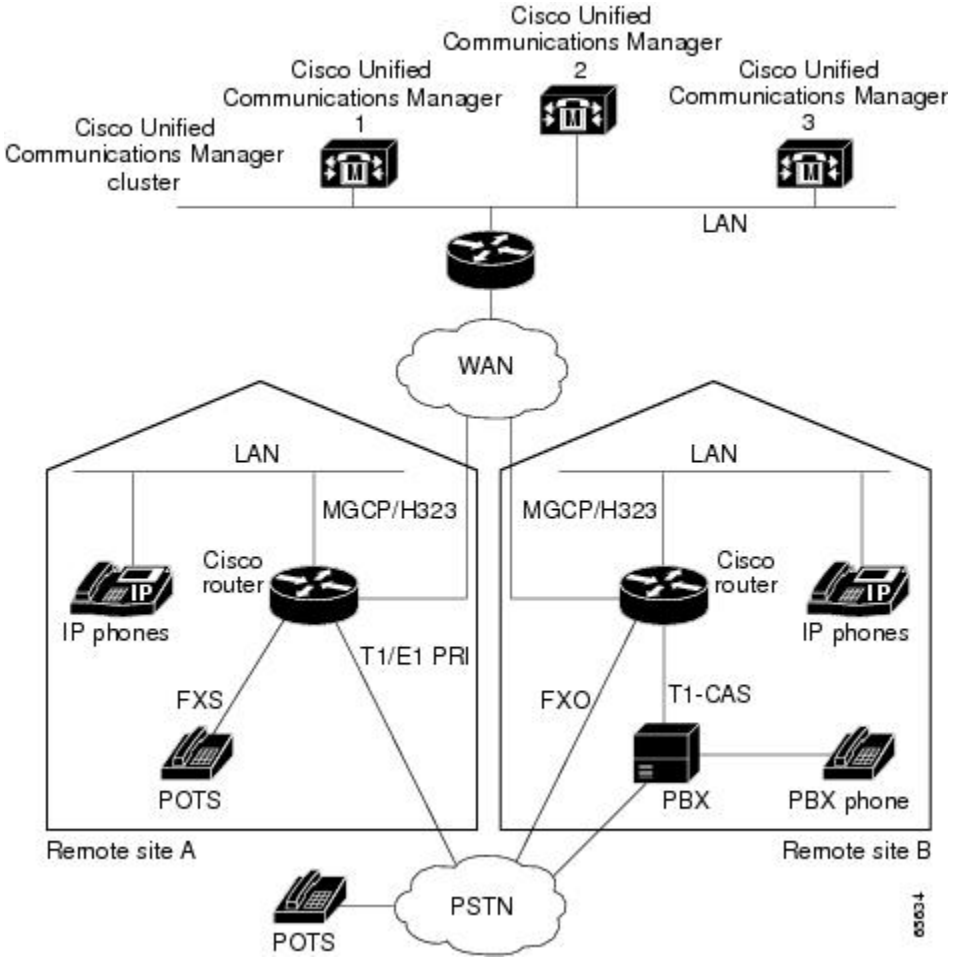
MGCP Gateway Fallback

The MGCP gateway maintains a remote connection to a centralized Cisco Unified Communications Manager cluster by sending MGCP keepalive messages to the Cisco Unified Communications Manager server at 15-second intervals. If the active Cisco Unified Communications Manager server fails to acknowledge receipt of the keepalive message within 30 seconds, the gateway attempts to switch over to the next available Cisco Unified Communications Manager server.

If none of the Cisco Unified Communications Manager servers respond, the gateway switches into fallback mode and reverts to the default H.323 session application for basic call control. H.323 is a standardized communication protocol that enables dissimilar devices to communicate with each other through use of a common set of codecs, call setup and negotiating procedures, and basic data transport methods. The gateway processes calls on its own using H.323 until one of the Cisco Unified Communications Manager connections is restored.

The figure below illustrates a typical VoIP network topology in which MGCP gateway fallback is supported.

Figure 7: Typical VoIP Network Topology Supporting the MGCP Gateway Fallback Feature



The MGCP Gateway Fallback feature provides the following functionality:

- MGCP gateway fallback support--All active MGCP analog and T1 CAS calls are maintained during the fallback transition. Callers are unaware of the fallback transition, and the active MGCP calls are cleared only when the communicating callers hang up. Active MGCP PRI backhaul calls are released during fallback.

Any transient MGCP calls (that is, calls that are not in the connected state) are cleared at the onset of the fallback transition and must be attempted again later.

- Basic connection services in fallback mode--Provides basic connection services for IP telephony traffic that passes through the gateway. When the local MGCP gateway transitions into fallback mode, the default H.323 session application assumes responsibility for handling new calls. Only basic two-party voice calls are supported during the fallback period.

Except for ISDN T1 and E1 PRI calls, all the MGCP calls that are active at the time of fallback are preserved, but transient calls are released. When a user completes (hangs up) an active MGCP call, the MGCP application handles the on-hook event and clears all call resources.

- Rehome support--Provides a rehome function in the gateway fallback mode that detects the restoration of a WAN TCP connection to the primary Cisco Unified Communications Manager server.

When the fallback mode is in effect, the affected MGCP gateway repeatedly tries to open a TCP connection to a Cisco Unified Communications Manager server in the prioritized list of call agents. This process continues until one of the Cisco Unified Communications Manager servers in the prioritized list responds.

The TCP open request from the MGCP gateway is honored, and the gateway reverts to MGCP mode. The gateway sends a Restart-in-Progress (RSIP) message to begin registration with the responding Cisco Unified Communications Manager.

All currently active calls that are initiated and set up during the fallback period are maintained by the default H.323 session application, except ISDN T1 and E1 PRI calls. Transient calls are released. After rehome occurs, the new Cisco Unified Communications Manager assumes responsibility for controlling new IP telephony activity.

The following types of interfaces on the gateway are supported:

- FXS analog interfaces--For connecting to the PSTN or analog phones
- FXO analog interfaces--For connecting to the PSTN or PBXs
- T1 CAS digital interfaces--For connecting to the PSTN or PBXs
- T1 and E1 PRI digital interfaces--For connecting to PBXs and central offices (COs)

MGCP Gateway Registration with Cisco Unified Communications Manager

The table below describes what can happen when either the gateway loses connection to the primary Cisco Unified Communications Manager or the gateway also loses connection to all backup Cisco Unified Communications Manager servers.

Table 2: Registration Scenarios

Terminology	Connection	Registration
Gateway Connection to Primary Cisco Unified Communications Manager		
Failover (also called switchover)	Gateway loses connection to primary Cisco Unified Communications Manager.	Gateway switches over to a backup.
Switchback	Gateway reconnects to primary Cisco Unified Communications Manager.	Gateway switches back to the primary.

Terminology	Connection	Registration
Gateway connection to all Cisco Unified Communications Manager Servers		
Fallback	Gateway loses connection to primary and all backup Cisco Unified Communications Manager servers.	Gateway falls back to H.323 call processing.
Rehome	Gateway reconnects to one of the Cisco Unified Communications Manager servers.	Gateway rehomes, resuming MGCP call processing.

Any calls at the time of reregistration (even those in a transient state such as call setup) remain undisturbed. The newly registered Cisco Unified Communications Manager determines the status of existing calls and maintains or deletes them as appropriate.

Benefits of Cisco Unified Communications Manager Switchover and MGCP Gateway Fallback

- Eliminates a potential single point of failure in the VoIP network by allowing you to designate up to two backup Cisco Unified Communications Manager servers. Your MGCP voice gateways can continue working if the primary Cisco Unified Communications Manager server fails.
- Ensures greater stability in the voice network by preserving existing connections during a switchover to a backup Cisco Unified Communications Manager server.
- Prevents call-processing interruptions or dropped calls in the event of a Cisco Unified Communications Manager or WAN failure.

MGCP Gateway Fallback and Cisco SRST

Cisco Survivable Remote Site Telephony (SRST) provides Cisco Unified Communications Manager with fallback support for Cisco IP phones that are attached to a Cisco router on your local network. Cisco SRST enables routers to provide call-handling support for Cisco IP phones when they lose connection to remote primary, secondary, or tertiary Cisco Unified Communications Manager installations or when the WAN connection is down.

MGCP gateway fallback is a different feature than SRST, and when MGCP gateway fallback is configured as an individual feature, it can be used by a PSTN gateway if you configure H.323 (or some other voice application) as a backup service. To use SRST as your fallback mode on an MGCP gateway, you must configure SRST and MGCP fallback on the same gateway. MGCP and SRST have had the capability to be configured on the same gateway since Cisco IOS Release 12.2(11)T.

Cisco SRST Description

Cisco Unified Communications Manager supports Cisco IP phones at remote sites that are attached to Cisco multiservice routers across the WAN. Prior to Cisco SRST, when the WAN connection between a router and the Cisco Unified Communications Manager failed or when connectivity with Cisco Unified Communications Manager was lost for some reason, Cisco Unified IP phones on the network became unusable for the duration of the failure. Cisco SRST overcomes this problem and ensures that Cisco Unified IP phones offer continuous (although minimal) service by providing call-handling support for Cisco Unified IP phones directly from the Cisco SRST router. The system automatically detects a failure and uses Simple Network Auto Provisioning (SNAP) technology to autoconfigure the branch office router to provide call processing for Cisco Unified IP phones that are registered with the router. When the WAN link or connection to the primary Cisco Unified Communications Manager is restored, call handling reverts back to the primary Cisco Unified Communications Manager.

For more information on Cisco SRST, see Overview of Cisco IOS SRST .

Configuring MGCP Gateway Fallback and Cisco SRST

To make outbound calls while in SRST mode on your MGCP gateway, you must configure two fallback commands on the MGCP gateway. These two commands allow SRST to assume control over the voice port and over call processing on the MGCP gateway. With Cisco IOS releases prior to 12.3(14)T, you must configure MGCP gateway fallback by using the **ccm-manager fallback-mgcp** and **call application alternate** commands. With Cisco IOS releases after 12.3(14)T, you must configure MGCP gateway fallback by using the **ccm-manager fallback-mgcp** and **service** commands.

Note You must configure both commands. For instance, your configuration will not work if you only configure the **ccm-manager fallback-mgcp** command.

Enabling SRST on an MGCP Gateway

To use SRST as your fallback mode with an MGCP gateway, you must configure both SRST and MGCP fallback on the same gateway. The following configuration allows SRST to assume control over the voice port and over call processing on the MGCP gateway.

Gateway Single-Point Configuration for MGCP Gateways

When you configure MGCP gateways to support Cisco Unified Communications Manager, you can use a centralized TFTP boot directory on a host device in your network to automatically download most of the configuration in the XML files. Each MGCP gateway in your VoIP network has an associated gateway-specific configuration that is stored in the centralized TFTP boot directory. A tailored XML file can be created and downloaded from the TFTP server to your designated MGCP gateway. The Cisco Unified Communications Manager server can be configured concurrently as a TFTP server.

When you make changes to the configuration in the database, a message is sent by Cisco Unified Communications Manager to the affected MGCP gateway, instructing the gateway devices to download the new XML configuration file. Each device has an XML parser that interprets the XML file according to its

device-specific requirements. Cisco MGCP gateways, for example, translate the content of the XML file into specific Cisco IOS commands for local execution.

When an MGCP gateway is first started up, it is preconfigured with the following information or it obtains the information through Dynamic Host Configuration Protocol (DHCP):

- A unique device identifier, which can be either of the following:
  - Specific device name on the Cisco MGCP gateway
  - MAC address of the device for gateways that are not using Cisco IOS software
- IP address of the TFTP server in the network and routing information required for access
- Sufficient information for configuration of an IP interface on the device

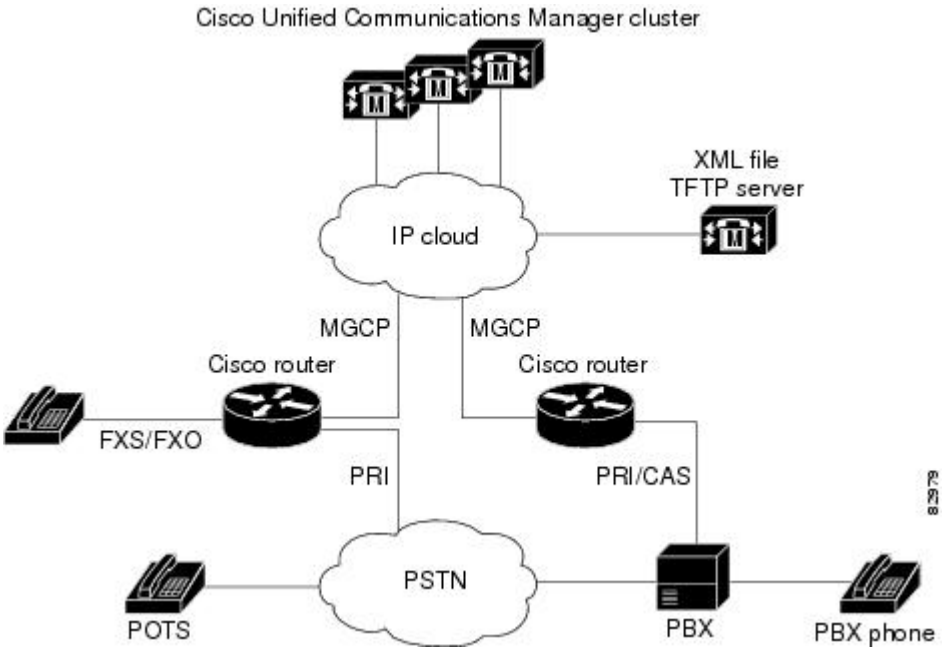
With this configuration information available at startup, the MGCP gateway downloads the XML file from the TFTP server. The gateway parses the XML file, converts the information to appropriate Cisco IOS configuration commands, and configures itself to run in the VoIP network. Finally, the gateway registers itself with Cisco Unified Communications Manager using an RSIP message. At that point, the MGCP gateway is ready for service in the network.

After a successful configuration download, the MGCP gateway saves the running configuration to nonvolatile random-access memory (NVRAM), which updates the startup configuration. Any manually-added configuration parameters are also saved to NVRAM if they were not previously saved. Manually-added configuration parameters are updates to the configuration that were made using the command-line interface (CLI). Manual configuration updates are separate from the automatic configuration updates made during the configuration download process.

In the event of a configuration failure, the MGCP gateway attempts to restore its current configuration by copying the startup configuration from NVRAM into the running configuration. Because this overwrites the

running configuration, any manually-added configuration parameters could be lost if they were not saved to NVRAM before running the automatic configuration-download process.

Figure 8: Single-Point Configuration for Cisco MGCP Gateways



MLPP Service on Cisco MGCP Gateway

Multilevel Precedence and Preemption (MLPP) is a service that allows authorized users to preempt lower priority voice calls to targeted stations or fully subscribed shared resources such as TDM trunks or conference bridges. This capability ensures high-ranking personnel of communication to critical organizations and personnel during network stress situations such as a national emergency. MLPP enables the voice gateway to interoperate with other MLPP-capable networks for call preemption and precedence. MLPP is supported only for MGCP endpoints over T1 CAS (E&M wink start) and T1 PRI using the backhaul feature.

MLPP service applies only to the subscribers and network resources within a specific domain. Connections and resources for a call from an MLPP subscriber are marked with a precedence level and domain identifier. A call can only be preempted by calls of higher precedence from MLPP users in the same domain. The Cisco Communications Manager or defense switched network (DSN) switch sets the maximum precedence level of a subscriber at subscription time.

For more information about MLPP, see the "Multilevel Precedence and Preemption" chapter in the *Cisco CallManager Features and Services Guide* , Release 4.0(1).

MLPP Call Treatment During Cisco Unified Communications Manager Switchover

When a Cisco Unified Communications Manager server fails during the processing of an MLPP call, the call is treated as a transient call and is dropped. The gateway releases the trunks and does a switchover to the backup Cisco Communications Manager server or falls back to H.323 mode, depending on the availability of the backup server. All currently connected MLPP calls are preserved during the switchover, switchback, or

fallback process. After the gateway reregisters with Cisco Communications Manager, call precedence and domain are preserved. During fallback, an incoming MLPP call is treated as a routine priority call.

Multicast Music-on-Hold

The Music-on-Hold (MOH) feature enables you to subscribe to a music streaming service when you are using a Cisco IOS MGCP voice gateway. Music streams from an MOH server to the voice interfaces of on-net and off-net callers that have been placed on hold. Cisco Communications Manager supports the capability to place callers on hold with music supplied from a streaming multicast MOH server. This integrated multicast capability is implemented through the H.323 signaling in Cisco Communications Manager.

By means of a preconfigured multicast address on the gateway, the gateway can "listen" for Real-Time Transport Protocol (RTP) packets that are broadcast from a default router in the network and can relay the packets to designated voice interfaces in the network. Whenever a called party places a calling party on hold, Cisco Communications Manager requests the MOH server to stream RTP packets to the "on-hold" interface through the preconfigured multicast address. In this way, RTP packets are relayed to appropriately configured voice interfaces that have been placed on hold. When you configure a multicast address on a gateway, the gateway sends an Internet Gateway Management Protocol (IGMP) "join" message to the default router, indicating to the default router that the gateway is ready to receive RTP multicast packets.

Multiple MOH servers can be present in the same network, but each server must have a different Class D IP address, and the address must be configured in Cisco Communications Manager and the MGCP voice gateways.

How to Configure MGCP Gateway Support

Enabling MGCP on Cisco IOS Gateways

Perform this task to enable MGCP on a Cisco IOS gateway to support Cisco Unified Communications Manager.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface ethernet** *slot /port*
4. **ip address** *ip-address subnetmask*
5. **no shutdown**
6. **exit**
7. **hostname** *name*
8. **mgcp validate domain-name**
9. **mgcp**
10. **mgcp call-agent** {*ip-address* | *host-name*} [*port*] [**service-type** *type*] [**version** *version-number*]
11. **mgcp dtmf-relay voip codec** {**all** | **low-bit-rate**} **mode** {**cisco**| **nse** | **out-of-band**}
12. **ccm-manager mgcp**
13. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password when prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface ethernet** *slot /port* **Example:** `Router(config)# interface ethernet 0/1`	Enters interface configuration mode so that you can configure the Ethernet interface for communicating with Cisco Unified Communications Manager. • *Slot* and *port* syntax is platform-dependent; type **?** to determine.
Step 4	**ip address** *ip-address subnetmask* **Example:** `Router(config-if)# ip address 10.10.2.23 255.255.255.255`	Configures an IP address and subnet mask on the router's Ethernet interface.
Step 5	**no shutdown** **Example:** `Router(config-if)# no shutdown`	Activates the Ethernet port.
Step 6	**exit** **Example:** `Router(config-if)# exit`	Exits interface mode and enters global configuration mode.
Step 7	**hostname** *name* **Example:** `Router(config)# hostname smith`	Assigns a unique name to a network router which enables Cisco Unified Communications Manager to identify the device. • Default device name is Router.
Step 8	**mgcp validate domain-name** **Example:** `Router(config)# mgcp validate domain-name`	(Optional) Verifies that the domain name or IP address received as part of the endpoint names in the MGCP messages match those configured on the gateway.

	Command or Action	Purpose
		Note This feature was modified to be disabled by default. You need to use this command to enable hostname and domain (or specific IP address) validation. See the Cisco IOS Voice Command Reference for detailed information about when this modification was made for your release.
Step 9	**mgcp** **Example:** `Router(config)# mgcp`	Enables the MGCP protocol.
Step 10	**mgcp call-agent** {*ip-address* | *host-name*} [*port*] [**service-type** *type*] [**version** *version-number*] **Example:** `Router(config)# mgcp call-agent 10.0.0.21 mgcp 0.1`	Specifies the primary Cisco Unified Communications Manager server's IP address or domain name, and the port gateway service type and version number.
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 mode cisco`	Selects the codec type and the dual tone multifrequency (DTMF) relay services.
Step 12	**ccm-manager mgcp** **Example:** `Router(config)# ccm-manager mgcp`	Enables the MGCP gateway to support Cisco Unified Communications Manager.
Step 13	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

Verifying MGCP Configuration on the Cisco IOS Gateway

SUMMARY STEPS

1. **show running-config**
2. **show interfaces ethernet**
3. **show mgcp**

DETAILED STEPS

Step 1 **show running-config**

Use the **show running-config** command to verify that MGCP is enabled on the voice gateway:

Example:

```
Router# show running-config
...
hostname voice-3640
!
...
mgcp
mgcp call-agent 10.0.0.21 service-type mgcp version 0.1
mgcp dtmf-relay voip codec all mode out-of-band
!
ccm-manager mgcp
!
interface Ethernet0/1
 ip address 10.10.2.23 255.255.255.0
 half-duplex
```

Step 2 **show interfaces ethernet**

Use the **show interfaces ethernet** command to verify that an Ethernet interface is configured to communicate with the Cisco Unified Communications Manager server, for example:

Example:

```
Router# show interfaces ethernet 4/2
Ethernet4/2 is up, line protocol is up
 Hardware is cxBus Ethernet, address is 0000.0c02.d0ce (bia 0000.0c02.d0ce)
 Internet address is 10.10.7.1, subnet mask is 255.255.255.0
 MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
 Encapsulation ARPA, loopback not set, keepalive set (10 sec)
 ARP type: ARPA, ARP Timeout 4:00:00
 Last input 0:00:00, output 0:00:09, output hang never
 Last clearing of "show interface" counters 0:56:40
 Output queue 0/40, 0 drops; input queue 0/75, 0 drops
 Five minute input rate 3000 bits/sec, 4 packets/sec
 Five minute output rate 0 bits/sec, 0 packets/sec
     4961 packets input, 715381 bytes, 0 no buffer
     Received 2014 broadcasts, 0 runts, 0 giants
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     567 packets output, 224914 bytes, 0 underruns
     0 output errors, 168 collisions, 0 interface resets, 0 restarts
     0 babbles, 2 late collision, 7 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

Step 3 **show mgcp**

Use the **show mgcp** command to display the MGCP settings on the Cisco IOS gateway:

Example:

```
Router# show mgcp
MGCP Admin State ACTIVE, Oper State ACTIVE - Cause Code NONE
!MGCP call agent with IP address for Cisco Unified Communications Manager:
MGCP call-agent: 10.0.0.21 2427 Initial protocol service is MGCP, v. 0.1
MGCP block-newcalls DISABLED
MGCP send RSIP for SGCP is DISABLED
MGCP quarantine mode discard/step
MGCP quarantine of persistent events is ENABLED
```

```
!DTMF-relay voip codec parameters:
MGCP dtmf-relay voip codec all mode out-of-band
MGCP dtmf-relay for VoAAL2 disabled for all codec types
MGCP voip modem passthrough mode: CISCO, codec: g711ulaw, redundancy: DISABLED,
MGCP voaal2 modem passthrough mode: NSE, codec: g711ulaw
MGCP TSE payload: 0
MGCP Network (IP/AAL2) Continuity Test timer: 200
MGCP 'RTP stream loss' timer: 5
MGCP request timeout 500, MGCP request retries 3
MGCP rtp unreachable timeout 1000
MGCP gateway port: 2427, MGCP maximum waiting delay 3000
MGCP restart delay 0, MGCP vad 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 rtp-package ms-package dt-package sst-packagc-package
MGCP VoAAL2 ignore-lco-codec DISABLED
MGCP T.38 Fax is DISABLED
```

Note For a description of the fields displayed in this output, see the *Cisco IOSVoice Command Reference* .

Configuring Switchover and MGCP Gateway Fallback

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. ccm-manager redundant-host {*ip-address* | *DNS-name*} [*ip-address* | *DNS-name*]
4. **ccm-manager switchback** {**graceful** | **immediate** | **schedule-time** *hh:mm* | **uptime-delay** *minutes*}
5. **ccm-manager fallback-mgcp**
6. **call application alternate**
7. **exit**
8. **ccm-manager switchover-to-backup**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password when prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	ccm-manager redundant-host {*ip-address* | *DNS-name*} [*ip-address* | *DNS-name*] **Example:** `Router(config)# ccm-manager redundant-host 10.0.0.50`	Identifies up to two backup Cisco Unified Communications Manager servers.
Step 4	**ccm-manager switchback** {**graceful** | **immediate** | **schedule-time** *hh:mm* | **uptime-delay** *minutes*} **Example:** `Router(config)# ccm-manager switchback immediate`	Configures switchback mode for returning control to the primary Cisco Unified Communications Manager. • Default is **graceful**.
Step 5	**ccm-manager fallback-mgcp** **Example:** `Router(config)# ccm-manager fallback-mgcp`	Enables the MGCP fallback feature.
Step 6	**call application alternate** **Example:** `Router(config)# call application alternate`	Specifies that the default voice application takes over if the MGCP application is not available.
Step 7	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.
Step 8	**ccm-manager switchover-to-backup** **Example:** `Router# ccm-manager switchover-to-backup`	Manually redirects the MGCP gateway to the backup Cisco Unified Communications Manager server. The switchover to the backup Cisco Unified Communications Manager server occurs immediately.

	Command or Action	Purpose
		Note This command does not switch the gateway to the backup Cisco Unified Communications Manager server if you have set the **ccm-manager switchback** command to **immediate** and the primary Cisco Unified Communications Manager server is still running.

Configuring MGCP Gateway Fallback and Cisco SRST

Note Effective with Cisco IOS Release 12.3(14)T, the **call application alternate** command has been replaced by the **service** command. You can use the **service** command cin all releases after Cisco IOS Release 12.3(14)T. Both commands are reflected in Step Configuring MGCP Gateway Fallback and Cisco SRST.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ccm-manager fallback-mgcp**
4. **call application alternate** [*application name*]
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ccm-manager fallback-mgcp** **Example:** `Router(config)# ccm-mananger fallback-mgcp`	Enables the gateway fallback feature and allows an MGCP voice gateway to provide call processing services through SRST or other configured applications when Cisco Unified Communications Manager is unavailable.

	Command or Action	Purpose

Step 4	**call application alternate** [*application name*]
	
	Example:
	
	service [alternate|default] *service-name location*
	
	Example:
	
	`Router(config)# call application alternate`
	
	Example:
	
	`Router(config)# service default`
		With Cisco IOS releases prior to 12.3(14)T, the **call application alternate**command specifies that the default voice application takes over if the MGCP application is not available. The *application-name* argument is optional and indicates the name of the specific voice application to use if the application dial peer fails. If a specific application name is not entered, the gateway uses the DEFAULT application.
		
		or
		
		With Cisco IOS releases after 12.3(14)T, the **service** command loads and configures a specific, standalone application on a dial peer. The keywords and arguments are as follows:
		
		• **alternate** --Optional. Alternate service to use if the service that is configured on the dial peer fails.
		• **default** --Optional. Specifies that the default service ("DEFAULT") on the dial peer is used if the alternate service fails.
		• *service-name* --Name that identifies the voice application.
		• *location* --Directory and filename of the Tcl script or VoiceXML document in URL format. For example, flash memory (flash:filename), a TFTP (tftp://../filename) or an HTTP server (http://../filename) are valid locations.

Step 5	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Verifying Switchover and MGCP Gateway Fallback

SUMMARY STEPS

1. **show running-config**
2. **show ccm-manager**
3. **show ccm-manager fallback-mgcp**

DETAILED STEPS

Step 1 **show running-config**

Use the **show running-config** command to verify configuration of the Cisco Unified Communications Manager failover options, for example:

Example:

```
Router# show running-config
...
ccm-manager switchback immediate
ccm-manager fallback-mgcp
ccm-manager redundant-host 10.0.0.50
ccm-manager mgcp
.
.
.
call application alternate DEFAULT
!
```

Step 2 **show ccm-manager**

Use the **show ccm-manager** command to verify the Cisco Unified Communications Manager failover options.

The following example shows one Cisco Unified Communications Manager backup server is configured. Switchback mode is set for immediate return to the primary Cisco Unified Communications Manager server as soon as the server is available.

Example:

```
Router# show ccm-manager
MGCP Domain Name: router.cisco.com
Total number of host: 2
Priority        Status         Host
================================================
Primary         Registered     10.0.0.201
First backup    Backup polling 10.0.0.50
Second backup   Undefined
Current active Communications Manager: 10.0.0.201
Current backup Communications Manager: 10.0.0.50
Redundant link port:         2428
Failover Interval:           30 seconds
Keepalive Interval:          15 seconds
Last keepalive sent:         00:20:18 (elapsed time: 00:00:06)
Last MGCP traffic time:      00:20:18 (elapsed time: 00:00:06)
Last switchover time:        None
Switchback mode:             Immediate
```

Step 3 **show ccm-manager fallback-mgcp**

Use the **show ccm-manager fallback-mgcp** command to verify whether MGCP fallback is enabled and whether it is active or not (on or off), for example:

Example:

```
Router# show ccm-manager fallback-mgcp
Current active Communications Manager:    10.00.71.29
MGCP Fallback mode:            Enabled/OFF
Last MGCP Fallback start time: 00:00:00
Last MGCP Fallback end time:   00:00:00
```

Note For a description of the fields displayed in these output examples, see the *Cisco IOS Voice Command Reference* .

Configuring POTS Dial Peers on MGCP Gateways

Perform this task to enable the POTS dial peers on your MGCP gateway to communicate with Cisco Unified Communications Manager.

When you have finished this procedure, the voice gateway is ready to communicate with Cisco Unified Communications Manager. It periodically sends out messages attempting to establish a connection. When the Cisco Unified Communications Manager configuration is complete, the connection should automatically establish itself. You should not have to make any further changes on the MGCP gateway.

Note

- All dial-plan configuration elements are controlled by Cisco Unified Communications Manager and should not be configured on the MGCP gateway for MGCP-managed endpoints (that is, any endpoint with an **application mgcpapp**command in its associated dial-peer).
- Do not use the **destination-pattern** or **session target** dial-peer configuration commands or the **connection** voice-port configuration command on the MGCP gateway, unless you are configuring MGCP gateway fallback. To configure MGCP gateway fallback, you must configure the H.323 dial peers with the destination-pattern and session target dial-peer configuration commands.
- Direct inward dial (DID) is required for T1/E1 PRI dial peers.
- Do not use the **application mgcpapp** command in dial peers that support PRI backhaul or BRI backhaul.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *tag* **pots**
4. **application mgcpapp**
5. **direct-inward-dial**
6. **port** *slot* /*subunit*/*port*
7. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password when prompted.

	Command or Action	Purpose
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 101 pots`	Designates the specified dial peer as a POTS device and enters dial-peer configuration mode.
Step 4	**application mgcpapp** **Example:** `Router(config-dial-peer)# application 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	**direct-inward-dial** **Example:** `Router(config-dial-peer)# direct-inward-dial`	(Optional) Enables the direct inward dialing (DID) call treatment for an incoming called number. • Required for T1/E1 PRI dial peers.
Step 6	**port** *slot /subunit/port* **Example:** `Router(config-dial-peer)# port 1/0/1`	Binds the MGCP application to the specified voice port. • S*lot* and *port* syntax is platform-dependent; type **?** to determine.
Step 7	**exit** **Example:** `Router(config-dial-peer)# exit`	Exits dial-peer configuration mode and returns to global configuration mode.

Verifying Dial Peer Configuration for MGCP Gateways

SUMMARY STEPS

1. **show running-config**
2. **show dial-peer voice**
3. **show voice port**

DETAILED STEPS

Step 1 **show running-config**

Use the **show running-config** command to verify the dial peer configuration.

The following example shows two Foreign Exchange Office (FXO) ports and one Foreign Exchange Station (FXS) port that are configured to run under MGCP control. Slot numbering and port numbering begin at 0.

Example:

```
! FXO port
dial-peer voice 1 pots
 application mgcpapp
 port 1/0/0
!
! FXO port
dial-peer voice 2 pots
 application mgcpapp
 port 1/0/1
!
! FXS port
dial-peer voice 3 pots
 application mgcpapp
 port 1/1/0
```

The following example shows a configuration on MGCP voice gateways for T1 CAS with e&m-wink-start emulation.

Example:

```
ccm-manager switchback immediate
ccm-manager fallback-mgcp
ccm-manager mgcp
!
controller T1 1/0
 framing esf
 linecode b8zs
 ds0-group 1 timeslots 1-24 type e&m-wink-start
!
voice-port 1/0:1
!
dial-peer voice 1 pots
 application mgcpapp
 destination-pattern 91.........
 port 1/0:1
```

The following example shows a configuration on MGCP voice gateways for FXS ports.

Example:

```
dial-peer voice 1 pots
 application mgcpapp
 destination-pattern 555-1212
 port 1/0/0
```

The following example shows a configuration on MGCP voice gateways for FXO ports.

Example:

```
dial-peer voice 2 pots
 application mgcpapp
 destination-pattern 527....
```

```
 prefix 527
 port 1/1/1
```

The following example shows a configuration on MGCP gateways for VoIP calls, when the fallback feature is used.

Example:

```
dial-peer voice 555 voip
 application mgcpapp
 destination pattern 555...
 incoming-called-number 444...
 session-target ipv4:172.20.21.8
 codec g711ulaw
```

Note When you configure MGCP gateway fallback support, the POTS dial peer must include the **application mgcpapp**command and must specify the voice port. For the default session application to take over during fallback, you must also configure a destination pattern.

Step 2 **show dial-peer voice**

Use the show dial-peer voice command to verify the configuration of the POTS dial peer, for example:

Example:

```
Router# show dial-peer voice 1000
VoiceEncapPeer1000
information type = voice,
description = `',
tag = 1000, destination-pattern = `',
answer-address = `', preference=0,
numbering Type = `unknown'
group = 1000, Admin state is up, Operation state is down,
incoming called-number = `', connections/maximum = 0/unlimited,
DTMF Relay = disabled,
huntstop = disabled,
in bound application associated: 'mgcpapp'

out bound application associated: ''
dnis-map =
permission :both
incoming COR list:maximum capability
outgoing COR list:minimum requirement
type = pots, prefix = `',
forward-digits default
session-target = `', voice-port = `',
direct-inward-dial = disabled,
digit_strip = enabled,
register E.164 number with GK = TRUE
Connect Time = 0, Charged Units = 0,
Successful Calls=0, Failed Calls=0, Incomplete Calls=0
Accepted Calls = 0, Refused Calls = 0,
Last Disconnect Cause is "",
Last Disconnect Text is "",
Last Setup Time = 0.
```

Step 3 **show voice port**

Use the show voice port command to verify that the voice port is operational. The following is sample output from a Cisco 3600 series router with an FXS analog voice port:

Example:

```
Router# show voice port 1/0/0
Foreign Exchange Office 1/0/0 Slot is 1, Sub-unit is 0, Port is 0
Type of VoicePort is FXO
```

```
Operation State is DORMANT
Administrative State is UP
No Interface Down Failure
Description is not set
Noise Regeneration is enabled
Non Linear Processing is enabled
Non Linear Mute is disabled
Non Linear Threshold is -21 dB
Music On Hold Threshold is Set to -38 dBm
In Gain is Set to 0 dB
Out Attenuation is Set to 3 dB
Echo Cancellation is enabled
Echo Cancellation NLP mute is disabled
Echo Cancellation NLP threshold is -21 dB
Echo Cancel Coverage is set to 8 ms
Playout-delay Mode is set to default
Playout-delay Nominal is set to 60 ms
Playout-delay Maximum is set to 200 ms
Playout-delay Minimum mode is set to default, value 40 ms
Playout-delay Fax is set to 300 ms
Connection Mode is normal
Connection Number is not set
Initial Time Out is set to 10 s
Interdigit Time Out is set to 10 s
Call Disconnect Time Out is set to 60 s
Ringing Time Out is set to 180 s
Wait Release Time Out is set to 30 s
Companding Type is u-law
Region Tone is set for US
Analog Info Follows:
Currently processing none
Maintenance Mode Set to None (not in mtc mode)
Number of signaling protocol errors are 0
Impedance is set to 600r Ohm
Station name None, Station number None
Translation profile (Incoming):
Translation profile (Outgoing):
Voice card specific Info Follows:
Signal Type is loopStart
Number Of Rings is set to 1
Supervisory Disconnect is inactive
Answer Supervision is inactive
Hook Status is On Hook
Ring Detect Status is inactive
Ring Ground Status is inactive
Tip Ground Status is inactive
Dial Type is dtmf
Digit Duration Timing is set to 100 ms
InterDigit Duration Timing is set to 100 ms
Pulse Rate Timing is set to 10 pulses/second
InterDigit Pulse Duration Timing is set to 750 ms
Percent Break of Pulse is 60 percent
GuardOut timer is 2000 ms
```

Note For a description of the fields displayed in this output, see the *Cisco IOS Voice Command Reference* .

Verifying Single-Point Configuration for MGCP Gateways

SUMMARY STEPS

1. **show running-config**
2. **show ccm-manager config-download**

DETAILED STEPS

Step 1 **show running-config**

Use the **show running-config** command to verify the single-point download configuration, for example:

Example:

```
Router# show running-config
...
ccm-manager switchback immediate
ccm-manager fallback-mgcp
ccm-manager redundant-host 10.10.10.1
ccm-manager mgcp
ccm-manager music-on-hold
ccm-manager config server 10.10.1.10
ccm-manager config
!
```

Step 2 **show ccm-manager config-download**

Use the **show ccm-manager config-download** command to verify the download status. The output indicates that four downloads were successful.

Example:

```
Router# show ccm-manager config-download
Configuration Auto-download Information
=======================================
Current version-id: {1645327B-F59A-4417-8E01-7312C61216AE}
Last config-downloaded:00:00:49
Current state: Waiting for commands
Configuration Download statistics:
        Download Attempted             : 4
          Download Successful          : 4
          Download Failed              : 0
        Configuration Attempted        : 1
          Configuration Successful     : 1
          Configuration Failed(Parsing): 0
          Configuration Failed(config) : 0
Last config download command: New Registration
```

Note For a description of the fields displayed in this output, see the *Cisco IOS Voice Command Reference* .

Configuring Multicast Music-on-Hold

This section describes how to configure your gateway to provide music to customers on hold.

Before You Begin

The default router in the network for handling multicast traffic must have the following enabled:

- Multicast routing
- A multicast routing protocol, for example Protocol Independent Multicast (PIM) or Distance Vector Multicast Routing Protocol (DVMRP)
- An IP routing protocol, for example Routing Information Protocol (RIP) or Open Shortest Path First (OSPF)
- Cisco Unified Communications Manager 3.1 (formerly known as Cisco CallManager 3.1) or higher

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ccm-manager music-on-hold**
4. **ccm-manager music-on-hold bind** *interface*
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password when prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ccm-manager music-on-hold** **Example:** `Router(config)# ccm-manager music-on-hold`	Enables music-on-hold.

	Command or Action	Purpose
Step 4	**ccm-manager music-on-hold bind** *interface* **Example:** `Router(config)# ccm-manager music-on-hold bind async`	(Optional) Binds the multicast MOH feature to a designated interface.
Step 5	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

Verifying Music-on-Hold

SUMMARY STEPS

1. **show running-config**
2. **show ccm-manager music-on-hold**

DETAILED STEPS

Step 1 **show running-config**

Use the **show running-config** command to verify the MOH configuration, for example:

Example:

```
Router# show running-config
...
ccm-manager redundant-host 10.0.0.21
ccm-manager mgcp
ccm-manager music-on-hold
ccm-manager config server 10.0.0.21
ccm-manager config
!
```

Step 2 **show ccm-manager music-on-hold**

Use the **show ccm-manager music-on-hold** command to display information about the currently active MOH sessions, for example:

Example:

```
Router#
 show ccm-manager music-on-hold
Multicast      RTP      Packets       Call               Incoming
Address        Port     In/Out        ID       Protocol  Interface
10.10.20.22    16256    3000/3000     1        IGMP      fe0/0
```

Note For a description of the fields displayed in this output, see the *Cisco IOS Voice Command Reference* .

Configuring MLPP Service on Cisco MGCP Gateways

Perform this task to configure the MGCP package capability for MLPP.

Note If you downloaded the default configuration file from TFTP, you do not need to manually configure MLPP on the MGCP gateway. The MLPP configuration is contained in the default configuration.

Before You Begin

- Cisco IOS Release 12.3(11)T or later
- Cisco Unified Communications Manager 4.0 (formerly known as Cisco CallManager 4.0) or later
- DSPWare 4.0
- Telogy DSP4 (Catalyst 6000 switches)
- Preemptions and precedences should be configured in Cisco Communications Manager. Interfaces, dial peers, voice ports, controllers, framing, and line codes should also be configured.
- Cisco Catalyst 6500 series and Cisco 7600 series Communication Media Module (CMM) requires WS-SVC-CMM-6T1 port adapter.

Note

- Supported only for MGCP endpoints over T1 CAS (E&M wink start) and T1 PRI (backhaul).
- Supported only by Cisco Communications Manager; does not work with other call agents.
- Conferenced call legs are not supported for preemption with Cisco Communications Manager.
- H.323, FXS, and FXO endpoints are not supported.
- Not supported for calls that originate or terminate in the gateway when the gateway is in H.323 fallback mode.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. mgcp package-capability **pre-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 **pre-package** **Example:** `Router(config)# mgcp package-capability pre-package`	Enables MLPP as an MGCP package capability type on the voice gateway.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits to privileged EXEC mode.

Configuring Fallback when Using MLPP on T1 CAS

When the gateway is in fallback mode, the precedence digit must be stripped from the dial string for T1 CAS calls. Perform this task to configure SRST to handle stripping the precedence digit.

Note For information on configuring digit stripping options for your specific dial plan, see the "Setting Up Call Handling" chapter in the *Cisco Survivable Remote Site Telephony Version 3.2 System Administration Guide* .

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **call-manager-fallback**
4. **ip source-address** *ip-address* [**port** *port*] [**any-match** | **strict-match**]
5. **max-dn** *max-directory-numbers*
6. **max-ephones** *max-phones*
7. **dialplan-pattern** *tag pattern* **extension-length** *length* [**extension-pattern** *extension-pattern*] [**no-reg**]
8. **translate** {**called** | **calling**} *translation-rule-tag*
9. **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	**call-manager-fallback** **Example:** `Router(config)# call-manager-fallback`	Enters call-manager-fallback configuration mode.
Step 4	**ip source-address** *ip-address* [**port** *port*] [**any-match** | **strict-match**] **Example:** `Router(config-cm-fallback)# ip source-address 10.10.200.23 port 2000`	Enables the voice gateway to receive messages from the Cisco IP phones through the specified IP addresses and provides for strict IP address verification.
Step 5	**max-dn** *max-directory-numbers* **Example:** `Router(config-cm-fallback)# max-dn 12`	Sets the maximum number of directory numbers or virtual voice ports that can be supported by the voice gateway. The maximum number is platform dependent.

	Command or Action	Purpose
Step 6	**max-ephones** *max-phones* **Example:** `Router(config-cm-fallback)# max-ephones 10`	Configures the maximum number of Cisco IP phones that can be supported by the voice gateway. The maximum number is platform dependent.
Step 7	**dialplan-pattern** *tag pattern* **extension-length** *length* [**extension-pattern** *extension-pattern*] [**no-reg**] **Example:** `Router(config-cm-fallback)# dialplan-pattern 1 [A-D].... extension-length 4`	Creates a global prefix that can be used to expand the abbreviated extension numbers into fully qualified E.164 numbers.
Step 8	**translate** {**called** | **calling**} *translation-rule-tag* **Example:** `Router(config-cm-fallback)# translate calling 1`	Applies a translation rule to modify the phone number dialed or received by any Cisco IP phone user while Cisco Communications Manager fallback is active.
Step 9	**end** **Example:** `Router(config-cm-fallback)# end`	Exits to privileged EXEC mode.

Verifying MLPP Configuration

SUMMARY STEPS

1. Use the **show running-config** command to verify the configuration of the MGCP package, for example:
2. Use the **show mgcp** command to display the MGCP configuration details, for example:

DETAILED STEPS

Step 1 Use the **show running-config** command to verify the configuration of the MGCP package, for example:

Example:

```
Router# show running-config
...
mgcp
mgcp call-agent OTHERCLUSTER 2427 service-type mgcp version 0.1
mgcp dtmf-relay voip codec all mode out-of-band
mgcp rtp unreachable timeout 1000 action notify
mgcp package-capability rtp-package
```

```
no mgcp package-capability res-package
mgcp package-capability sst-package
no mgcp package-capability fxr-package
mgcp package-capability pre-package
no mgcp timer receive-rtcp
mgcp sdp simple
no mgcp validate domain-name
mgcp fax t38 inhibit
mgcp rtp payload-type g726r16 static
!
mgcp profile default
!
```

Step 2 Use the **show mgcp** command to display the MGCP configuration details, for example:

Example:

```
Router# show mgcp
MGCP Admin State ACTIVE, Oper State ACTIVE - Cause Code NONE
MGCP call-agent: 172.18.195.147 2300 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 voaal2 codec all
MGCP voip modem passthrough mode: NSE, codec: g711ulaw, redundancy: DISABLED,
MGCP voaal2 modem passthrough mode: NSE, codec: g711ulaw
MGCP TSE payload: 100
MGCP T.38 Named Signalling Event (NSE) response timer: 200
MGCP Network (IP/AAL2) Continuity Test timer: 3000
MGCP 'RTP stream loss' timer: 2
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 DISABLED, 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 pre-package
```

Configuration Examples for MGCP Gateway Support

Note To view relevant configuration examples, go to the Cisco Systems Technologies website at http://cisco.com/en/US/tech/index.html . From the website, select **Voice > IP Telephony/VoIP**, then click **Technical Documentation > Configuration Examples**.

MGCP Gateway with T1 CAS Example

The following example shows MGCP fallback configured on a voice gateway with T1 CAS.

```
Current configuration : 2181 bytes
!
version 12.2
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Test-3640a
!
logging rate-limit console 10 except errors
!
memory-size iomem 25
voice-card 3
!
ip subnet-zero
!
no ip domain-lookup
ip domain-name test.com
!
no ip dhcp-client network-discovery
frame-relay switching
mgcp
mgcp call-agent 10.0.0.21 service-type mgcp version 0.1
mgcp dtmf-relay voip codec all mode out-of-band
mgcp rtp unreachable timeout 1000
mgcp package-capability rtp-package
no mgcp timer receive-rtcp
call rsvp-sync
!
ccm-manager switchback immediate
ccm-manager fallback-mgcp
ccm-manager redundant-host 10.0.0.21
ccm-manager mgcp
!
controller T1 3/0
 framing esf
 linecode b8zs
 ds0-group 1 timeslots 1 type e&m-wink-start
!
controller T1 3/1
 framing sf
 linecode ami
!
interface FastEthernet0/0
 ip address 10.0.0.21 255.255.255.224
 duplex auto
 speed auto
!
interface Serial0/0
```

```
 ip address 10.0.0.21 255.255.255.224
 encapsulation frame-relay
 no keepalive
 frame-relay interface-dlci 300
!
interface Serial0/1
 no ip address
 shutdown
 clockrate 2000000
!
interface Ethernet2/0
 ip address 10.0.0.21 255.255.255.224
 half-duplex
!
interface TokenRing2/0
 no ip address
 shutdown
 ring-speed 16
!
ip classless
ip route 10.0.0.21 255.255.255.0 14.0.0.1
ip route 10.0.0.21 255.255.255.0 14.0.0.1
ip route 10.0.0.21 255.255.255.0 14.0.0.1
ip route 10.0.0.21 255.255.255.0 14.0.0.1
ip route 10.0.0.21 255.255.255.255 Ethernet2/0
ip route 10.0.0.21 255.255.255.255 Ethernet2/0
no ip http server
!
snmp-server manager
!
voice-port 1/0/0
!
voice-port 1/0/1
!
voice-port 1/1/0
!
voice-port 1/1/1
!
voice-port 3/0:1
!
dial-peer cor custom
!
dial-peer voice 44 pots
 application mgcpapp
 destination-pattern 4301
 port 1/1/0
!
dial-peer voice 55 pots
 application mgcpapp
 destination-pattern 4302
 port 1/1/1
!
dial-peer voice 85 voip
 destination-pattern 805....
 session target ipv4:10.0.0.21
 codec g711ulaw
!
dial-peer voice 33 pots
 application mgcpapp
 destination-pattern 807....
 port 3/0:1
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
end
```

Note If the ccm-manager config command is enabled and you separate the MGCP and H.323 dial peers under different tags, make sure that the MGCP dial peers are configured before the H.323 dial peers.

MGCP Gateway with T1 PRI Example

The following example shows MGCP fallback configured on a voice gateway with T1 PRI ports.

```
version 12.2
no parser cache
no service single-slot-reload-enable
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname voice-3640
!
logging rate-limit console 10 except errors
!
voice-card 1
!
ip subnet-zero
!
no ip domain-lookup
!
no ip dhcp-client network-discovery
mgcp
mgcp call-agent 172.16.240.124 2427 service-type mgcp version 0.1
mgcp dtmf-relay voip codec all mode out-of-band
mgcp rtp unreachable timeout 1000 action notify
mgcp modem passthrough voip mode cisco
mgcp package-capability rtp-package
mgcp package-capability sst-package
no mgcp timer receive-rtcp
!
ccm-manager fallback-mgcp
ccm-manager redundant-host CM-B
ccm-manager mgcp
ccm-manager music-on-hold
ccm-manager config server cm-a
ccm-manager config
!
controller T1 1/0
 framing esf
 linecode b8zs
 pri-group timeslots 1-24 service mgcp
!
controller T1 1/1
 framing esf
 linecode b8zs
 pri-group timeslots 1-24 service mgcp
!
interface Serial1/0:23
 no ip address
 no logging event link-status
 isdn switch-type primary-ni
 isdn incoming-voice voice
 isdn T306 30000
 isdn bind-l3 ccm-manager
 no cdp enable
!
voice-port 1/0:23
!
dial-peer voice 9991023 pots
 application mgcpapp
```

```
 direct-inward-dial
 port 1/0:23
!
dial-peer voice 9991123 pots
 application mgcpapp
 direct-inward-dial
 port 1/1:23
!
dial-peer voice 1640001 pots
 destination-pattern 16.....
 direct-inward-dial
 port 1/0:23
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
end
```

Note DID is required for T1/E1 PRI dial peers.

Multicast Music-on-Hold Example

The following example shows multicast MOH configured for an MGCP voice gateway:

```
version 12.2
no parser cache
no service single-slot-reload-enable
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname voice-3640
!
logging rate-limit console 10 except errors
!
memory-size iomem 10
voice-card 1
!
ip subnet-zero
!
ip domain-name test.com
!
no ip dhcp-client network-discovery
mgcp
mgcp call-agent 10.0.0.21 2427 service-type mgcp version 0.1
mgcp dtmf-relay voip codec all mode out-of-band
mgcp rtp unreachable timeout 1000
mgcp modem passthrough voip mode cisco
mgcp package-capability rtp-package
mgcp package-capability sst-package
no mgcp timer receive-rtcp
call rsvp-sync
!
ccm-manager redundant-host 10.0.0.21
ccm-manager mgcp
ccm-manager music-on-hold
ccm-manager config server 10.0.0.21
ccm-manager config
!
controller T1 2/0
 framing sf
 linecode ami
```

```
 ds0-group 0 timeslots 1 type e&m-wink-start
!
controller T1 2/1
 framing sf
 linecode ami
!
interface FastEthernet0/0
 ip address 10.0.0.21 255.255.255.0
 no ip mroute-cache
 duplex auto
 speed auto
 no cdp enable
!
voice-port 1/0/0
!
voice-port 1/0/1
!
voice-port 2/0:0
!
dial-peer cor custom
!
dial-peer voice 125 pots
 application mgcpapp
 port 1/0/0
!
dial-peer voice 150 pots
 application mgcpapp
 port 2/0:0
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
no scheduler max-task-time
scheduler allocate 4000 4000
!
end
```

MLPP on Cisco 2801 Example

The following configuration includes both MLPP T1 CAS and T1 PRI.

```
Current configuration :1851 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname 2801_router
!
boot-start-marker
boot-end-marker
!
!
no network-clock-participate wic 1
network-clock-participate wic 2
no network-clock-participate wic 3
no network-clock-participate wic 4
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
no aaa new-model
ip subnet-zero
ip cef
!
```

```
!
!
no ftp-server write-enable
isdn switch-type primary-ni
voice-card 0
!
!
!
ccm-manager mgcp
ccm-manager music-on-hold
ccm-manager config server 192.168.12.125
!
!
controller T1 2/0
 framing esf
 clock source internal
 linecode b8zs
 ds0-group 1 timeslots 1-3 type e&m-wink-start
!
controller T1 2/1
 framing esf
 linecode b8zs
 pri-group timeslots 1,24 service mgcp
!
!
!
interface FastEthernet0/0
 ip address 192.168.12.38 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial2/1:23
 no ip address
 isdn switch-type primary-ni
 isdn incoming-voice voice
 isdn bind-l3 ccm-manager
 no cdp enable
!
ip classless
ip http server
!
!
!
control-plane
!
!
voice-port 1/0
!
voice-port 1/1
!
voice-port 2/0:1
!
voice-port 2/1:23
!
mgcp
mgcp call-agent 192.168.12.125 2427 service-type mgcp version 0.1
mgcp rtp unreachable timeout 1000 action notify
mgcp package-capability rtp-package
no mgcp package-capability res-package
mgcp package-capability sst-package
no mgcp package-capability fxr-package
no mgcp timer receive-rtcp
mgcp sdp simple
mgcp fax t38 inhibit
mgcp rtp payload-type g726r16 static
!
mgcp profile default
```

```
!
!
!
dial-peer voice 1 pots
 application mgcapp
 port 2/0:1
!
!
line con 0
line aux 0
line vty 0 4
 login
!
end
```

Note If you are using Cisco 4000 Series Integrated Service Routers, use clock source network command instead of clock source internal. For more information, refer to the Configuring the Cisco Fourth-generation T1/E1 Voice and WAN Network Interface Module and Network Synchronization for the Cisco ISR 4400 Series.

MLPP on Cisco 2621 Example

```
Current configuration :2530 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname 2621-other
!
boot-start-marker
boot system flash:c2600-ipvoice-mz
boot-end-marker
!
logging buffered 10000000 debugging
enable password lab
!
voice-card 1
!
no aaa new-model
ip subnet-zero
ip tcp synwait-time 13
!
!
ip domain name sample-vlan200.cisco.com
ip host demo 10.69.1.129
ip name-server 10.10.100.100
no ftp-server write-enable
isdn switch-type primary-ni
!
!
voice call carrier capacity active
!
!
ccm-manager fallback-mgcp
ccm-manager mgcp
ccm-manager music-on-hold
ccm-manager config server OTHER
ccm-manager config
!
!
controller T1 1/0
 framing esf
```

```
 crc-threshold 320
 clock source internal
 linecode b8zs
 ds0-group 1 timeslots 1-23 type e&m-wink-start
!
controller T1 1/1
 framing esf
 crc-threshold 320
 clock source internal
 linecode b8zs
 ds0-group 1 timeslots 1-23 type e&m-wink-start
!
!
interface FastEthernet0/0
 ip address 10.10.200.23 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
ip classless
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
ip http server
!
control-plane
!
!
call application alternate default
!
!
voice-port 1/0:1
!
voice-port 1/1:1
!
mgcp
mgcp call-agent OTHER 2427 service-type mgcp version 0.1
mgcp dtmf-relay voip codec all mode out-of-band
mgcp rtp unreachable timeout 1000 action notify
mgcp package-capability rtp-package
no mgcp package-capability res-package
mgcp package-capability sst-package
no mgcp package-capability fxr-package
mgcp package-capability pre-package
no mgcp timer receive-rtcp
mgcp sdp simple
no mgcp validate domain-name
mgcp fax t38 inhibit
mgcp rtp payload-type g726r16 static
!
mgcp profile default
!
!
dial-peer cor custom
!
!
dial-peer voice 999101 pots
 application mgcpapp
 port 1/0:1
!
dial-peer voice 999111 pots
 application mgcpapp
 port 1/1:1
!
dial-peer voice 999222 pots
 preference 1
 destination-pattern 100.
 direct-inward-dial
 port 1/0:1
 forward-digits all
```

```
!
!
call-manager-fallback
 max-conferences 4
 ip source-address 10.10.200.23 port 2000
 max-ephones 10
 max-dn 10
 dialplan-pattern 1 [A-D].... extension-length 4
 translate calling 1
!
!
line con 0
 exec-timeout 0 0
line aux 0
 exec-timeout 0 0
 no exec
 transport input all
line vty 0 4
 password lab
 login
!
exception core-file core_2621 compress
exception region-size 65536
exception dump 10.10.100.101
!
!
end
```

Note If you are using Cisco 4000 Series Integrated Service Routers, use clock source network command instead of clock source internal. For more information, refer to the Configuring the Cisco Fourth-generation T1/E1 Voice and WAN Network Interface Module and Network Synchronization for the Cisco ISR 4400 Series.

Feature Information for Configuring MGCP Gateway Support

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 Configuring MGCP Gateway Support

Feature Name	Releases	Feature Configuration Information
Configuring MLPP Service on Cisco MGCP Gateways	Cisco IOS XE Release 3.17S	This feature was introduced in Cisco IOS XE Release 3.17S.

Where to Go Next

- To configure conferencing, transcoding, and MTP support on a Cisco IOS gateway, see "Configuring Enhanced Conferencing and Transcoding for Voice Gateway Routers" on page 67 .

- To enable MGCP PRI backhaul support, see "Configuring MGCP PRI Backhaul and T1 CAS Support for Cisco Unified Communications Manager" on page 113 .
- To enable MGCP BRI backhaul support, see "Configuring MGCP-Controlled Backhaul of BRI Signaling in Conjunction with Cisco Unified Communications Manager" on page 129 .
- To download region-specific tones and their associated frequencies, amplitudes, and cadences, see "Configuring Tone Download to MGCP Gateways" on page 145 .

Additional References

- "Overview of Cisco Unified Communications Manager and Cisco IOS Interoperability" on page 13 --Describes basics of underlying technology and lists related documents.
- Configuring Media Gateway Control Protocol and Related Protocols --Describes MGCP concepts and configuration procedures.
- Configuring the Cisco IOS MGCP Gateway --Describes the basics of configuring an MGCP gateway to support Cisco Communications Manager.
- How to Configure MGCP with Digital PRI and Cisco Unified Communications Manager --Describes how to configure MGCP with PRI.
- MGCP Gateway Fallback Transition to Default H.323 Session Application --Describes how to enable an MGCP gateway to fallback to an H323 session application when the WAN connection to the primary Cisco Communications Manager server is lost, and no backup Cisco Communications Manager server is available.
- MGCP with Digital CAS and Cisco Unified Communications Manager Configuration Example --Describes how to use MGCP between a Cisco IOS gateway and a Cisco Communications Manager Media Convergence Server (MCS).
- MLPP Service on Cisco MGCP Gateway -Describes about Multilevel Precedence and Preemption (MLPP).
- Multilevel Precedence and Preemption - Describes about Multilevel Precedence and Preemption.
- Media and Signaling Authentication and Encryption -Describes about Secure Voice (MGCP Gateway).

CUCM MGCP PRI Backhaul, PRI Fallback and Rehome to CUCM:

- Configuring MGCP PRI Backhaul and T1 CAS Support
- Network Synchronization for the Cisco ISR 4400 Series
- Configuring the Cisco Fourth-generation T1/E1 Voice and WAN Network Interface Module