Overview of Cisco Unified Communications Manager and Interoperability

This chapter provides an overview of Cisco Unified Communications Manager and Cisco IOS interoperability.

Note For more information about Cisco IOS voice features--including library preface and glossary, feature documents, and troubleshooting information--see the entire Cisco IOS Voice Configuration Library .

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 at the end of this module.

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.

Information About Cisco Unified Communications Manager and Interoperability

Cisco AVVID

Cisco voice gateway routers can be deployed in a Cisco Unified Communications Manager IP-telephony network using the Cisco Architecture for Voice, Video, and Integrated Data (AVVID), a baseline infrastructure that enables enterprises to design networks that scale to meet e-business demands for business solutions such as e-learning and customer care.

Voice and video solutions based on Cisco AVVID include:

- Client devices such as IP phones
- Directory services
- IP-based business applications
- Network management
- Scalable call processing
- Service and support
- Video conferencing

Cisco Unified Communications Manager Interoperability

Cisco Unified Communications Manager is the software-based call-processing component of voice gateways in a VoIP network. It extends enterprise telephony features and functions to packet telephony network devices such as IP phones, media processing devices, VoIP gateways, and multimedia applications.

Additional data, voice, and video services such as unified messaging, multimedia conferencing, collaborative contact centers, and interactive multimedia response systems interact through the Cisco Unified Communications Manager application programming interface (API). Cisco Unified Communications Manager also supports third-party applications.

Cisco IOS gateways connect AVVID networks to traditional telephone trunks or analog and digital devices. The trunks are connected to the PSTN or existing PBX systems, legacy telephones, and voice conference units. Cisco IOS voice gateways communicate with Cisco Unified Communications Manager using H.323 or Media Gateway Control Protocol (MGCP).

- In H.323 mode, the Cisco voice gateway communicates with Cisco Unified Communications Manager as an intelligent gateway device.
- In MGCP mode, the Cisco voice gateway operates as a stateless client, giving Cisco Unified Communications Manager full control.

MGCP Voice Gateways

Cisco Unified Communications Manager provides a central point of configuration, administration, and control for MGCP voice gateways. Using Cisco IOS software, voice gateways are configured as MGCP gateways. Cisco Unified Communications Manager acts as an MGCP call agent, controlling the setting up and tearing down of connections between the endpoints in a VoIP network and endpoints in the public switched telephone network (PSTN), while managing all dial-plan related configuration elements.

With MGCP, dial plans are configured centrally in Cisco Unified Communications Manager, instead of in each gateway. All Cisco MGCP gateways in a Cisco AVVID-enabled IP telephony network can be automatically configured by downloading XML files from Cisco Unified Communications Manager. Cisco MGCP gateways also provide multiple levels of failover capabilities, including Survivable Remote Site Telephony (SRST) support to prevent call-processing interruptions or dropped calls if there is a Cisco Unified Communications Manager or WAN failure.

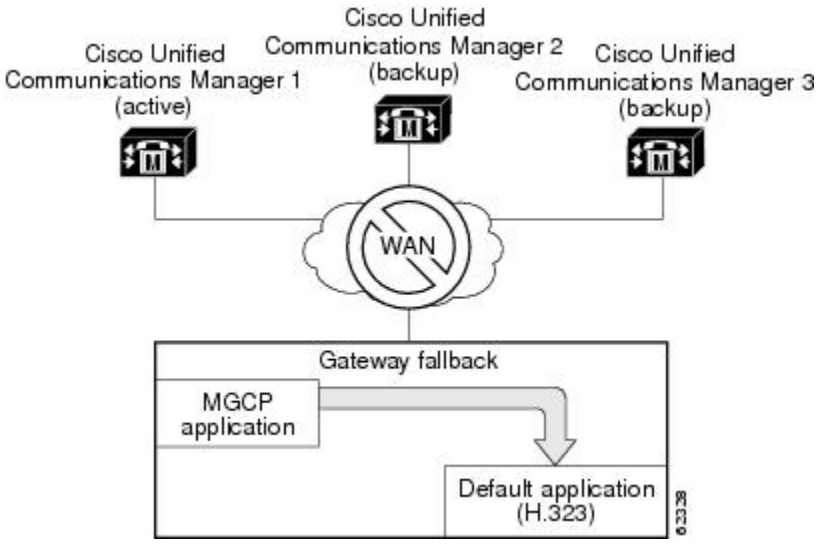
MGCP gateways support the following Cisco Unified Communications Manager features:

MGCP Gateway Fallback

MGCP gateway fallback improves the reliability of PSTN interfaces in an IP-telephony network by providing basic call processing support when an MGCP gateway loses connectivity to all of its configured Cisco Unified Communications Manager servers. Each Cisco Unified Communications Manager server is potentially available as a backup call agent through a prioritized list of call agents that is configured on the MGCP gateway.

On startup, the MGCP voice gateway attempts to establish a connection to the highest order Cisco Unified Communications Manager server on the configured list. If the attempt is successful, the gateway registers itself with the primary (highest priority) call agent. If no call agent in this prioritized list is accessible, the gateway uses its default H.323 session application (Version 2) to perform basic call-handling functions (see the figure below).

Figure 1: MGCP Gateway Fallback Transition to Default H.323 Session Application



MGCP PRI Backhaul

MGCP PRI backhaul is a method for transporting complete IP telephony signaling information from an ISDN PRI interface on an MGCP gateway to Cisco Unified Communications Manager through a Transmission Control Protocol (TCP) connection. It terminates all of the ISDN PRI Layer 2 (Q.921) signaling functions on the MGCP gateway and packages all of the ISDN PRI Layer 3 (Q.931) signaling information into packets for transmission to Cisco Unified Communications Manager through an IP tunnel. This ensures the integrity of the Q.931 signaling information that passes through the network for managing IP telephony devices.

MGCP BRI Backhaul

MGCP-controlled backhaul of BRI signaling provides service to remote-office gateways that connect by means of ISDN BRI trunks to a centralized Cisco Unified Communications Manager. D-channel signaling information is backhauled to Cisco Unified Communications Manager through a TCP session. All Q.931 messages are passed through the TCP connection between the Cisco MGCP gateway and Cisco Unified Communications Manager. The feature enables you to connect remote ISDN PBXs and key systems to a Cisco ISDN BRI network termination (network side) or a PSTN Class 4/5 switch through a Cisco ISDN BRI terminal equipment (as user side) interface.

Multicast Music-On-Hold

Multicast music-on-hold (MOH) functionality enables the streaming of music from an MOH server to the voice interfaces of on-net and off-net callers that are placed on hold. This integrated multicast capability is implemented through the H.323 signaling in Cisco Unified Communications Manager.

Network Specific Facilities

The MGCP Gateway Support for Cisco Unified Communications Manager Network Specific Facilities (NSF) feature supports the use of the ISDN NSF information element in the route pattern, enabling facilities or services to be invoked on a call-by-call basis. Without NSF configuration, you must configure associated gateways as standalone H.323 gateways for which NSF services are configured locally within the router. No configuration is required on the MGCP gateway to use the NSF feature.

Single-Point Configuration

When you configure MGCP gateways to interoperate with 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 Cisco IOS configuration in an XML file. A Cisco Unified Communications Manager server can be concurrently configured as a TFTP server.

The XML file is generated by using the web-based Cisco Unified Communications Manager graphical user interface (GUI). When the network administrator changes the configuration information in the database, Cisco Unified Communications Manager instructs the MGCP gateway to download the modified XML file.

Supplementary Services

Supplementary services include call forwarding, call hold, call transfer when the line is busy or there is no answer, and three-party call conferencing to and from the PSTN or a private branch exchange (PBX).

- Call forwarding--Enables you to forward calls dialed from the original location to a remote location within or across the network.
- Call hold--Places the handset in mute mode. The transmitter and receiver functions are disengaged until the hold button is pressed again to reconnect the parties.
- Call transfer--Transfers a call to a third party through a preprogrammed button that produces a recall dial tone. The receiver of the call then dials the third-party number, waits for the line to ring and for the new called party to answer, and then hangs up.
- Three-party call conferencing--Adds a third party to a call. It is similar to the transfer function, but rather than the call being transferred to a third party, the third party called is added to the call.

Switchover (Failover)

A Cisco MGCP gateway first connects--that is, registers--to a primary Cisco Unified Communications Manager. If connection to the primary fails, the gateway registers automatically to a backup if one exists and, if that connection also fails, to a second backup if one exists. When connection to the primary is restored, the gateway automatically registers to the primary. Existing connections are preserved during the switchover.

Switchback

Switchback is the process that MGCP gateways use to reestablish communication with the primary Cisco Unified Communications Manager server when it becomes available after losing connectivity. Switchback mode can occur immediately, at a specified time after the last active call ends, or after a specified length of time. During the switchback, existing connections are preserved.

Tones and Cadences

Tones and cadences are preconfigured based on the network locale in Cisco Unified Communications Manager. It is no longer necessary to configure the cptone command on the MGCP gateway. The static tone table used for a voice port is determined by the network locale that is specified for the voice port in Cisco Unified Communications Manager. The network locale for each voice port is downloaded in the gateway's XML configuration file.

The Customizable Tone Download to Cisco IOS MGCP Gateways from Cisco Unified Communications Manager feature enables the downloading of region-specific tones and the associated frequencies, amplitudes, and cadences in up to two custom tone files.

MGCP Advantages Over H.323

Using MGCP provides advantages over H.323, including the following:

- Centralized call-management architecture

MGCP enables external control of network signaling. Handling of Layer 3 call processing centrally in the network is advantageous to network operators who need a high degree of control over their networks.

- Shorter voice cut-through times

MGCP speeds voice cut-through as compared to H.323 for both initial call setup and redirects. Voice cut-through is the time from when the called party goes offhook to when both parties are able to receive voice from the other. Long cut-through times can prevent deployment of viable IP telephony solutions in centralized environments.

Conferencing and Transcoding

The digital-signal-processor (DSP) farm functionality on Cisco IOS gateways provides conference, transcode, and hardware MTP capability by using DSP resources on high-density digital voice/fax network modules such as the NM-HDV and NM-HDV2. DSP farms are configured on the voice gateway and managed by Cisco Unified Communications Manager through Skinny Client Control Protocol (SCCP).

Toll Fraud Prevention

When a Cisco router platform is installed with a voice-capable Cisco IOS software image, appropriate features must be enabled on the platform to prevent potential toll fraud exploitation by unauthorized users. Deploy these features on all Cisco router Unified Communications applications that process voice calls, such as Cisco Unified Communications Manager Express (CME), Cisco Survivable Remote Site Telephony (SRST), Cisco Unified Border Element (UBE), Cisco IOS-based router and standalone analog and digital PBX and public-switched telephone network (PSTN) gateways, and Cisco contact-center VoiceXML gateways. These features include, but are not limited to, the following:

- Disable secondary dial tone on voice ports--By default, secondary dial tone is presented on voice ports on Cisco router gateways. Use private line automatic ringdown (PLAR) for foreign exchange office (FXO) ports and direct-inward-dial (DID) for T1/E1 ports to prevent secondary dial tone from being presented to inbound callers.
- Cisco router access control lists (ACLs)--Define ACLs to allow only explicitly valid sources of calls to the router or gateway, and therefore to prevent unauthorized Session Initiation Protocol (SIP) or H.323 calls from unknown parties to be processed and connected by the router or gateway.
- Close unused SIP and H.323 ports--If either the SIP or H.323 protocol is not used in your deployment, close the associated protocol ports. If a Cisco voice gateway has dial peers configured to route calls outbound to the PSTN using either time division multiplex (TDM) trunks or IP, close the unused H.323 or SIP ports so that calls from unauthorized endpoints cannot connect calls. If the protocols are used and the ports must remain open, use ACLs to limit access to legitimate sources.
- Change SIP port 5060--If SIP is actively used, consider changing the port to something other than well-known port 5060.
- SIP registration--If SIP registration is available on SIP trunks, turn on this feature because it provides an extra level of authentication and validation that only legitimate sources can connect calls. If it is not available, ensure that the appropriate ACLs are in place.
- SIP Digest Authentication--If the SIP Digest Authentication feature is available for either registrations or invites, turn this feature on because it provides an extra level of authentication and validation that only legitimate sources can connect calls.
- Explicit incoming and outgoing dial peers--Use explicit dial peers to control the types and parameters of calls allowed by the router, especially in IP-to-IP connections used on CME, SRST, and Cisco UBE. Incoming dial peers offer additional control on the sources of calls, and outgoing dial peers on the

destinations. Incoming dial peers are always used for calls. If a dial peer is not explicitly defined, the implicit dial peer 0 is used to allow all calls.

- Explicit destination patterns--Use dial peers with more granularity than .T for destination patterns to block disallowed off-net call destinations. Use class of restriction (COR) on dial peers with specific destination patterns to allow even more granular control of calls to different destinations on the PSTN.
- Translation rules--Use translation rules to manipulate dialed digits before calls connect to the PSTN to provide better control over who may dial PSTN destinations. Legitimate users dial an access code and an augmented number for PSTN for certain PSTN (for example, international) locations.
- Tcl and VoiceXML scripts--Attach a Tcl/VoiceXML script to dial peers to do database lookups or additional off-router authorization checks to allow or deny call flows based on origination or destination numbers. Tcl/VoiceXML scripts can also be used to add a prefix to inbound DID calls. If the prefix plus DID matches internal extensions, then the call is completed. Otherwise, a prompt can be played to the caller that an invalid number has been dialed.
- Host name validation--Use the "permit hostname" feature to validate initial SIP Invites that contain a fully qualified domain name (FQDN) host name in the Request Uniform Resource Identifier (Request URI) against a configured list of legitimate source hostnames.
- Dynamic Domain Name Service (DNS)--If you are using DNS as the "session target" on dial peers, the actual IP address destination of call connections can vary from one call to the next. Use voice source groups and ACLs to restrict the valid address ranges expected in DNS responses (which are used subsequently for call setup destinations).

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

Additional References

The following sections provide references for Cisco IOS Interoperability with Cisco Unified Communications Manager.

Related Documents

Related Topic	Document Title
Additional Cisco IOS Voice Configuration Library documents, including library preface and glossary	Cisco IOS Voice Configuration Library
Cisco IOS command references	• *Cisco IOS Debug Command Reference*, Release 12.4T • *Cisco IOS Voice Command Reference*
Cisco IOS configuration examples	Cisco Systems Technologies website From the website, select a technology category and subsequent hierarchy of subcategories, then click **Technical Documentation > Configuration Examples**.

Related Topic	Document Title
Cisco IOS software system messages	*Cisco IOS Software System Messages*
Cisco IOS troubleshooting information	*Cisco IOS Voice Troubleshooting and Monitoring Guide*
Cisco Unified Communications Manager • Administration and configuration	• *Cisco Unified CallManager Administration Guide* , Release 4.0(1) • *Cisco Unified CallManager System Guide* , Release 4.0(1) • *Cisco Unified CallManager Features and Services Guide* , Release 4.0(1)
• Upgrading	• *Upgrading Cisco Unified CallManager*, Release 4.0(1)
• Transcoder services and configuration	• "Transcoders" chapter in the *Cisco Unified Communications Manager System Guide* • "Transcoder Configuration" chapter in the *Cisco Unified Communications Manager Administration Guide*
• Voice-conference services and configuration	• "Conference Bridges" chapter in *Cisco Unified CallManager System Guide* , Release 4.0(1) • "Conference Bridge Configuration" chapter in *Cisco Unified CallManager Administration Guide,* Release 4.0(1)
• MCID	"Malicious Call Identification" chapter in the *Cisco Unified Communications Manager Features and Services Guide*
• MLPP	"Multilevel Precedence and Preemption" chapter in the *Cisco Unified Communications Manager Features and Services Guide*
Fallback support for Cisco IP phones	Cisco Survivable Remote Site Telephony (SRST) Version 3.0
Interface configuration	*Cisco IOS Interface and Hardware Component Command Reference*, Release 12.4T
IP addressing and services	*Cisco IOS IP Addressing Services* Release 12.4T

Related Topic	Document Title
Routing process and routing protocols for networks	*Cisco IOS IP Application Services Configuration Guide* , Release 12.4T
MGCP concepts and configuration procedures	*Cisco IOS MGCP and Related Protocols Configuration Guide*
Hardware installation	Modular Access Routers documentation

Standards

Standards	Title
H.225	Call Signaling Protocols and Media Stream Packetization for Packet-based Multimedia Communication Systems
H.323 Annex M.1	Tunnelling of Signalling Protocol (QSIG) in H.323
I.251.7	Malicious Call Identification (MCID)
I.255.3	Multi-Level Precedence and Preemption Service (MLPP)
ITU-T Recommendation Q.931	*ISDN User-Network Interface Layer 3 specification* (ITU-T specification for signaling to establish, maintain, and clear ISDN network connections).
Q.81.7	Malicious Call Identification (MCID)
Q.951.7	Stage 3 Description for Number Identification Supplementary Services Using DSS 1: Malicious Call Identification (MCID)
TIA/EIA-464-B	*Requirements for Private Branch Exchange (PBX) Switching Equipment*

MIBs

MIBs	MIBs Link

• Transcoding:
  • Access Environment MIB
  • CDP MIB
  • Cisco Stack MIB
  • DSP Management MIB
  • RFC 1157 SNMP
  • RFC 1213 MIB II
  • RFC 1573 MIB II Interface Extensions
  • RFC 1643 Ethernet MIB
  • RFC 1757 Ethernet RMON
  • Voice Common Interface MIB
  • Voice Dial MIB
	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:
	http://www.cisco.com/go/mibs

RFCs

RFCs	Title
RFC 2833	RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals

Technical Assistance

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