



Cisco Unified Communications Manager and Cisco IOS Interoperability Guide

Release 12.4

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.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flip Video, Flip Video (Design), Flipshare (Design), Flip Ultra, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0907R)

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

Cisco Unified Communications Manager and Cisco IOS Interoperability Guide
© 2009 Cisco Systems, Inc. All rights reserved.



About Cisco IOS and Cisco IOS XE Software Documentation

Last Updated: March 5, 2009

This document describes the objectives, audience, conventions, and organization used in Cisco IOS and Cisco IOS XE software documentation, collectively referred to in this document as Cisco IOS documentation. Also included are resources for obtaining technical assistance, additional documentation, and other information from Cisco. This document is organized into the following sections:

- [Documentation Objectives, page i](#)
- [Audience, page i](#)
- [Documentation Conventions, page ii](#)
- [Documentation Organization, page iii](#)
- [Additional Resources and Documentation Feedback, page xi](#)

Documentation Objectives

Cisco IOS documentation describes the tasks and commands available to configure and maintain Cisco networking devices.

Audience

The Cisco IOS documentation set is intended for users who configure and maintain Cisco networking devices (such as routers and switches) but who may not be familiar with the configuration and maintenance tasks, the relationship among tasks, or the Cisco IOS commands necessary to perform particular tasks. The Cisco IOS documentation set is also intended for those users experienced with Cisco IOS who need to know about new features, new configuration options, and new software characteristics in the current Cisco IOS release.

Documentation Conventions

In Cisco IOS documentation, the term *router* may be used to refer to various Cisco products; for example, routers, access servers, and switches. These and other networking devices that support Cisco IOS software are shown interchangeably in examples and are used only for illustrative purposes. An example that shows one product does not necessarily mean that other products are not supported.

This section includes the following topics:

- [Typographic Conventions, page ii](#)
- [Command Syntax Conventions, page ii](#)
- [Software Conventions, page iii](#)
- [Reader Alert Conventions, page iii](#)

Typographic Conventions

Cisco IOS documentation uses the following typographic conventions:

Convention	Description
^ or Ctrl	Both the ^ symbol and Ctrl represent the Control (Ctrl) key on a keyboard. For example, the key combination ^D or Ctrl-D means that you hold down the Control key while you press the D key. (Keys are indicated in capital letters but are not case sensitive.)
<i>string</i>	A string is a nonquoted set of characters shown in italics. For example, when setting a Simple Network Management Protocol (SNMP) community string to <i>public</i> , do not use quotation marks around the string; otherwise, the string will include the quotation marks.

Command Syntax Conventions

Cisco IOS documentation uses the following command syntax conventions:

Convention	Description
bold	Bold text indicates commands and keywords that you enter as shown.
<i>italic</i>	Italic text indicates arguments for which you supply values.
[x]	Square brackets enclose an optional keyword or argument.
...	An ellipsis (three consecutive nonbolded periods without spaces) after a syntax element indicates that the element can be repeated.
	A vertical line, called a pipe, indicates a choice within a set of keywords or arguments.
[x y]	Square brackets enclosing keywords or arguments separated by a pipe indicate an optional choice.
{x y}	Braces enclosing keywords or arguments separated by a pipe indicate a required choice.
[x {y z}]	Braces and a pipe within square brackets indicate a required choice within an optional element.

Software Conventions

Cisco IOS uses the following program code conventions:

Convention	Description
Courier font	Courier font is used for information that is displayed on a PC or terminal screen.
Courier font	Bold Courier font indicates text that the user must enter.
< >	Angle brackets enclose text that is not displayed, such as a password. Angle brackets also are used in contexts in which the italic font style is not supported; for example, ASCII text.
!	An exclamation point at the beginning of a line indicates that the text that follows is a comment, not a line of code. An exclamation point is also displayed by Cisco IOS software for certain processes.
[]	Square brackets enclose default responses to system prompts.

Reader Alert Conventions

The Cisco IOS documentation set uses the following conventions for reader alerts:



Caution

Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.



Note

Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.



Timesaver

Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Documentation Organization

This section describes the Cisco IOS documentation set, how it is organized, and how to access it on Cisco.com. Included are lists of configuration guides, command references, and supplementary references and resources that make up the documentation set. The following topics are included:

- [Cisco IOS Documentation Set, page iv](#)
- [Cisco IOS Documentation on Cisco.com, page iv](#)
- [Configuration Guides, Command References, and Supplementary Resources, page v](#)

Cisco IOS Documentation Set

Cisco IOS documentation consists of the following:

- Release notes and caveats provide information about platform, technology, and feature support for a release and describe severity 1 (catastrophic), severity 2 (severe), and severity 3 (moderate) defects in released Cisco IOS code. Review release notes before other documents to learn whether or not updates have been made to a feature.
- Sets of configuration guides and command references organized by technology and published for each standard Cisco IOS release.
 - Configuration guides—Compilations of documents that provide informational and task-oriented descriptions of Cisco IOS features.
 - Command references—Compilations of command pages that provide detailed information about the commands used in the Cisco IOS features and processes that make up the related configuration guides. For each technology, there is a single command reference that covers all Cisco IOS releases and that is updated at each standard release.
- Lists of all the commands in a specific release and all commands that are new, modified, removed, or replaced in the release.
- Command reference book for **debug** commands. Command pages are listed in alphabetical order.
- Reference book for system messages for all Cisco IOS releases.

Cisco IOS Documentation on Cisco.com

The following sections describe the documentation organization and how to access various document types.

Use Cisco Feature Navigator to find information about platform support and Cisco IOS, Cisco IOS XE, and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

New Features List

The New Features List for each release provides a list of all features in the release with hyperlinks to the feature guides in which they are documented.

Feature Guides

Cisco IOS features are documented in feature guides. Feature guides describe one feature or a group of related features that are supported on many different software releases and platforms. Your Cisco IOS software release or platform may not support all the features documented in a feature guide. See the Feature Information table at the end of the feature guide for information about which features in that guide are supported in your software release.

Configuration Guides

Configuration guides are provided by technology and release and comprise a set of individual feature guides relevant to the release and technology.

Command References

Command reference books describe Cisco IOS commands that are supported in many different software releases and on many different platforms. The books are provided by technology. For information about all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the *Cisco IOS Master Command List, All Releases*, at http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html.

Cisco IOS Supplementary Documents and Resources

Supplementary documents and resources are listed in [Table 2 on page xi](#).

Configuration Guides, Command References, and Supplementary Resources

[Table 1](#) lists, in alphabetical order, Cisco IOS and Cisco IOS XE software configuration guides and command references, including brief descriptions of the contents of the documents. The Cisco IOS command references are comprehensive, meaning that they include commands for both Cisco IOS software and Cisco IOS XE software, for all releases. The configuration guides and command references support many different software releases and platforms. Your Cisco IOS software release or platform may not support all these technologies.

For additional information about configuring and operating specific networking devices, go to the Product Support area of Cisco.com at <http://www.cisco.com/web/psa/products/index.html>.

[Table 2](#) lists documents and resources that supplement the Cisco IOS software configuration guides and command references. These supplementary resources include release notes and caveats; master command lists; new, modified, removed, and replaced command lists; system messages; and the debug command reference.

Table 1 *Cisco IOS and Cisco IOS XE Configuration Guides and Command References*

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
<i>Cisco IOS AppleTalk Configuration Guide</i>	AppleTalk protocol.
<i>Cisco IOS XE AppleTalk Configuration Guide</i>	
<i>Cisco IOS AppleTalk Command Reference</i>	
<i>Cisco IOS Asynchronous Transfer Mode Configuration Guide</i>	LAN ATM, multiprotocol over ATM (MPoA), and WAN ATM.
<i>Cisco IOS Asynchronous Transfer Mode Command Reference</i>	

Table 1 Cisco IOS and Cisco IOS XE Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
<p><i>Cisco IOS Bridging and IBM Networking Configuration Guide</i></p> <p><i>Cisco IOS Bridging Command Reference</i></p> <p><i>Cisco IOS IBM Networking Command Reference</i></p>	<ul style="list-style-type: none"> • Transparent and source-route transparent (SRT) bridging, source-route bridging (SRB), Token Ring Inter-Switch Link (TRISL), and token ring route switch module (TRRSM). • Data-link switching plus (DLSw+), serial tunnel (STUN), block serial tunnel (BSTUN); logical link control, type 2 (LLC2), synchronous data link control (SDLC); IBM Network Media Translation, including Synchronous Data Logical Link Control (SDLLC) and qualified LLC (QLLC); downstream physical unit (DSPU), Systems Network Architecture (SNA) service point, SNA frame relay access, advanced peer-to-peer networking (APPN), native client interface architecture (NCIA) client/server topologies, and IBM Channel Attach.
<p><i>Cisco IOS Broadband and DSL Configuration Guide</i></p> <p><i>Cisco IOS XE Broadband and DSL Configuration Guide</i></p> <p><i>Cisco IOS Broadband and DSL Command Reference</i></p>	Point-to-Point Protocol (PPP) over ATM (PPPoA) and PPP over Ethernet (PPPoE).
<p><i>Cisco IOS Carrier Ethernet Configuration Guide</i></p> <p><i>Cisco IOS Carrier Ethernet Command Reference</i></p>	Connectivity fault management (CFM), Ethernet Local Management Interface (ELMI), IEEE 802.3ad link bundling, Link Layer Discovery Protocol (LLDP), media endpoint discovery (MED), and operations, administration, and maintenance (OAM).
<p><i>Cisco IOS Configuration Fundamentals Configuration Guide</i></p> <p><i>Cisco IOS XE Configuration Fundamentals Configuration Guide</i></p> <p><i>Cisco IOS Configuration Fundamentals Command Reference</i></p>	Autoinstall, Setup, Cisco IOS command-line interface (CLI), Cisco IOS file system (IFS), Cisco IOS web browser user interface (UI), basic file transfer services, and file management.
<p><i>Cisco IOS DECnet Configuration Guide</i></p> <p><i>Cisco IOS XE DECnet Configuration Guide</i></p> <p><i>Cisco IOS DECnet Command Reference</i></p>	DECnet protocol.
<p><i>Cisco IOS Dial Technologies Configuration Guide</i></p> <p><i>Cisco IOS XE Dial Technologies Configuration Guide</i></p> <p><i>Cisco IOS Dial Technologies Command Reference</i></p>	Asynchronous communications, dial backup, dialer technology, dial-in terminal services and AppleTalk remote access (ARA), large scale dialout, dial-on-demand routing, dialout, modem and resource pooling, ISDN, multilink PPP (MLP), PPP, virtual private dialup network (VPDN).
<p><i>Cisco IOS Flexible NetFlow Configuration Guide</i></p> <p><i>Cisco IOS Flexible NetFlow Command Reference</i></p>	Flexible NetFlow.

Table 1 Cisco IOS and Cisco IOS XE Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
<i>Cisco IOS H.323 Configuration Guide</i>	Gatekeeper enhancements for managed voice services, Gatekeeper Transaction Message Protocol, gateway codec order preservation and shutdown control, H.323 dual tone multifrequency relay, H.323 version 2 enhancements, Network Address Translation (NAT) support of H.323 v2 Registration, Admission, and Status (RAS) protocol, tokenless call authorization, and VoIP gateway trunk and carrier-based routing.
<i>Cisco IOS High Availability Configuration Guide</i> <i>Cisco IOS XE High Availability Configuration Guide</i> <i>Cisco IOS High Availability Command Reference</i>	A variety of High Availability (HA) features and technologies that are available for different network segments (from enterprise access to service provider core) to facilitate creation of end-to-end highly available networks. Cisco IOS HA features and technologies can be categorized in three key areas: system-level resiliency, network-level resiliency, and embedded management for resiliency.
<i>Cisco IOS Integrated Session Border Controller Command Reference</i>	A VoIP-enabled device that is deployed at the edge of networks. An SBC is a toolkit of functions, such as signaling interworking, network hiding, security, and quality of service (QoS).
<i>Cisco IOS Intelligent Services Gateway Configuration Guide</i> <i>Cisco IOS Intelligent Services Gateway Command Reference</i>	Subscriber identification, service and policy determination, session creation, session policy enforcement, session life-cycle management, accounting for access and service usage, session state monitoring.
<i>Cisco IOS Interface and Hardware Component Configuration Guide</i> <i>Cisco IOS XE Interface and Hardware Component Configuration Guide</i> <i>Cisco IOS Interface and Hardware Component Command Reference</i>	LAN interfaces, logical interfaces, serial interfaces, virtual interfaces, and interface configuration.
<i>Cisco IOS IP Addressing Services Configuration Guide</i> <i>Cisco IOS XE Addressing Services Configuration Guide</i> <i>Cisco IOS IP Addressing Services Command Reference</i>	Address Resolution Protocol (ARP), Network Address Translation (NAT), Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), and Next Hop Address Resolution Protocol (NHRP).
<i>Cisco IOS IP Application Services Configuration Guide</i> <i>Cisco IOS XE IP Application Services Configuration Guide</i> <i>Cisco IOS IP Application Services Command Reference</i>	Enhanced Object Tracking (EOT), Gateway Load Balancing Protocol (GLBP), Hot Standby Router Protocol (HSRP), IP Services, Server Load Balancing (SLB), Stream Control Transmission Protocol (SCTP), TCP, Web Cache Communication Protocol (WCCP), User Datagram Protocol (UDP), and Virtual Router Redundancy Protocol (VRRP).
<i>Cisco IOS IP Mobility Configuration Guide</i> <i>Cisco IOS IP Mobility Command Reference</i>	Mobile ad hoc networks (MANet) and Cisco mobile networks.
<i>Cisco IOS IP Multicast Configuration Guide</i> <i>Cisco IOS XE IP Multicast Configuration Guide</i> <i>Cisco IOS IP Multicast Command Reference</i>	Protocol Independent Multicast (PIM) sparse mode (PIM-SM), bidirectional PIM (bidir-PIM), Source Specific Multicast (SSM), Multicast Source Discovery Protocol (MSDP), Internet Group Management Protocol (IGMP), and Multicast VPN (MVPN).

Table 1 Cisco IOS and Cisco IOS XE Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
<i>Cisco IOS IP Routing Protocols Configuration Guide</i> <i>Cisco IOS XE IP Routing Protocols Configuration Guide</i> <i>Cisco IOS IP Routing Protocols Command Reference</i>	Border Gateway Protocol (BGP), multiprotocol BGP, multiprotocol BGP extensions for IP multicast, bidirectional forwarding detection (BFD), Enhanced Interior Gateway Routing Protocol (EIGRP), Interior Gateway Routing Protocol (IGRP), Intermediate System-to-Intermediate System (IS-IS), on-demand routing (ODR), Open Shortest Path First (OSPF), and Routing Information Protocol (RIP).
<i>Cisco IOS IP SLAs Configuration Guide</i> <i>Cisco IOS XE IP SLAs Configuration Guide</i> <i>Cisco IOS IP SLAs Command Reference</i>	Cisco IOS IP Service Level Agreements (IP SLAs).
<i>Cisco IOS IP Switching Configuration Guide</i> <i>Cisco IOS XE IP Switching Configuration Guide</i> <i>Cisco IOS IP Switching Command Reference</i>	Cisco Express Forwarding, fast switching, and Multicast Distributed Switching (MDS).
<i>Cisco IOS IPv6 Configuration Guide</i> <i>Cisco IOS XE IPv6 Configuration Guide</i> <i>Cisco IOS IPv6 Command Reference</i>	For IPv6 features, protocols, and technologies, go to the IPv6 “Start Here” document at the following URL: http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-roadmap.html
<i>Cisco IOS ISO CLNS Configuration Guide</i> <i>Cisco IOS XE ISO CLNS Configuration Guide</i> <i>Cisco IOS ISO CLNS Command Reference</i>	ISO connectionless network service (CLNS).
<i>Cisco IOS LAN Switching Configuration Guide</i> <i>Cisco IOS XE LAN Switching Configuration Guide</i> <i>Cisco IOS LAN Switching Command Reference</i>	VLANs, Inter-Switch Link (ISL) encapsulation, IEEE 802.10 encapsulation, IEEE 802.1Q encapsulation, and multilayer switching (MLS).
<i>Cisco IOS Mobile Wireless Gateway GPRS Support Node Configuration Guide</i> <i>Cisco IOS Mobile Wireless Gateway GPRS Support Node Command Reference</i>	Cisco IOS Gateway GPRS Support Node (GGSN) in a 2.5-generation general packet radio service (GPRS) and 3-generation universal mobile telecommunication system (UMTS) network.
<i>Cisco IOS Mobile Wireless Home Agent Configuration Guide</i> <i>Cisco IOS Mobile Wireless Home Agent Command Reference</i>	Cisco Mobile Wireless Home Agent, an anchor point for mobile terminals for which mobile IP or proxy mobile IP services are provided.
<i>Cisco IOS Mobile Wireless Packet Data Serving Node Configuration Guide</i> <i>Cisco IOS Mobile Wireless Packet Data Serving Node Command Reference</i>	Cisco Packet Data Serving Node (PDSN), a wireless gateway that is between the mobile infrastructure and standard IP networks and that enables packet data services in a code division multiple access (CDMA) environment.
<i>Cisco IOS Mobile Wireless Radio Access Networking Configuration Guide</i> <i>Cisco IOS Mobile Wireless Radio Access Networking Command Reference</i>	Cisco IOS radio access network products.

Table 1 Cisco IOS and Cisco IOS XE Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
<p><i>Cisco IOS Multiprotocol Label Switching Configuration Guide</i></p> <p><i>Cisco IOS XE Multiprotocol Label Switching Configuration Guide</i></p> <p><i>Cisco IOS Multiprotocol Label Switching Command Reference</i></p>	MPLS Label Distribution Protocol (LDP), MPLS Layer 2 VPNs, MPLS Layer 3 VPNs, MPLS Traffic Engineering (TE), and MPLS Embedded Management (EM) and MIBs.
<p><i>Cisco IOS Multi-Topology Routing Configuration Guide</i></p> <p><i>Cisco IOS Multi-Topology Routing Command Reference</i></p>	Unicast and multicast topology configurations, traffic classification, routing protocol support, and network management support.
<p><i>Cisco IOS NetFlow Configuration Guide</i></p> <p><i>Cisco IOS XE NetFlow Configuration Guide</i></p> <p><i>Cisco IOS NetFlow Command Reference</i></p>	Network traffic data analysis, aggregation caches, export features.
<p><i>Cisco IOS Network Management Configuration Guide</i></p> <p><i>Cisco IOS XE Network Management Configuration Guide</i></p> <p><i>Cisco IOS Network Management Command Reference</i></p>	Basic system management; system monitoring and logging; troubleshooting, logging, and fault management; Cisco Discovery Protocol; Cisco IOS Scripting with Tool Control Language (Tcl); Cisco networking services (CNS); DistributedDirector; Embedded Event Manager (EEM); Embedded Resource Manager (ERM); Embedded Syslog Manager (ESM); HTTP; Remote Monitoring (RMON); SNMP; and VPN Device Manager Client for Cisco IOS Software (XSM Configuration).
<p><i>Cisco IOS Novell IPX Configuration Guide</i></p> <p><i>Cisco IOS XE Novell IPX Configuration Guide</i></p> <p><i>Cisco IOS Novell IPX Command Reference</i></p>	Novell Internetwork Packet Exchange (IPX) protocol.
<p><i>Cisco IOS Optimized Edge Routing Configuration Guide</i></p> <p><i>Cisco IOS Optimized Edge Routing Command Reference</i></p>	Optimized edge routing (OER) monitoring, policy configuration, routing control, logging and reporting, and VPN IPsec/generic routing encapsulation (GRE) tunnel interface optimization.
<p><i>Cisco IOS Quality of Service Solutions Configuration Guide</i></p> <p><i>Cisco IOS XE Quality of Service Solutions Configuration Guide</i></p> <p><i>Cisco IOS Quality of Service Solutions Command Reference</i></p>	Class-based weighted fair queuing (CBWFQ), custom queuing, distributed traffic shaping (DTS), generic traffic shaping (GTS), IP- to-ATM class of service (CoS), low latency queuing (LLQ), modular QoS CLI (MQC), Network-Based Application Recognition (NBAR), priority queuing, Security Device Manager (SDM), Multilink PPP (MLPPP) for QoS, header compression, AutoQoS, QoS features for voice, Resource Reservation Protocol (RSVP), weighted fair queuing (WFQ), and weighted random early detection (WRED).
<p><i>Cisco IOS Security Configuration Guide</i></p> <p><i>Cisco IOS XE Security Configuration Guide</i></p> <p><i>Cisco IOS Security Command Reference</i></p>	Access control lists (ACLs), authentication, authorization, and accounting (AAA), firewalls, IP security and encryption, neighbor router authentication, network access security, network data encryption with router authentication, public key infrastructure (PKI), RADIUS, TACACS+, terminal access security, and traffic filters.

Table 1 Cisco IOS and Cisco IOS XE Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
<i>Cisco IOS Service Selection Gateway Configuration Guide</i> <i>Cisco IOS Service Selection Gateway Command Reference</i>	Subscriber authentication, service access, and accounting.
<i>Cisco IOS Software Activation Configuration Guide</i> <i>Cisco IOS Software Activation Command Reference</i>	An orchestrated collection of processes and components to activate Cisco IOS software feature sets by obtaining and validating Cisco software licenses.
<i>Cisco IOS Software Modularity Installation and Configuration Guide</i> <i>Cisco IOS Software Modularity Command Reference</i>	Installation and basic configuration of software modularity images, including installations on single and dual route processors, installation rollbacks, software modularity binding, software modularity processes and patches.
<i>Cisco IOS Terminal Services Configuration Guide</i> <i>Cisco IOS Terminal Services Command Reference</i> <i>Cisco IOS XE Terminal Services Command Reference</i>	DEC, local-area transport (LAT), and X.25 packet assembler/disassembler (PAD).
<i>Cisco IOS Virtual Switch Command Reference</i>	Virtual switch redundancy, high availability, and packet handling; converting between standalone and virtual switch modes; virtual switch link (VSL); Virtual Switch Link Protocol (VSLP). Note For information about virtual switch configuration, refer to the product-specific software configuration information for the Cisco Catalyst 6500 series switch or for the Metro Ethernet 6500 series switch.
<i>Cisco IOS Voice Configuration Library</i> <i>Cisco IOS Voice Command Reference</i>	Cisco IOS support for voice call control protocols, interoperability, physical and virtual interface management, and troubleshooting. The library includes documentation for IP telephony applications.
<i>Cisco IOS VPDN Configuration Guide</i> <i>Cisco IOS XE VPDN Configuration Guide</i> <i>Cisco IOS VPDN Command Reference</i>	Layer 2 Tunneling Protocol (L2TP) dial-out load balancing and redundancy, L2TP extended failover, L2TP security VPDN, multihop by Dialed Number Identification Service (DNIS), timer and retry enhancements for L2TP and Layer 2 Forwarding (L2F), RADIUS Attribute 82: tunnel assignment ID, shell-based authentication of VPDN users, tunnel authentication via RADIUS on tunnel terminator.
<i>Cisco IOS Wide-Area Networking Configuration Guide</i> <i>Cisco IOS XE Wide-Area Networking Configuration Guide</i> <i>Cisco IOS Wide-Area Networking Command Reference</i>	Frame Relay, Layer 2 Tunneling Protocol Version 3 (L2TPv3), Link Access Procedure, Balanced (LAPB), Switched Multimegabit Data Service (SMDS), and X.25.
<i>Cisco IOS Wireless LAN Configuration Guide</i> <i>Cisco IOS Wireless LAN Command Reference</i>	Broadcast key rotation, IEEE 802.11x support, IEEE 802.1x authenticator, IEEE 802.1x local authentication service for Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST), Multiple Basic Service Set ID (BSSID), Wi-Fi Multimedia (WMM) required elements, and Wi-Fi Protected Access (WPA).

Table 2 Cisco IOS Supplementary Documents and Resources

Document Title	Description
<i>Cisco IOS Master Command List, All Releases</i>	Alphabetical list of all the commands documented in all Cisco IOS releases.
<i>Cisco IOS New, Modified, Removed, and Replaced Commands</i>	List of all the new, modified, removed, and replaced commands for a Cisco IOS release.
<i>Cisco IOS Software System Messages</i>	List of Cisco IOS system messages and descriptions. System messages may indicate problems with your system; be informational only; or may help diagnose problems with communications lines, internal hardware, or the system software.
<i>Cisco IOS Debug Command Reference</i>	Alphabetical list of debug commands including brief descriptions of use, command syntax, and usage guidelines.
Release Notes and Caveats	Information about new and changed features, system requirements, and other useful information about specific software releases; information about defects in specific Cisco IOS software releases.
MIBs	Files used for network monitoring. To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator at the following URL: http://www.cisco.com/go/mibs
RFCs	Standards documents maintained by the Internet Engineering Task Force (IETF) that Cisco IOS documentation references where applicable. The full text of referenced RFCs may be obtained at the following URL: http://www.rfc-editor.org/

Additional Resources and Documentation Feedback

What's New in Cisco Product Documentation is published monthly and describes all new and revised Cisco technical documentation. The *What's New in Cisco Product Documentation* publication also provides information about obtaining the following resources:

- Technical documentation
- Cisco product security overview
- Product alerts and field notices
- Technical assistance

Cisco IOS technical documentation includes embedded feedback forms where you can rate documents and provide suggestions for improvement. Your feedback helps us improve our documentation.

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0812R)

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.

© 2008–2009 Cisco Systems, Inc. All rights reserved.



Using the Command-Line Interface in Cisco IOS and Cisco IOS XE Software

Last Updated: March 5, 2009

This document provides basic information about the command-line interface (CLI) in Cisco IOS and Cisco IOS XE software and how you can use some of the CLI features. This document contains the following sections:

- [Initially Configuring a Device, page i](#)
- [Using the CLI, page ii](#)
- [Saving Changes to a Configuration, page xii](#)
- [Additional Information, page xii](#)

For more information about using the CLI, see the “[Using the Cisco IOS Command-Line Interface](#)” section of the *Cisco IOS Configuration Fundamentals Configuration Guide*.

For information about the software documentation set, see the “[About Cisco IOS and Cisco IOS XE Software Documentation](#)” document.

Initially Configuring a Device

Initially configuring a device varies by platform. For information about performing an initial configuration, see the hardware installation documentation that is provided with the original packaging of the product or go to the Product Support area of Cisco.com at <http://www.cisco.com/web/psa/products/index.html>.

After you have performed the initial configuration and connected the device to your network, you can configure the device by using the console port or a remote access method, such as Telnet or Secure Shell (SSH), to access the CLI or by using the configuration method provided on the device, such as Security Device Manager.

Changing the Default Settings for a Console or AUX Port

There are only two changes that you can make to a console port and an AUX port:

- Change the port speed with the **config-register 0x** command. Changing the port speed is not recommended. The well-known default speed is 9600.
- Change the behavior of the port; for example, by adding a password or changing the timeout value.

**Note**

The AUX port on the Route Processor (RP) installed in a Cisco ASR1000 series router does not serve any useful customer purpose and should be accessed only under the advisement of a customer support representative.

Using the CLI

This section describes the following topics:

- [Understanding Command Modes, page ii](#)
- [Using the Interactive Help Feature, page v](#)
- [Understanding Command Syntax, page vi](#)
- [Understanding Enable and Enable Secret Passwords, page viii](#)
- [Using the Command History Feature, page viii](#)
- [Abbreviating Commands, page ix](#)
- [Using Aliases for CLI Commands, page ix](#)
- [Using the no and default Forms of Commands, page x](#)
- [Using the debug Command, page x](#)
- [Filtering Output Using Output Modifiers, page x](#)
- [Understanding CLI Error Messages, page xi](#)

Understanding Command Modes

The CLI command mode structure is hierarchical, and each mode supports a set of specific commands. This section describes the most common of the many modes that exist.

[Table 1](#) lists common command modes with associated CLI prompts, access and exit methods, and a brief description of how each mode is used.

Table 1 CLI Command Modes

Command Mode	Access Method	Prompt	Exit Method	Mode Usage
User EXEC	Log in.	Router>	Issue the logout or exit command.	<ul style="list-style-type: none"> • Change terminal settings. • Perform basic tests. • Display device status.
Privileged EXEC	From user EXEC mode, issue the enable command.	Router#	Issue the disable command or the exit command to return to user EXEC mode.	<ul style="list-style-type: none"> • Issue show and debug commands. • Copy images to the device. • Reload the device. • Manage device configuration files. • Manage device file systems.
Global configuration	From privileged EXEC mode, issue the configure terminal command.	Router(config)#	Issue the exit command or the end command to return to privileged EXEC mode.	Configure the device.
Interface configuration	From global configuration mode, issue the interface command.	Router(config-if)#	Issue the exit command to return to global configuration mode or the end command to return to privileged EXEC mode.	Configure individual interfaces.
Line configuration	From global configuration mode, issue the line vty or line console command.	Router(config-line)#	Issue the exit command to return to global configuration mode or the end command to return to privileged EXEC mode.	Configure individual terminal lines.

Table 1 CLI Command Modes (continued)

Command Mode	Access Method	Prompt	Exit Method	Mode Usage
ROM monitor	From privileged EXEC mode, issue the reload command. Press the Break key during the first 60 seconds while the system is booting.	rommon # > The # symbol represents the line number and increments at each prompt.	Issue the continue command.	<ul style="list-style-type: none"> Run as the default operating mode when a valid image cannot be loaded. Access the fall-back procedure for loading an image when the device lacks a valid image and cannot be booted. Perform password recovery when a CTRL-Break sequence is issued within 60 seconds of a power-on or reload event.
Diagnostic (available only on the Cisco ASR1000 series router)	<p>The router boots or enters diagnostic mode in the following scenarios. When a Cisco IOS process or processes fail, in most scenarios the router will reload.</p> <ul style="list-style-type: none"> A user-configured access policy was configured using the transport-map command, which directed the user into diagnostic mode. The router was accessed using an RP auxiliary port. A break signal (Ctrl-C, Ctrl-Shift-6, or the send break command) was entered, and the router was configured to enter diagnostic mode when the break signal was received. 	Router(diag)#	<p>If a Cisco IOS process failure is the reason for entering diagnostic mode, the failure must be resolved and the router must be rebooted to exit diagnostic mode.</p> <p>If the router is in diagnostic mode because of a transport-map configuration, access the router through another port or using a method that is configured to connect to the Cisco IOS CLI.</p> <p>If the RP auxiliary port was used to access the router, use another port for access. Accessing the router through the auxiliary port is not useful for customer purposes.</p>	<ul style="list-style-type: none"> Inspect various states on the router, including the Cisco IOS state. Replace or roll back the configuration. Provide methods of restarting the Cisco IOS software or other processes. Reboot hardware, such as the entire router, an RP, an ESP, a SIP, a SPA, or possibly other hardware components. Transfer files into or off of the router using remote access methods such as FTP, TFTP, and SCP.

EXEC commands are not saved when the software reboots. Commands that you issue in a configuration mode can be saved to the startup configuration. If you save the running configuration to the startup configuration, these commands will execute when the software is rebooted. Global configuration mode is the highest level of configuration mode. From global configuration mode, you can enter a variety of other configuration modes, including protocol-specific modes.

ROM monitor mode is a separate mode that is used when the software cannot load properly. If a valid software image is not found when the software boots or if the configuration file is corrupted at startup, the software might enter ROM monitor mode. Use the question symbol (?) to view the commands that you can use while the device is in ROM monitor mode.

```
rommon 1 > ?
alias                set and display aliases command
boot                 boot up an external process
confreg              configuration register utility
cont                 continue executing a downloaded image
context              display the context of a loaded image
cookie               display contents of cookie PROM in hex
.
.
.
rommon 2 >
```

The following example shows how the command prompt changes to indicate a different command mode:

```
Router> enable
Router# configure terminal
Router(config)# interface ethernet 1/1
Router(config-if)# ethernet
Router(config-line)# exit
Router(config)# end
Router#
```



Note

A keyboard alternative to the **end** command is Ctrl-Z.

Using the Interactive Help Feature

The CLI includes an interactive Help feature. [Table 2](#) describes how to use the Help feature.

Table 2 CLI Interactive Help Commands

Command	Purpose
help	Provides a brief description of the help feature in any command mode.
?	Lists all commands available for a particular command mode.
<i>partial command?</i>	Provides a list of commands that begin with the character string (no space between the command and the question mark).
<i>partial command</i> <Tab>	Completes a partial command name (no space between the command and <Tab>).
<i>command ?</i>	Lists the keywords, arguments, or both associated with the command (space between the command and the question mark).
<i>command keyword ?</i>	Lists the arguments that are associated with the keyword (space between the keyword and the question mark).

The following examples show how to use the help commands:

help

```
Router> help
```

Help may be requested at any point in a command by entering a question mark '?'. If nothing matches, the help list will be empty and you must backup until entering a '?' shows the available options.

Two styles of help are provided:

1. Full help is available when you are ready to enter a command argument (e.g. 'show ?') and describes each possible argument.
2. Partial help is provided when an abbreviated argument is entered and you want to know what arguments match the input (e.g. 'show pr?'.)

?

```
Router# ?
```

```
Exec commands:
```

access-enable	Create a temporary access-List entry
access-profile	Apply user-profile to interface
access-template	Create a temporary access-List entry
alps	ALPS exec commands
archive	manage archive files

```
<snip>
```

partial command?

```
Router(config)# zo?
```

```
zone zone-pair
```

partial command<Tab>

```
Router(config)# we<Tab> webvpn
```

command?

```
Router(config-if)# pppoe ?
```

enable	Enable pppoe
max-sessions	Maximum PPPOE sessions

command keyword?

```
Router(config-if)# pppoe enable ?
```

group	attach a BBA group
-------	--------------------

```
<cr>
```

Understanding Command Syntax

Command syntax is the format in which a command should be entered in the CLI. Commands include the name of the command, keywords, and arguments. Keywords are alphanumeric strings that are used literally. Arguments are placeholders for values that a user must supply. Keywords and arguments may be required or optional.

Specific conventions convey information about syntax and command elements. [Table 3](#) describes these conventions.

Table 3 CLI Syntax Conventions

Symbol/Text	Function	Notes
< > (angle brackets)	Indicate that the option is an argument.	Sometimes arguments are displayed without angle brackets.
A.B.C.D.	Indicates that you must enter a dotted decimal IP address.	Angle brackets (< >) are not always used to indicate that an IP address is an argument.
WORD (all capital letters)	Indicates that you must enter one word.	Angle brackets (< >) are not always used to indicate that a WORD is an argument.
LINE (all capital letters)	Indicates that you must enter more than one word.	Angle brackets (< >) are not always used to indicate that a LINE is an argument.
<cr> (carriage return)	Indicates the end of the list of available keywords and arguments, and also indicates when keywords and arguments are optional. When <cr> is the only option, you have reached the end of the branch or the end of the command if the command has only one branch.	—

The following examples show syntax conventions:

```

Router(config)# ethernet cfm domain ?
    WORD domain name
Router(config)# ethernet cfm domain dname ?
    level
Router(config)# ethernet cfm domain dname level ?
    <0-7> maintenance level number
Router(config)# ethernet cfm domain dname level 7 ?
    <cr>
Router(config)# snmp-server file-transfer access-group 10 ?
    protocol protocol options
    <cr>
Router(config)# logging host ?
    Hostname or A.B.C.D IP address of the syslog server
    ipv6 Configure IPv6 syslog server
Router(config)# snmp-server file-transfer access-group 10 ?
    protocol protocol options
    <cr>

```

Understanding Enable and Enable Secret Passwords

Some privileged EXEC commands are used for actions that impact the system, and it is recommended that you set a password for these commands to prevent unauthorized use. Two types of passwords, enable (not encrypted) and enable secret (encrypted), can be set. The following commands set these passwords and are issued in global configuration mode:

- **enable** *password*
- **enable secret** *password*

Using an enable secret password is recommended because it is encrypted and more secure than the enable password. When you use an enable secret password, text is encrypted (unreadable) before it is written to the config.text file. When you use an enable password, the text is written as entered (readable) to the config.text file.

Each type of password is case sensitive, can contain from 1 to 25 uppercase and lowercase alphanumeric characters, and can start with a number. Spaces are also valid password characters; for example, “two words” is a valid password. Leading spaces are ignored, but trailing spaces are recognized.



Note

Both password commands have numeric keywords that are single integer values. If you choose a number for the first character of your password followed by a space, the system will read the number as if it were the numeric keyword and not as part of your password.

When both passwords are set, the enable secret password takes precedence over the enable password.

To remove a password, use the **no** form of the commands: **no enable** *password* or **no enable secret** *password*.

For more information about password recovery procedures for Cisco products, see http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00801746e6.shtml.

Using the Command History Feature

The CLI command history feature saves the commands you enter during a session in a command history buffer. The default number of commands saved is 10, but the number is configurable within the range of 0 to 256. This command history feature is particularly useful for recalling long or complex commands.

To change the number of commands saved in the history buffer for a terminal session, issue the **terminal history size** command:

```
Router# terminal history size num
```

A command history buffer is also available in line configuration mode with the same default and configuration options. To set the command history buffer size for a terminal session in line configuration mode, issue the **history** command:

```
Router(config-line)# history [size num]
```

To recall commands from the history buffer, use the following methods:

- Press Ctrl-P or the up arrow key—Recalls commands beginning with the most recent command. Repeat the key sequence to recall successively older commands.

- Press Ctrl-N or the down arrow key—Recalls the most recent commands in the history buffer after they have been recalled using Ctrl-P or the up arrow key. Repeat the key sequence to recall successively more recent commands.



Note The arrow keys function only on ANSI-compatible terminals such as the VT100.

- Issue the **show history** command in user EXEC or privileged EXEC mode—Lists the most recent commands that you entered. The number of commands that are displayed is determined by the setting of the **terminal history size** and **history** commands.

The CLI command history feature is enabled by default. To disable this feature for a terminal session, issue the **terminal no history** command in user EXEC or privileged EXEC mode or the **no history** command in line configuration mode.

Abbreviating Commands

Typing a complete command name is not always required for the command to execute. The CLI recognizes an abbreviated command when the abbreviation contains enough characters to uniquely identify the command. For example, the **show version** command can be abbreviated as **sh ver**. It cannot be abbreviated as **s ver** because **s** could mean **show**, **set**, or **systat**. The **sh v** abbreviation also is not valid because the **show** command has **vrp** as a keyword in addition to **version**. (Command and keyword examples from Cisco IOS Release 12.4(13)T.)

Using Aliases for CLI Commands

To save time and the repetition of entering the same command multiple times, you can use a command alias. An alias can be configured to do anything that can be done at the command line, but an alias cannot move between modes, type in passwords, or perform any interactive functions.

Table 4 shows the default command aliases.

Table 4 Default Command Aliases

Command Alias	Original Command
h	help
lo	logout
p	ping
s	show
u or un	undebug
w	where

To create a command alias, issue the **alias** command in global configuration mode. The syntax of the command is **alias mode command-alias original-command**. Following are some examples:

- Router(config)# **alias exec prt partition**—privileged EXEC mode
- Router(config)# **alias configure sb source-bridge**—global configuration mode
- Router(config)# **alias interface rl rate-limit**—interface configuration mode

To view both default and user-created aliases, issue the **show alias** command.

For more information about the **alias** command, see

http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_book.html.

Using the no and default Forms of Commands

Most configuration commands have a **no** form that is used to reset a command to its default value or disable a feature or function. For example, the **ip routing** command is enabled by default. To disable this command, you would issue the **no ip routing** command. To re-enable IP routing, you would issue the **ip routing** command.

Configuration commands may also have a **default** form, which returns the command settings to their default values. For commands that are disabled by default, using the **default** form has the same effect as using the **no** form of the command. For commands that are enabled by default and have default settings, the **default** form enables the command and returns the settings to their default values.

The **no** and **default** forms of commands are described in the command pages of command references.

Using the debug Command

A **debug** command produces extensive output that helps you troubleshoot problems in your network. These commands are available for many features and functions within Cisco IOS and Cisco IOS XE software. Some **debug** commands are **debug all**, **debug aaa accounting**, and **debug mpls packets**. To use **debug** commands during a Telnet session with a device, you must first enter the **terminal monitor** command. To turn off debugging completely, you must enter the **undebug all** command.

For more information about **debug** commands, see the *Cisco IOS Debug Command Reference* at

http://www.cisco.com/en/US/docs/ios/debug/command/reference/db_book.html.



Caution

Debugging is a high priority and high CPU utilization process that can render your device unusable. Use **debug** commands only to troubleshoot specific problems. The best times to run debugging are during periods of low network traffic and when few users are interacting with the network. Debugging during these periods decreases the likelihood that the **debug** command processing overhead will affect network performance or user access or response times.

Filtering Output Using Output Modifiers

Many commands produce lengthy output that may use several screens to display. Using output modifiers, you can filter this output to show only the information that you want to see.

Three output modifiers are available and are described as follows:

- **begin** *regular expression*—Displays the first line in which a match of the regular expression is found and all lines that follow.
- **include** *regular expression*—Displays all lines in which a match of the regular expression is found.
- **exclude** *regular expression*—Displays all lines except those in which a match of the regular expression is found.

To use one of these output modifiers, type the command followed by the pipe symbol (`|`), the modifier, and the regular expression that you want to search for or filter. A regular expression is a case-sensitive alphanumeric pattern. It can be a single character or number, a phrase, or a more complex string.

The following example illustrates how to filter output of the **show interface** command to display only lines that include the expression “protocol.”

```
Router# show interface | include protocol

FastEthernet0/0 is up, line protocol is up
Serial4/0 is up, line protocol is up
Serial4/1 is up, line protocol is up
Serial4/2 is administratively down, line protocol is down
Serial4/3 is administratively down, line protocol is down
```

Understanding CLI Error Messages

You may encounter some error messages while using the CLI. [Table 5](#) shows the common CLI error messages.

Table 5 Common CLI Error Messages

Error Message	Meaning	How to Get Help
% Ambiguous command: “show con”	You did not enter enough characters for the command to be recognized.	Reenter the command followed by a space and a question mark (?). The keywords that you are allowed to enter for the command appear.
% Incomplete command.	You did not enter all the keywords or values required by the command.	Reenter the command followed by a space and a question mark (?). The keywords that you are allowed to enter for the command appear.
% Invalid input detected at “^” marker.	You entered the command incorrectly. The caret (^) marks the point of the error.	Enter a question mark (?) to display all the commands that are available in this command mode. The keywords that you are allowed to enter for the command appear.

For more system error messages, see the following documents:

- [Cisco IOS Release 12.2SR System Message Guide](#)
- [Cisco IOS System Messages, Volume 1 of 2](#) (Cisco IOS Release 12.4)
- [Cisco IOS System Messages, Volume 2 of 2](#) (Cisco IOS Release 12.4)

Saving Changes to a Configuration

To save changes that you made to the configuration of a device, you must issue the **copy running-config startup-config** command or the **copy system:running-config nvram:startup-config** command. When you issue these commands, the configuration changes that you made are saved to the startup configuration and saved when the software reloads or power to the device is turned off or interrupted. The following example shows the syntax of the **copy running-config startup-config** command:

```
Router# copy running-config startup-config
Destination filename [startup-config]?
```

You press Enter to accept the startup-config filename (the default), or type a new filename and then press Enter to accept that name. The following output is displayed indicating that the configuration was saved:

```
Building configuration...
[OK]
Router#
```

On most platforms, the configuration is saved to NVRAM. On platforms with a Class A flash file system, the configuration is saved to the location specified by the CONFIG_FILE environment variable. The CONFIG_FILE variable defaults to NVRAM.

Additional Information

- “Using the Cisco IOS Command-Line Interface” section of the *Cisco IOS Configuration Fundamentals Configuration Guide*:
http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/cf_cli-basics.html
or
“Using Cisco IOS XE Software” chapter of the *Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide*:
http://www.cisco.com/en/US/docs/routers/asr1000/configuration/guide/chassis/Using_CLI.html
- Cisco Product Support Resources
<http://www.cisco.com/web/psa/products/index.html>
- Support area on Cisco.com (also search for documentation by task or product)
<http://www.cisco.com/en/US/support/index.html>
- Software Download Center (downloads; tools; licensing, registration, advisory, and general information) (requires Cisco.com User ID and password)
<http://www.cisco.com/kobayashi/sw-center/>
- Error Message Decoder, a tool to help you research and resolve error messages for Cisco IOS software
<http://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi>
- Command Lookup Tool, a tool to help you find detailed descriptions of Cisco IOS commands (requires Cisco.com user ID and password)
<http://tools.cisco.com/Support/CLILookup>

- Output Interpreter, a troubleshooting tool that analyzes command output of supported **show** commands

<https://www.cisco.com/pcgi-bin/Support/OutputInterpreter/home.pl>

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0812R)

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.

© 2008–2009 Cisco Systems, Inc. All rights reserved.



Cisco Unified Communications Manager and Cisco IOS Interoperability Features Roadmap

This guide provides configuration information about Cisco IOS voice features for Cisco Unified Communications Manager (formerly known as Cisco Unified CallManager) and Cisco IOS Interoperability. This first chapter describes how to access Cisco Feature Navigator and lists Cisco Unified Communications Manager and Cisco IOS Interoperability features by Cisco IOS release.



Note

For information about the full set of Cisco IOS voice features, see the entire Cisco IOS Voice Configuration Library—including library preface, glossary, and other documents—at http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/voice_c/vcl.htm.

Contents

- [Platforms and Cisco IOS Software Images, page 1](#)
- [Cisco Unified Communications Manager and Cisco IOS Interoperability Feature List, page 2](#)

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.



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Cisco Unified Communications Manager and Cisco IOS Interoperability Feature List

Table 1 lists Cisco Unified Communications Manager and Cisco IOS Interoperability features by Cisco IOS release. Features that are introduced in a particular release are available in that and subsequent releases.

Table 1 Cisco Unified Communications Manager and Cisco IOS Interoperability Features

Release	Features Introduced in That Release ¹	Feature Description	Feature Documentation
12.4(6)T	RSVP Agent	Enables Cisco Unified Communications Manager to provide resource reservation for voice and video media to ensure QoS and call admission control (CAC).	“Configuring RSVP Agent” on page 177 of this guide.
12.3(11)T	MCID for Cisco IOS Voice Gateways	Supports the Malicious Call Identification (MCID) supplementary service in Cisco Unified Communications Manager 4.0 (formerly known as Cisco Unified CallManager 4.0).	“Configuring MCID for Cisco IOS Voice Gateways” on page 163 of this guide.
	MLPP for Cisco IOS Voice Gateways	Supports Multilevel Precedence and Preemption (MLPP) service, allowing authorized users to preempt lower priority voice calls using Cisco Unified Communications Manager 4.0 (formerly known as Cisco Unified CallManager 4.0).	“Configuring MLPP Service on Cisco MGCP Gateways” section on page 50 of this guide.
	Out-of-Band to In-Band DTMF Relay for Cisco IOS Voice Gateways	RFC 2833 capability enabling DTMF relay communication between SIP devices and nonSIP endpoints using Cisco Unified Communications Manager 4.0 (formerly known as Cisco Unified CallManager 4.0).	“Configuring Conferencing and Transcoding (NM-HDV)” section on page 93 of this guide.
	QSIG Supplementary Features for Cisco IOS Voice Gateways	Supports Q Signaling (QSIG) over PRI backhaul interfaces on MGCP gateways to Cisco Unified Communications Manager 4.0 (formerly known as Cisco Unified CallManager 4.0).	“Configuring QSIG Supplementary Features for Cisco IOS Voice Gateways” section on page 124 of this guide.
12.3(8)T	Enhanced Conferencing and Transcoding for Voice Gateway Routers	Enables conferencing, transcoding, and MTP support for Cisco voice gateways using the NM-HDV2 and NM-HD high-density voice network modules.	“Configuring Enhanced Conferencing and Transcoding for Voice Gateway Routers” on page 67 of this guide.

Table 1 *Cisco Unified Communications Manager and Cisco IOS Interoperability Features (continued)*

Release	Features Introduced in That Release¹	Feature Description	Feature Documentation
12.3(4)T	MGCP Gateway Support for Cisco Unified Communications Manager Network Specific Facilities	Supports the configuration of the network specific facilities (NSF) ISDN information element in route patterns for Cisco Unified Communications Manager 3.3 (formerly known as Cisco Unified CallManager 3.3).	“Configuring MGCP Gateway Support for Cisco Unified Communications Manager Network Specific Facilities” section on page 120 of this guide.
	Customizable Tone Download to Cisco IOS MGCP Gateways from Cisco Unified Communications Manager	Enables the downloading of region-specific tones and associated frequencies, amplitudes, and cadences.	“Configuring Tone Download to MGCP Gateways” on page 145 of this guide.
12.3(2)T	MGCP-Controlled Backhaul of BRI Signaling in Conjunction with Cisco Unified Communications Manager	Enables the transporting of signaling information from remote-office MGCP gateways connected by ISDN BRI trunks to a centralized Cisco Unified Communications Manager.	“Configuring MGCP-Controlled Backhaul of BRI Signaling in Conjunction with Cisco Unified Communications Manager” on page 129 of this guide.
12.2(13)T	Conferencing and Transcoding for Voice Gateway Routers	Enables conferencing and transcoding support for Cisco voice gateways using NM-HDV high-density voice network modules.	“Configuring Enhanced Conferencing and Transcoding for Voice Gateway Routers” on page 67 of this guide.
	Update to the Interworking of Cisco MGCP Voice Gateways and Cisco Unified Communications Manager Version 3.2 (formerly known as Cisco CallManager Version 3.2)	Adds support for the mgcp validate domain-name command, which checks whether the domain name or IP address received in MGCP messages match those on the gateway.	“Enabling MGCP on Cisco IOS Gateways” section on page 27 of this guide.

Table 1 Cisco Unified Communications Manager and Cisco IOS Interoperability Features (continued)

Release	Features Introduced in That Release ¹	Feature Description	Feature Documentation
12.2(11)T	Globalized Cadence and Tone for Cisco IOS Gateways	Enables Cisco MGCP gateways to provide localized cadence and tones for Cisco Communications Manager 3.2 (formerly known as Cisco CallManager 3.2), eliminating the need for the cptone command.	“Configuring Tone Download to MGCP Gateways” on page 145 of this guide.
	MGCP Gateway Fallback	Provides basic call processing support in H.323 mode when an MGCP gateway loses connectivity to all of its configured Cisco Unified Communications Manager servers.	“Configuring Cisco Unified Communications Manager Switchover and MGCP Gateway Fallback” section on page 30 of this guide.
	MGCP Generic Configuration Support for Cisco Unified Communications Manager	Provides single-point configuration using a centralized TFTP server to automatically download XML configuration files to MGCP gateways.	“Enabling Single-Point Configuration for MGCP Gateways” section on page 45 of this guide.
	MGCP PRI Backhaul and T1-CAS Support for Cisco Unified Communications Manager	Enables transporting of complete IP-telephony signaling from an ISDN PRI interface on an MGCP gateway to Cisco Unified Communications Manager 3.1 and 3.2 (formerly known as Cisco CallManager 3.1 and 3.2).	“Configuring MGCP PRI Backhaul and T1 CAS Support for Cisco Unified Communications Manager” on page 113 of this guide.
	Multicast Music on Hold Support for Cisco Unified Communications Manager	Enables music streaming from a music-on-hold (MOH) server to callers placed on hold using an MGCP gateway and Cisco Unified Communications Manager 3.1 and 3.2 (formerly known as Cisco CallManager 3.1 and 3.2).	“Configuring Multicast Music-on-Hold Support for Cisco Unified Communications Manager” section on page 48 of this guide.
12.1(3)T	MGCP Support for Cisco Unified Communications Manager	Adds MGCP support to Cisco IOS gateways to provide supplementary services, failover, and redundancy support for Cisco Unified Communications Manager 3.0 (formerly known as Cisco CallManager 3.0).	“Configuring Cisco Unified Communications Manager Switchover and MGCP Gateway Fallback” section on page 30 of this guide.

1. Features that are introduced in a particular release are available in that and subsequent releases.

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0709R)

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

© 2007 Cisco Systems, Inc. All rights reserved.



Overview of Cisco Unified Communications Manager and Cisco IOS 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](#).

Contents

- [Information About Cisco Unified Communications Manager and Cisco IOS Interoperability, page 1](#)
- [Toll Fraud Prevention, page 6](#)
- [Additional References, page 7](#)

Information About Cisco Unified Communications Manager and Cisco IOS Interoperability

To configure a Cisco IOS voice gateway to interoperate with Cisco Unified Communications Manager, you should understand the following concepts:

- [Cisco AVVID, page 2](#)
- [Cisco Unified Communications Manager Interoperability, page 2](#)
- [MGCP Voice Gateways, page 2](#)
- [MGCP Advantages Over H.323, page 5](#)
- [Conferencing and Transcoding, page 6](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

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:

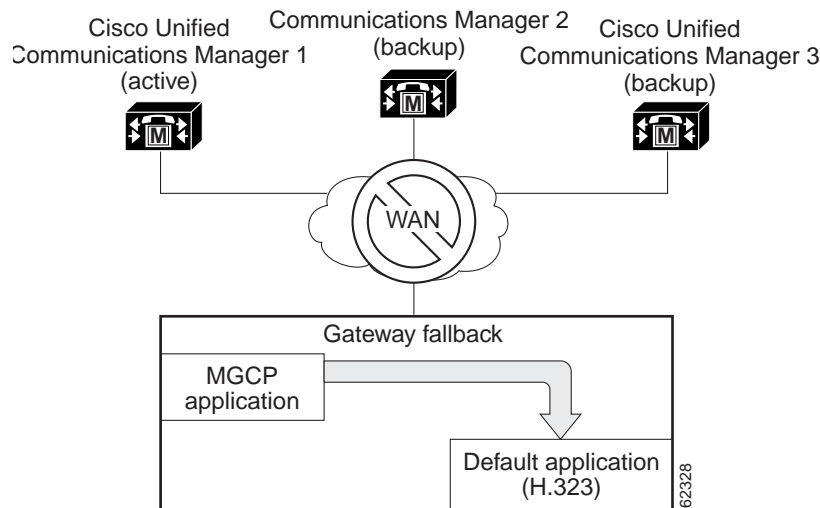
- [MGCP Gateway Fallback, page 3](#)
- [MGCP PRI Backhaul, page 4](#)
- [MGCP BRI Backhaul, page 4](#)
- [Multicast Music-On-Hold, page 4](#)
- [Network Specific Facilities, page 4](#)
- [Single-Point Configuration, page 4](#)
- [Supplementary Services, page 4](#)
- [Switchover \(Failover\), page 5](#)
- [Switchback, page 5](#)
- [Tones and Cadences, page 5](#)

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 [Figure 1](#)).

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
<i>Additional Cisco IOS Voice Configuration Library documents, including library preface and glossary</i>	Cisco IOS Voice Configuration Library
Cisco IOS command references	<ul style="list-style-type: none"> • 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 .
Cisco IOS software system messages	Cisco IOS Software System Messages
Cisco IOS troubleshooting information	Cisco IOS Voice Troubleshooting and Monitoring Guide

Related Topic	Document Title
Cisco Unified Communications Manager <ul style="list-style-type: none"> • Administration and configuration • Upgrading • Transcoder services and configuration • Voice-conference services and configuration 	<ul style="list-style-type: none"> • 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 Cisco Unified CallManager Release 4.0(1) • “Transcoders” chapter in the Cisco Unified Communications Manager System Guide • “Transcoder Configuration” chapter in the Cisco Unified Communications Manager Administration Guide • “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)
<ul style="list-style-type: none"> • MCID • MLPP 	“Malicious Call Identification” chapter in the Cisco Unified Communications Manager Features and Services Guide “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
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	<i>ISDN User-Network Interface Layer 3 specification</i> (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	<i>Requirements for Private Branch Exchange (PBX) Switching Equipment</i>

MIBs

MIBs	MIBs Link
<ul style="list-style-type: none"> • Transcoding: <ul style="list-style-type: none"> - 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 	<p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p>http://www.cisco.com/go/mibs</p>

RFCs

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

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>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.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p>http://www.cisco.com/techsupport</p>

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flip Video, Flip Video (Design), Flipshare (Design), Flip Ultra, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0907R)

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.

© 2009 Cisco Systems, Inc. All rights reserved.



Configuring MGCP Gateway Support for Cisco Unified Communications Manager

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

Feature History for MLPP for Cisco IOS Voice Gateways

Release	Modification
12.3(8)XY	This feature was introduced.
12.3(11)T	This feature was integrated into Cisco IOS Release 12.3(11)T.

Feature History for MGCP Generic Configuration Support for Cisco Unified Communications Manager

Release	Modification
12.2(2)XN	This feature was introduced.
12.2(11)T	This feature was integrated into Cisco IOS Release 12.2(11)T.

Feature History for Multicast Music-on-Hold

Release	Modification
12.2(2)XN	This feature was introduced.
12.2(11)T	This feature was integrated into Cisco IOS Release 12.2(11)T.

Feature History for MGCP Support for Cisco Unified Communications Manager

Release	Modification
12.1(3)T	This feature was introduced for Cisco Unified Communications Manager 3.0 (formerly known as Cisco CallManager 3.0).
12.1(5)XM	H.323 support was added for E1 and T1 PRI, E&M, E1-CAS, and BRI. Analog support for MGCP and analog DID were added.
12.2(2)XA	Support was added for Cisco Unified Communications Manager 3.0(8) (formerly known as Cisco CallManager 3.0(8)).



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

12.2(2)XN	Support was added for Cisco Unified Communications Manager 3.1 (formerly known as Cisco CallManager 3.1). New MGCP features included ISDN PRI Backhaul and T1 CAS, Single-Point Configuration, MGCP Gateway Fallback, and Multicast Music-on-Hold (MOH).
12.2(11)T	Support was added for Cisco Unified Communications Manager 3.2 (formerly known as Cisco CallManager 3.2).

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.



Note

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/univerd/cc/td/doc/product/software/ios123/123cgr/voice_c/vcl.htm.

Contents

- Prerequisites for Configuring MGCP Gateway Support for Cisco Unified Communications Manager, page 2
- Restrictions for Configuring MGCP Gateway Support for Cisco Unified Communications Manager, page 3
- Information about MGCP Gateway Support for Cisco Unified Communications Manager, page 3
- How to Configure MGCP Gateway Support for Cisco Unified Communications Manager, page 4
- Configuration Examples for MGCP Gateway Support for Cisco Communications Manager, page 33
- Where to Go Next, page 42
- Additional References, page 43

Prerequisites for Configuring MGCP Gateway Support for Cisco Unified Communications Manager

- 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 for Cisco Unified Communications Manager

- 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 for Cisco Unified Communications Manager

To configure MGCP gateways to act under the control of Cisco Unified Communications Manager, you should understand the following concept:

- [MGCP Gateways and Cisco Unified Communications Manager, page 3](#)

MGCP Gateways and Cisco Unified Communications Manager

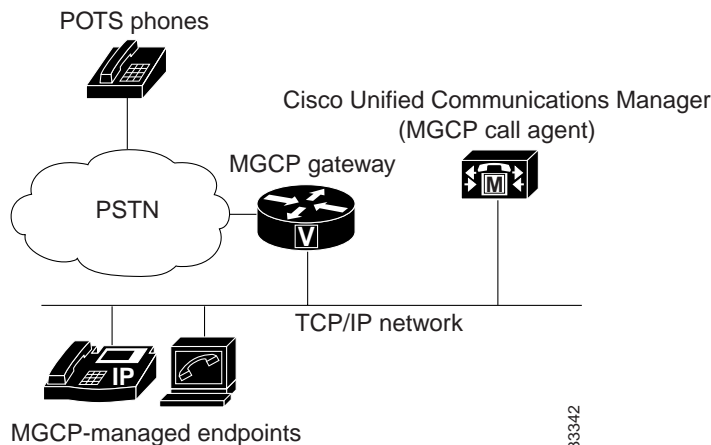
MGCP enables the remote control and management of voice and data communications devices at the edge of multiservice IP packet networks. Because of its centralized architecture, MGCP overcomes the distributed configuration and administration problems inherent in the use of protocols such as H.323. MGCP 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.

Figure 2 shows a typical MGCP gateway that is controlled by an MGCP call agent.

Figure 2 *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.

How to Configure MGCP Gateway Support for Cisco Unified Communications Manager

This section contains the following procedures:

- [Enabling MGCP on Cisco IOS Gateways, page 5](#) (required)
- [Verifying MGCP Configuration on the Cisco IOS Gateway, page 7](#) (optional)
- [Configuring Cisco Unified Communications Manager Switchover and MGCP Gateway Fallback, page 8](#) (required)
- [Verifying Cisco Unified Communications Manager Switchover and MGCP Gateway Fallback, page 16](#) (optional)
- [Configuring POTS Dial Peers on MGCP Gateways, page 18](#) (required)
- [Verifying Dial Peer Configuration for MGCP Gateways, page 19](#) (optional)
- [Enabling Single-Point Configuration for MGCP Gateways, page 23](#) (optional)
- [Verifying Single-Point Configuration for MGCP Gateways, page 25](#) (optional)
- [Configuring Multicast Music-on-Hold Support for Cisco Unified Communications Manager, page 26](#) (optional)
- [Verifying Music-on-Hold, page 27](#) (optional)
- [Configuring MLPP Service on Cisco MGCP Gateways, page 28](#) (optional)
- [Configuring Fallback when Using MLPP on T1 CAS, page 30](#) (optional)
- [Verifying MLPP Configuration, page 32](#) (optional)

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	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password when prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface ethernet <i>slot/port</i> 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. <ul style="list-style-type: none"> • <i>Slot</i> and <i>port</i> syntax is platform-dependent; type ? to determine.
Step 4	ip address <i>ip-address subnetmask</i> 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.

	Command	Purpose
Step 5	<code>no shutdown</code> Example: <code>Router(config-if)# no shutdown</code>	Activates the Ethernet port.
Step 6	<code>exit</code> Example: <code>Router(config-if)# exit</code>	Exits interface mode and enters global configuration mode.
Step 7	<code>hostname name</code> Example: <code>Router(config)# hostname smith</code>	Assigns a unique name to a network router which enables Cisco Unified Communications Manager to identify the device. <ul style="list-style-type: none"> • Default device name is Router.
Step 8	<code>mgcp validate domain-name</code> Example: <code>Router(config)# mgcp validate domain-name</code>	(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. <p>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.</p>
Step 9	<code>mgcp</code> Example: <code>Router(config)# mgcp</code>	Enables the MGCP protocol.
Step 10	<code>mgcp call-agent {ip-address host-name} [port] [service-type type] [version version-number]</code> Example: <code>Router(config)# mgcp call-agent 10.0.0.21 mgcp 0.1</code>	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	<code>mgcp dtmf-relay voip codec {all low-bit-rate} mode {cisco nse out-of-band}</code> Example: <code>Router(config)# mgcp dtmf-relay voip codec all mode cisco</code>	Selects the codec type and the dual tone multifrequency (DTMF) relay services.
Step 12	<code>ccm-manager mgcp</code> Example: <code>Router(config)# ccm-manager mgcp</code>	Enables the MGCP gateway to support Cisco Unified Communications Manager.
Step 13	<code>exit</code> Example: <code>Router(config)# exit</code>	Exits global configuration mode.

Verifying MGCP Configuration on the Cisco IOS Gateway

SUMMARY STEPS

1. **show running-config**
2. **show interfaces ethernet** *[number]*
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:

```
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:

```
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:

```
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 lwm 150, MGCP LAT threshold hwm 300
MGCP PL threshold lwm 1000, MGCP PL threshold hwm 10000
MGCP CL threshold lwm 1000, MGCP CL threshold hwm 10000
MGCP playout mode is adaptive 60, 4, 200 in msec
MGCP 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-packagec-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 IOS Voice Command Reference](#).

Configuring 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 (Failover)

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

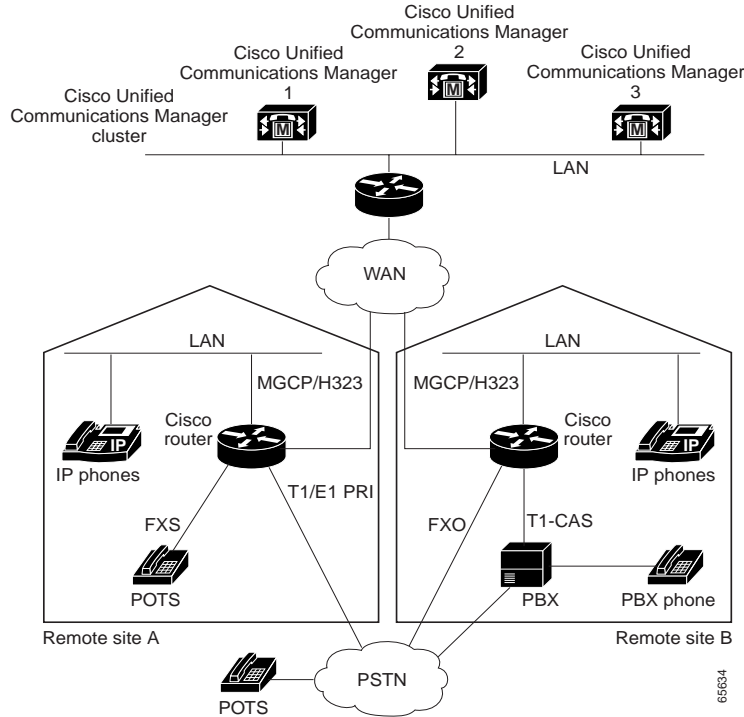
Switchback is the process a voice gateway uses to reestablish communication with the primary Cisco Unified Communications Manager server when the server becomes available again. Switchback can occur immediately, at a specified time after the last active call ends, or after a specified length of time.

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.

[Figure 3](#) illustrates a typical VoIP network topology in which MGCP gateway fallback is supported.

Figure 3 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

Table 2 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.
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.

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	<p><code>enable</code></p> <p>Example: Router> enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password when prompted.
Step 2	<p><code>configure terminal</code></p> <p>Example: Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p><code>ccm-manager redundant-host {ip-address DNS-name} [ip-address DNS-name]</code></p> <p>Example: Router(config)# ccm-manager redundant-host 10.0.0.50</p>	<p>Identifies up to two backup Cisco Unified Communications Manager servers.</p>
Step 4	<p><code>ccm-manager switchover {graceful immediate schedule-time hh:mm uptime-delay minutes}</code></p> <p>Example: Router(config)# ccm-manager switchover immediate</p>	<p>Configures switchover mode for returning control to the primary Cisco Unified Communications Manager.</p> <ul style="list-style-type: none"> • Default is graceful.
Step 5	<p><code>ccm-manager fallback-mgcp</code></p> <p>Example: Router(config)# ccm-manager fallback-mgcp</p>	<p>Enables the MGCP fallback feature.</p>
Step 6	<p><code>call application alternate</code></p> <p>Example: Router(config)# call application alternate</p>	<p>Specifies that the default voice application takes over if the MGCP application is not available.</p>

	Command or Action	Purpose
Step 7	<pre>exit</pre> <p>Example: Router(config)# exit </p>	Exits global configuration mode and returns to privileged EXEC mode.
Step 8	<pre>ccm-manager switchover-to-backup</pre> <p>Example: Router# ccm-manager switchover-to-backup </p>	<p>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.</p> <p>Note This command does not switch the gateway to the backup Cisco Unified Communications Manager server if you have set the ccm-manager switchover-to-backup command to immediate and the primary Cisco Unified Communications Manager server is still running.</p>

Configuring 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.

Restrictions

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 in all releases after Cisco IOS Release 12.3(14)T. Both commands are reflected in Step 4.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code> Example: Router> enable	Enters privileged EXEC mode. Enter your password if prompted.
Step 2	<code>configure terminal</code> Example: Router# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	<pre>ccm-manager fallback-mgcp</pre> <p>Example: Router(config)# ccm-mananger fallback-mgcp </p>	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.
Step 4	<pre>call application alternate [application name] or service [alternate default] service-name location</pre> <p>Example: Router(config)# call application alternate or Router(config)# service default </p>	<p>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 <i>application-name</i> 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.</p> <p>Or</p> <p>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:</p> <ul style="list-style-type: none"> • 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. • <i>service-name</i>—Name that identifies the voice application. • <i>location</i>—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	<pre>exit</pre> <p>Example: Router(config)# exit </p>	Exits global configuration mode and returns to privileged EXEC mode.

Verifying Cisco Unified Communications Manager 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:

```
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.

```
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:

```
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.

Restrictions for POTS Dial Peers on MGCP Gateways

- 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	<pre>enable</pre> <p>Example: Router> enable</p>	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password when prompted.
Step 2	<pre>configure terminal</pre> <p>Example: Router# configure terminal</p>	Enters global configuration mode.
Step 3	<pre>dial-peer voice tag pots</pre> <p>Example: Router(config)# dial-peer voice 101 pots</p>	Designates the specified dial peer as a POTS device and enters dial-peer configuration mode.
Step 4	<pre>application mgcpapp</pre> <p>Example: Router(config-dial-peer)# application mgcpapp</p>	Enables MGCP on the dial peer. <p>Note Do not use this command in dial peers that support PRI backhaul or BRI backhaul.</p>
Step 5	<pre>direct-inward-dial</pre> <p>Example: Router(config-dial-peer)# direct-inward-dial</p>	(Optional) Enables the direct inward dialing (DID) call treatment for an incoming called number. <ul style="list-style-type: none"> Required for T1/E1 PRI dial peers.
Step 6	<pre>port slot/subunit/port</pre> <p>Example: Router(config-dial-peer)# port 1/0/1</p>	Binds the MGCP application to the specified voice port. <ul style="list-style-type: none"> <i>Slot</i> and <i>port</i> syntax is platform-dependent; type ? to determine.
Step 7	<pre>exit</pre> <p>Example: Router(config-dial-peer)# exit</p>	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 tag`
3. `show voice port 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.

```
! 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.

```
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.

```
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.

```
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.

```
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:

```
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:

```
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](#).

Enabling 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):

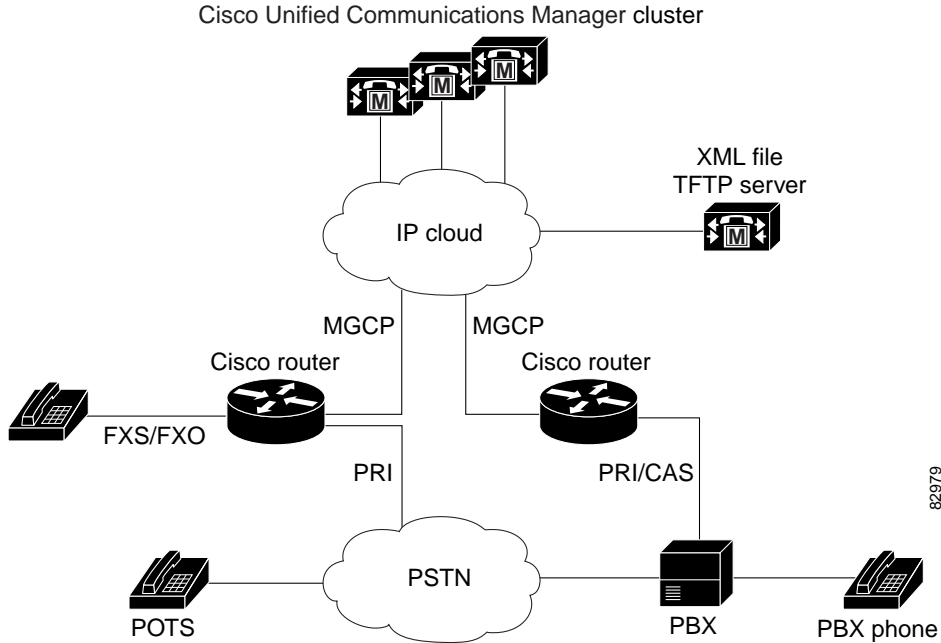
- A unique device identifier, which can be either of the following:
 - Specific device name on the Cisco MGCP gateway
 - MAC address of the device for gateways that are not using Cisco IOS software
- IP address of the TFTP server in the network and routing information required for access
- Sufficient 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 4 Single-Point Configuration for Cisco MGCP Gateways



Prerequisites for Single-Point Configuration for MGCP Gateways

- MGCP should be configured in your VoIP network through the Cisco Communications Manager web-based graphical user interface (GUI).
- The IP hostname should match the gateway name that is specified in the Cisco Unified Communications Manager configuration.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ccm-manager config server {ip-address | name}**
4. **ccm-manager config**
5. **exit**

	Command or Action	Purpose
Step 1	<code>enable</code> Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password when prompted.
Step 2	<code>configure terminal</code> Example: Router# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	<pre>ccm-manager config server {ip-address name}</pre> <p>Example: Router(config)# ccm-manager config server 10.10.1.10 </p>	Specifies the TFTP server by IP address or logical name.
Step 4	<pre>ccm-manager config</pre> <p>Example: Router(config)# ccm-manager config </p>	Enables the gateway to be configured by a centralized XML file and triggers the gateway to download a new configuration.
Step 5	<pre>exit</pre> <p>Example: Router(config)# exit </p>	Exits global configuration mode.

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:

```
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.

```
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 Support for Cisco Unified Communications Manager

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

Prerequisites for Multicast Music-on-Hold (MOH)

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

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.

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. <ul style="list-style-type: none">• 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.
Step 4	ccm-manager music-on-hold bind <i>interface</i> 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:

```
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:

```
Router# show ccm-manager music-on-hold
```

Multicast Address	RTP Port	Packets In/Out	Call ID	Protocol	Incoming 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.

Prerequisites

- 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.

Restrictions

- 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.

MLPP Overview

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 or Fallback

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.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mgcp package-capability pre-package**
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code> Example: Router> <code>enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<code>configure terminal</code> Example: Router# <code>configure terminal</code>	Enters global configuration mode.
Step 3	<code>mgcp package-capability pre-package</code> Example: Router(config)# <code>mgcp package-capability pre-package</code>	Enables MLPP as an MGCP package capability type on the voice gateway.
Step 4	<code>exit</code> Example: Router(config)# <code>exit</code>	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

- `enable`
- `configure terminal`
- `call-manager-fallback`
- `ip source-address ip-address [port port] [any-match | strict-match]`
- `max-dn max-directory-numbers`
- `max-ephones max-phones`
- `dialplan-pattern tag pattern extension-length length [extension-pattern extension-pattern] [no-reg]`
- `translate {called | calling} translation-rule-tag`
- `end`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<pre>enable</pre> <p>Example: Router> enable </p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<pre>configure terminal</pre> <p>Example: Router# configure terminal </p>	<p>Enters global configuration mode.</p>
Step 3	<pre>call-manager-fallback</pre> <p>Example: Router(config)# call-manager-fallback </p>	<p>Enters call-manager-fallback configuration mode.</p>
Step 4	<pre>ip source-address ip-address [port port] [any-match strict-match]</pre> <p>Example: Router(config-cm-fallback)# ip source-address 10.10.200.23 port 2000 </p>	<p>Enables the voice gateway to receive messages from the Cisco IP phones through the specified IP addresses and provides for strict IP address verification.</p>
Step 5	<pre>max-dn max-directory-numbers</pre> <p>Example: Router(config-cm-fallback)# max-dn 12 </p>	<p>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.</p>
Step 6	<pre>max-ephones max-phones</pre> <p>Example: Router(config-cm-fallback)# max-ephones 10 </p>	<p>Configures the maximum number of Cisco IP phones that can be supported by the voice gateway. The maximum number is platform dependent.</p>
Step 7	<pre>dialplan-pattern tag pattern extension-length length [extension-pattern extension-pattern] [no-reg]</pre> <p>Example: Router(config-cm-fallback)# dialplan-pattern 1 [A-D]... extension-length 4 </p>	<p>Creates a global prefix that can be used to expand the abbreviated extension numbers into fully qualified E.164 numbers.</p>
Step 8	<pre>translate {called calling} translation-rule-tag</pre> <p>Example: Router(config-cm-fallback)# translate calling 1 </p>	<p>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.</p>
Step 9	<pre>end</pre> <p>Example: Router(config-cm-fallback)# end </p>	<p>Exits to privileged EXEC mode.</p>

Verifying MLPP Configuration

SUMMARY STEPS

1. **show running-config**
2. **show mgcp**

DETAILED STEPS

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

```
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 lwm 150, MGCP LAT threshold hwm 300
MGCP PL threshold lwm 1000, MGCP PL threshold hwm 10000
MGCP CL threshold lwm 1000, MGCP CL threshold hwm 10000
MGCP playout mode is adaptive 60, 4, 200 in msec
MGCP 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 for Cisco Communications Manager

This section provides the following configuration examples:

- [MGCP Gateway with T1 CAS: Example, page 33](#)
- [MGCP Gateway with T1 PRI: Example, page 35](#)
- [Multicast Music-on-Hold: Example, page 37](#)
- [MLPP \(Cisco 2801\): Example, page 38](#)
- [MLPP \(Cisco 2621\): Example, page 40](#)



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-13 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 (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-13 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

```

MLPP (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
```

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

- [“Cisco Unified Communications Manager and Cisco IOS Interoperability Features Roadmap” on page 9](#)—Describes how to access Cisco Feature Navigator; also lists and describes, by Cisco IOS release, Cisco Communications Manager and Cisco IOS interoperability features.
- [“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).

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0709R)

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

© 2007 Cisco Systems, Inc. All rights reserved.



Configuring Enhanced Conferencing and Transcoding for Voice Gateway Routers

This chapter describes the steps for enabling conferencing and transcoding support on Cisco IOS voice gateways in a Cisco Unified Communications Manager network. This feature provides enhanced multiservice support by enabling audioconference and transcode functions in voice gateway routers. Locating conference resources in the branch reduces WAN utilization and using transcoding services reduces bandwidth needs resulting in tangible cost savings.

Digital signal processor (DSP) farms provide conferencing and transcoding services using DSP resources on high-density digital voice/fax network modules.

Feature History for G.722-64 and iLBC Codec Support on Cisco Unified Communications Manager Express

Release	Modification
12.4(15)XZ	This feature was introduced.

Feature History for G.722-64 and iLBC Codec Support on Cisco UBEs, DSP Farms, and Voice Gateways

Release	Modification
12.4(15)XY	This feature was introduced.

Feature History for Universal Voice Transcoding Support for Cisco Unified Border Elements

Release	Modification
12.4(11)XY	This feature was introduced.

Feature History for Out-of-Band to In-Band DTMF Relay for Voice Gateway Routers

Release	Modification
12.3(8)XY	This feature was introduced.
12.3(11)T	This feature was integrated into Cisco IOS Release 12.3(11)T.
12.3(14)T	Support was added for the PVDM2 on the Cisco 2800 series and Cisco 3800 series voice gateway routers.



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2008 Cisco Systems, Inc. All rights reserved.

Feature History for Enhanced Conferencing and Transcoding for Voice Gateway Routers

Release	Modification
12.3(8)T	This feature was introduced for the NM-HDV2, NM-HD-1V, NM-HD-2V, and NM-HD-2VE.
12.3(11)T	Support was added for the PVDM2 on the Cisco 2800 series and Cisco 3800 series voice gateway routers.

Feature History for Conferencing and Transcoding for Voice Gateway Routers

Release	Modification
12.1(5)YH	This feature was introduced for the NM-HDV-FARM on the Cisco VG200.
12.2(13)T	This feature was integrated into Cisco IOS Release 12.2(13)T and support was added for the NM-HDV on the Cisco 2600 series, Cisco 3600 series, Cisco 3700 series, and Cisco VG200.
12.3(2)XE	Support was added for the PVDM-256K on the Cisco 1751, Cisco 1751-V, and Cisco 1760.
12.3(8)T	Support for the PVDM-256K on the Cisco 1751, Cisco 1751-V, and Cisco 1760 was integrated into Cisco IOS Release 12.3(8)T.

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.

**Note**

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/ios123/123cgr/voice_c/vcl.htm.

Contents

- [Prerequisites for Conferencing and Transcoding for Voice Gateway Routers](#), page 3
- [Information About Conferencing and Transcoding for Voice Gateway Routers](#), page 5
- [How to Configure Conferencing and Transcoding for Voice Gateway Routers](#), page 15
- [Configuration Examples for Conferencing and Transcoding](#), page 36
- [Where to Go Next](#), page 53
- [Additional References](#), page 54

Prerequisites for Conferencing and Transcoding for Voice Gateway Routers

DSP Resources

The router must be equipped with one or more of the following network modules or voice DSP modules to provide DSP resources for conferencing, transcoding, and hardware MTP services:

- NM-HD-1V
- NM-HD-2V
- NM-HD-2VE
- NM-HDV2
- NM-HDV2-1T1/E1
- NM-HDV2-2T1/E1
- NM-HDV¹
- NM-HDV-FARM¹
- PVDM-256K¹
- PVDM2 on Cisco 2800 series or Cisco 3800 series

1. Does not support hardware MTP services.

Cisco Unified Communications Manager and Cisco IOS Release

- Minimum software requirements for type of network or voice module:

Module	Cisco Unified Communications Manager version	Cisco IOS Release
NM-HDV2, NM-HD-1V/2V/2VE	Cisco Unified Communications Manager 3.3(4) (formerly known as Cisco CallManager 3.3(4)) or later for conferencing and transcoding, Cisco Unified Communications Manager 4.0(1) (formerly known as Cisco CallManager 4.0(1)) or later for MTP	Cisco IOS Release 12.3(8)T or later
PVDM2 (Cisco 2800 series)	Cisco Unified Communications Manager 3.3(5) (formerly known as Cisco CallManager 3.3(5)) or later for conferencing and transcoding, Cisco Unified Communications Manager 4.0(2a) (formerly known as Cisco CallManager 4.0(2a)) or later for MTP	Cisco IOS Release 12.3(8)T4 or later
PVDM2 (Cisco 3800 series)	Cisco Unified Communications Manager 3.3(5) (formerly known as Cisco CallManager 3.3(5)) or later for conferencing and transcoding, Cisco Unified Communications Manager 4.0(2a) (formerly known as Cisco CallManager 4.0(2a)) or later for MTP	Cisco IOS Release 12.3(11)T or later
NM-HDV	Cisco Unified Communications Manager 3.2(2c) (formerly known as Cisco CallManager 3.2(2c)) or later	Cisco IOS Release 12.2(13)T or later

- Conference bridge, transcoder, and MTP services must be configured in Cisco Unified Communications Manager. See the following chapters in the *Cisco Unified Communications Manager Administration Guide*:

Release 4.0(1):

- “[Conference Bridge Configuration](#)”
- “[Media Termination Point Configuration](#)”
- “[Transcoder Configuration](#)”

Release 3.3(4):

- “[Conference Bridge Configuration](#)”
- “[Transcoder Configuration](#)”

Codecs

End-user devices must be equipped with one of the following codecs:

Codec	Packetization Periods for Transcoding (ms)
G.711 a-law, G.711 u-law, G.722-64	10, 20, or 30
G.729, G.729A, G.729B, G.729AB	10, 20, 30, 40, 50, or 60
GSM EFR, GSM FR ¹	20
iLBC	20 or 30

1. Supported for NM-HDV2 and NM-HD-1V/2V/2VE only

Restrictions for Conferencing and Transcoding for Voice Gateway Routers

- DSP farm services communicate with Cisco Unified Communications Manager using Skinny Client Control Protocol (SCCP); other protocols are not supported.
- DSP farm services are not supported for Cisco Survivable Remote Site Telephony (SRST) or Cisco Unified Communications Manager Express.
- DSP farm services cannot be enabled for a slot on the Cisco 1700 series so the **dsp services dspfarm** command is not supported and cannot be configured for a voice card on the Cisco 1700 series.
- Conferencing is not supported on a Cisco 3640 using the NM-HD-1V, NM-HD-2V, or NM-HD-2VE.
- Simultaneous use of DSP farm services on the NM-HDV and NM-HDV2 is not supported.
- Hardware MTPs are not supported on the NM-HDV or NM-HDV-FARM.
- Hardware MTPs support only G.711 a-law and G.711 u-law. If you configure a profile as a hardware MTP, and you want to change the codec to other than G.711, you must first remove the hardware MTP by using the **no maximum sessions hardware** command.
- Software MTPs are supported on the NM-HDV only if the **dsp services dspfarm** command is not enabled on the voice card.
- Only one codec is supported for each MTP profile. To support multiple codecs, you must define a separate MTP profile for each codec.
- If an MTP call is received but MTP is not configured, transcoding is used if resources are available.
- Dynamic conference and transcoding resource allocation is not supported.
- Fax is not supported for transcoding.

Information About Conferencing and Transcoding for Voice Gateway Routers

To configure Cisco conferencing and transcoding, you should understand the following concepts:

- [DSP Farms, page 6](#)
- [DSP Farm Profiles, page 6](#)
- [Conferencing, page 7](#)

- [Transcoding, page 7](#)
- [MTP, page 8](#)
- [Conferencing and Transcoding Features on the NM-HDV2 and NM-HD-1V/2V/2VE, page 8](#)
- [Conferencing and Transcoding Features on the NM-HDV, page 9](#)
- [Conferencing and Transcoding Features on the Cisco 1751 and Cisco 1760, page 9](#)
- [Allocation of DSP Resources, page 10](#)

DSP Farms

A DSP farm is the collection of DSP resources available for conferencing, transcoding, and MTP services. DSP farms are configured on the voice gateway and managed by Cisco Unified Communications Manager through Skinny Client Control Protocol (SCCP).

The DSP farm can support a combination of transcoding sessions, MTP sessions, and conferences simultaneously. The DSP farm maintains the DSP resource details locally. Cisco Unified Communications Manager requests conferencing or transcoding services from the gateway, which either grants or denies these requests, depending on resource availability. The details of whether DSP resources are used, and which DSP resources are used, are transparent to Cisco Unified Communications Manager.

The DSP farm uses the DSP resources in network modules on Cisco routers to provide voice-conferencing, transcoding, and hardware MTP services.

**Note**

Hardware MTP services are not supported on the NM-HDV.

**Tip**

To determine how many DSP resources your router supports, see the [“Allocation of DSP Resources” section on page 10](#).

DSP Farm Profiles

DSP-farm profiles are created to allocate DSP-farm resources. Under the profile you select the service type (conference, transcode, MTP), associate an application, and specify service-specific parameters such as codecs and maximum number of sessions. A DSP-farm profile allows you to group DSP resources based on the service type. Applications associated with the profile, such as SCCP, can use the resources allocated under the profile. You can configure multiple profiles for the same service, each of which can register with one Cisco Unified Communications Manager group. The profile ID and service type uniquely identify a profile, allowing the profile to uniquely map to a Cisco Unified Communications Manager group that contains a single pool of Cisco Unified Communications Manager servers.

Conferencing

Voice conferencing involves adding several parties to a phone conversation. In a traditional circuit-switched voice network, all voice traffic passes through a central device such as a PBX. Conference services are provided within this central device. In contrast, IP phones normally send voice signals directly between phones, without the need to go through a central device. Conference services, however, require a network-based conference bridge.

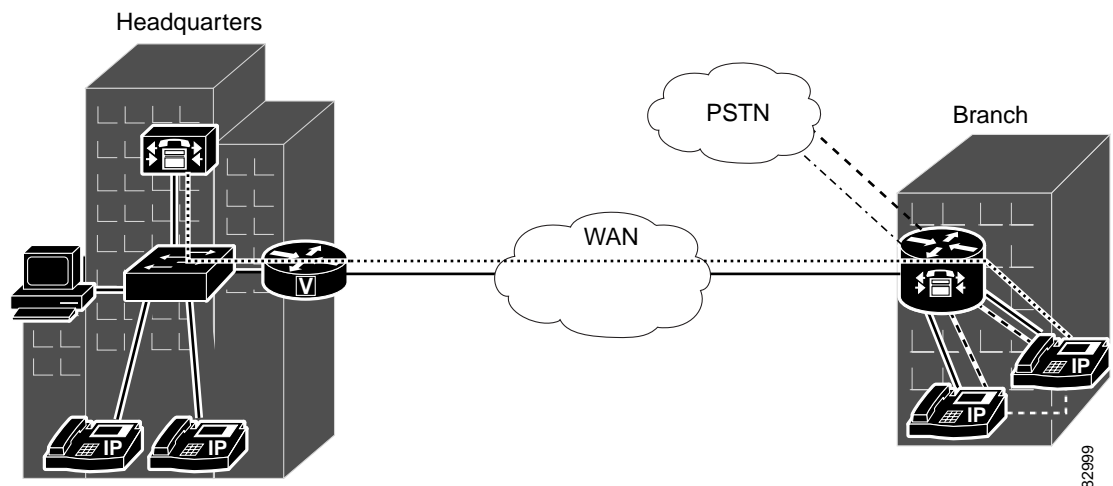
In an IP telephony network using Cisco Unified Communications Manager, the Conferencing and Transcoding for Voice Gateway Routers feature provides the conference-bridging service. Cisco Unified Communications Manager uses a DSP farm to mix voice streams from multiple participants into a single conference-call stream. The mixed stream is played out to all conference attendees, minus the voice of the receiving attendee.

The following conferencing features are supported:

- A conference can be either of the following types:
 - Ad hoc—The person controlling the conference presses the telephone conference button and adds callers one by one.
 - Meet me—Participants call in to a central number and are joined in a single conference.
- Participants whose end devices use different codec types are joined in a single conference; no additional transcoding resource is needed.

This feature provides voice conferencing at the remote site, without the need for access to the central site (see [Figure 5](#)).

Figure 5 Conferencing Service



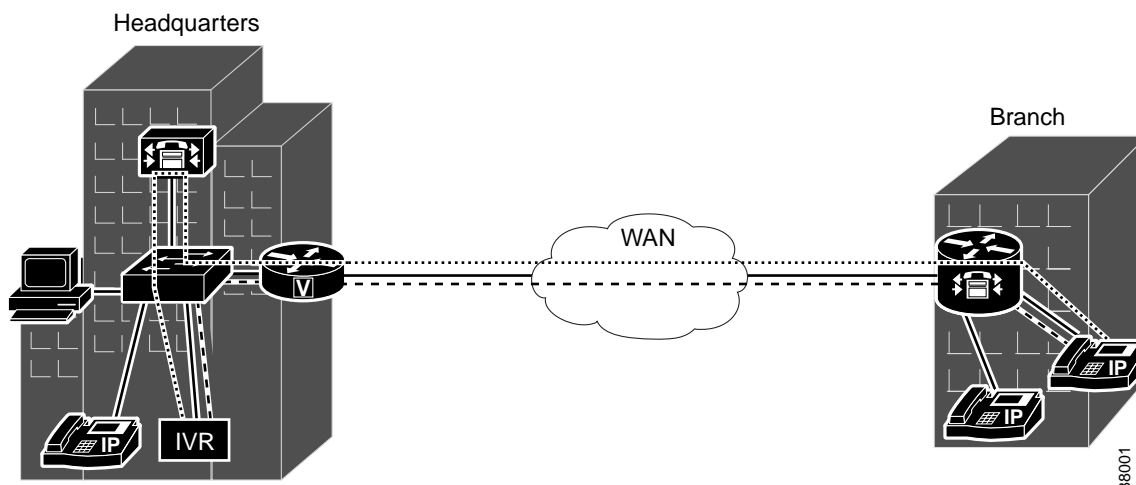
Transcoding

Transcoding compresses and decompresses voice streams to match endpoint-device capabilities. Transcoding is required when an incoming voice stream is digitized and compressed (by means of a codec) to save bandwidth, but the local device does not support that type of compression. Ideally, all IP telephony devices would support the same codecs, but this is not the case. Rather, different devices support different codecs.

Transcoding is processed by DSPs on the DSP farm; sessions are initiated and managed by Cisco Unified Communications Manager which also refers to transcoders as hardware MTPs.

This feature provides transcoding at the remote site, without the need for access to the central site (see [Figure 6](#)).

Figure 6 Transcoding Service



MTP

A Media Termination Point (MTP) bridges the media streams between two connections allowing Cisco Unified Communications Manager to relay calls that are routed through SIP or H.323 endpoints.

The following MTP resources are supported for Cisco Unified Communications Manager 4.0 (formerly known as Cisco CallManager 4.0) and later releases:

- Software MTP—Software-only implementation that does not use a DSP resource for endpoints using the same codec and the same packetization time.
- Hardware MTP—Hardware-only implementation that uses a DSP resource for endpoints using the same G.711 codec but a different packetization time. The repacketization requires a DSP resource so it cannot be done by software only. Cisco Unified Communications Manager also uses the term software MTP when referring to a hardware MTP.

For MTP and transcoding, the DSP farm supports only two IP streams connected to each other at a time. If more than two streams need connecting, the streams must be connected using conferencing.

Conferencing and Transcoding Features on the NM-HDV2 and NM-HD-1V/2V/2VE

Conferencing

- Cisco Unified Communications Manager meet-me and ad-hoc conferences with up to eight participants each
- Up to 50 eight-party conferences on a single NM-HDV2, up to 24 eight-party conferences on a single NM-HD-2VE, and up to 8 eight-party conferences on a single NM-HD-1V/2V

- Participants using G.711 and G.729 codecs joined in a single conference; no additional transcoding resources are needed to include the disparate codec types
- Easy deployment of conference resources in routers across the network, reducing WAN use and improving voice-network performance

Transcoding

- Transcoding between G.711 and G.729, G.729a, G.729b, G.729ab, GSM FR, and GSM EFR codecs
- Up to 128 transcoding sessions on a single NM-HDV2

MTP

- Software-only implementation that does not use a DSP resource for endpoints with the same codec and the same packetization time.
- Hardware-only implementation using a DSP resource for endpoints with the same G.711 codec but a different packetization time.

Conferencing and Transcoding Features on the NM-HDV

Conferencing

- Cisco Unified Communications Manager meet-me and ad-hoc conferences with up to six participants each
- Up to 15 six-party conferences on a single NM-HDV
- Participants using G.711 and G.729 codecs joined in a single conference; no additional transcoding resources are needed to include the disparate codec types
- Easy deployment of conference resources in routers across the network, reducing WAN use and improving voice-network performance

Transcoding

- Transcoding between G.711 and G.729, G.729a, G.729b, and G.729ab codecs
- Up to 60 transcoding sessions on a single NM-HDV

Conferencing and Transcoding Features on the Cisco 1751 and Cisco 1760

Conferencing

- Cisco Unified Communications Manager meet-me and ad-hoc conferences with up to six participants each
- Up to 5 six-party conferences
- One conference on a single DSP
- Participants using G.711 and G.729 codecs joined in a single conference; no additional transcoding resources are needed to include the disparate codec types
- Easy deployment of conference resources in routers across the network, reducing WAN use and improving voice-network performance

Transcoding

- Transcoding between G.711 and G.729, G.729a, G.729b, and G.729ab codecs

- Up to 16 transcoding sessions on the Cisco 1751
- Up to 20 transcoding sessions on the Cisco 1760
- Two transcoding sessions on a single DSP

Allocation of DSP Resources

You must allocate DSP resources on two levels:

- Within the voice network module, between the DSP farm and your voice trunk group that handles standard voice termination
- Within the DSP farm, between transcoding and voice-conferencing services

Allocation of DSP Resources Within the Voice Network Module

You allocate DSP resources either to voice termination of the voice trunk group or to the DSP farm. Occasionally these allocations can conflict.

If you previously allocated DSP resources to voice termination and you now try to configure a DSP farm, you might find that insufficient DSP resources are available. Conversely, if you previously allocated DSP resources to a DSP farm and you now try to configure a trunk group, you might find that insufficient DSP resources are available.

If your requested configuration is rejected, you have two options:

- Insert more DSPs on the voice network module (NM-HDV or NM-HDV2)
- Allocate a different voice network module for either the DSP farm or the trunk group

Allocation of DSP Resources Within the DSP Farm

You should know the following about your system:

- Number of DSPs required to handle your anticipated number of conference calls and transcoding sessions
- Number of DSPs that your system can support

DSP resources can reside in packet-voice DSP modules (PVDMs) installed in voice network modules, for example the NM-HDV2, or directly in the network module, for example the NM-HD-2V. Cisco 2800 series and 3800 series voice gateway routers have onboard DSP resources located on PVDM2s installed directly on the motherboard. Your router supports one or more voice network modules.

Table 3 lists the total DSPs that are supported on a fully-loaded voice network module.

Table 3 Total DSPs Supported Per Voice Network Module

Network Module	Maximum DSPs per PVDM2/PVDM	Maximum PVDM2s/PVDMs per Network Module	Maximum DSPs
NM-HDV2	4	4	16
NM-HD-1V/2V	—	—	1
NM-HD-2VE	—	—	3
NM-HDV	3	5	15

Table 4 lists the total number of network modules that are supported per router.

Table 4 Maximum Voice Network Modules Supported Per Router

Router	NM-HDV2	NM-HD-1V, NM-HD-2V, NM-HD-2VE	NM-HDV
Cisco 2600 series	—	—	1
Cisco 2600 XM	1	1	1
Cisco 2691	1	1	1
Cisco 2801	—	—	—
Cisco 3620	—	—	1 ¹
Cisco 3640	—	—	3 ¹
Cisco 3660	—	6	6
Cisco 3725	2	2	2
Cisco 3745	4 ²	4 ²	4
Cisco VG200	—	—	1

1. Although the chassis has a slot for an additional module, it cannot operate with more than the specified number.
2. Provided processor resources are available.

Conferencing and Transcoding Session Capacities

Each DSP is individually configurable to support either conferencing or transcoding and standard voice termination. The total number of conferencing, transcoding, and voice termination sessions is limited by the capacity of the entire system, which includes the DSPs, hardware platform, physical voice interface, and Cisco Unified Communications Manager.

Table 5 and Table 6 list the maximum number of conference calls and transcoding sessions that DSPs can handle, in theory. Actual capacity may be less based on the total system design.

Table 5 DSP Theoretical Session Capacities

Application	NM-HD-1V/2V (1 DSP)	NM-HD-2VE (3 DSPs)	NM-HDV2 (16 DSPs)	2801/2811 (2 PVDM2-64)	2821/2851 (3 PVDM2-64)	3825, 3845 (4 PVDM2-64)
Conferencing						
G.711	8 sessions (64 conferees)	24 sessions (192 conferees)	50 sessions (400 conferees)	50 sessions (400 conferees)	50 sessions (400 conferees)	50 sessions (400 conferees)
G.722-64	2 sessions (16 conferees)	6 sessions (48 conferees)	32 sessions (256 conferees)	16 sessions (128 conferees)	24 sessions (192 conferees)	32 sessions (256 conferees)
G.729	2 sessions (16 conferees)	6 sessions (48 conferees)	32 sessions (256 conferees)	16 sessions (128 conferees)	24 sessions (192 conferees)	32 sessions (256 conferees)
GSM FR	—	2 sessions (16 conferees)	14 sessions (112 conferees)	7 sessions (56 conferees)	10 sessions (80 conferees)	14 sessions (112 conferees)
GSM EFR	—	1 session (8 conferees)	10 sessions (80 conferees)	5 sessions (40 conferees)	8 sessions (64 conferees)	10 sessions (80 conferees)
iLBC	1 session (8 conferees)	3 sessions (24 conferees)	16 sessions (128 conferees)	8 sessions (64 conferees)	12 sessions (96 conferees)	16 sessions (128 conferees)

Table 5 DSP Theoretical Session Capacities (continued)

Application	NM-HD-1V/2V (1 DSP)	NM-HD-2VE (3 DSPs)	NM-HDV2 (16 DSPs)	2801/2811 (2 PVDM2-64)	2821/2851 (3 PVDM2-64)	3825, 3845 (4 PVDM2-64)
Transcoding						
G.711 a-law/u-law <-> any (with high complexity codec in dspfarm profile)	6 sessions	18 sessions	96 sessions	48 sessions	72 sessions	96 sessions
G.711 a-law/u-law <-> any (without high complexity codec in dspfarm profile)	8 sessions	24 sessions	128 sessions	64 sessions	96 sessions	128 sessions
G.711 a-law/u-law <-> G.729a/G.729ab/ GSM FR	8 sessions	24 sessions	128 sessions	64 sessions	96 sessions	128 sessions
G.711 a-law/u-law <-> G.729/G.729b/ GSM EFR	6 sessions	18 sessions	96 sessions	48 sessions	72 sessions	96 sessions
G.722-64<-> any	4 sessions	12 sessions	64 sessions	32 sessions	48 sessions	64 sessions
G.722-64 <-> G.711	8 sessions	24 sessions	128 sessions	64 sessions	96 sessions	128 sessions
iLBC <-> any	3 sessions	9 sessions	48 sessions	24 sessions	36 sessions	48 sessions
iLBC <-> G.711	6 sessions	18 sessions	96 sessions	48 sessions	72 sessions	96 sessions
Universal Transcoding (with high complexity codec in dspfarm profile)	3 sessions	9 sessions	48 sessions	24 sessions	36 sessions	48 sessions
Universal Transcoding (without high complexity codec in dspfarm profile)	4 sessions	12 sessions	64 sessions	32 sessions	48 sessions	64 sessions
Voice Termination						
G.711 a-law/u-law	16 sessions	48 sessions	256 sessions	128 sessions	192 sessions	256 sessions
G.726, G.729a, G.729ab, GSM FR	8 sessions	24 sessions	128 sessions	64 sessions	96 sessions	128 sessions
G.729, G.729b, G.723.1, G.728, GSM EFR	6 sessions	18 sessions	96 sessions	48 sessions	72 sessions	96 sessions

Table 6 Theoretical System Capacities for One DSP

Application	G.711 a-law/u-law	G.722-64	G729 a/ab	G.729, G.729b	GSM FR	GSM EFR	iLBC
Conferencing	8 sessions (8 x 8 = 64 conferees)	2 sessions (8 x 2 = 16 conferees)	2 sessions (8 x 2 = 16 conferees)	2 sessions (8 x 2 = 16 conferees)	—	—	1 session (1 x 8 = 8 conferees)
Conferencing on PVDM2-8	4 sessions (4 x 8 = 32 conferees)	1 session (1 x 8 = 8 conferees)	1 session (1 x 8 = 8 conferees)	1 session (1 x 8 = 8 conferees)	—	—	1 session (1 x 8 = 8 conferees)
Hardware MTP	16 sessions	—	—	—	—	—	—
Transcoding	8 sessions	8 sessions	8 sessions	6 sessions	8 sessions	6 sessions	8 sessions

NM-HDV System Capacities

Table 7 lists the number of transcoding sessions and conference calls supported on the NM-HDV.

Table 7 NM-HDV Theoretical System Capacities

Device	Capacity
A single DSP	4 transcoding sessions
	1 conference call with up to 6 participants
A single PVDM (3 DSPs)	12 transcoding sessions
	3 conference calls, each with up to 6 participants, for a total of up to 18 participants
A fully loaded NM-HDV (5 PVDMs holding 15 DSPs)	60 transcoding sessions
	15 concurrent conference calls, each with up to 6 participants, for a total of up to 90 participants

Use the following tables to determine the number of PVDMs required to support your DSP needs and whether your router is capable of holding enough NM-HDVs to accommodate these PVDMs:

- See Table 8 if you use either of the following:
 - 20-, 30-, 40-, 50-, or 60-ms packetization
 - 10-ms packetization with voice-activity detection (VAD) enabled
- See Table 9 if you use 10-ms packetization with VAD disabled

Table 8 PVDM Requirements Using 20-, 30-, 40-, 50-, or 60-ms Packetization or 10-ms Packetization with VAD Enabled ¹

Transcoding Sessions	Conference Calls															
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	—	1	1	1	2	2	2	3	3	3	4	4	4	5	5	5
1-4	1	1	1	2	2	2	3	3	3	4	4	4	5	5	5	—
5-8	1	1	2	2	2	3	3	3	4	4	4	5	5	5	—	—

Table 8 *PVDM Requirements Using 20-, 30-, 40-, 50-, or 60-ms Packetization or 10-ms Packetization with VAD Enabled (continued)¹ (continued)*

Transcoding Sessions	Conference Calls															
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
9–12	1	2	2	2	3	3	3	4	4	4	5	5	5	—	—	—
13–16	2	2	2	3	3	3	4	4	4	5	5	5	—	—	—	—
17–20	2	2	3	3	3	4	4	4	5	5	5	—	—	—	—	—
21–24	2	3	3	3	4	4	4	5	5	5	—	—	—	—	—	—
25–28	3	3	3	4	4	4	5	5	5	—	—	—	—	—	—	—
29–32	3	3	4	4	4	5	5	5	—	—	—	—	—	—	—	—
33–36	3	4	4	4	5	5	5	—	—	—	—	—	—	—	—	—
37–40	4	4	4	5	5	5	—	—	—	—	—	—	—	—	—	—
41–44	4	4	5	5	5	—	—	—	—	—	—	—	—	—	—	—
45–48	4	5	5	5	—	—	—	—	—	—	—	—	—	—	—	—
49–52	5	5	5	—	—	—	—	—	—	—	—	—	—	—	—	—
53–56	5	5	—	—	—	—	—	—	—	—	—	—	—	—	—	—
57–60	5	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—

1. Numbers given represent the number of PVDMs required within a single NM-HDV or NM-HDV-FARM to support the desired configuration. Where numbers are not given, the configuration is not possible using a single NM-HDV.

Table 9 *PVDM Requirements Using 10-ms Packetization and with VAD Disabled¹*

Transcoding Sessions	Conference Calls										
	0	1	2	3	4	5	6	7	8	9	10
0	—	1	1	1	2	2	2	3	3	3	4
1–4	1	1	1	2	2	2	3	3	3	—	—
5–8	1	1	2	2	2	3	3	3	—	—	—
9–12	1	2	2	2	3	3	3	—	—	—	—
13–16	2	2	2	3	3	—	—	—	—	—	—
17–20	2	2	3	3	—	—	—	—	—	—	—
21–24	2	3	3	—	—	—	—	—	—	—	—
25–28	3	—	—	—	—	—	—	—	—	—	—
29–30	3	—	—	—	—	—	—	—	—	—	—

1. Numbers given represent the number of PVDMs required within a single NM-HDV to support the desired configuration. Where numbers are not given, the configuration is not possible using a single NM-HDV.

How to Configure Conferencing and Transcoding for Voice Gateway Routers

This section contains the procedures for configuring conferencing and transcoding support on Cisco IOS voice gateways. The procedures that you perform depend on the type of voice network module you are using to allocate DSP resources:

- [Determining DSP Resource Requirements, page 16](#) (required)
- [Enabling SCCP on the Cisco Unified Communications Manager Interface, page 17](#) (required)
- [Configuring Enhanced Conferencing and Transcoding, page 18](#) (required)
- [Configuring Conferencing and Transcoding \(NM-HDV\), page 29](#) (required)
- [Configuring Conferencing and Transcoding \(PVDM-256K\), page 32](#) (required)
- [Configuring Out-of-Band to In-Band DTMF Relay, page 33](#) (optional)

Determining DSP Resource Requirements

DSPs reside either directly on a voice network module, such as the NM-HD-2VE, on PVDM2s that are installed in a voice network module, such as the NM-HDV2, or on PVDM2s that are installed directly onto the motherboard, such as on the Cisco 2800 and 3800 series voice gateway routers. You must determine the number of PVDM2s or network modules that are required to support your conferencing and transcoding services and install the modules on your router.

SUMMARY STEPS

1. Determine performance requirements.
2. Determine the number of DSPs that are required.
3. Determine the number of network modules that are supportable.
4. Verify your solution.
5. Install hardware.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Determine the number of transcoding sessions and conference calls that your router must support.	Establishes your performance requirements.
Step 2	Determine the number of DSPs that are required to support the transcoding sessions and conference calls (see Table 5 on page 11 and Table 6 on page 13). If voice termination is also required, determine the additional DSPs required. Example: 8 G.711 conferences and 32 transcoding sessions require 1 PVDM2-64 (4 DSPs) on the NM-HDV2.	Establishes your hardware requirements.
Step 3	Determine the maximum number of network modules that your router can support (see Table 4 on page 11). Example: A Cisco 3745 router can support up to 4 NM-HDV2s (provided processor resources are available).	Establishes your router capabilities.
Step 4	Ensure that your requirements fall within router capabilities, taking into account whether your router supports multiple network modules. If necessary, reassess performance requirements.	Verifies your proposed solution.
Step 5	Install PVDM2s and network modules, as needed (see the “ Connecting Voice Network Modules ” chapter in the <i>Cisco Network Modules Hardware Installation Guide</i> , and the <i>Cisco Network Modules and Interface Cards Regulatory Compliance and Safety Information</i>).	Prepares your system for DSP-farm configuration.

Enabling SCCP on the Cisco Unified Communications Manager Interface

Perform this task to enable SCCP on the local interface that the voice gateway uses to communicate with Cisco Unified Communications Manager.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **sccp ccm** *{ip-address | dns}* **identifier** *identifier-number* [**port** *port-number*] [**version** *version-number*]
or
sccp ccm *{ip-address | dns}* **priority** *priority* [**port** *port-number*] [**version** *version-number*]
4. **sccp local** *interface-type interface-number*
5. **sccp ip precedence** *value*
6. **sccp**
7. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	NM-HDV2, NM-HD-1V, NM-HD-2V, NM-HD-2VE, or PVDM2 sccp ccm <i>{ip-address dns}</i> identifier <i>identifier-number</i> [port <i>port-number</i>] [version <i>version-number</i>] NM-HDV, Cisco 1751, or Cisco 1760 sccp ccm <i>{ip-address dns}</i> priority <i>priority</i> [port <i>port-number</i>] [version <i>version-number</i>] Example: Router(config)# sccp ccm 10.0.0.0 identifier 1 version 4.0 Example: Router(config)# sccp ccm 10.0.0.0 priority 1 version	Adds a Cisco Unified Communications Manager server to the list of available servers to which the Cisco voice gateway can register. <ul style="list-style-type: none">• Repeat this step for each Cisco Unified Communications Manager server that the gateway registers with.

	Command or Action	Purpose
Step 4	<code>sccp local interface-type interface-number</code> Example: Router(config)# sccp local Ethernet 1	Selects the local interface that SCCP applications use to register with Cisco Unified Communications Manager.
Step 5	<code>sccp ip precedence value</code> Example: Router(config)# sccp ip precedence 3	(Optional) Sets the IP precedence value for SCCP. <ul style="list-style-type: none"> This command enables you to increase the priority of voice packets over connections controlled by SCCP. <i>value</i>—Range is 1(highest) to 7 (lowest). Default is 5.
Step 6	<code>sccp</code> Example: Router(config)# sccp	Enables SCCP and brings it up administratively.
Step 7	<code>exit</code> Example: Router(config)# exit	Exits global configuration mode.

Configuring Enhanced Conferencing and Transcoding

Perform the following procedures to configure enhanced conferencing and transcoding on the NM-HDV2, NM-HD-1V, NM-HD-2V, NM-HD-2VE, or PVDM2:

- [Configuring a DSP Farm Profile, page 18](#) (required)
- [Associating a DSP Farm Profile to a Cisco Unified Communications Manager Group, page 21](#) (required)
- [Modifying Default Settings for SCCP Connection to Cisco Unified Communications Manager, page 23](#) (optional)
- [Verifying DSP Farm Configuration, page 25](#) (optional)
- [Troubleshooting DSP-Farm Services, page 29](#) (optional)

Configuring a DSP Farm Profile

Perform this procedure to define a DSP farm on the NM-HDV2, NM-HD-1V, NM-HD-2V, NM-HD-2VE, or PVDM2. You must configure each conferencing, transcoding, and MTP profile separately.



Note

Because a software-only MTP does not require DSP resources, you can configure a software-only MTP without a voice network module, or on the NM-HDV if you do not enable the `dsp services dspfarm` command for the voice card.

Prerequisites

Requires Cisco IOS Release 12.3(8)T or a later release. Universal transcoding requires Cisco IOS Release 12.4(11)XY or a later release.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice-card slot**
4. **dsp services dspfarm**
5. **exit**
6. **dspfarm profile profile-identifier {conference | mtp | transcode [universal]}**
7. **description text**
8. **codec codec-type**
9. **maximum sessions number**
or
maximum sessions {hardware | software} number
10. **associate application sccp**
11. **no shutdown**
12. **exit**
13. **gateway**
14. **timer receive-rtp seconds**
15. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	voice-card slot Example: Router(config)# voice-card 1	Enters voice-card configuration mode for the network module on which you want to enable DSP-farm services.
Step 4	dsp services dspfarm Example: Router(config-voicecard)# dsp services dspfarm	Enables DSP-farm services for the voice card.

	Command or Action	Purpose
Step 5	<code>exit</code> Example: Router(config-voicecard)# exit	Exits voice-card configuration mode.
Step 6	<code>dspfarm profile profile-identifier</code> <code>{conference mtp transcode [universal]}</code> Example: Router(config)# dspfarm profile 20 conference	Enters DSP farm profile configuration mode to define a profile for DSP farm services. Note The <i>profile-identifier</i> and service type uniquely identifies a profile. If the service type and <i>profile-identifier</i> pair is not unique, you are prompted to choose a different <i>profile-identifier</i> .
Step 7	<code>description text</code> Example: Router(config-dspfarm-profile)# description art_dept	(Optional) Includes a specific description about the Cisco DSP farm profile.
Step 8	<code>codec codec-type</code> Example: Router(config-dspfarm-profile)# codec ilbc	Specifies the codecs supported by a DSP farm profile. <ul style="list-style-type: none">Repeat this step for each codec supported by the profile. Note Hardware MTPs support only G.711 a-law and G.711 u-law. If you configure a profile as a hardware MTP, and you want to change the codec to other than G.711, you must first remove the hardware MTP by using the no maximum sessions hardware command. Note Only one codec is supported for each MTP profile. To support multiple codecs, you must define a separate MTP profile for each codec.
Step 9	<code>maximum sessions number</code> OR <code>maximum sessions {hardware software} number</code> Example: Router(config-dspfarm-profile)# maximum sessions 4	Specifies the maximum number of sessions that are supported by the profile. <ul style="list-style-type: none"><i>number</i>—Range is determined by the available registered DSP resources. Default is 0. Note The hardware and software keywords apply only to MTP profiles.
Step 10	<code>associate application sccp</code> Example: Router(config-dspfarm-profile)# associate application sccp	Associates the SCCP protocol to the DSP farm profile.
Step 11	<code>no shutdown</code> Example: Router(config-dspfarm-profile)# no shutdown	Enables the profile, allocates DSP farm resources, and associates the application.

	Command or Action	Purpose
Step 12	<code>exit</code> Example: Router(config-dspfarm-profile)# <code>exit</code>	Exits DSP farm profile configuration mode.
Step 13	<code>gateway</code> Example: Router(config)# <code>gateway</code>	Enters gateway configuration mode.
Step 14	<code>timer receive-rtp seconds</code> Example: Router(config-gateway)# <code>timer receive-rtp 600</code>	Sets the Real-Time Transport Protocol (RTP) timeout interval to clear hanging connections. <ul style="list-style-type: none"> <code>seconds</code>—Range is 180 to 1800. Default is 1200.
Step 15	<code>exit</code> Example: Router(config-gateway)# <code>exit</code>	Exits to global configuration mode.

Associating a DSP Farm Profile to a Cisco Unified Communications Manager Group

Perform this procedure to define a Cisco Unified Communications Manager group and to associate a DSP farm profile with the Cisco Unified Communications Manager group.

Prerequisites

This procedure requires Cisco IOS Release 12.3(8)T or later release.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `sccp ccm group group-number`
4. `associate ccm identifier-number priority priority-number`
5. `associate profile profile-identifier register device-name`
6. `bind interface interface-type interface-number`
7. `description string`
8. `end`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<pre>enable</pre> <p>Example: Router> enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<pre>configure terminal</pre> <p>Example: Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<pre>sccp ccm group group-number</pre> <p>Example: Router(config)# sccp ccm group 118</p>	<p>Creates a Cisco Unified Communications Manager group and enters SCCP Cisco Unified Communications Manager configuration mode.</p>
Step 4	<pre>associate ccm identifier-number priority priority-number</pre> <p>Example: Router(config-sccp-ccm)# associate ccm 125 priority 2</p>	<p>Adds a Cisco Unified Communications Manager server to the Cisco Unified Communications Manager group and establishes its priority within the group.</p> <ul style="list-style-type: none"> Repeat this step for each Cisco Unified Communications Manager server that you want to add to the group.
Step 5	<pre>associate profile profile-identifier register device-name</pre> <p>Example: Router(config-sccp-ccm)# associate profile register abgz12345</p>	<p>Associates a DSP farm profile to the Cisco Unified Communications Manager group.</p> <ul style="list-style-type: none"> <i>device-name</i>—Must match the device name configured in Cisco Unified Communications Manager; otherwise profile is not registered to Cisco Unified Communications Manager. Repeat this step for each DSP farm profile that you want to register with this Cisco Unified Communications Manager group.
Step 6	<pre>bind interface interface-type interface-number</pre> <p>Example: Router(config-sccp-ccm)# bind interface fastethernet 2:1</p>	<p>Binds an interface to the Cisco Unified Communications Manager group.</p>
Step 7	<pre>description text</pre> <p>Example: Router(config-sccp-ccm)# description boston office</p>	<p>(Optional) Includes a specific description of the Cisco Unified Communications Manager group.</p>
Step 8	<pre>end</pre> <p>Example: Router(config)# end</p>	<p>Exits to privileged EXEC mode.</p>

Modifying Default Settings for SCCP Connection to Cisco Unified Communications Manager

Perform this task to tune the performance of the SCCP connection between the DSP farm and Cisco Unified Communications Manager.



Note

The optimum settings for these commands depend on your platform and individual network characteristics. Modify the defaults to meet your performance requirements.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **sccp ccm group** *group-number*
4. **connect interval** *seconds*
5. **connect retries** *number*
6. **keepalive retries** *number*
7. **keepalive timeout** *seconds*
8. **registration retries** *retry-attempts*
9. **registration timeout** *seconds*
10. **switchover method** { **graceful** | **immediate** }
11. **switchback method** { **graceful** | **guard** [*timeout-value*] | **immediate** | **uptime** *uptime-value* }
12. **switchback interval** *seconds*
13. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	sccp ccm group <i>group-number</i> Example: Router(config)# sccp ccm group 118	Enters SCCP Cisco Unified Communications Manager configuration mode. <ul style="list-style-type: none"> • <i>group-number</i>—Range is 1 to 65535.

	Command or Action	Purpose
Step 4	<p><code>connect interval seconds</code></p> <p>Example: Router(config-sccp-ccm)# connect interval 1200</p>	<p>(Optional) Specifies the amount of time that a DSP farm profile waits before attempting to connect to another Cisco Unified Communications Manager when the current Cisco Unified Communications Manager fails to connect.</p> <ul style="list-style-type: none"> <code>seconds</code>—Range is 1 to 3600. Default is 60.
Step 5	<p><code>connect retries number</code></p> <p>Example: Router(config-sccp-ccm)# connect retries 5</p>	<p>(Optional) Specifies the number of times that a DSP farm attempts to connect to a Cisco Unified Communications Manager when the current Cisco Unified Communications Manager connections fails.</p> <ul style="list-style-type: none"> <code>number</code>—Range is 1 to 32. Default is 3.
Step 6	<p><code>keepalive retries number</code></p> <p>Example: Router(config-sccp-ccm)# keepalive retries 7</p>	<p>(Optional) Sets the number of keepalive retries from SCCP to the Cisco Unified Communications Manager.</p> <ul style="list-style-type: none"> <code>number</code>—Range is 1 to 32. Default is 3.
Step 7	<p><code>keepalive timeout seconds</code></p> <p>Example: Router(config-sccp-ccm)# keepalive timeout 50</p>	<p>(Optional) Sets the number of seconds between keepalive messages from SCCP to the Cisco Unified Communications Manager.</p> <ul style="list-style-type: none"> <code>seconds</code>—Range is 1 to 180. Default is 30.
Step 8	<p><code>registration retries retry-attempts</code></p> <p>Example: Router(config-sccp-ccm)# registration retries 15</p>	<p>(Optional) Sets the number of registration retries that SCCP tries to register with the Cisco Unified Communications Manager.</p> <ul style="list-style-type: none"> <code>retry-attempts</code>—Range is 1 to 32. Default is 3.
Step 9	<p><code>registration timeout seconds</code></p> <p>Example: Router(config-sccp-ccm)# registration timeout 8</p>	<p>(Optional) Sets the number of seconds between registration messages sent from SCCP to the Cisco Unified Communications Manager.</p> <ul style="list-style-type: none"> <code>seconds</code>—Range is 1 to 180. Default is 3.
Step 10	<p><code>switchover method {graceful immediate}</code></p> <p>Example: Router(config-sccp-ccm)# switchover method graceful</p>	<p>(Optional) Sets the switchover method that the SCCP client uses when the communication link to the active Cisco Unified Communications Manager fails.</p> <ul style="list-style-type: none"> Default is graceful.
Step 11	<p><code>switchback method {graceful guard [timeout-value] immediate uptime uptime-value}</code></p> <p>Example: Router(config-sccp-ccm)# switchback method graceful</p>	<p>(Optional) Sets the switchback method to use when the primary or higher priority Cisco Unified Communications Manager becomes available again.</p> <ul style="list-style-type: none"> Default is guard, with a timeout value of 7200 seconds.

	Command or Action	Purpose
Step 12	<pre>switchback interval seconds</pre> <p>Example: Router(conf-sccp-ccm)# switchback interval 120 </p>	(Optional) Sets the number of seconds that the DSP farm waits before polling the primary Cisco Unified Communications Manager when the current Cisco Unified Communications Manager fails to connect. <ul style="list-style-type: none"> <i>seconds</i>—Range is 1 to 3600. Default is 60.
Step 13	<pre>end</pre> <p>Example: Router(config-sccp-ccm)# end </p>	Exits to privileged EXEC mode.

Verifying DSP Farm Configuration

To verify conferencing, transcoding, and MTP services, perform the following steps.

SUMMARY STEPS

1. `show running-config`
2. `show sccp ccm group [group-number]`
3. `show dspfarm profile [profile-number]`
4. `show dspfarm all`
5. `show sccp`
6. `show sccp connections`
7. `show media resource status`

DETAILED STEPS

- Step 1** Use the `show running-config` command to display the configuration of the MTP profile, for example:

```
Router# show running-config
...
sccp local FastEthernet0/0
sccp ccm 10.40.10.10 identifier 10 version 4.0
sccp
!
sccp ccm group 999
  associate ccm 10 priority 1
  associate profile 12 register MTP123456789
  associate profile 2 register XCODE123456
!
dspfarm profile 12 mtp
  codec g711ulaw
  maximum sessions hardware 4
  maximum sessions software 40
  associate application SCCP
!
```

- Step 2** `show sccp ccm group [group-number]`

Use this command to verify the configuration of the Cisco Unified Communications Manager group, for example:

```
Router# show sccp ccm group 999
```

```

CCM Group Identifier: 999
Description: None
Associated CCM Id: 10, Priority in this CCM Group: 1
Associated Profile: 2, Registration Name: XCODE1234567
Associated Profile: 12, Registration Name: MTP123456789
Registration Retries: 3, Registration Timeout: 10 sec
Keepalive Retries: 3, Keepalive Timeout: 30 sec
CCM Connect Retries: 3, CCM Connect Interval: 10 sec
Switchover Method: GRACEFUL, Switchback Method: GRACEFUL_GUARD
Switchback Interval: 10 sec, Switchback Timeout: 7200 sec
Signaling DSCP value: default, Audio DSCP value: default

```

Step 3 **show dspfarm profile** [*profile-number*]

Use this command to verify the configured DSP farm profiles, for example:

```
Router# show dspfarm profile 12
```

Dspfarm Profile Configuration

```

Profile ID = 12, Service = MTP, Resource ID = 2
Profile Admin State : UP
Profile Operation State : ACTIVE
Application : SCCP Status : ASSOCIATED
Resource Provider : FLEX_DSPRM Status : UP
Number of Resource Configured : 14
Number of Resource Available : 14
Hardware Configured Resources 4
Hardware Available Resources 4
Software Resources 10
Codec Configuration
Codec : g711ulaw, sa

```

```
Router# show dspfarm profile 6
```

Dspfarm Profile Configuration

```

Profile ID = 6, Service = TRANSCODING, Resource ID = 1
Profile Admin State : UP
Profile Operation State : ACTIVE
Application : SCCP Status : ASSOCIATED
Resource Provider : FLEX_DSPRM Status : UP
Number of Resource Configured : 4
Number of Resource Available : 4
Codec Configuration
Codec : g711ulaw, Maximum Packetization Period : 30
Codec : g711alaw, Maximum Packetization Period : 30
Codec : g729ar8, Maximum Packetization Period : 60
Codec : g729abr8, Maximum Packetization Period : 60
Codec : gsmfr, Maximum Packetization Period : 20
Codec : g729br8, Maximum Packetization Period : 60
Codec : gsmefr, Maximum Packetization Period : 20

```



Note This command is not supported on the NM-HDV or Cisco 1700 series.

Step 4 **show dspfarm all**

Use this command to verify the status of the DSP farm, for example:

```
Router# show dspfarm all
```

```
DSPFARM Configuration Information:
Admin State: UP, Oper Status: ACTIVE - Cause code: NONE
Transcoding Sessions: 0(Avail: 0), Conferencing Sessions: 2 (Avail: 2)
Trans sessions for mixed-mode conf: 0 (Avail: 0), RTP Timeout: 600
Connection check interval 600 Codec G729 VAD: ENABLED
```

Total number of active session(s) 0, and connection(s) 0

SLOT	DSP	CHNL	STATUS	USE	TYPE	SESS-ID	CONN-ID	PKTS-RXED	PKTS-TXED
0	0	1	UP	FREE	conf	-	-	-	-
0	0	2	UP	FREE	conf	-	-	-	-
0	0	3	UP	FREE	conf	-	-	-	-
0	0	4	UP	FREE	conf	-	-	-	-
0	0	5	UP	FREE	conf	-	-	-	-
0	0	6	UP	FREE	conf	-	-	-	-

Step 5 show sccp

Use the **show sccp** command to verify that the DSP farm is registered, for example:

```
Router# show sccp

SCCP Admin State: UP
Gateway IP Address: 10.10.100.29, Port Number: 0
IP Precedence: 5
User Masked Codec list:
Call Manager: 10.10.100.51, Port Number: 2000
                Priority: N/A, Version: 4.0, Identifier: 2
Call Manager: 10.10.100.50, Port Number: 2000
                Priority: N/A, Version: 4.0, Identifier: 1

Transcoding Oper State: ACTIVE - Cause Code: NONE
Active Call Manager: 10.10.100.51, Port Number: 2000
TCP Link Status: CONNECTED, Profile Identifier: 10
Reported Max Streams: 6, Reported Max OOS Streams: 0
Supported Codec: g711ulaw, Maximum Packetization Period: 30
Supported Codec: g711alaw, Maximum Packetization Period: 30
Supported Codec: g729ar8, Maximum Packetization Period: 60
Supported Codec: g729abr8, Maximum Packetization Period: 60
Supported Codec: gsmfr, Maximum Packetization Period: 20
Supported Codec: g729br8, Maximum Packetization Period: 60
Supported Codec: rfc2833 dtmf, Maximum Packetization Period: 20

Software MTP Oper State: ACTIVE - Cause Code: NONE
Active Call Manager: 10.10.100.51, Port Number: 2000
TCP Link Status: CONNECTED, Profile Identifier: 20
Reported Max Streams: 176, Reported Max OOS Streams: 0
Supported Codec: g711ulaw, Maximum Packetization Period: 30
Supported Codec: rfc2833 dtmf, Maximum Packetization Period: 20
```

Step 6 show sccp connections

Use this command to verify the active SCCP connections, for example:

```
Router# show sccp connections

sess_id   conn_id   stype mode   codec   ripaddr   rport sport
-----
16777268  2164263392 mtp  recvonly g711u   0.0.0.0   0      17540

Total number of active session(s) 1, and connection(s) 1
```

Step 7 show media resource status

Use this command to verify the current media resource status, for example:

```
Router# show media resource status

Resource Providers:

Resource Provider ID :: FLEX_DSPRM Status :: REGISTERED
Service Profiles
MTP ::
TRANSCODING :: 6 11
CONFERENCING :: 10
Applications :
Application ID : SCCP, Status : REGISTERED
```

Troubleshooting Tips for Conferencing and Transcoding on Voice Gateway Routers

This section describes techniques for troubleshooting DSP-farm services.

Basic Troubleshooting Procedures

1. Verify the Cisco Unified Communications Manager 4.0 (formerly known as Cisco CallManager 4.0) or later.
2. Verify that Cisco Unified Communications Manager is properly configured to provision conferencing, transcoding, and MTP resources.
3. Organize your Cisco Unified Communications Manager group IDs, device IDs, and DSP farm profile names. Use the **show dsp** command to verify that the association between SCCP Cisco Unified Communications Manager and the DSP farm profiles match your organizational plan.
4. Verify that the VoIP dial peer application exists on the terminating gateway.
5. Collect relevant information from **debug** and **show** commands, and configuration files before contacting Cisco Technical Support for assistance.
6. You can clear any of the following by disabling the DSP farm or SCCP:
 - Active calls
 - DSPs
 - Active connection to a Cisco Unified Communications Manager

MTP Troubleshooting Tips

- MTP profiles can use only G.711 a-law or G.711 u-law. If you define a profile for a hardware MTP, and you want to change the codec to other than G.711, you must first remove the hardware MTP by using the **no maximum sessions hardware** command.
- Verify that only one codec is assigned for each MTP profile. To support multiple codecs, you must define a separate MTP profile for each codec.

Troubleshooting DSP-Farm Services

You can troubleshoot performance by performing any of the following steps.

SUMMARY STEPS

1. `debug sccp {all | errors | events | packets | parser}`
2. `debug dspfarm {all | errors | events | packets}`
3. `debug media resource provisioning {all | errors | events}`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<pre>debug sccp {all errors events packets parser}</pre> <p>Example: Router# debug sccp all</p>	(Optional) Sets debugging levels for SCCP and its applications.
Step 2	<pre>debug dspfarm {all errors events packets}</pre> <p>Example: Router# debug dspfarm all</p>	(Optional) Sets debugging levels for DSP-farm service.
Step 3	<pre>debug media resource provisioning {all errors events}</pre> <p>Example: Router# debug media resource provisioning all</p>	(Optional) Sets debugging levels for media resource provisioning.

Configuring Conferencing and Transcoding (NM-HDV)

Perform the following procedures to configure enhanced conferencing and transcoding on the NM-HDV.

- [Configuring the DSP Farm on the NM-HDV, page 29](#)
- [Tuning DSP-Farm Performance on the NM-HDV, page 31](#)

Configuring the DSP Farm on the NM-HDV

Perform this task to configure a DSP farm on an NM-HDV.



Note

If you configured a DSP farm in Cisco IOS Release 12.1(5)YH and have now upgraded to Cisco IOS Release 12.2(13)T or later, you must reconfigure the DSP farm, including enabling DSP-farm services on the NM-HDV and specifying maximum session numbers in each category as appropriate. Your previous configuration no longer works.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice-card slot**
4. **dsp services dspfarm**
5. **exit**
6. **dspfarm confbridge maximum sessions number**
7. **dspfarm transcoder maximum sessions number**
8. **dspfarm**
9. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code> Example: <code>Router> enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password when prompted.
Step 2	<code>configure terminal</code> Example: <code>Router# configure terminal</code>	Enters global configuration mode.
Step 3	<code>voice-card slot</code> Example: <code>Router(config)# voice-card 1</code>	Enters voice-card configuration mode for the network module on which you want to enable DSP-farm services.
Step 4	<code>dsp services dspfarm</code> Example: <code>Router(config-voicecard)# dsp services dspfarm</code>	Enables DSP-farm services on the voice card.
Step 5	<code>exit</code> Example: <code>Router(config-voicecard)# exit</code>	Returns to global configuration mode.
Step 6	<code>dspfarm confbridge maximum sessions number</code> Example: <code>Router(config)# dspfarm confbridge maximum sessions 3</code>	Specifies the maximum number of conferencing sessions to be supported by the DSP farm. A DSP can support 1 conference session with up to 6 participants. Note When you assign this value, take into account the number of DSPs allocated for transcoding services.

	Command or Action	Purpose
Step 7	<p><code>dspfarm transcoder maximum sessions number</code></p> <p>Example: Router(config)# dspfarm transcoder maximum sessions 12</p>	<p>Specifies the maximum number of transcoding sessions to be supported by the DSP farm. A DSP can support up to 4 transcoding sessions.</p> <p>Note When you assign this value, take into account the number of DSPs allocated for conferencing services.</p>
Step 8	<p><code>dspfarm</code></p> <p>Example: Router(config)# dspfarm</p>	<p>Enables the DSP farm.</p>
Step 9	<p><code>exit</code></p> <p>Example: Router(config)# exit</p>	<p>Exits global configuration mode.</p>

Tuning DSP-Farm Performance on the NM-HDV

Use the following optional commands to tune performance.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `sccp switchback timeout guard seconds`
4. `dspfarm rtp timeout seconds`
5. `dspfarm connection interval seconds`
6. `exit`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><code>enable</code></p> <p>Example: Router> enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password when prompted.
Step 2	<p><code>configure terminal</code></p> <p>Example: Router# configure terminal</p>	<p>Enters global configuration mode.</p>

	Command or Action	Purpose
Step 3	<code>sccp switchback timeout guard seconds</code> Example: Router(config)# sccp switchback timeout guard 180	(Optional) Sets the guard timer.
Step 4	<code>dspfarm rtp timeout seconds</code> Example: Router(config)# dspfarm rtp timeout 60	(Optional) Configures the Real-Time Transport Protocol (RTP) timeout interval for when the error condition “RTP port unreachable” occurs.
Step 5	<code>dspfarm connection interval seconds</code> Example: Router(config)# dspfarm connection interval 60	(Optional) Specifies how long to monitor RTP inactivity before deleting an RTP stream.
Step 6	<code>exit</code> Example: Router(config)# exit	Exits global configuration mode.

What to Do Next

- To verify the configuration of conferencing and transcoding services on the NM-HDV, see the [“Verifying DSP Farm Configuration” section on page 25](#).
- For information on troubleshooting, see the [“Troubleshooting DSP-Farm Services” section on page 29](#).

Configuring Conferencing and Transcoding (PVDM-256K)

Perform this task to configure a DSP farm for conferencing and transcoding services using the PVDM-256K on the Cisco 1751 or Cisco 1760.

Prerequisites for Conferencing and Transcoding on the Cisco 1751 or Cisco 1760

Determine that there are enough DSPs available for conferencing and transcoding services by using the `show voice dsp` command.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `dspfarm confbridge maximum sessions number`
4. `dspfarm transcoder maximum sessions number`
5. `dspfarm`
6. `exit`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<pre>enable</pre> <p>Example: Router> enable </p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password when prompted.
Step 2	<pre>configure terminal</pre> <p>Example: Router# configure terminal </p>	<p>Enters global configuration mode.</p>
Step 3	<pre>dspfarm confbridge maximum sessions number</pre> <p>Example: Router(config)# dspfarm confbridge maximum sessions 3 </p>	<p>Specifies the maximum number of conferencing sessions to be supported by the DSP farm. A DSP can support 1 conference session with up to 6 participants.</p> <p>Note When you assign this value, take into account the number of DSPs allocated for transcoding services.</p>
Step 4	<pre>dspfarm transcoder maximum sessions number</pre> <p>Example: Router(config)# dspfarm transcoder maximum sessions 12 </p>	<p>Specifies the maximum number of transcoding sessions to be supported by the DSP farm. A DSP can support up to 4 transcoding sessions.</p> <p>Note When you assign this value, take into account the number of DSPs allocated for conferencing services.</p>
Step 5	<pre>dspfarm</pre> <p>Example: Router(config)# dspfarm </p>	<p>Enables the DSP farm.</p>
Step 6	<pre>exit</pre> <p>Example: Router(config)# exit </p>	<p>Exits global configuration mode.</p>

What to Do Next

- To verify the configuration of conferencing and transcoding services on the NM-HDV, see the [“Verifying DSP Farm Configuration” section on page 25](#).
- For information on troubleshooting, see the [“Troubleshooting DSP-Farm Services” section on page 29](#).

Configuring Out-of-Band to In-Band DTMF Relay

There are no specific configuration tasks necessary to support the Out-of-Band to In-Band DTMF Relay for Cisco IOS Voice Gateways feature except those described in the following Prerequisites section.

Prerequisites

Hardware

- NM-HDV2, NM-HD-2VE, or onboard PVDM2 (Cisco 2800 series or Cisco 3800 series).
- WS-SVC-CMM-6T1 or WS-SVC-CMM-6E1 port adapter for Cisco Catalyst 6500 series and Cisco 7600 series Communication Media Module (CMM).

Software

- Enable SCCP on the local interface that the MTP resource uses to communicate with Cisco Unified Communications Manager. For instructions, see the [“Enabling SCCP on the Cisco Unified Communications Manager Interface”](#) section on page 17.
- Configure a DSP farm profile for MTP resources. For instructions, see the [“Configuring a DSP Farm Profile”](#) section on page 18.
- Associate the MTP profile with the Cisco Unified Communications Manager group. For instructions, see the [“Associating a DSP Farm Profile to a Cisco Unified Communications Manager Group”](#) section on page 21.
- Configure DTMF relay in the SIP dial peers using the **dtmf-relay rtp-nte** command.
- Configure DTMF relay in Cisco Unified Communications Manager 4.0 (formerly known as Cisco CallManager 4.0) or later. For information, see the [Cisco Unified CallManager 4.0](#) documentation.
- Consider your system requirements when configuring DSP farms and SCCP because the defaults for some commands might not result in expected behavior. In particular, the correct settings for the following commands are platform-specific and depend on your individual network characteristics:
 - **connect interval**
 - **connect retries**
 - **keepalive retries**
 - **keepalive timeout**
 - **sccp registration retries**
 - **sccp registration timeout**
 - **switchback interval**

Restrictions

- Multifrequency is supported by MTPs but Cisco Unified Communications Manager does not support it.
- Software MTP supports G.711 codecs only.

Out-of-Band to In-Band DTMF Relay for Cisco IOS Voice Gateways

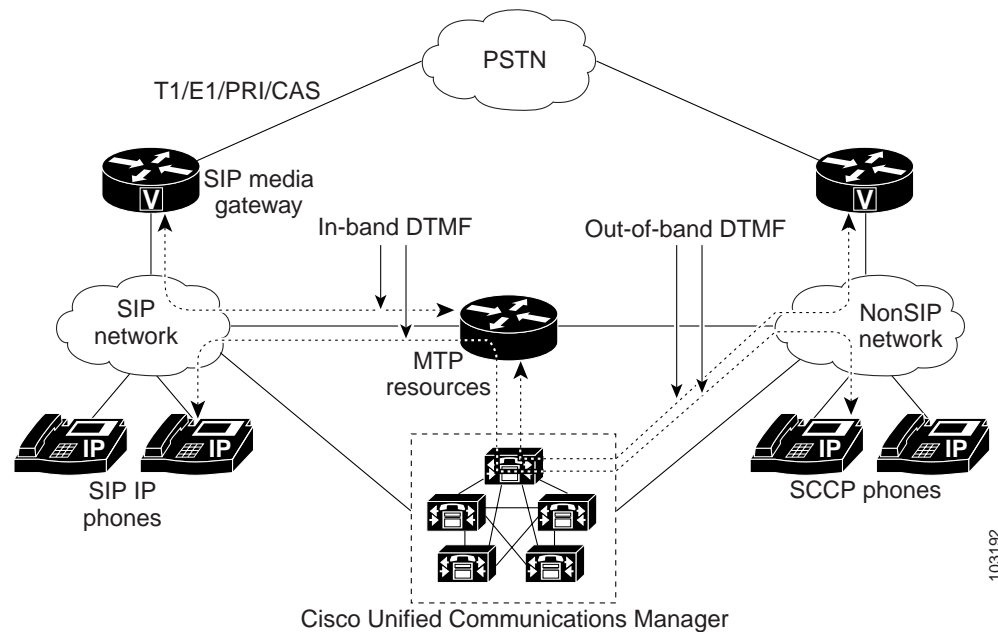
The Out-of-Band to In-Band DTMF Relay for Cisco IOS Voice Gateways feature provides the event processing capability in RFC 2833 that enables DTMF relay communication between SIP devices and nonSIP endpoints using Cisco Unified Communications Manager. RFC 2833 defines a method of transporting tones and other telephony events over Real-Time Transport Protocol (RTP) to ensure DTMF digits are accurately transmitted in a packet environment. A single packet representing a DTMF tone as

an event code is passed within an RTP audio stream instead of sending the DTMF tone in-band, where it could be corrupted because of packet loss. When the packet reaches the receiver, it re-creates a tone of the correct frequency and duration.

DTMF detection and generation capabilities are added to the hardware and software MTP. The MTP generates out-of-band SCCP events to Cisco Unified Communications Manager when it detects a DTMF tone. The MTP creates event packets for DTMF digits and inserts the packets into the outgoing RTP stream after receiving an SCCP request from Cisco Unified Communications Manager.

Figure 7 illustrates the media setup and DTMF tone flow between a SIP network and nonSIP network over a DSP farm MTP.

Figure 7 DTMF Tone Flow Between a SIP and NonSIP Network



This feature supports DTMF relay using the following MTP and transcoder resources for Cisco Unified Communications Manager 4.0 (formerly known as Cisco CallManager 4.0):

- Software MTP—Software-only implementation that does not use a DSP resource for endpoints using the same codec and the same packetization time.
- Hardware MTP—Hardware-only implementation that uses a DSP resource for endpoints using the same G.711 codec but a different packetization time. Cisco Unified Communications Manager refers to it also as a software MTP.
- Transcoder—Hardware-only implementation using a DSP resource for endpoints using different codecs. Cisco Unified Communications Manager also refers to it as a hardware MTP.

For MTP and transcoding, the DSP farm supports only two IP streams connected to each other at a time. If more than two streams need connecting, the streams must be connected using conferencing.



Note

For more information on MTPs and transcoders, see the *Cisco Unified Communications Manager System Guide Release 4.0(1)*.

Configuration Examples for Conferencing and Transcoding

This section provides the following configuration examples:

- [DSP-Farm Services on the NM-HDV2/PVDM2: Example, page 36](#)
- [DSP-Farm Services on the NM-HDV: Example, page 39](#)
- [Tuning DSP-Farm Services on the NM-HDV: Example, page 40](#)
- [DSP-Farm Services on the Cisco 1760: Example, page 40](#)
- [Dut-Band to In-Band DTMF Relay \(Cisco 2801\): Example, page 42](#)
- [Out-Band to In-Band DTMF Relay \(Cisco 3725\): Example, page 45](#)
- [Universal Transcoding with an Inbox on a Universal Gateway: Example, page 48](#)
- [G.711 to Any Transcoding with an Inbox on a Universal Gateway: Example, page 49](#)
- [Universal and G.711 to Any Transcoding with an Inbox on a Universal Gateway: Example, page 51](#)
- [Universal and G.711 to Any Transcoding with an Inbox on an Integrated Services Router: Example, page 52](#)



Note

Universal transcoding using the AMR-NB codec in either direction is supported only on the Cisco AS5350XM and Cisco AS5450XM universal gateways.

DSP-Farm Services on the NM-HDV2/PVDM2: Example

The following example shows a configuration of conferencing and transcoding services on an NM-HDV2 or PVDM2. DSP farm profile 6, which supports transcoding, and profile 10, which supports conferencing are both assigned to Cisco Unified Communications Manager group 988.



Note

This configuration requires Cisco IOS Release 12.3(8)T or later.

```

Current configuration : 2661 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname sjl23
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
ip subnet-zero
!
!
ip host boating 223.255.254.254
no ftp-server write-enable
!
voice-card 1

```

```
no dspfarm
dsp services dspfarm
!
!
voice service voip
h323
!
!
controller T1 4/1
framing sf
crc-threshold 0
linecode ami
!
controller T1 4/2
framing sf
crc-threshold 0
linecode ami
!
!
interface FastEthernet0/0
ip address 10.4.20.7 255.255.255.0
no ip mroute-cache
speed auto
half-duplex
no cdp enable
!
interface FastEthernet0/1
no ip address
no ip mroute-cache
shutdown
duplex auto
speed auto
no cdp enable
!
ip default-gateway 10.4.0.1
ip classless
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
ip route 223.255.254.254 255.255.255.255 10.4.0.1
no ip http server
!
!
no cdp run
!
!
control-plane
!
!
voice-port 1/0/0
!
voice-port 1/0/1
!
!
sccp local FastEthernet0/0
sccp ccm 10.4.20.24 identifier 1 version 4.0
sccp ccm 10.4.20.25 identifier 2 version 4.0
sccp ccm 10.4.20.26 identifier 3 version 4.0
sccp ip precedence 3
sccp
!
sccp ccm group 988
associate ccm 1 priority 1
associate ccm 2 priority 2
associate ccm 3 priority 3
```

```

associate profile 10 register CFB123456789966
associate profile 6 register MTP123456789988
keepalive retries 5
switchover method immediate
switchback method immediate
switchback interval 15
!
dspfarm profile 6 transcode
codec g711ulaw
codec g711alaw
codec g729ar8
codec g729abr8
codec gsmfr
maximum sessions 4
associate application SCCP
!
dspfarm profile 10 conference
codec g711ulaw
codec g711alaw
codec g729ar8
codec g729abr8
codec g729r8
codec g729br8
maximum sessions 1
associate application SCCP
!
dial-peer cor custom
!
!
dial-peer voice 200 voip
destination-pattern 111...
session target ipv4:10.4.205.24
!
dial-peer voice 2600 voip
destination-pattern 666...
session target ipv4:10.4.205.24
codec g711ulaw
!
dial-peer voice 100 voip
destination-pattern 5550...
session target ipv4:10.4.205.24
codec g711ulaw
!
dial-peer voice 10 pots
destination-pattern 7770000
forward-digits 0
!
dial-peer voice 11 pots
destination-pattern 7771111
!
dial-peer voice 999 voip
session target ipv4:10.4.205.8
!
gateway
timer receive-rtcp 1200
!
!
line con 0
exec-timeout 0 0
line aux 0
line vty 0 4
password test
login
!

```

```
!
end
```

DSP-Farm Services on the NM-HDV: Example

The following sample configuration shows voice conferencing and transcoding are both configured on the same NM-HDV.

```
Current configuration : 1163 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname router
!
voice-card 1
  dsp services dspfarm
!
ip subnet-zero
!
mta receive maximum-recipients 0
!
controller T1 1/0
  framing sf
  linecode ami
  no yellow generation
  no yellow detection
!
controller T1 1/1
  framing sf
  linecode ami
  no yellow generation
  no yellow detection
!
interface FastEthernet0/0
  ip address 10.10.10.11 255.255.255.0
  load-interval 30
  duplex auto
  speed auto
!
interface FastEthernet0/1
  ip address 10.3.150.139 255.0.0.0
  load-interval 30
  duplex auto
  speed auto
!
ip classless
ip route 192.255.254.254 255.255.255.255 FastEthernet0/1
ip http server
!
call rsvp-sync
!
mgcp profile default
!
sccp local FastEthernet0/0
sccp
sccp ccm 10.10.10.1 priority 1
sccp ccm 10.10.10.2 priority 2
!
dspfarm transcoder maximum sessions 1
```

```

dspfarm confbridge maximum sessions 1
dspfarm
!
voice-port 1/0/0
!
voice-port 1/0/1
!
voice-port 1/1/0
!
voice-port 1/1/1
!
mgcp profile default
!
dial-peer cor custom
!
dial-peer voice 10 pots
 destination-pattern 3140001
 port 1/0/0
!
! Following dial peer is for calls to H.323 end-point 313.... for transcoding.
! Session target is IP address of Cisco Unified Communications Manager.
!
dial-peer voice 100 voip
 destination-pattern 313....
 session target ipv4:10.10.10.1
!
! Following dial peer is for calls to IP Phones for conferencing.
! Session target is IP address of Cisco Unified Communications Manager.
!
dial-peer voice 200 voip
 destination-pattern 700....
 session target ipv4:10.10.10.1
 codec g711alaw
!
line con 0
line aux 0
line vty 0 4
 login
!
end

```

Tuning DSP-Farm Services on the NM-HDV: Example

```

...
sccp local FastEthernet 0/0
sccp
sccp ccm 10.10.10.1 priority 1 version 3.1+
sccp ccm 10.10.10.2 priority 2
sccp ip precedence 5
sccp switchback timeout guard 180
!
dspfarm confbridge maximum sessions 3
dspfarm rtp timeout 60
dspfarm connection interval 60
dspfarm

```

DSP-Farm Services on the Cisco 1760: Example

```
Current configuration :1763 bytes
```

```
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname c1760
!
boot-start-marker
boot-end-marker
!
logging buffered 40960 debugging
no logging console
!
tdm clock E1 1/0 both export line
tdm clock bri-auto
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
voice-card 0
!
voice-card 1
!
no aaa new-model
ip subnet-zero
ip cef
!
!
no ip domain lookup
ip multicast-routing
no ftp-server write-enable
isdn switch-type basic-net3
!
!
ccm-manager music-on-hold
!
!
controller E1 1/0
!
!
interface FastEthernet0/0
 ip address 10.1.1.34 255.255.0.0
 ip igmp join-group 172.16.1.10
 speed auto
 no keepalive
!
interface BRI0/0
 no ip address
 isdn switch-type basic-net3
 isdn incoming-voice voice
!
interface BRI0/1
 no ip address
 shutdown
 isdn switch-type basic-net3
!
ip default-gateway 10.5.0.1
ip classless
no ip http server
ip rtcp report interval 2000
!
!
control-plane
```

```

!
!
!
voice-port 0/0
!
voice-port 0/1
!
!
sccp local FastEthernet0/0
sccp
sccp ccm 10.1.1.30 priority 1
sccp ccm 10.1.1.0 priority 2
sccp switchback timeout guard 180
!
dspfarm transcoder maximum sessions 4
dspfarm confbridge maximum sessions 1
dspfarm rtp timeout 60
dspfarm connection interval 60
dspfarm
!
!
dial-peer voice 500 pots
 destination-pattern 241760....
 incoming called-number 261760....
 direct-inward-dial
 port 0/0
 prefix 241760
!
dial-peer voice 600 voip
 destination-pattern 261760....
 session target ipv4:10.1.1.30
 incoming called-number 241760....
 playout-delay minimum low
 codec g711ulaw
 no vad
!
gateway
 timer receive-rtcp 5
 timer receive-rtp 1200
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
end

```

Dut-Band to In-Band DTMF Relay (Cisco 2801): Example

In the following configuration, the voice gateway acts as both a H.323 gateway and DSP farm.

Building configuration...

```

Current configuration :2091 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 logging console
!
no network-clock-participate wic 1
network-clock-participate wic 2
no network-clock-participate wic 3
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-net5
voice-card 0
dsp services dspfarm
!
!
!
controller T1 2/0
shutdown
framing esf
linecode b8zs
!
controller T1 2/1
framing esf
linecode b8zs
!
!
!
interface FastEthernet0/0
ip address 192.168.12.21 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
interface BRI4/0
no ip address
isdn switch-type basic-net3
!
interface BRI4/1
no ip address
isdn switch-type basic-net3
!
ip classless
ip http server
!
!
!
control-plane
```

```

!
!
!
voice-port 3/0
!
voice-port 3/1
!
voice-port 4/0
!
voice-port 4/1
!
!
sccp local FastEthernet0/0
sccp ccm 192.168.12.131 identifier 1 version 4.0
sccp ip precedence 4
sccp
!
sccp ccm group 1
  bind interface FastEthernet0/0
  associate ccm 1 priority 1
  associate profile 2 register amalthea-mtp
  associate profile 1 register amalthea-xcode
  registration retries 20
  registration timeout 30
  keepalive retries 10
  connect retries 30
  connect interval 30
!
dspfarm profile 1 transcode
  description xcode func
  codec g711ulaw
  codec g711alaw
  codec g729ar8
  codec g729abr8
  codec gsmfr
  codec g729r8
  maximum sessions 2
  associate application SCCP
!
dspfarm profile 2 mtp
  codec g711ulaw
  maximum sessions hardware 2
  maximum sessions software 2
  associate application SCCP
!
!
dial-peer voice 1 pots
  destination-pattern 4444
  port 3/0
!
dial-peer voice 2 voip
  destination-pattern 52..
  session target ipv4:192.168.12.131
  dtmf-relay h245-alphanumeric
!
gateway
  timer receive-rtcp 1200
!
!
line con 0
line aux 0
line vty 0 4
  login
!

```

```
end
```

Out-Band to In-Band DTMF Relay (Cisco 3725): Example

The following running configuration example shows the MTP device configuration:

Building configuration...

```
Current configuration : 1435 bytes
!
version 12.3
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname router1
!
voice-card 1
  no dspfarm
  dsp services dspfarm
!
voice-card 2
  dspfarm
!
no aaa new-model
ip subnet-zero
!
ip host sample 10.10.10.5
mpls ldp logging neighbor-changes
no ftp-server write-enable
no scripting tcl init
no scripting tcl encdir
!
no voice hpi capture buffer
no voice hpi capture destination
!
interface FastEthernet0/0
  ip address 10.4.118.13 255.255.255.255
  duplex auto
  speed auto
!
interface FastEthernet0/1
  no ip address
  shutdown
  duplex auto
  speed auto
!
ip default-gateway 10.4.0.10
ip classless
ip route 10.0.0.0 255.255.255.255 FastEthernet0/0
ip route 223.255.255.255 255.255.255.255 FastEthernet0/0
!
ip http server
!
sccp local FastEthernet0/0
sccp ccm 10.40.10.10 identifier 10 version 4.0
sccp ccm 10.10.10.51 identifier 20 version 4.0
sccp
!
sccp ccm group 999
  associate ccm 10 priority 1
  associate ccm 20 priority 2
```

```

    associate profile 12 register MTP123456789
    associate profile 2 register XCODE123456
!
dspfarm profile 2 transcode
  codec g711ulaw
  codec g711alaw
  codec g729ar8
  codec g729abr8
  codec gsmfr
  maximum sessions 2
  associate application SCCP
!
dspfarm profile 12 mtp
  codec g711ulaw
  maximum sessions hardware 4
  maximum sessions software 40
  associate application SCCP
!

```

SIP Gateway: Example

The following running configuration example shows the SIP gateway configuration for the Out-Band to In-Band DTMF Relay feature:

Building configuration...

```

Current configuration : 2051 bytes
!
version 12.3
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname cisco_sip_gw
!
logging buffered 6000000 debugging
!
voice-card 2
  dspfarm
!
no aaa new-model
ip subnet-zero
!
!
ip domain name cisco.com
ip host sample 10.10.10.5
ip host myhost 10.4.175.2
mpls ldp logging neighbor-changes
no ftp-server write-enable
no scripting tcl init
no scripting tcl encdir
!
!
no voice hpi capture buffer
no voice hpi capture destination
!
!
ccm-manager mgcp
ccm-manager music-on-hold
ccm-manager config server 10.4.175.2
ccm-manager config
!

```

```
!  
controller T1 2/0  
  framing esf  
  linecode b8zs  
  ds0-group 1 timeslots 1-24 type e&m-wink-start  
!  
controller T1 2/1  
  framing sf  
  linecode ami  
!  
!  
!  
interface FastEthernet0/0  
  ip address 10.4.175.14 255.255.0.0  
  duplex auto  
  speed auto  
!  
interface FastEthernet0/1  
  no ip address  
  shutdown  
  duplex auto  
  speed auto  
!  
interface BRI1/0  
  no ip address  
!  
ip default-gateway 10.4.0.1  
ip classless  
ip route 0.0.0.0 255.255.0.0 FastEthernet0/0  
ip route 223.255.254.254 255.255.255.255 FastEthernet0/0  
!  
ip http server  
!  
!  
voice-port 1/0/0  
!  
voice-port 1/0/1  
!  
voice-port 1/1/0  
!  
voice-port 2/0:1  
!  
mgcp profile default  
!  
!  
dial-peer voice 1 voip  
  destination-pattern 2000  
  session protocol sipv2  
  session target ipv4:10.4.175.2  
  dtmf-relay rtp-nte  
  codec g711ulaw  
!  
dial-peer voice 3 pots  
  application mgcpapp  
  port 2/0:1  
!  
dial-peer voice 999201 pots  
  application mgcpapp  
  port 2/0:1  
!  
dial-peer voice 2 pots  
  destination-pattern 2005  
  port 1/0/0  
!
```

```

dial-peer voice 5 pots
 destination-pattern 2001
 port 1/0/0
!
!
line con 0
line aux 0
line vty 0 4
 login
!
!
end

```

Universal Transcoding with an Inbox on a Universal Gateway: Example

The following example shows a universal transcoding configuration with an inbox on a Cisco Unified Border Element on a universal gateway. Universal gateways include the Cisco AS5350XM and Cisco AS5400XM platforms:

```

iLBC_UUT1#sh run
Building configuration...

Current configuration : 3244 bytes
!
!
voice-card 5
 dsp services dspfarm
!
voice-card 6
!
voice-card 7
 dsp services dspfarm
!
!
voice service voip
 allow-connections h323 to h323
 allow-connections h323 to sip
 allow-connections sip to h323
 fax protocol t38 ls-redundancy 0 hs-redundancy 0 fallback cisco
 modem passthrough none codec g729r8 pre-ietf
!
!
interface GigabitEthernet0/0
 ip address 10.10.10.2 255.255.0.0
 duplex auto
 speed auto
 negotiation auto
!
interface GigabitEthernet0/1
 ip address 10.20.20.2 255.255.0.0
 duplex auto
 speed auto
 negotiation auto
!
!
sccp local GigabitEthernet0/0
sccp ccm 10.10.10.2 identifier 1
sccp
!
sccp ccm group 1

```

```

associate ccm 1 priority 1
associate profile 10 register MTPNEWONE
!
dspfarm profile 10 transcode universal
  codec g711ulaw
  codec g711alaw
  codec ilbc
  codec g723r63
  codec g723r53
  codec gsmamr-nb
  codec g729ar8
  codec g729abr8
  maximum sessions 10
  associate application SCCP
!
!
dial-peer voice 10 voip
  destination-pattern 9991...
  session protocol sipv2
  session target ipv4:20.20.20.1

!
dial-peer voice 20 voip
  session target ipv4:10.10.10.1
  incoming called-number 9991...
  codec ilbc
!
!
telephony-service -----> Only Required for InBox
  sdspfarm units 1
  sdspfarm transcode sessions 128
  sdspfarm tag 1 MTPNEWONE
  ip source-address 10.10.10.2 port 2000
  max-conferences 8 gain -6
  transfer-system full-consult
!

```

G.711 to Any Transcoding with an Inbox on a Universal Gateway: Example

The following example shows the configuration for transcoding for G.711 to any codec with an inbox on a Cisco Unified Border Element on a universal gateway. Universal gateways include the Cisco AS5350XM and Cisco AS5400XM platforms:

```

iLBC_UUT1#sh run
Building configuration...

Current configuration : 3244 bytes
!
!
voice-card 5
  dsp services dspfarm
!
voice-card 6
!
voice-card 7
  dsp services dspfarm
!
!
voice service voip

```

```

allow-connections h323 to h323
allow-connections h323 to sip
allow-connections sip to h323
fax protocol t38 ls-redundancy 0 hs-redundancy 0 fallback cisco
modem passthrough none codec g729r8 pre-ietf
!
!
interface GigabitEthernet0/0
ip address 10.10.10.2 255.255.0.0
duplex auto
speed auto
negotiation auto
!
interface GigabitEthernet0/1
ip address 10.20.20.2 255.255.0.0
duplex auto
speed auto
negotiation auto
!
!
sccp local GigabitEthernet0/0
sccp ccm 10.10.10.2 identifier 1
sccp
!
sccp ccm group 1
associate ccm 1 priority 1
associate profile 20 register traditional
!
!
dspfarm profile 20 transcode
codec g711ulaw
codec g711alaw
codec ilbc
codec g723r63
codec g723r53
codec gsmamr-nb
codec g729ar8
codec g729abr8
maximum sessions 20
associate application SCCP
!
!
dial-peer voice 10 voip
destination-pattern 9991...
session protocol sipv2
session target ipv4:10.20.20.1
codec g711ulaw
!
dial-peer voice 20 voip
session target ipv4:10.10.10.1
incoming called-number 9991...
codec ilbc
!
!
telephony-service -----> Only Required for InBox
sdspfarm units 1
sdspfarm transcode sessions 128
sdspfarm tag 1 traditional
ip source-address 10.10.10.2 port 2000
max-conferences 8 gain -6
transfer-system full-consult
!

```

Universal and G.711 to Any Transcoding with an Inbox on a Universal Gateway: Example

The following example shows the configuration for transcoding for both universal and G.711 to any codec with an inbox on a Cisco Unified Border Element on a universal gateway. Universal gateways include the Cisco AS5350XM and Cisco AS5400XM platforms:

```
iLBC_UUT1#sh run
Building configuration...

!
voice-card 5
 dsp services dspfarm
!
voice-card 6
!
voice-card 7
 dsp services dspfarm
!
voice service voip
 allow-connections h323 to h323
 allow-connections h323 to sip
 allow-connections sip to h323
 fax protocol t38 ls-redundancy 0 hs-redundancy 0 fallback cisco
 modem passthrough none codec g729r8 pre-ietf
!
!
interface GigabitEthernet0/0
 ip address 10.10.10.2 255.255.0.0
 duplex auto
 speed auto
 negotiation auto
!
interface GigabitEthernet0/1
 ip address 10.20.20.2 255.255.0.0
 duplex auto
 speed auto
 negotiation auto
!
!
sccp local GigabitEthernet0/0
sccp ccm 10.10.10.2 identifier 1
sccp
!
sccp ccm group 1
 associate ccm 1 priority 1
 associate profile 20 register traditional
 associate profile 10 register MTPNEWONE
!
dspfarm profile 10 transcode universal
 codec g711ulaw
 codec g711alaw
 codec ilbc
 codec g723r63
 codec g723r53
 codec gsmamr-nb
 codec g729ar8
 codec g729abr8
 maximum sessions 10
 associate application SCCP
!
dspfarm profile 20 transcode
```

```

codec g711ulaw
codec g711alaw
codec ilbc
codec g723r63
codec g723r53
codec gsmamr-nb
codec g729ar8
codec g729abr8
maximum sessions 20
associate application SCCP
!
dial-peer voice 10 voip
destination-pattern 9991...
session protocol sipv2
session target ipv4:10.20.20.1
codec g711ulaw
!
dial-peer voice 20 voip
session target ipv4:10.10.10.1
incoming called-number 9991...
codec ilbc
!
!
telephony-service -----> Only Required for InBox
sdspfarm units 2
sdspfarm transcode sessions 128
sdspfarm tag 1 traditional
sdspfarm tag 2 MTPNEWONE
ip source-address 10.10.10.2 port 2000
max-conferences 8 gain -6
transfer-system full-consult
!

```

Universal and G.711 to Any Transcoding with an Inbox on an Integrated Services Router: Example

The following example shows the configuration for transcoding for both universal and G.711 to any codec with an inbox on a Cisco Unified Border Element on an integrated services router. Integrated services routers include the Cisco 2800 and Cisco 3800 platforms:

```

crosby-3845#
!
voice-card 0
no dspfarm
dsp services dspfarm !
!
voice service voip
allow-connections h323 to h323
!
interface GigabitEthernet0/0
ip address 10.3.65.102 255.255.0.0
duplex auto
speed auto
media-type rj45
!
!
sccp local GigabitEthernet0/0
sccp ccm 10.3.65.102 identifier 1
sccp
!

```

```

sccp ccm group 1
  associate ccm 1 priority 1
  associate profile 20 register MTP000ABCD
  associate profile 10 register OLDONE
  keepalive retries 5
  switchback method immediate
!
dspfarm profile 10 transcode -----> for g711 to any
  codec g711ulaw
  codec g711alaw
  codec ilbc
  codec g723r63
  codec g723r53
  codec gsmamr-nb
  codec g729ar8
  codec g729abr8
  maximum sessions 10
  associate application SCCP
!
dspfarm profile 20 transcode universal -----> for Any to Any
  codec g711ulaw
  codec g711alaw
  codec ilbc
  codec g723r63
  codec g723r53
  codec gsmamr-nb
  codec g729ar8
  codec g729abr8
  maximum sessions 2
  associate application SCCP
!
!
dial-peer voice 10 voip
  destination-pattern 2...
  session target ipv4:1.3.65.12
  codec ilbc
!
dial-peer voice 11 voip
  destination-pattern 1...
  session target ipv4:10.3.65.11
  codec g711ulaw
!
!
telephony-service -----> Minimum config for telephony is required for InBox
  ip source-address 10.3.65.102 port 2000
  sdspfarm units 2
  sdspfarm transcode sessions 30
  sdspfarm tag 1 MTP000ABCD
  sdspfarm tag 2 OLDONE
  max-ephones 20
  max-dn 20
  max-conferences 12 gain -6
  transfer-system full-consult
  create cnf-files version-stamp 7960 Sep 27 2006 20:39:40

```

Where to Go Next

- To enable MGCP on a Cisco IOS gateway, see [Configuring MGCP Gateway Support for Cisco Unified Communications Manager, page 23](#).

- 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 the associated frequencies, amplitudes, and cadences, see [“Configuring Tone Download to MGCP Gateways”](#) on page 145.

Additional References

- [“Cisco Unified Communications Manager and Cisco IOS Interoperability Features Roadmap”](#) on page 9—Describes how to access Cisco Feature Navigator; also lists and describes, by Cisco IOS release, Cisco Unified Communications Manager and Cisco IOS interoperability features.
- [“Overview of Cisco Unified Communications Manager and Cisco IOS Interoperability”](#) on page 13—Describes basics of underlying technology and lists related documents.
- [“Conference Bridges”](#) chapter in the *Cisco Unified CallManager System Guide*, Release 4.0(1)—Overview of conference devices in Cisco Unified CallManager 4.0.
- [“Conference Bridge Configuration”](#) chapter in the *Cisco Unified CallManager Administration Guide*, Release 4.0(1)—Describes how to configure conference bridges in Cisco Unified CallManager 4.0.
- [“Transcoders”](#) chapter in the *Cisco Unified CallManager System Guide*—Overview of transcoder devices in Cisco Unified CallManager 4.0.
- [“Transcoder Configuration”](#) chapter in the *Cisco Unified CallManager Administration Guide*—Describes how to configure transcoders in Cisco Unified CallManager 4.0.
- [IP Communications High-Density Digital Voice/Fax Network Module](#) feature document—Describes how to configure support for the NM-HDV2 in Cisco IOS gateways.
- [“Connecting Voice Network Modules”](#) chapter in the *Cisco Network Modules Hardware Installation Guide*—Describes how to install the voice network modules.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0711R)

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

© 2007 Cisco Systems, Inc. All rights reserved.



Configuring MGCP PRI Backhaul and T1 CAS Support for Cisco Unified Communications Manager

This chapter describes the procedures for enabling MGCP PRI backhaul support on the Cisco IOS gateway and describes related features.

Feature History for QSIG Supplementary Features for Voice Gateway Routers

Release	Modification
12.3(8)XY	This feature was introduced.
12.3(11)T	This feature was integrated into Cisco IOS Release 12.3(11)T.

Feature History for MGCP Gateway Support for Cisco Unified Communications Manager Network Specific Facilities

Release	Modification
12.2(15)ZJ	This feature was introduced.
12.3(4)T	This feature was integrated into Cisco IOS Release 12.3(4)T.

Feature History for MGCP PRI Backhaul and T1 CAS Support for Cisco Unified Communications Manager

Release	Modification
12.2(2)XN	This feature was introduced for Cisco Unified Communications Manager 3.0 (formerly known as Cisco CallManager 3.0).
12.2(11)T	Support was added for Cisco Unified Communications Manager 3.2 (formerly known as Cisco CallManager 3.2).

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.



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

**Note**

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/ios123/123cgr/voice_c/vcl.htm.

Contents

- [Restrictions for MGCP PRI Backhaul and T1 CAS Support](#), page 2
- [Information About MGCP PRI Backhaul and T1 CAS Support](#), page 2
- [How to Configure MGCP PRI Backhaul Support for Cisco Unified Communications Manager](#), page 3
- [Configuration Examples for MGCP PRI Backhaul and T1 CAS](#), page 14
- [Where to Go Next](#), page 15
- [Additional References](#), page 15

Prerequisites for MGCP PRI Backhaul and T1 CAS Support

- Cisco IOS Release 12.2(11)T.
- QSIG signaling is required to support supplementary services over the T1 and E1 time-division multiplexing (TDM) trunks that support the PRI backhaul mechanism.

Restrictions for MGCP PRI Backhaul and T1 CAS Support

- Voice interfaces on the NM-HDA and the AIM-VOICE-30 are not supported.
- Integrated access, in which the channels on a T1 or E1 interface are divided between a group used for voice and another group used for WAN access, is not supported when voice is controlled by Cisco Unified Communications Manager through MGCP.
- T1 and E1 protocols, such as QSIG, E1 R2, T1 FGD, and PRI NFAS, are not supported with MGCP only with H.323.
- E1 CAS is not supported.
- Do not add the **application mgcpapp** command to dial peers that support PRI backhaul.

Information About MGCP PRI Backhaul and T1 CAS Support

To configure MGCP PRI backhaul, you should understand the following concepts:

- [MGCP PRI Backhaul Overview](#), page 3
- [ISDN NSF in Route Patterns](#), page 3

MGCP PRI Backhaul Overview

MGCP PRI backhaul is a method for transporting complete IP telephony signaling information from an ISDN PRI interface in an MGCP gateway to Cisco Unified Communications Manager using a highly reliable TCP connection. The gateway uses a single TCP connection to backhaul all ISDN D channels to Cisco Unified Communications Manager. The “SAP/Channel ID” parameter in the header of each message identifies individual D channels. In addition to carrying the backhaul traffic, the TCP keepalive mechanism also determines MGCP voice gateway connectivity to an available call agent.

MGCP PRI backhaul terminates all ISDN PRI Layer 2 (Q.921) signaling functions on the MGCP gateway while, at the same time, packaging all the ISDN PRI Layer 3 (Q.931) signaling information into packets for transmission to Cisco Unified Communications Manager through an IP tunnel over a TCP connection. This ensures the integrity of the Q.931 signaling information that passes through the network for managing IP telephony devices. A rich set of user-side and network-side ISDN PRI calling functions is supported by MGCP PRI backhaul.

The MGCP gateway also establishes a TCP link to the backup (secondary) Cisco Unified Communications Manager server. In the event of a Cisco Unified Communications Manager switchover, the secondary Cisco Unified Communications Manager server performs the MGCP PRI backhaul functions. During the switchover, all active ISDN PRI calls are preserved, and the affected MGCP gateway is registered with the new Cisco Unified Communications Manager server through a Restart-in-Progress (RSIP) message. In this way, continued gateway operation is ensured.

T1 CAS is supported in nonbackhaul fashion. Cisco Unified Communications Manager supports the following CAS signaling types: E&M, wink-start, and E&M delay-dial. E1 CAS is not supported.

ISDN NSF in Route Patterns

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. This feature is compatible with Cisco Communications Manager 3.3(2) (formerly known as Cisco CallManager 3.3(2)) and later.

The route pattern design in Cisco Unified Communications Manager enables facilities or services to be invoked on a call-by-call basis. The NSF information element, which is used in ISDN PRI setup messages for outgoing calls, includes the carrier identification code (CIC) and service parameters. The NSF configuration is done in Cisco Unified Communications Manager as part of the route pattern for MGCP-controlled PRI ports. The NSF information element is inserted in the Q.931 stream so that the attached PSTN switch can interpret the information elements and select the service and route the call to a network.

With NSF configured, NSF can be used 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.

How to Configure MGCP PRI Backhaul Support for Cisco Unified Communications Manager

This section contains the following procedures for configuring MGCP PRI backhaul and related features on Cisco IOS MGCP gateways.

- [Configuring MGCP PRI Backhaul on the Cisco Voice Gateway, page 4](#) (required)

- [Verifying MGCP PRI Backhaul Configuration, page 5](#) (optional)
- [Configuring MGCP Gateway Support for Cisco Unified Communications Manager Network Specific Facilities, page 8](#) (optional)
- [Verifying Configuration of MGCP Gateway Support for Cisco Unified Communications Manager Network Specific Facilities, page 9](#) (optional)
- [Configuring QSIG Supplementary Features for Cisco IOS Voice Gateways, page 12](#) (optional)

Configuring MGCP PRI Backhaul on the Cisco Voice Gateway

Perform this task to configure MGCP PRI backhaul on a Cisco Voice Gateway.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **controller** {t1 | e1} *slot/port*
4. **framing** {esf | sf | crc4 | no crc4 | mp-crc4} [australia]
5. **clock source** {internal | line}
6. **linecode** {ami | b8zs | hdb3}
7. **isdn switch-type** {primary-4ess | primary-5ess | primary-dms100 | primary-ni | primary-net5 | primary-ntt | primary-qsig | primary-ts014}
8. **pri-group timeslots** *timeslot-range* **service mgcp**
9. **exit**
10. **interface serial** *slot/port:timeslot*
11. **isdn bind-L3 ccm-manager**
12. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password when prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	controller {t1 e1} <i>slot/port</i> Example: Router(config)# controller t1 3/0	Enters controller configuration mode.

	Command or Action	Purpose
Step 4	<pre>framing {esf sf crc4 no-crc4 mp-crc4} [australia]</pre> <p>Example: Router(config-controller)# framing esf</p>	<p>Specifies the framing type on a E1 or T1 PRI line.</p> <ul style="list-style-type: none"> Default is sf (super frame) for T1 lines; CRC4 for E1 lines.
Step 5	<pre>clock source {internal line}</pre> <p>Example: Router(config-controller)# clock source internal</p>	<p>Configures the clock source used by the E1 or T1 controller.</p> <ul style="list-style-type: none"> Default is line.
Step 6	<pre>linecode {ami b8zs hdb3}</pre> <p>Example: Router(config-controller)# linecode b8zs</p>	<p>Specifies the line encoding method for the link.</p> <ul style="list-style-type: none"> Default is ami (alternate mark inversion) for T1 lines; hdb3 (high-density bipolar 3) for E1 lines.
Step 7	<pre>isdn switch-type {primary-4ess primary-5ess primary-dms100 primary-ni primary-net5 primary-ntt primary-qsig primary-ts014}</pre> <p>Example: Router(config-if)# isdn switch-type primary-5ess</p>	<p>Specifies the ISDN switch type.</p> <p>Note This command can be entered in either global configuration mode or interface configuration mode.</p>
Step 8	<pre>pri-group timeslots timeslot-range service mgcp</pre> <p>Example: Router(config-controller)# pri-group timeslots 1-24 service mgcp</p>	<p>Specifies MGCP as the control protocol used for backhaul.</p> <p>Note The controller time slots cannot be shared between backhaul and other Layer 3 protocols.</p>
Step 9	<pre>exit</pre> <p>Example: Router(config-dial-peer)# exit</p>	<p>Exits controller configuration mode and returns to global configuration mode.</p>
Step 10	<pre>interface serial slot/port:timeslot</pre> <p>Example: Router(config)# interface serial 3/0:0</p>	<p>Enters serial interface configuration mode.</p> <ul style="list-style-type: none"> The syntax of this command is platform-dependent; type ? to determine.
Step 11	<pre>isdn bind-L3 ccm-manager</pre> <p>Example: Router(config-if)# isdn bind-L3 ccm-manager</p>	<p>Enables ISDN to backhaul Q.931.</p>
Step 12	<pre>exit</pre> <p>Example: Router(config-if)# exit</p>	<p>Exits interface configuration mode and returns to global configuration mode.</p>

Verifying MGCP PRI Backhaul Configuration

Perform this task to verify the configuration.

SUMMARY STEPS

1. **show isdn status**
2. **show ccm-manager**
3. **show ccm-manager backhaul**

DETAILED STEPS

Step 1 **show isdn status**

Use the **show isdn status** command to verify connectivity.

In the following sample output, the Layer 2 protocol is Q.921, and the Layer 3 protocol is CCM-MANAGER. This output verifies that the Layer 2 and Layer 3 protocols are configured to backhaul ISDN. If you are connected to a live line, you should see Layer 1 status as active and Layer 2 as MULTIPLE_FRAME_ESTABLISHED.

```
Router# show isdn status

*00:03:34.423 UTC Sat Jan 1 2000
Global ISDN Switchtype = primary-net5
ISDN Serial1:23 interface
!
***** Network side configuration *****
!
 dsl 0, interface ISDN Switchtype = primary-net5
!
**** Master side configuration ****
!
L2 Protocol = Q.921 L3 Protocol(s) = CCM-MANAGER
Layer 1 Status:
ACTIVE
Layer 2 Status:
TEI = 0, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
Layer 3 Status:
NLCB:callid=0x0, callref=0x0, state=31, ces=0 event=0x0
NLCB:callid=0x0, callref=0x0, state=0, ces=1 event=0x0
0 Active Layer 3 Call(s)
Activated dsl 0 CCBs = 0
Number of active calls = 0
Number of available B-channels = 23
Total Allocated ISDN CCBs = 0
```

Step 2 **show ccm-manager**

Use the **show ccm-manager** command to view the registration status with Cisco Unified Communications Manager, for example:

```
Router# show ccm-manager

MGCP Domain Name: AV-2620-4
Priority          Status                    Host
=====
Primary          Registered                10.16.240.124
First Backup     Backup Ready              10.16.240.128
Second Backup    None

Current active Call Manager: 10.16.240.124
Backhaul/Redundant link port: 2428
Failover Interval: 30 seconds
Keepalive Interval: 15 seconds
```

```

Last keepalive sent:          00:45:31 (elapsed time: 00:00:04)
Last MGCP traffic time:      00:45:31 (elapsed time: 00:00:04)
Last failover time:         None
Switchback mode:           Graceful
MGCP Fallback mode:         Not Selected
Last MGCP Fallback start time: 00:00:00
Last MGCP Fallback end time: 00:00:00
PRI Backhaul Link info:
  Link Protocol:            TCP
  Remote Port Number:       2428
  Remote IP Address:        10.16.240.124
  Current Link State:       OPEN
  Statistics:
    Packets recvd:          32
    Recv failures:          0
    Packets xmitted:        32
    Xmit failures:          0
  PRI Ports being backhauled:
    Slot 1, port 0

```

```

Configuration Auto-Download Information
=====
Current version-id: {1645327B-F59A-4417-8E01-7312C61216AE}
Last config-downloaded:00:00:49
Current state: Waiting for commands
Configuration Download statistics:
  Download Attempted          : 6
  Download Successful         : 6
  Download Failed             : 0
  Configuration Attempted    : 1
  Configuration Successful    : 1
  Configuration Failed(Parsing): 0
  Configuration Failed(config) : 0
Last config download command: New Registration
Configuration Error History:
FAX mode: cisco

```

Step 3 show ccm-manager backhaul

Use the **show ccm-manager backhaul** command to verify the PRI backhaul link information, for example:

```

Router# show ccm-manager backhaul

PRI Backhaul Link info:
  Link Protocol:            TCP
  Remote Port Number:       2428
  Remote IP Address:        10.20.71.38
  Current Link State:       OPEN
  Statistics:
    Packets recvd:          0
    Recv failures:          0
    Packets xmitted:        21
    Xmit failures:          0
  PRI Ports being backhauled:
    Slot 1, port 1

```



Note

For a description of the fields displayed in these output examples, see the [Cisco IOS Voice Command Reference](#), Release 12.3T.

Configuring MGCP Gateway Support for Cisco Unified Communications Manager Network Specific Facilities

There are no specific Cisco IOS configuration tasks necessary to support the NSF feature other than enabling MGCP PRI backhaul as described in the “[Configuring MGCP PRI Backhaul on the Cisco Voice Gateway](#)” section on page 4.

Prerequisites for MGCP Gateway Support for Cisco Unified Communications Manager Network Specific Facilities

- Cisco IOS Release 12.3(4)T or later
- NM-HDV or NM-HDV2
- Supported interface cards:
 - AIM-ATM-VOICE-30
 - AIM-VOICE-30
- Supported switch types:
 - PRI 4ESS
 - PRI 5E8
 - PRI 5E9
 - DMS 100
 - DMS 250
 - PRI NI-2
- MGCP PRI backhaul configuration. For information, see:
 - “[Configuring MGCP PRI Backhaul and T1 CAS Support for Cisco Unified Communications Manager](#)” on page 1
 - *[How to Configure MGCP with Digital PRI and Cisco Unified Communications Manager](#)*
- Cisco Unified Communications Manager 3.3(2) (formerly known as Cisco CallManager 3.3(2)) or later with the following configured:
 - Network Service Protocol—Choose the PRI protocol that matches the protocol of the terminating gateway from the Network Service Protocol drop-down field.
 - Network Service—Choose the appropriate network service. The values vary depending on the network service protocol that you choose from the Network Service Protocol drop-down field.
 - Service Parameter Name—Displays the service parameter name that is associated with the chosen network service. If no service parameter exists for the network service, the field displays <Not Exist>.
 - Service Parameter Value—Enter the appropriate service parameter value. Valid entries include the digits 0 to 9. If a service parameter does not exist for the network service, Cisco Unified Communications Manager disables this field.
 - Route patterns—For more information, see the *[Cisco Unified CallManager Administration Guide, Release 4.0\(1\)](#)*.

- Cisco Unified Communications Manager supports NSF only if the appropriate carrier identification code (CIC) is entered in the CIC field. CICs, which can be 3 or 4 digits or no digits, enable you to reach the services of interexchange carriers. For a complete list of CICs, go to <http://www.nanpa.com>. The following are examples of commonly used CICs:
 - 0222—WorldCom and MCI
 - 0288—ATT
 - 0333—Sprint

Verifying Configuration of MGCP Gateway Support for Cisco Unified Communications Manager Network Specific Facilities

Perform this task to verify the configuration.

SUMMARY STEPS

1. **show ccm-manager**
2. **show mgcp endpoints**
3. **debug ccm-manager backhaul**
4. **debug isdn q931**

DETAILED STEPS

Step 1 **show ccm-manager**

Use the **show ccm-manager** command to verify the registration status of Cisco Unified Communications Manager, for example:

```
Router# show ccm-manager

MGCP Domain Name: Router
Priority Status Host

=====
Primary Registered 10.16.240.124

First Backup      None
Second Backup     None
Current active Call Manager: 10.16.240.124
Backhaul/Redundant link port: 2428
Failover Interval: 30 seconds
Keepalive Interval: 15 seconds
Last keepalive sent: 00:45:31 (elapsed time: 00:00:04)
Last MGCP traffic time: 00:45:31 (elapsed time: 00:00:04)
Last failover time: None
Switchback mode: Graceful
MGCP Fallback mode: Not Selected
Last MGCP Fallback start time: 00:00:00
Last MGCP Fallback end time:    00:00:00
PRI Backhaul Link info
  Link Protocol:    TCP
  Remote Port Number: 2428
  Remote IP Address: 10.16.240.124
  Current Link State: OPEN
  Statistics:
```

```

Packets recvd: 32
Recv failures: 0
Packets xmitted: 32
Xmit failures: 0
PRI Ports being backhauled: Slot 1, port 0
!
Configuration Auto-Download Information

=====

No configurations downloaded
Current state: Automatic Configuration Download feature is disabled
Configuration Error History:
FAX mode: cisco

```

Step 2 show mgcp endpoints

Use the **show mgcp endpoints** command to verify the status of the ports on the T1 interface, for example:

```

Router# show mgcp endpoints

Interface T1 1/0
!
ENDPOINT-NAME          V-PORT  SIG-TYPE  ADMIN
S1/ds1-0/1@AV-2620-4  1/0:23  none      up
S1/ds1-0/2@AV-2620-4  1/0:23  none      up
S1/ds1-0/3@AV-2620-4  1/0:23  none      up
S1/ds1-0/4@AV-2620-4  1/0:23  none      up
S1/ds1-0/5@AV-2620-4  1/0:23  none      up
S1/ds1-0/6@AV-2620-4  1/0:23  none      up
S1/ds1-0/7@AV-2620-4  1/0:23  none      up
S1/ds1-0/8@AV-2620-4  1/0:23  none      up
S1/ds1-0/9@AV-2620-4  1/0:23  none      up
S1/ds1-0/10@AV-2620-  1/0:23  none      up
S1/ds1-0/11@AV-2620-  1/0:23  none      up
S1/ds1-0/12@AV-2620-  1/0:23  none      up
S1/ds1-0/13@AV-2620-  1/0:23  none      up
S1/ds1-0/14@AV-2620-  1/0:23  none      up
S1/ds1-0/15@AV-2620-  1/0:23  none      up
S1/ds1-0/16@AV-2620-  1/0:23  none      up
S1/ds1-0/17@AV-2620-  1/0:23  none      up
S1/ds1-0/18@AV-2620-  1/0:23  none      up
S1/ds1-0/19@AV-2620-  1/0:23  none      up
S1/ds1-0/20@AV-2620-  1/0:23  none      up
S1/ds1-0/21@AV-2620-  1/0:23  none      up
S1/ds1-0/22@AV-2620-  1/0:23  none      up
S1/ds1-0/23@AV-2620-  1/0:23  none      up

```

Step 3 debug ccm-manager backhaul

Use the **debug ccm-manager backhaul** command to verify that the NSF messages are backhauled correctly between the gateway and Cisco Unified Communications Manager, for example:

```

Router# debug ccm-manager backhaul events
!
Call Manager backhaul events debugging is ON.
!
3:05:20:
1w0d:
cmbh_rcv_callback: <-- Receiving backhaul msg for Se1/1:23 :
| bk_msg_type = DATA_REQ
| bk_chan_id (slot:port) = 1:1
| Q.931 length = 52

```

```
| Q.931 message type: SETUP
| Q.931 message = 080200040504038090A21803A983971E028083200604A1323838E7
```

The bold portion of the above number is the NSF related information in the setup message of the backhaul packet.

```
28086E616D65343430316C0600813434303170058039393939
lw0d:
cmbrl_send_pak: >-- Sending backhauled msg for Se1/1:23 :
| bk_msg_type = DATA_IND
| bk_chan_id (slot:port) = 1:1
| Q.931 length = 12
| Q.931 message type: STATUS
| Q.931 message = 080280047D080280E4140101
lw0d:
cmbrl_send_pak: --> Sending backhauled msg for Se1/1:23 :
| bk_msg_type = DATA_IND
| bk_chan_id (slot:port) = 1:1
| Q.931 length = 10
| Q.931 message type: CALL PROCEEDING
| Q.931 message = 08028004021803A98397
lw0d:
cmbrl_send_pak: --> Sending backhauled msg for Se1/1:23 :
| bk_msg_type = DATA_IND
| bk_chan_id (slot:port) = 1:1
| Q.931 length = 9
| Q.931 message type: PROGRESS
| Q.931 message = 08028004031E028188
lw0d:
cmbrl_send_pak: --> Sending backhauled msg for Se1/1:23 :
| bk_msg_type = DATA_IND
| bk_chan_id (slot:port) = 1:1
| Q.931 length = 9
| Q.931 message type: CONNECT
| Q.931 message = 08028004071E028182
lw0d:
cmbh_rcv_callback: <-- Receiving backhaul msg for Se1/1:23 :
| bk_msg_type = DATA_REQ
| bk_chan_id (slot:port) = 1:1
| Q.931 length = 5
| Q.931 message type: CONNECT ACK
| Q.931 message = 080200040F
lw0d:
cmbrl_send_pak: --> Sending backhauled msg for Se1/1:23 :
| bk_msg_type = DATA_IND
| bk_chan_id (slot:port) = 1:1
| Q.931 length = 9
| Q.931 message type: DISCONNECT
| Q.931 message = 080280044508028290
lw0d:
cmbh_rcv_callback: <-- Receiving backhaul msg for Se1/1:23 :
| bk_msg_type = DATA_REQ
| bk_chan_id (slot:port) = 1:1
| Q.931 length = 5
| Q.931 message type: RELEASE
| Q.931 message = 080200044D
lw0d:
cmbrl_send_pak: --> Sending backhauled msg for Se1/1:23 :
| bk_msg_type = DATA_IND
| bk_chan_id (slot:port) = 1:1
| Q.931 length = 5
| Q.931 message type: RELEASE COMPLETE
| Q.931 message = 080280045A
```

Step 4 debug isdn q931

Use the **debug isdn q931** command to display the ISDN Layer 3 processing, for example:

```
Router# debug isdn q931
!
debug isdn q931 is ON.
1w0d: ISDN Se1/1:23 Q931: TX -> SETUP pd = 8 callref = 0x0003
      Bearer Capability i = 0x8090A2
          Standard = CCITT
          Transfer Capability = Speech
          Transfer Mode = Circuit
          Transfer Rate = 64 kbit/s
      Channel ID i = 0xA98397
          Exclusive, Channel 23
      Progress Ind i = 0x8083 - Origination address is non-ISDN
      Net Specific Fac i = 0x04A1323838E7
      Display i = 'name4401'
      Calling Party Number i = 0x0081, '4401'
          Plan:Unknown, Type:Unknown
      Called Party Number i = 0x80, '9999'
          Plan:Unknown, Type:Unknown
1w0d: ISDN Se1/1:23 Q931: RX <- STATUS pd = 8 callref = 0x8003
      Cause i = 0x80E4 - Invalid information element contents
      Call State i = 0x01
1w0d: ISDN Se1/1:23 Q931: RX <- CALL_PROC pd = 8 callref = 0x8003
      Channel ID i = 0xA98397
          Exclusive, Channel 23
1w0d: ISDN Se1/1:23 Q931: RX <- PROGRESS pd = 8 callref = 0x8003
      Progress Ind i = 0x8188 - In-band info or appropriate now available
1w0d: ISDN Se1/1:23 Q931: RX <- CONNECT pd = 8 callref = 0x8003
      Progress Ind i = 0x8182 - Destination address is non-ISDN
1w0d: ISDN Se1/1:23 Q931: TX -> CONNECT_ACK pd = 8 callref = 0x0003
1w0d: ISDN Se1/1:23 Q931: RX <- DISCONNECT pd = 8 callref = 0x8003
      Cause i = 0x8290 - Normal call clearing
1w0d: ISDN Se1/1:23 Q931: TX -> RELEASE pd = 8 callref = 0x0003
1w0d: ISDN Se1/1:23 Q931: RX <- RELEASE_COMP pd = 8 callref = 0x8003
```

**Note**

For a description of the fields displayed in these output examples, see the [Cisco IOS Voice Command Reference](#), Release 12.3T and the [Cisco IOS Debug Command Reference](#), Release 12.3.

Configuring QSIG Supplementary Features for Cisco IOS Voice Gateways

There are no specific configuration tasks necessary to support QSIG features on the voice gateway except those described in the following Prerequisites section.

Prerequisites

- Cisco IOS Release 12.3(11)T or later
- MGCP must be configured on the voice gateway. For information, see “[Configuring MGCP Gateway Support for Cisco Unified Communications Manager](#)” on page 23.
- ISDN PRI Backhaul must be configured on the MGCP gateway. For information, see the “[Configuring MGCP PRI Backhaul on the Cisco Voice Gateway](#)” section on page 4.

- QSIG signaling is required to support supplementary services over the T1 and E1 time-division multiplexing (TDM) trunks that support the PRI backhaul mechanism.
- Cisco Catalyst 6500 series and Cisco 7600 series Communication Media Module (CMM) requires WS-SVC-CMM-6T1 or WS-SVC-CMM-6E1 port adapter.

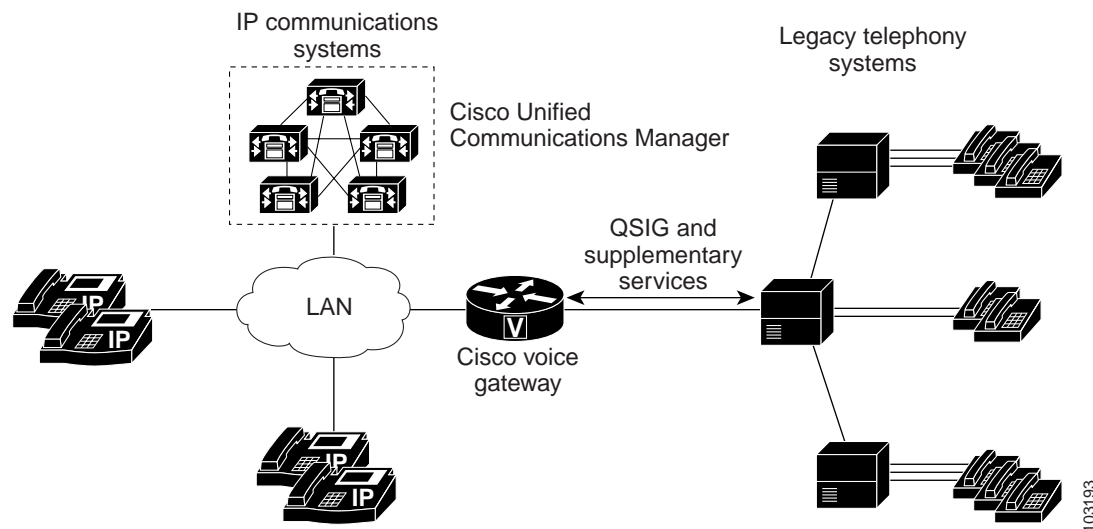
QSIG Supplementary Features for Cisco IOS Voice Gateways

The QSIG protocol, a variation of ISDN PRI signaling that is used by PBXs, supports basic calls and supplementary services over TDM trunks. Cisco Unified Communications Manager can interoperate with PBXs using QSIG. The voice gateway supports QSIG over PRI backhaul interfaces. Call control is transparent to the voice gateway as all layer 3 messages are passed through PRI backhaul.

These additional QSIG features and services are supported for Cisco Unified Communications Manager 4.0 (formerly known as Cisco CallManager 4.0) and later:

- Call diversion (forwarding)
- Call transfer
- Identification services
- Message waiting indication services

Figure 8 QSIG and Supplementary Services Overview



For more information about QSIG support in Cisco Unified Communications Manager, see the [“Understanding IP Telephony Protocols”](#) chapter in the *Cisco Unified Communications Manager System Guide*.

Configuration Examples for MGCP PRI Backhaul and T1 CAS

This section provides the following configuration example:

- [MGCP PRI Backhaul and T1 CAS: Example, page 14](#)



Note

To view relevant configuration examples, go to the Cisco Systems Technologies website at <http://cisco.com/web/psa/technologies/index.html>. From the website, select **Voice > IP Telephony/VoIP**, then click **Configure > Configuration Examples and Tech Notes**.

MGCP PRI Backhaul and T1 CAS: Example

In the following example, T1 CAS and PRI backhaul is configured for an MGCP gateway:

```
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 modem passthrough voip mode cisco
mgcp modem passthrough voip codec g711alaw
mgcp modem passthrough voip redundancy
mgcp package-capability dtmf-package
mgcp package-capability mf-package
mgcp package-capability rtp-package
mgcp package-capability sst-package
mgcp default-package line-package
mgcp timer net-cont-test 3000
isdn switch-type primary-ni
call rsvp-sync
!
ccm-manager fallback-mgcp
ccm-manager redundant-host 10.0.0.21
ccm-manager mgcp
ccm-manager music-on-hold

! This is the PRI backhaul circuit
controller T1 3/0
 framing esf
 linecode b8zs
 pri-group 0 timeslots 1-24 service mgcp
!
! This is the T1-CAS circuit
controller T1 3/1
 framing esf
 linecode b8zs
 ds0-group 0 timeslots 1-24 type e&m-wink-start
!
interface Serial3/0:23
 no ip address
 no logging event link-status
 isdn switch-type primary-ts014
 isdn incoming-voice voice
 isdn T306 60000
 isdn bind-L3 ccm-manager
 no cdp enable
!
dial-peer voice 501 pots
 service mgcpapp
 incoming called-number
 port 3/1:0
```

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 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

- [“Cisco Unified Communications Manager and Cisco IOS Interoperability Features Roadmap”](#) on page 9—Describes how to access Cisco Feature Navigator; also lists and describes, by Cisco IOS release, Cisco Unified Communications Manager and Cisco IOS interoperability features.
- [“Overview of Cisco Unified Communications Manager and Cisco IOS Interoperability”](#) on page 13—Describes basics of underlying technology and lists related documents.
- [How to Configure MGCP with Digital PRI and Cisco Unified Communications Manager](#)—Technical support configuration document that includes sample configurations and troubleshooting tips.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0711R)

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

© 2007 Cisco Systems, Inc. All rights reserved.

■ Additional References



Configuring MGCP-Controlled Backhaul of BRI Signaling in Conjunction with Cisco Unified Communications Manager

The MGCP-Controlled Backhaul of Basic Rate Interface (BRI) Signaling in Conjunction with Cisco Unified Communications Manager feature provides MGCP service to remote-office gateways that connect by means of ISDN BRI trunks to a centralized Cisco Unified Communications Manager.

Feature benefits include the following:

- Centralized call-management architecture, enabling a high degree of network control
- Short voice cut-through times
- Graceful evolution to new technology and to AVVID

Only the ETSI BRI basic-net3 switch type is supported.

Feature History for MGCP-Controlled Backhaul of BRI Signaling in Conjunction with Cisco Unified Communications Manager

Release	Modification
12.2(15)ZJ	This feature was introduced for Cisco Communications Manager 3.3(2) (formerly known as Cisco CallManager 3.3(2)).
12.3(2)T	This feature was integrated into Cisco IOS Release 12.3(2)T.
12.3(11)T	Support was added for Cisco Unified Communications Manager 4.1.
12.4(2)T	This feature was implemented on the Cisco 2600XM, Cisco 2691, Cisco 2800 series, Cisco 3700 series, and Cisco 3800 series.



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

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.

**Note**

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/ios123/123cgr/voice_c/vcl.htm.

Contents

- [Prerequisites for MGCP-Controlled Backhaul of BRI Signaling](#), page 2
- [Restrictions for MGCP-Controlled Backhaul of BRI Signaling](#), page 3
- [Information About MGCP-Controlled Backhaul of BRI Signaling](#), page 3
- [How to Configure MGCP-Controlled Backhaul of BRI Signaling](#), page 5
- [Configuration Examples for MGCP-Controlled Backhaul of BRI Signaling](#), page 9
- [Where to Go Next](#), page 15
- [Additional References](#), page 16

Prerequisites for MGCP-Controlled Backhaul of BRI Signaling

Cisco Unified Communications Manager

- Cisco Unified Communications Manager 4.1(1) or a later release

Cisco Voice Gateway

- 20-MB flash memory
- 64-MB DRAM
- One of the supported combinations of BRI voice interface card (VIC) and network module:
 - VIC-2BRI-NT/TE or VIC-2BRI-S/T in NM-1V or NM-2V with Cisco IOS Release 12.3(11)T or a later release
 - VIC2-2BRI-NT/TE in NM-HD-1V, NM-HD-2V, NM-HD-2VE, or NM-HDV2 with Cisco IOS Release 12.4(2)T or a later release
 - EM-4BRI-NT/TE in EVM-HD-8FXS/DID with Cisco IOS Release 12.4(2)T or a later release
- MGCP enabled globally in a VoIP network

- MGCP control of dial peers and voice ports
- MGCP single-point configuration enabled



Note For MGCP configuration instructions, see [“Configuring MGCP Gateway Support for Cisco Unified Communications Manager” on page 23.](#)

Restrictions for MGCP-Controlled Backhaul of BRI Signaling

- BRI backhaul uses the enhanced interface numbering support available in Cisco IOS Release 12.3(11)T and later. Previous releases supported only the slot/subslot/port format with the subslot forced to 0 on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series. Cisco IOS Release 12.3(11)T and later releases support both the slot/port and slot/subslot/port interface numbering formats for BRI backhaul.
- Only the ETSI BRI Basic-NET3 switch type is supported.
- BRI calls are cleared during MGCP gateway fallback and rehome because ISDN BRI L2 must be reinitiated and brought up again by the new L3 task.
- Do not add the **application mgcpapp** command to voice dial peers that support BRI backhaul.

Information About MGCP-Controlled Backhaul of BRI Signaling

To configure MGCP-controlled backhaul of BRI signaling, you should understand the following concept:

- [MGCP-Controlled Backhaul of BRI Signaling, page 3](#)

MGCP-Controlled Backhaul of BRI Signaling

The MGCP-Controlled Backhaul of BRI Signaling feature supports a centralized Cisco Unified Communications Manager architecture with BRI trunks connected to remote branch offices. Transporting signaling information from a branch-office MGCP gateway to a centralized media-gateway controller for processing is called backhaul. D-channel signal 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 MGCP gateway neither parses nor has any knowledge of the contents of those messages.

This feature enables you to connect remote ISDN PBXs and key systems to a Cisco ISDN BRI network termination (network side) or PSTN Class 4/5 switch through a Cisco ISDN BRI terminal equipment (as user side) interface. External call-control entities, such as one or more Cisco Unified Communications Manager servers, provide voice service between local and remote branch offices.

[Figure 9](#) depicts a typical network-side scenario. NT denotes network termination; TE denotes terminal equipment.

Figure 9 Typical ISDN BRI Network-Side Scenario

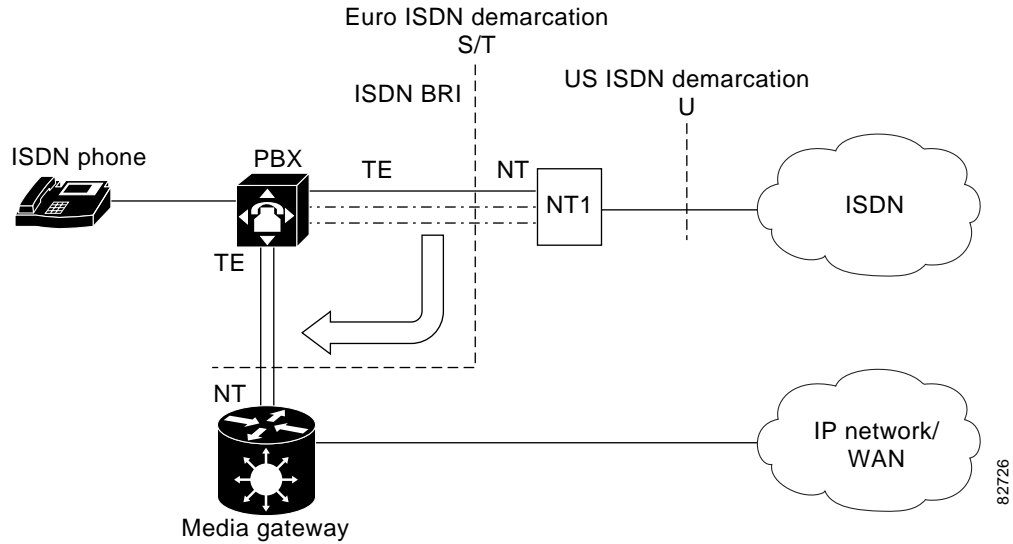
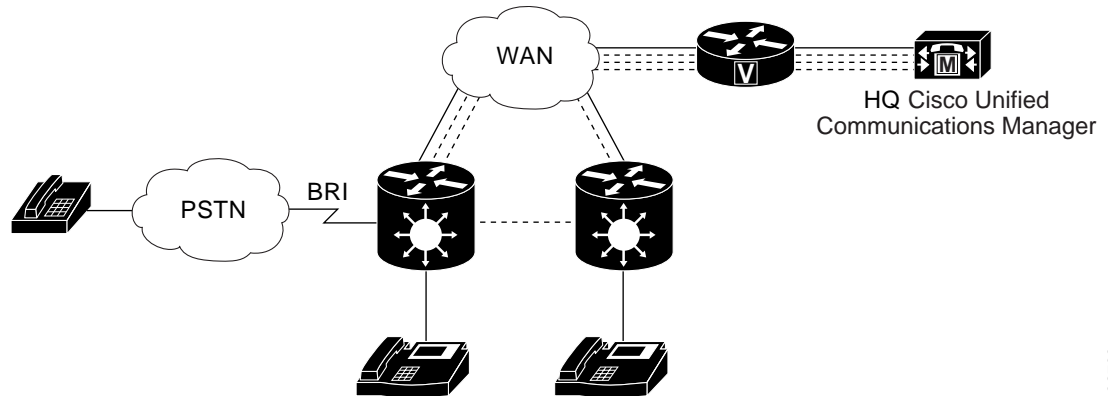


Figure 10 shows a typical user-side scenario.

Figure 10 ISDN BRI User-Side Scenario



The following is the sequence of events during normal backhaul:

1. A call comes in from the PSTN and passes over the BRI trunk to the MGCP gateway.
2. The MGCP gateway passes signaling information from the call across the WAN to the Cisco Unified Communications Manager at headquarters.
3. The Cisco Unified Communications Manager instructs the MGCP gateway on how to set up and manage the call.
4. The call is established.

How to Configure MGCP-Controlled Backhaul of BRI Signaling

This section contains the following procedures:

- [Configuring the BRI Interface as an MGCP-BRI Backhaul Endpoint, page 5](#) (required)
- [Verifying MGCP-BRI Backhaul Configuration, page 6](#) (optional)
- [Troubleshooting Tips for MGCP-Controlled Backhaul of BRI Signaling, page 8](#) (optional)

Configuring the BRI Interface as an MGCP-BRI Backhaul Endpoint

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface bri slot/port`
4. `shutdown`
5. `isdn switch-type basic-net3`
6. `isdn bind-L3 ccm-manager service mgcp`
7. `no shutdown`
8. `no mgcp`
9. `mgcp`
10. `exit`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code> Example: Router> <code>enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<code>configure terminal</code> Example: Router# <code>configure terminal</code>	Enters global configuration mode on the BRI slot and port.
Step 3	<code>interface bri slot/port</code> Example: Router(config)# <code>interface bri 1/0</code>	Configures the BRI interface as the MGCP-BRI backhaul endpoint. <ul style="list-style-type: none"> • <i>Slot</i> and <i>port</i> syntax is platform-dependent; type ? to determine. <p>Note This command is supported only for a user-side ETSI NET3 switch-type.</p>

	Command or Action	Purpose
Step 4	<code>shutdown</code> Example: <code>Router(config-if)# shutdown</code>	(Optional) Clears the interface of any active calls. If there are no active calls, you can skip this step.
Step 5	<code>isdn switch-type basic-net3</code> Example: <code>Router(config-if)# isdn switch-type basic-net3</code>	Sets the central-office switch type on the ISDN interface to basic-net3 .
Step 6	<code>isdn bind-L3 ccm-manager service mgcp</code> Example: <code>Router(config-if)# isdn bind-L3 ccm-manager service mgcp</code>	Sets ISDN L3 binding on the BRI interface.
Step 7	<code>no shutdown</code> Example: <code>Router(config-if)# no shutdown</code>	Restarts the interface if it was previously disabled.
Step 8	<code>no mgcp</code> Example: <code>Router(config-if)# no mgcp</code>	Disables all MGCP applications and protocols.
Step 9	<code>mgcp</code> Example: <code>Router(config-if)# mgcp</code>	Restarts MGCP and reregisters the gateway to Cisco Unified Communications Manager.
Step 10	<code>exit</code> Example: <code>Router(config-if)# end</code>	Exits interface-configuration mode.

Verifying MGCP-BRI Backhaul Configuration

SUMMARY STEPS

1. `show isdn status`
2. `show ccm-manager`
3. `show ccm-manager backhaul`
4. `show mgcp endpoint`

DETAILED STEPS

Step 1 `show isdn status`

Use the **show isdn status** command to verify that Layer 2 is established and that Layer 3 is configured as Cisco Unified Communications Manager. This output displays only if TEI negotiation is performed at startup.

```
Router# show isdn status

ISDN BRI1/1 interface
  dsl 1, interface ISDN Switchtype = basic-net3
  L2 Protocol = Q.921 L3 Protocol(s) = CCM-MANAGER
  Layer 1 Status:
    ACTIVE
  Layer 2 Status:
    TEI = 64, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
```



Note Use this command only if TEI negotiation is done at startup. Otherwise, TEI negotiation is done when the first call is placed, so output shows Layer 2 with no TEI negotiated and Layer 3 as down.

Step 2 show ccm-manager

Use the **show ccm-manager** command to verify your Cisco Unified Communications Manager configuration on the gateway.

```
Router# show ccm-manager

MGCP Domain Name:3845-1.cisco.com
Priority      Status      Host
=====
Primary      Registered  10.3.102.99
First Backup  None
Second Backup None

Current active Call Manager:  10.3.102.99
Backhaul/Redundant link port: 2428
Failover Interval:           30 seconds
Keepalive Interval:          15 seconds
Last keepalive sent:         20:58:35 UTC Sep 3 2004 (elapsed time:00:00:11)
Last MGCP traffic time:      20:58:35 UTC Sep 3 2004 (elapsed time:00:00:11)
Last failover time:          None
Last switchback time:        None
Switchback mode:             Graceful
MGCP Fallback mode:          Not Selected
Last MGCP Fallback start time: None
Last MGCP Fallback end time:  None
MGCP Download Tones:         Disabled

Configuration Error History:
FAX mode:cisco
```

Step 3 show ccm-manager backhaul

Use the **show ccm-manager backhaul** command to display information about the BRI backhaul link.

```
Router# show ccm-manager backhaul

Backhaul Link info:
  Link Protocol:      TCP
  Remote Port Number:2428
  Remote IP Address: 10.3.102.99
  Current Link State:OPEN
  Statistics:
    Packets recvd:    4
    Recv failures:    0
```

```

Packets xmitted:2
Xmit failures: 0
BRI Ports being backhauled:
Slot 0, VIC 0, port 0
Slot 1, VIC 0, port 0

```

Step 4 show mgcp endpoint

Use the **show mgcp endpoint** command to display a list of your MGCP endpoints.

```
Router# show mgcp endpoint
```

```

BRI/S1/SU0/P1/1@3745-1
BRI/S1/SU0/P1/2@3745-1

```

Troubleshooting Tips for MGCP-Controlled Backhaul of BRI Signaling

Table 10 lists commands that are available for troubleshooting your configuration.

Table 10 Troubleshooting Commands

Command	Purpose
command-type a-law	Enables you to address poor voice quality. If your system uses a-law pulse-code modulation (PCM), use this command in interface-BRI configuration mode to reconfigure the BRI voice port in the gateway for a-law PCM. The system default is mu-law PCM.
debug ccm-manager backhaul packets	Displays debugging information about Cisco Unified Communications Manager backhaul message packets.
debug isdn q931	Displays debugging information about ISDN L3 Q.931 message packets.
debug mgcp packets	Displays debugging information about MGCP message packets.

Configuring SRTP Mode on Cisco IOS MGCP Gateways

SRTP mode provides secure VoIP calls by addressing security requirements for privacy, integrity, and confidentiality of voice conversations. IPsec, a standards-based set of security protocols and algorithms, ensures that signaling information that is sent between the gateway and Cisco Unified Communications Manager are encrypted. Media encryption using standards-based Secure Real-Time Transport Protocol (SRTP) ensures that media streams between supported devices are secure.

Perform this task to configure SRTP mode on the gateway.

Prerequisites for SRTP Mode

You should first establish an IPsec connection between Cisco Unified Communications Manager and the MGCP gateway before using the MGCP SRTP package. Otherwise, media keys are sent in clear text and your voice call is not considered secure.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mgcp package-capability srtp-package**
4. **mgcp validate call-agent source-ipaddr**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code> Example: <code>Router> enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	<code>configure terminal</code> Example: <code>Router# configure terminal</code>	Enters global configuration mode.
Step 3	<code>mgcp package-capability srtp-package</code> Example: <code>Router(config)# mgcp package-capability srtp-package</code>	Enables the MGCP gateway capability to process SRTP packages.
Step 4	<code>mgcp validate call-agent source-ipaddr</code> Example: <code>Router(config)# mgcp validate call-agent source-ipaddr</code>	(Optional) Enables the MGCP application validation that packets received are sent by a configured call agent.
Step 5	<code>exit</code> Example: <code>Router(config)# exit</code>	Exits global configuration mode.

Configuration Examples for MGCP-Controlled Backhaul of BRI Signaling

This section provides the following configuration example:

- [MGCP BRI Backhaul on Cisco 3745: Example, page 10](#)
- [MGCP BRI Backhaul on Cisco 3640: Example, page 13](#)

MGCP BRI Backhaul on Cisco 3745: Example

```

Router# show running-config

Building configuration...

Current configuration :3913 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
no network-clock-participate slot 1
no network-clock-participate slot 2
no network-clock-participate slot 3
no network-clock-participate slot 4
no network-clock-participate wic 0
no network-clock-participate wic 1
no network-clock-participate wic 2
no network-clock-participate aim 0
no network-clock-participate aim 1
no aaa new-model
ip subnet-zero
ip cef
!
!
!
ip dhcp pool phone1
  host 10.3.102.102 255.255.0.0
  client-identifier 0100.1121.116b.dd
  option 150 ip 10.3.102.99
  default-router 10.3.102.2
!
!
ip domain name cisco.com
ip ids po max-events 100
no ftp-server write-enable
isdn switch-type basic-net3
voice-card 1
  no dspfarm
!
voice-card 2
  no dspfarm
!
voice-card 3
  no dspfarm
!
!
!
ccm-manager switchback immediate
ccm-manager fallback-mgcp

```

```
ccm-manager redundant-host 10.3.102.98
ccm-manager mgcp
!
!
!
interface FastEthernet0/0
 ip address 10.3.102.2 255.255.0.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface BRI1/0
 no ip address
 isdn switch-type basic-net3
 isdn incoming-voice voice
 isdn bind-l3 ccm-manager service mgcp
 isdn skipsend-idverify
!
interface BRI1/1
 no ip address
 isdn switch-type basic-net3
 isdn protocol-emulate network
 isdn layer1-emulate network
 isdn incoming-voice voice
 isdn skipsend-idverify
!
interface BRI2/0
 no ip address
 isdn switch-type basic-net3
 isdn incoming-voice voice
 isdn bind-l3 ccm-manager service mgcp
 isdn skipsend-idverify
!
interface BRI2/1
 no ip address
 isdn switch-type basic-net3
 isdn protocol-emulate network
 isdn layer1-emulate network
 isdn incoming-voice voice
 isdn skipsend-idverify
!
interface BRI3/0
 no ip address
 isdn switch-type basic-net3
 isdn incoming-voice voice
 isdn bind-l3 ccm-manager service mgcp
 isdn skipsend-idverify
!
interface BRI3/1
 no ip address
 isdn switch-type basic-net3
 isdn protocol-emulate network
 isdn layer1-emulate network
 isdn incoming-voice voice
 isdn skipsend-idverify
!
!
ip default-gateway 10.3.0.1
ip classless
```

```
ip route 0.0.0.0 0.0.0.0 10.3.0.1
!
ip http server
no ip http secure-server
!
!
access-list 10 deny 10.3.102.99 log
access-list 10 permit any
!
!
!
control-plane
!
!
call application alternate DEFAULT
!
!
voice-port 1/1/0
!
voice-port 1/1/1
!
voice-port 2/0/0
!
voice-port 2/0/1
!
voice-port 3/0/0
!
voice-port 3/0/1
!
voice-port 3/1/0
!
voice-port 3/1/1
!
voice-port 3/1/2
!
voice-port 3/1/3
!
!
mgcp
mgcp call-agent 10.3.102.99 service-type mgcp version 0.1
mgcp package-capability srtp-package
!
mgcp profile default
!
!
!
dial-peer voice 1 pots
  application mgcpapp
  direct-inward-dial
  port 3/0/0
  forward-digits all
!
dial-peer voice 100 voip
  application mgcpapp
  destination-pattern 9...
  session target ipv4:10.3.102.1
  incoming called-number .
!
dial-peer voice 2 pots
  destination-pattern 5001
  port 3/1/0
!
dial-peer voice 4 pots
  destination-pattern 6T
```

```
direct-inward-dial
port 3/0/1
!
dial-peer voice 3 pots
destination-pattern 5002
port 3/1/3
!
dial-peer voice 11 pots
destination-pattern 2T
direct-inward-dial
port 2/0/1
!
dial-peer voice 12 pots
application mgcpapp
direct-inward-dial
port 2/0/0
forward-digits all
!
!
!
call-manager-fallback
max-conferences 8
ip source-address 10.3.102.2 port 2000
max-ephones 2
max-dn 4
!
!
line con 0
exec-timeout 0 0
line aux 0
line vty 0 4
login
!
end
```

MGCP BRI Backhaul on Cisco 3640: Example

```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
no service dhcp
!
hostname 3640
!
!
voice-card 3
!
ip subnet-zero
!
!
ip domain name cisco.com
!
isdn switch-type primary-qsig
!
!
voice call carrier capacity active
!
voice service voip
h323
call start slow
!
```

```

!
!
!
mta receive maximum-recipients 0
ccm-manager mgcp
!
controller T1 3/0
  framing esf
  clock source internal
  linecode b8zs
  pri-group timeslots 1-24 service mgcp
!
controller T1 3/1
  framing esf
  linecode b8zs
!
!
!
interface FastEthernet0/0
  ip address 10.15.43.101 255.255.0.0
  duplex auto
  speed auto
  no cdp enable
!
interface Serial0/0
  no ip address
  encapsulation frame-relay
  shutdown
  clockrate 125000
  frame-relay lmi-type ansi
!
interface FastEthernet0/1
  no ip address
  shutdown
  duplex auto
  speed auto
!
interface Serial0/1
  no ip address
  shutdown
  clockrate 125000
!
interface BRI1/0
  no ip address
  isdn switch-type basic-net3
  isdn incoming-voice voice
  isdn bind-13 ccm-manager service mgcp
!
interface BRI1/1
  no ip address
  isdn switch-type basic-qsig
!
interface Serial3/0:23
  no ip address
  no logging event link-status
  isdn switch-type primary-qsig
  isdn incoming-voice voice
  no cdp enable
!
ip default-gateway 10.15.10.11
ip classless
ip route 0.0.0.0 0.0.0.0 10.15.10.11
ip http server
!

```

```
ip pim bidir-enable
!
!
!
call rsvp-sync
!
voice-port 1/0/0
!
voice-port 1/0/1
!
voice-port 2/0/0
!
voice-port 2/0/1
!
voice-port 2/1/0
!
voice-port 2/1/1
!
voice-port 3/0:23
!
mgcp
mgcp call-agent 10.14.181.10 service-type mgcp version 0.1
mgcp sdp simple
!
mgcp profile default
!
!
!
dial-peer cor custom
!
!
!
dial-peer voice 6000 pots
  application mgcpapp
  port 2/0/0
!
dial-peer voice 4000 pots
  application mgcpapp
  port 2/0/1
!
!
line con 0
  exec-timeout 0 0
line aux 0
line vty 0 4
  login
!
!
end
```

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 download region-specific tones and their associated frequencies, amplitudes, and cadences, see [“Configuring Tone Download to MGCP Gateways” on page 145](#).

Additional References

- [“Cisco Unified Communications Manager and Cisco IOS Interoperability Features Roadmap” on page 9](#)—Describes how to access Cisco Feature Navigator; also lists and describes, by Cisco IOS release, Cisco Unified Communications Manager and Cisco IOS interoperability features.
- [“Overview of Cisco Unified Communications Manager and Cisco IOS Interoperability” on page 13](#)—Describes basics of underlying technology and lists related documents.
- [“Configuring ISDN BRI”](#) in the *Cisco IOS Dial Technologies Configuration Guide*, Release 12.4—Describes how to configure ISDN BRI on the voice gateway.
- [“ISDN Switch Types, Codes, and Values”](#) appendix in the *Debug Command Reference*, Release 12.4—Describes supported switch types.
- [Cisco Unified Communications Manager documentation](#)—Describes how to install and configure Cisco Unified Communications Manager.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0711R)

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

© 2007 Cisco Systems, Inc. All rights reserved.



Configuring Tone Download to MGCP Gateways

The Customizable Tone Download to Cisco IOS MGCP Gateways from Cisco Unified Communications Manager feature enables the Cisco IOS gateway to download region-specific tones and the associated frequencies, amplitudes, and cadences in its XML configuration files.

Cisco IOS gateways support static tone tables that are predefined for each country in Cisco IOS tone tables. Voice ports use the static tone tables associated with the Cisco Unified Communications Manager network locale unless the custom tone download feature is enabled

Feature History for Customizable Tone Download to Cisco IOS MGCP Gateways from Cisco Unified Communications Manager

Release	Modification
12.2(15)ZJ	This feature was introduced.
12.3(4)T	This feature was integrated into Cisco IOS Release 12.3(4)T.

Feature History for Globalized Cadence and Tone for Cisco IOS Gateways

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

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.



Note

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.



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Contents

- [Information About Tone Download to MGCP Gateways, page 2](#)
- [How to Configure Tone Download to MGCP Gateways, page 4](#)
- [Configuration Examples for Tone Download to MGCP Gateways, page 16](#)
- [Where to Go Next, page 17](#)
- [Additional References, page 17](#)

Information About Tone Download to MGCP Gateways

To configure tone download, you should be familiar with the following concepts:

- [Tone Download Process for MGCP Gateways, page 2](#)
- [Static Tones, page 2](#)
- [Custom Tones, page 4](#)

Tone Download Process for MGCP Gateways

When configuring MGCP gateways in a Cisco IP-telephony network, you can use a centralized TFTP server in your network to automatically download an XML file with the gateway-specific configuration.

The XML configuration file includes the network locale for each voice port on the gateway. The network locale configured in Cisco Unified Communications Manager defines the tones and cadences that are used by a device in a specific geographic area. A network locale is associated with each voice port in the MGCP gateway.

When the XML file is downloaded to the gateway, it is parsed, converted to Cisco IOS commands, and the active configuration is updated. If the gateway is restarted or reset, it triggers a download of the XML file from the TFTP server. If the specified TFTP server is not available, the gateway keeps trying to download the updated XML file and does not alter the current configuration.

For information on downloading XML configuration files to your MGCP gateway, see the [“Enabling Single-Point Configuration for MGCP Gateways”](#) section on page 45.

Static Tones

The Globalized Cadence and Tone for Cisco IOS Gateways feature enables Cisco IOS gateways to support Cisco Unified Communications Manager localization using static tone tables that are predefined for each country in Cisco IOS tone tables. The static tone table that is used for a voice port is determined by the network locale that is specified for the voice port in Cisco Unified Communications Manager. When an MGCP gateway registers to Cisco Unified Communications Manager, or if the gateway restarts or resets, the network locale for each voice port is downloaded in the gateway’s XML configuration file.

The static tones and cadences associated with the Cisco Unified Communications Manager network locale are used by a voice port unless a custom tone table is downloaded. No configuration is required on the MGCP gateway to use the static tones.

Table 11 shows the list of valid two-letter country codes and the corresponding countries.

Table 11 **Country Codes**

Code	Country	Code	Country
AR	Argentina	KE	Kenya
AT	Austria	KR	Korea Republic
AU	Australia	LB	Lebanon
BE	Belgium	LU	Luxemborg
BR	Brazil	MX	Mexico
CA	Canada	MY	Malaysia
CH	Switzerland	NG	Nigeria
CN	China	NL	Netherlands
CO	Colombia	NO	Norway
CY	Cyprus	NP	Nepal
CZ	Czech Republic	NZ	New Zealand
DE	Germany	PA	Panama
DK	Denmark	PE	Peru
EG	Egypt	PH	Philippines
ES	Spain	PK	Pakistan
FI	Finland	PL	Poland
FR	France	PT	Portugal
GB	United Kingdom	RU	Russian Federation
GH	Ghana	SA	Saudi Arabia
GR	Greece	SE	Sweden
HK	Hong Kong	SG	Singapore
HU	Hungary	SI	Slovenia
ID	Indonesia	SK	Slovakia
IE	Ireland	TH	Thailand
IL	Israel	TR	Turkey
IN	India	TW	Taiwan
IS	Iceland	US	United States
IT	Italy	VE	Venezuela
JO	Jordan	ZA	South Africa
JP	Japan	ZW	Zimbabwe

Custom Tones

The Customizable Tone Download to Cisco IOS MGCP Gateways from Cisco Unified Communications Manager feature enables an MGCP gateway to download locale-specific tones and their associated frequency, amplitude, and cadence information from the XML-based configuration file.

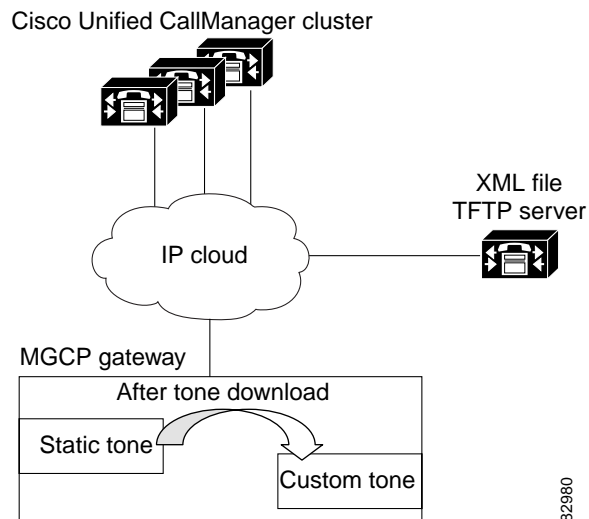
The XML tone file includes all supported tones for one country with the frequency, amplitude, and cadence information. The XML tone file is parsed and saved into a custom tone table on the MGCP gateway. Each gateway supports up to two custom tone tables. The default values for North America are overwritten with the new values specified in the XML file. Dual tones and sequential tones, and up to 4 frequencies for standard or custom tones are supported.

When Cisco Unified Communications Manager requests a specific tone, the gateway references the custom tone table associated with the network locale of the voice port. After the custom tone specification is downloaded to the gateway, it can be used even if the gateway loses connectivity to Cisco Unified Communications Manager and reverts to H.323 control in fallback mode.

If custom tone download is not configured, the voice port uses the static tone table associated with the network locale of the voice port. If custom tone download is configured but fails, the voice port continues to use the static tone table for the network locale.

Figure 11 shows the download of the XML file from the TFTP server to the MGCP gateway.

Figure 11 Download of XML File from TFTP Server



How to Configure Tone Download to MGCP Gateways

This section contains the following procedures:

- [Verifying Globalized Cadence and Tone Configuration, page 5](#) (optional)
- [Configuring Customizable Tone Download to Cisco IOS MGCP Gateways, page 9](#) (required)
- [Verifying Customizable Tone Download, page 10](#) (optional)

Verifying Globalized Cadence and Tone Configuration

Perform this task to verify which network locale is configured in Cisco Unified Communications Manager.

**Note**

There are no configuration tasks necessary to enable globalized cadence and tone except those described in [Prerequisites](#).

Prerequisites

- Cisco IOS Release 12.2(11)T or later
- Cisco Unified Communications Manager 3.2 (formerly known as Cisco CallManager 3.2) or higher
- Cisco Unified Communications Manager 4.0 (formerly known as Cisco CallManager 4.0) or higher
- Cisco IOS gateway must be configured for MGCP and must have single-point configuration enabled. See “[Configuring MGCP Gateway Support for Cisco Unified Communications Manager](#)” on [page 23](#) for information.

**Note**

The IP hostname should match the gateway name that is specified in the Cisco Unified Communications Manager configuration.

- Ad-hoc conferencing and transcoding port adapter (WS-SVC-CMM-ACT) must be installed and configured on the Cisco Catalyst 6500 Series and Cisco 7600 Series Router Communication Media Module (CMM).

SUMMARY STEPS

1. **show voice port** *slot/port*

DETAILED STEPS

Step 1 **show voice port** *slot/port*

Use the **show voice port** command to verify the globalized cadence and tone configuration as shown in the following examples.

Cisco IAD2420 series

```
Router# show voice port 0/5

E&M 0:5 Slot is 0, Port is 5
Type of VoicePort is E&M
Operation State is DOWN
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
Coder Type is g729ar8
Voice Activity Detection is enabled
Nominal Playout Delay is 60 milliseconds
Maximum Playout Delay is 200 milliseconds
Rx A bit no conditioning set
Rx B bit no conditioning set
Rx C bit no conditioning set
Rx D bit no conditioning set
Tx A bit no conditioning set
Tx B bit no conditioning set
Tx C bit no conditioning set
Tx D bit no conditioning set
Rx Seize ABCD bits = 1111 Default pattern
Rx Idle ABCD bits = 0000 Default pattern
Tx Seize ABCD bits = 1111 Default pattern
Tx Idle ABCD bits = 0000 Default pattern
Ignored Rx ABCD bits = BCD
Region Tone is set for CN

```

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:

```

Operation Type is 2-wire
E&M Type is 1
Signal Type is immediate
Dial Type is dtmf
In Seizure is inactive
Out Seizure is active
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
Clear Wait Duration Timing is set to 400 ms
Wink Wait Duration Timing is set to 200 ms
Wait Wink Duration Timing is set to 550 ms
Wink Duration Timing is set to 200 ms
Delay Start Timing is set to 150 ms
Delay Duration Timing is set to 2000 ms
Dial Pulse Min. Delay is set to 140 ms
Percent Break of Pulse is 60 percent

```

```
Auto Cut-through is disabled
Dialout Delay is 300 ms
```

Cisco 2600 series

```
Router# show voice port
TE Basic Rate Interface 1/0/0 Slot is 1, Sub-unit is 0, Port is 0
  Type of VoicePort is ISDN-BRI
  Operation State is DORMANT
  Administrative State is UP
  The Last Interface Down Failure Cause is Administrative Shutdown
  Description is not set
  Noise Regeneration is enabled
  Non Linear Processing is enabled
  Music On Hold Threshold is Set to -38 dBm
  In Gain is Set to 0 dB
  Out Attenuation is Set to 0 dB
  Echo Cancellation is enabled
  Echo 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
  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
  Ringing Time Out is set to 180 s
  Busyout on interface monitor
    Ethernet0/0
  Companding Type is u-law
  Region Tone is set for US
  Wait Release Time Out is 30 s
  Station name None, Station number None
TE Basic Rate Interface 1/0/1 Slot is 1, Sub-unit is 0, Port is 1
  Type of VoicePort is ISDN-BRI
  Operation State is DORMANT
  Administrative State is UP
  No Interface Down Failure
  Description is not set
  Noise Regeneration is enabled
  Non Linear Processing is enabled
  Music On Hold Threshold is Set to -38 dBm
  In Gain is Set to 0 dB
  Out Attenuation is Set to 0 dB
  Echo Cancellation is enabled
  Echo 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
  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
  Ringing Time Out is set to 180 s
  Companding Type is u-law
  Region Tone is set for US
  Wait Release Time Out is 30 s
  Station name None, Station number None
```

Cisco 3660

```

Router# show voice port
Foreign Exchange Station 2/0/0 Slot is 2, Sub-unit is 0, Port is 0
Type of VoicePort is FXS
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

```

Cisco VG200

```

Router# show voice port

DS0 Group 1/0:15 - 1/0:15
Type of VoicePort is XCC
Operation State is DORMANT
Administrative State is UP
No Interface Down Failure
Description is not set
Noise Regeneration is enabled
Non Linear Processing is enabled
Non Linear Mute is disabled
Non Linear Threshold is -21 dB
Music On Hold Threshold is Set to -38 dBm
In Gain is Set to 0 dB
Out Attenuation is Set to 0 dB
Echo Cancellation is enabled
Echo Cancellation NLP mute is disabled
Echo Cancellation NLP threshold is -21 dB
Echo Cancel Coverage is set to 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 A-law
Rx A bit no conditioning set
Rx B bit no conditioning set
Rx C bit no conditioning set
Rx D bit no conditioning set
Tx A bit no conditioning set
Tx B bit no conditioning set
Tx C bit no conditioning set
Tx D bit no conditioning set
Region Tone is set for US
Continuity Test Tone CO1 is set to 2010
Continuity Test Tone CO2 is set to 1780
Station name None, Station number None
Translation profile (Incoming):
Translation profile (Outgoing):
```

Configuring Customizable Tone Download to Cisco IOS MGCP Gateways

Perform this task to download custom tones to the Cisco IOS gateway.

Prerequisites

- Cisco Unified Communications Manager 3.3(2) (formerly known as Cisco CallManager 3.3(2)) or higher.
- Cisco Unified Communications Manager 4.0 (formerly known as Cisco CallManager 4.0) or higher
- DSP 3.6.16 or later for analog interfaces; DSP 4.0 or later for digital interfaces.
- For languages other than English and countries other than the United States, locale files that provide regional tones and cadences must be installed in Cisco Unified Communications Manager. The locale installer adds the files to the correct directories and updates the Cisco Unified Communications Manager database.

See the [Using the Cisco IP Telephony Locale Installer](#) document for information.

- The following cards are supported:
 - AIM-ATM-VOICE
 - AIM-VOICE
 - NM-HDA
 - NM-HDV
 - VIC-2FXO
 - VIC-2FXS

Restrictions

Up to two custom tone tables are supported on a gateway; that is, no more than two custom tone tables can be downloaded to one gateway even if there are more than two countries or regions configured for the gateway.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ccm-manager config {server ip-address | name}**
4. **ccm-manager config**
5. **ccm-manager download-tones**
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code> Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password when prompted.
Step 2	<code>configure terminal</code> Example: Router# configure terminal	Enters global configuration mode.
Step 3	<code>ccm-manager config {server ip-address name}</code> Example: Router(config)# ccm-manager config server 10.10.10.0	Specifies the TFTP server that contains the XML configuration file to download. Note Up to three servers can be configured.
Step 4	<code>ccm-manager config</code> Example: Router(config)# ccm-manager config	Enables single-point download and configuration.
Step 5	<code>ccm-manager download-tones</code> Example: Router(config)# ccm-manager download-tones	Enables the custom tone download to the gateway.
Step 6	<code>exit</code> Example: Router(config)# exit	Exits the session.

Verifying Customizable Tone Download

Perform this task to verify that the customizable tone download and voice ports are configured correctly.

SUMMARY STEPS

1. **show voice port port/slot**

2. **show ccm-manager download-tones**
3. **debug ccm-manager config-download all**
4. **debug ccm-manager config-download tone**

DETAILED STEPS

Step 1 **show voice port *port/slot***

Use the **show voice port** command to verify that the custom tones are assigned. The following sample shows that voice port 1/0/1 has C1 assigned, which corresponds to France:

```
Router# show voice port
!
recEive and transMit Slot is 1, Sub-unit is 0, Port is 1
  Type of VoicePort is E&M
  Operation State is DORMANT
  Administrative State is UP
  No Interface Down Failure
  Description is not set
  Noise Regeneration is enabled
  Non Linear Processing is enabled
  Non Linear Mute is disabled
  Non Linear Threshold is -21 dB
  Music On Hold Threshold is Set to -38 dBm
  In Gain is Set to 0 dB
  Out Attenuation is Set to 0 dB
  Echo Cancellation is enabled
  Echo Cancellation NLP mute is disabled
  Echo Cancellation NLP threshold is -21 dB
  Echo Cancel Coverage is set to 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
.
.
.
Rx Seize ABCD bits = 1111 Default pattern
Rx Idle ABCD bits = 0000 Default pattern
Tx Seize ABCD bits = 1111 Default pattern
Tx Idle ABCD bits = 0000 Default pattern
Ignored Rx ABCD bits = BCD
Region Tone is set for C1
!
! Custom Tone 1 is assigned to this voice port.
```



Note Voice ports are automatically configured during the initial download of the XML file from the TFTP server.

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

Use the **show ccm-manager download-tones** command to verify that the custom tones have been downloaded. The following sample output shows that Custom Tone 1 is assigned to France and that Custom Tone 2 is assigned to Spain:

```
Router# show ccm-manager download-tones
```


Use the **debug ccm-manager config-download tone** command to troubleshoot the download procedure. The following sample output shows the locale name as United Kingdom and lists all of the dual-tone parameters for that region:

```
Router# debug ccm-manager config-download tone

00:09:07:
cmapp_prefix_process_tag_tones:
00:09:07: cmapp_process_tag_trkLocaleName: region = United Kingdom
00:09:07: cmapp_process_tag_pulse_ratio: pulse ratio = 40
00:09:07: cmapp_process_tag_dtmf_llevel: low frequency level = 65438
00:09:07: cmapp_process_tag_dtmf_hlevel: high frequency level = 65463
00:09:07: cmapp_process_tag_special_oper: operation = uLaw
00:09:07: cmapp_prefix_process_tag_lpig:
00:09:07: cmapp_process_tag_fxs: ignore LPIG for fxs
00:09:07: cmapp_process_tag_fxo: ignore LPIG for fxo
00:09:07: cmapp_process_tag_digital: ignore LPIG for digital
00:09:07: cmapp_prefix_process_tag_lpog:
00:09:07: cmapp_process_tag_fxs: ignore LPOG for fxsBoth ports are in service
00:09:07: cmapp_process_tag_fxo: ignore LPOG for fxo
00:09:07: cmapp_process_tag_digital: ignore LPOG for digital
00:09:07: cmapp_prefix_process_tag_tonetable_info:
00:09:07:
cmapp_prefix_process_tag_dualtone: TID=[0:CPTONE_BUSY]
00:09:07: cmapp_process_tag_nf: number of frequencies = 1
00:09:07: cmapp_process_tag_dr: direction = 0
00:09:07: cmapp_process_tag_fof: frequency 1 = 400
00:09:07: cmapp_process_tag_fos: frequency 2 = 0
00:09:07: cmapp_process_tag_fot: frequency 3 = 0
00:09:07: cmapp_process_tag_fo4: frequency 4 = 0
00:09:07: cmapp_prefix_process_tag_aof_level:
00:09:07: cmapp_process_tag_fxs: amplitude of 1st = -200
00:09:07: cmapp_process_tag_fxo: amplitude of 1st = -200
00:09:07: cmapp_process_tag_digital: amplitude of 1st = -240
00:09:07: cmapp_prefix_process_tag_aos_level:
00:09:07: cmapp_process_tag_fxs: amplitude of 2nd = 0
00:09:07: cmapp_process_tag_fxo: amplitude of 2nd = 0
00:09:07: cmapp_process_tag_digital: amplitude of 2nd = 0
00:09:07: cmapp_prefix_process_tag_aot_level:
00:09:07: cmapp_process_tag_fxs: amplitude of 3rd = 0
00:09:07: cmapp_process_tag_fxo: amplitude of 3rd = 0
00:09:07: cmapp_process_tag_digital: amplitude of 3rd = 0
00:09:07: cmapp_prefix_process_tag_ao4_level:
00:09:07: cmapp_process_tag_fxs: amplitude of 4th = 0
00:09:07: cmapp_process_tag_fxo: amplitude of 4th = 0
00:09:07: cmapp_process_tag_digital: amplitude of 4th = 0
00:09:07: cmapp_process_tag_ontf: frequency 1 on time = 375
00:09:07: cmapp_process_tag_oftf: frequency 1 off time = 375
00:09:07: cmapp_process_tag_onts: frequency 2 on time = 0
00:09:07: cmapp_process_tag_ofts: frequency 2 off time = 0
00:09:07: cmapp_process_tag_ontt: frequency 3 on time = 0
00:09:07: cmapp_process_tag_oftt: frequency 3 off time = 0
00:09:07: cmapp_process_tag_ont4: frequency 4 on time = 0
00:09:07: cmapp_process_tag_of4: frequency 4 off time = 0
00:09:07: cmapp_process_tag_fof2: frequency 1 cadence 2 = 0
00:09:07: cmapp_process_tag_fos2: frequency 2 cadence 2 = 0
00:09:07: cmapp_process_tag_fof3: frequency 1 cadence 3 = 0
00:09:07: cmapp_process_tag_fos3: frequency 2 cadence 3 = 0
00:09:07: cmapp_process_tag_fof4: frequency 1 cadence 4 = 0
00:09:07: cmapp_process_tag_fos4: frequency 2 cadence 4 = 0
00:09:07: cmapp_process_tag_rct1: cadence 1 repeat count = 0
00:09:07: cmapp_process_tag_rct2: cadence 2 repeat count = 0
00:09:07: cmapp_process_tag_rct3: cadence 3 repeat count = 0
00:09:07: cmapp_process_tag_rct4: cadence 4 repeat count = 0
```

```

00:09:07:
cmapp_prefix_process_tag_dualtone: TID=[1:CPTONE_RING_BACK]
00:09:07: cmapp_process_tag_nf: number of frequencies = 2
00:09:07: cmapp_process_tag_dr: direction = 0
00:09:07: cmapp_process_tag_fof: frequency 1 = 400
00:09:07: cmapp_process_tag_fos: frequency 2 = 450
00:09:07: cmapp_process_tag_fot: frequency 3 = 0
00:09:07: cmapp_process_tag_fo4: frequency 4 = 0
00:09:07: cmapp_prefix_process_tag_aof_level:
00:09:07: cmapp_process_tag_fxs: amplitude of 1st = -190
00:09:07: cmapp_process_tag_fxo: amplitude of 1st = -190
00:09:07: cmapp_process_tag_digital: amplitude of 1st = -190
00:09:07: cmapp_prefix_process_tag_aos_level:
00:09:07: cmapp_process_tag_fxs: amplitude of 2nd = -190
00:09:07: cmapp_process_tag_fxo: amplitude of 2nd = -190
00:09:07: cmapp_process_tag_digital: amplitude of 2nd = -190
00:09:07: cmapp_prefix_process_tag_aot_level:
00:09:07: cmapp_process_tag_fxs: amplitude of 3rd = 0
00:09:07: cmapp_process_tag_fxo: amplitude of 3rd = 0
00:09:07: cmapp_process_tag_digital: amplitude of 3rd = 0
00:09:07: cmapp_prefix_process_tag_ao4_level:
00:09:07: cmapp_process_tag_fxs: amplitude of 4th = 0
00:09:07: cmapp_process_tag_fxo: amplitude of 4th = 0
00:09:07: cmapp_process_tag_digital: amplitude of 4th = 0
00:09:07: cmapp_process_tag_ontf: frequency 1 on time = 400
00:09:07: cmapp_process_tag_oftf: frequency 1 off time = 200
00:09:07: cmapp_process_tag_onts: frequency 2 on time = 400
00:09:07: cmapp_process_tag_ofts: frequency 2 off time = 2000
00:09:07: cmapp_process_tag_ontt: frequency 3 on time = 0
00:09:07: cmapp_process_tag_oftt: frequency 3 off time = 0
00:09:07: cmapp_process_tag_ont4: frequency 4 on time = 0
00:09:07: cmapp_process_tag_of4: frequency 4 off time = 0
00:09:07: cmapp_process_tag_fof2: frequency 1 cadence 2 = 0
00:09:07: cmapp_process_tag_fos2: frequency 2 cadence 2 = 0
00:09:07: cmapp_process_tag_fof3: frequency 1 cadence 3 = 0
00:09:07: cmapp_process_tag_fos3: frequency 2 cadence 3 = 0
00:09:07: cmapp_process_tag_fof4: frequency 1 cadence 4 = 0
00:09:07: cmapp_process_tag_fos4: frequency 2 cadence 4 = 0
00:09:07: cmapp_process_tag_rct1: cadence 1 repeat count = 0
00:09:07: cmapp_process_tag_rct2: cadence 2 repeat count = 0
00:09:07: cmapp_process_tag_rct3: cadence 3 repeat count = 0
00:09:07: cmapp_process_tag_rct4: cadence 4 repeat count = 0
00:09:07:
cmapp_prefix_process_tag_dualtone: TID=[2:CPTONE_CONGESTION]
00:09:07: cmapp_process_tag_nf: number of frequencies = 1
00:09:07: cmapp_process_tag_dr: direction = 0
00:09:07: cmapp_process_tag_fof: frequency 1 = 400
00:09:07: cmapp_process_tag_fos: frequency 2 = 0
00:09:07: cmapp_process_tag_fot: frequency 3 = 0
00:09:07: cmapp_process_tag_fo4: frequency 4 = 0
00:09:07: cmapp_prefix_process_tag_aof_level:
00:09:07: cmapp_process_tag_fxs: amplitude of 1st = -200
00:09:07: cmapp_process_tag_fxo: amplitude of 1st = -200
00:09:07: cmapp_process_tag_digital: amplitude of 1st = -200
00:09:07: cmapp_prefix_process_tag_aos_level:
00:09:07: cmapp_process_tag_fxs: amplitude of 2nd = 0
00:09:07: cmapp_process_tag_fxo: amplitude of 2nd = 0
00:09:07: cmapp_process_tag_digital: amplitude of 2nd = 0
00:09:07: cmapp_prefix_process_tag_aot_level:
00:09:07: cmapp_process_tag_fxs: amplitude of 3rd = 0
00:09:07: cmapp_process_tag_fxo: amplitude of 3rd = 0
00:09:07: cmapp_process_tag_digital: amplitude of 3rd = 0
00:09:07: cmapp_prefix_process_tag_ao4_level:
00:09:07: cmapp_process_tag_fxs: amplitude of 4th = 0

```

```

00:09:07: cmapp_process_tag_fxo: amplitude of 4th = 0
00:09:07: cmapp_process_tag_digital: amplitude of 4th = 0
00:09:07: cmapp_process_tag_ontf: frequency 1 on time = 400
00:09:07: cmapp_process_tag_oftf: frequency 1 off time = 350
00:09:07: cmapp_process_tag_onts: frequency 2 on time = 225
00:09:07: cmapp_process_tag_ofts: frequency 2 off time = 525
00:09:07: cmapp_process_tag_ontt: frequency 3 on time = 0
00:09:07: cmapp_process_tag_oftt: frequency 3 off time = 0
00:09:07: cmapp_process_tag_ont4: frequency 4 on time = 0
00:09:07: cmapp_process_tag_of4: frequency 4 off time = 0
00:09:07: cmapp_process_tag_fof2: frequency 1 cadence 2 = 0
00:09:07: cmapp_process_tag_fos2: frequency 2 cadence 2 = 0
00:09:07: cmapp_process_tag_fof3: frequency 1 cadence 3 = 0
00:09:07: cmapp_process_tag_fos3: frequency 2 cadence 3 = 0
00:09:07: cmapp_process_tag_fof4: frequency 1 cadence 4 = 0
00:09:07: cmapp_process_tag_fos4: frequency 2 cadence 4 = 0
00:09:07: cmapp_process_tag_rctl: cadence 1 repeat count = 0
00:09:07: cmapp_process_tag_rct2: cadence 2 repeat count = 0
00:09:07: cmapp_process_tag_rct3: cadence 3 repeat count = 0
00:09:07: cmapp_process_tag_rct4: cadence 4 repeat count = 0

```

The following sample output shows the network locales in the XML file:

```

Router# debug ccm-manager config-download tone
!
00:54:08: cmapp_xml_tftp_download_file line 170
File (tftp://10.10.10.55/Hong_Kong/gateway-tones.xml) read 20993 bytes
00:54:08: cmapp_prefix_process_tag_tones
00:54:08: cmapp_process_tag_trkLocaleName: region = Hong Kong
!
00:54:08: cmapp_xml_tftp_download_file line 170
File (tftp://10.10.10.55/United_Kingdom/gateway-tones.xml) read 20993 bytes
00:54:08: cmapp_prefix_process_tag_tones
00:54:08: cmapp_process_tag_trkLocaleName: region = United Kingdom

```



Note

For a description of the significant fields displayed in these output examples, see the [Cisco IOS Voice Command Reference](#) and [Cisco IOS Debug Command Reference](#), Release 12.3T.

Troubleshooting Tips for Customizable Tone Download

If the custom tone file is not downloaded at least once, the North America tones are used. When a download fails, the static tones associated with the network locale of the voice port are used. For example, if a voice port is defined with a static tone for Hong Kong, and the download fails, the static tone for Hong Kong is used.

The administrator, after correcting the problem (a glitch in the network, a TFTP server that is down, or missing XML tone files), must reset the gateway from Cisco Unified Communications Manager. Resetting the gateway triggers a download of the XML configuration file.

If tone download is successful, the downloaded tone file overwrites the default custom tone table, and the voice port refers to the downloaded custom tones.

Configuration Examples for Tone Download to MGCP Gateways

This section contains the following examples:

- [Customizable Tone Download Voice-Port Configuration: Example, page 16](#)
- [Customizable Tone Download Using Single-Point Configuration: Example, page 16](#)

Customizable Tone Download Voice-Port Configuration: Example

The following sample output shows that voice port 1/0/0 has been configured to use C1:

```
Router# show voice port 1/0/0
!
Foreign Exchange Station 1/0/0 Slot is 1, Sub-unit is 0, Port is 0
Type of VoicePort is FXS
Operation State is DORMANT
Administrative State is UP
Companding Type is u-law
Region Tone is set for C1
```

Customizable Tone Download Using Single-Point Configuration: Example

The following example shows single-point configuration enabled for an MGCP gateway:

```
Router# show running-config
!
version 12.3
no parser cache
no service single-slot-reload-enable
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
logging rate-limit console 10 except errors
!
memory-size iomem 10
voice-card 1
!
ip subnet-zero
!
ip domain-name anything.com
!
no ip dhcp-client network-discovery
mgcp
mgcp call-agent 10.10.1.10 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
isdn switch-type primary-ni
call rsvp-sync
!
! The following output shows that the TFTP server has an IP address of 10.10.10.50 and
that the download has been enabled.
!
```

```
ccm-manager config server 10.10.10.50
ccm-manager config
ccm-manager download-tones
!
```

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.

Additional References

- [“Cisco Unified Communications Manager and Cisco IOS Interoperability Features Roadmap”](#) on page 9—Describes how to access Cisco Feature Navigator; also lists and describes, by Cisco IOS release, Cisco Unified Communications Manager and Cisco IOS interoperability features.
- [“Overview of Cisco Unified Communications Manager and Cisco IOS Interoperability”](#) on page 13—Describes basics of underlying technology and lists related documents.
- [“Enabling Single-Point Configuration for MGCP Gateways”](#) section on page 45 in [Configuring MGCP Gateway Support for Cisco Unified Communications Manager](#)—Describes how to configure MGCP gateways by downloading XML configuration files.
- [Using the Cisco IP Telephony Locale Installer](#)—Describes how to install the Cisco IP Telephony Locale Installer for Cisco Unified Communications Manager.

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0709R)

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

© 2007 Cisco Systems, Inc. All rights reserved.



Configuring MCID for Cisco IOS Voice Gateways

The MCID for Cisco IOS Voice Gateways feature supports the Malicious Call Identification (MCID) supplementary service that enables Cisco Unified Communications Manager to identify the source of malicious calls.

Feature History for MCID for Cisco IOS Voice Gateways

Release	Modification
12.3(8)XY	This feature was introduced.
12.3(11)T	This feature was integrated into Cisco IOS Release 12.3(11)T.
12.3(14)T	Support was added for the new Cisco IOS command structure for voice applications in the HTTP Client API for TCL IVR feature.

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.



Note

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.



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Contents

- “Prerequisites for MCID for Cisco IOS Voice Gateways” on page 2
- “Restrictions for MCID for Cisco IOS Voice Gateways” on page 2
- “Information About MCID for Cisco IOS Voice Gateways” on page 3
- “How to Configure MCID for Cisco IOS Voice Gateways” on page 4
- “Configuration Examples for MCID for Cisco IOS Voice Gateways” on page 9
- “Where to Go Next” on page 13
- “Additional References” on page 13

Prerequisites for MCID for Cisco IOS Voice Gateways

- MCID must be configured in Cisco Unified Communications Manager 4.0 (formerly known as Cisco CallManager 4.0) or later. For information, see the “[Malicious Call Identification](#)” chapter in the *Cisco Unified CallManager Features and Services Guide*, Release 4.0(1).
- Your platform must support MCID and TCL IVR 2.0.
- You must either use the script `app_mcid.2.0.0.40.tcl` or a later version, or write your own TCL IVR 2.0 script that implements MCID. To download the script, go to the Software Download site at <http://www.cisco.com/cgi-bin/tablebuild.pl/tclware>. To write your own script, see the *TCL IVR API Version 2.0 Programming Guide*.
- If you require an MCID service log in RADIUS, you can write a script that supports the RADIUS service and uses the **aaa accounting update** command to generate an accounting record.
- Cisco Catalyst 6500 series and Cisco 7600 series Communication Media Module (CMM) requires WS-SVC-CMM-6T1, WS-SVC-CMM-6E1, or WS-SVC-CMM-24 FXS port adapter in H.323 environment.

Restrictions for MCID for Cisco IOS Voice Gateways

- Supported only for NET5 switches that have MCID functionality enabled. Other switch types are not supported.
- Supported only for incoming calls from the ISDN network.
- MCID requests from the central office are ignored by Cisco Unified Communications Manager and are not supported by the Cisco voice gateway.
- Service provider on the time-division multiplexing (TDM) side of the PSTN must have MCID functionality enabled.
- ISDN interface on the voice gateway must have the ISDN switch type set to `primary-net5` with the **isdn switch-type** command and operate in user-side mode (default).
- Voice gateways with PRI interfaces should provide the following capabilities:
 - Receive MCID requests relating to the call from upper layers and relay them to the connected network using the PRI protocol specified for the MCID service.

- Receive MCID related response signals and information from the connected network using the PRI protocol specified for the MCID service. Cisco Unified Communications Manager ignores the signals and information.
- Not supported on the Access Gateway Module (AGM).

Information About MCID for Cisco IOS Voice Gateways

To configure a voice gateway for MCID, you should understand the following concept:

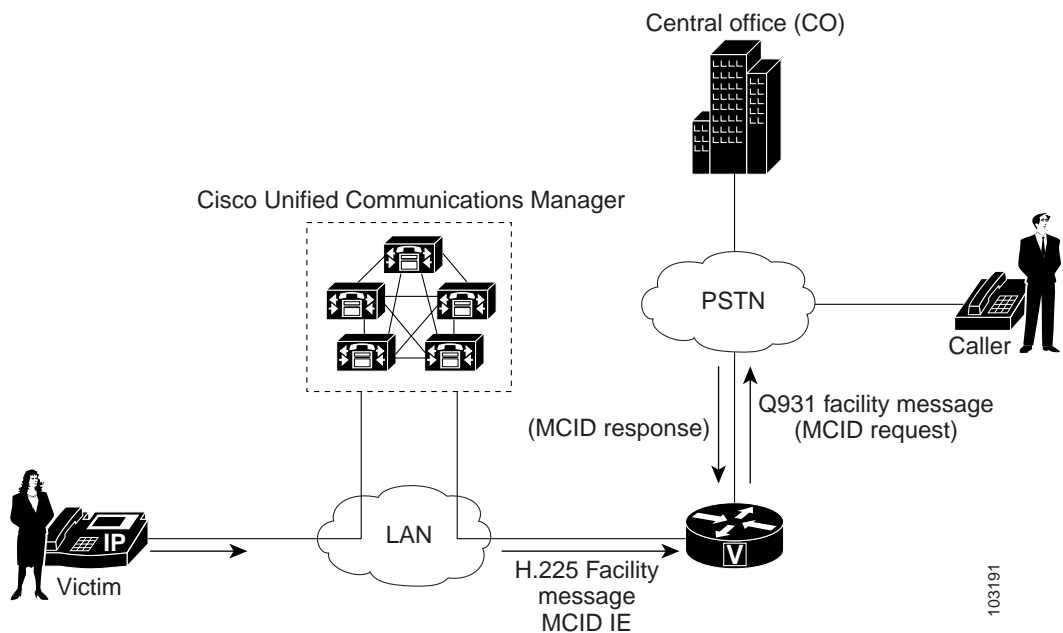
- [MCID, page 3](#)

MCID

Malicious Call Identification (MCID) is a supplementary service that enables Cisco Unified Communications Manager to identify the source of malicious calls. A user who receives a malicious call from another network, typically the PSTN, can select a softkey on the IP phone which immediately notifies the system administrator, flags the call detail record (CDR) for the Cisco Unified Communications Manager cluster, and notifies the PSTN of the malicious nature of the call, allowing the offnet system to take action, such as notifying legal authorities.

[Figure 12](#) shows an example of the MCID call flow. After receiving an MCID request from an endpoint device (victim), Cisco Unified Communications Manager sends an H.225 Facility message with the MCID information element (IE) to the voice gateway. The gateway sends a Q.931 Facility message with the MCID IE to the ISDN network (central office).

Figure 12 MCID Functionality



A called party invokes MCID by pressing the appropriate softkey on the IP phone. A configurable timer is available when awaiting a response after sending a Facility message to the PSTN. If a response is not received within the specified time, the TCL IVR script is notified. Depending on how the script is written, it could try to reinvoke MCID or perform some other action, for example, playing a message to the user that the MCID attempt did not work.

How to Configure MCID for Cisco IOS Voice Gateways

Perform these tasks to support MCID on your MGCP gateway:

- [Enabling the ISDN Interface to Send MCID Requests, page 4](#) (required)
- [Configuring MCID on the Voice Gateway \(Cisco IOS Release 12.3\(14\)T\), page 5](#) (required)
- [Configuring MCID on the Voice Gateway \(Cisco IOS Release 12.3\(11\)T\), page 7](#) (required)

Enabling the ISDN Interface to Send MCID Requests

Perform this task to enable an ISDN interface to send MCID requests and to set the timer.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface serial *slot/port:timeslot***
4. **isdn switch-type {primary-net5 | primary-ni2}**
5. **isdn incoming-voice {data | modem | voice}**
6. **isdn supp-service mcid**
7. **isdn t-activate *msec***
8. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code> Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password when prompted.
Step 2	<code>configure terminal</code> Example: Router# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	<code>interface serial slot/port:timeslot</code> Example: Router(config)# interface serial 2/1:23	Enters interface configuration mode and specifies a serial interface created on a channelized E1 or channelized T1 controller.
Step 4	<code>isdn switch type {primary-net5 primary-ni}</code> Example: Router(config-if)# isdn switch-type primary-net5	Specifies the user-side switch type. Note Only NET5 switches are supported.
Step 5	<code>isdn incoming-voice {data modem voice}</code> Example: Router(config-if)# isdn incoming-voice voice	Specifies whether incoming voice calls are handled as data, voice, or modems.
Step 6	<code>isdn supp-service mcid</code> Example: Router(config-if)# isdn supp-service mcid	Configures the ISDN interface to send the MCID invocation and response on the specified serial interface.
Step 7	<code>isdn t-activate msec</code> Example: Router(config-if)# isdn t-activate 4000	(Optional) Specifies how long to wait for a response from the PSTN after sending the MCID request. When the timer expires, the TCL IVR script receives an expiration event and depending on your script, it could trigger an announcement or initiate another attempt. Note The timer starts when there is a disconnect message, and both calls legs are reclaimed after the timer expires.
Step 8	<code>end</code> Example: Router(config-if)# end	Exits to privileged EXEC mode.

Configuring MCID on the Voice Gateway (Cisco IOS Release 12.3(14)T)

Use this procedure to define the MCID application on a voice gateway that is running Cisco IOS Release 12.3(14)T or later. To verify your release, use the **show version** command.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `application`
4. `service mcid location`
5. `param mcid-release-timer seconds`
6. `param retry-count number`

7. **exit**
8. **dial-peer voice tag pots**
9. **service mcid**
10. **incoming called-number string**
11. **direct-inward-dial**
12. **port**
13. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password when prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	application Example: Router(config)# application	Enters application configuration mode.
Step 4	service mcid flash:app_mcid.2.0.0.40.tcl Example: Router(config-app)# service mcid flash:app_mcid.2.0.0.40.tcl	Specifies the name and location of the MCID script.
Step 5	param mcid-release-timer seconds Example: Router(config-app-param)# param mcid-release-timer 30	(Optional) Number of seconds the script waits before releasing both call legs after it receives a disconnect message. Default is 60 seconds.
Step 6	param retry-count number Example: Router(config-app-param)# param retry-count 3	(Optional) Maximum number of times the called party can trigger MCID if all previous attempts failed. Default is 0, which means the user can invoke MCID as many times as needed.
Step 7	exit Example: Router(config-app-param)# exit	Exits to global configuration mode.

	Command or Action	Purpose
Step 8	<code>dial-peer voice tag pots</code> Example: Router(config)# dial-peer voice 250 pots	Configures incoming dial peer and enters dial-peer configuration mode.
Step 9	<code>service mcid</code> Example: Router(config-dial-peer)# service mcid	Configures the incoming dial peer to use the MCID application.
Step 10	<code>incoming called-number string</code> Example: Router(config-dial-peer)# incoming called-number 222....	Configures the incoming called number for the MCID application.
Step 11	<code>direct-inward-dial</code> Example: Router(config-dial-peer)# direct-inward-dial	Configures direct-inward-dial (DID) for the MCID application.
Step 12	<code>port slot/port:timeslot</code> Example: Router(config-dial-peer)# port 3/0:23	Configures the port for the MCID application. Note The syntax of the <code>port</code> command is platform-specific. For information on the specific syntax for your platform, see the Cisco IOS Voice Command Reference .
Step 13	<code>exit</code> Example: Router(config-dial-peer)# exit	Exits to global configuration mode.

Configuring MCID on the Voice Gateway (Cisco IOS Release 12.3(11)T)

Use this procedure to define the MCID application on a voice gateway that is running Cisco IOS Release 12.3(11)T. To verify your release, use the `show version` command.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `call application voice mcid location`
4. `call application voice mcid mcid-release-timer seconds`
5. `dial-peer voice tag pots`
6. `application mcid`
7. `incoming called-number string`
8. `direct-inward-dial`
9. `port`

10. exit

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code> Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password when prompted.
Step 2	<code>configure terminal</code> Example: Router# configure terminal	Enters global configuration mode.
Step 3	<code>call application voice mcid location</code> Example: Router(config)# call application voice mcid flash:app_mcid.2.0.0.40.tcl	Specifies the name and location of the MCID script.
Step 4	<code>call application voice mcid mcid-release-timer seconds</code> Example: Router(config)# call application voice mcid mcid-release-timer 30	(Optional) Number of seconds the script waits to release both call legs after it receives a disconnect message. Default is 60 seconds.
Step 5	<code>dial-peer voice tag pots</code> Example: Router(config)# dial-peer voice 250 pots	Configures incoming dial peer and enters dial-peer configuration mode.
Step 6	<code>application mcid</code> Example: Router(config-dial-peer)# application mcid	Configures the incoming dial peer to use the MCID application.
Step 7	<code>incoming called-number string</code> Example: Router(config-dial-peer)# incoming called-number 222....	Configures the incoming called number for the MCID application.
Step 8	<code>direct-inward-dial</code> Example: Router(config-dial-peer)# direct-inward-dial	Configures direct-inward-dial (DID) for the MCID application.

	Command or Action	Purpose
Step 9	<pre>port slot/port:timeslot</pre> <p>Example: Router(config-dial-peer)# port 3/0:23</p>	<p>Configures the port for the MCID application.</p> <p>Note The syntax of the port command is platform-specific. For information on the specific syntax for your platform, see the Cisco IOS Voice Command Reference.</p>
Step 10	<pre>exit</pre> <p>Example: Router(config-dial-peer)# exit</p>	<p>Exits to global configuration mode.</p>

Configuration Examples for MCID for Cisco IOS Voice Gateways

This section provides the following configuration examples:

- [Configuring MCID in Cisco IOS Release 12.3\(14\)T \(Cisco 2801\): Example, page 9](#)
- [Configuring MCID in Cisco IOS Release 12.3\(11\)T \(Cisco 3745\): Example, page 119](#)

Configuring MCID in Cisco IOS Release 12.3(14)T (Cisco 2801): Example

```
Current configuration : 1695 bytes
!
version 12.3
no service timestamps debug uptime
no service timestamps log uptime
no service password-encryption
!
hostname router_2801
!
boot-start-marker
boot-end-marker
!
logging buffered 40960 debugging
no logging console
!
no aaa new-model
!
resource manager
!
network-clock-participate wic 2
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
ip cef
!
!
no ip dhcp use vrf connected
!
!
no ip domain lookup
no ftp-server write-enable
isdn switch-type primary-net5
```

```

!
voice-card 0
!
!
!
application
  service mcid flash:app_mcid.2.0.0.40.tcl
  param mcid-release-timer 10
  param retry-count 3
!
!
controller T1 0/2/0
  framing esf
  clock source internal
  linecode b8zs
  pri-group timeslots 1-24
!
controller T1 0/2/1
  framing esf
  linecode b8zs
!
!
interface FastEthernet0/0
  ip address 9.1.0.102 255.255.0.0
  duplex auto
  speed auto
  no keepalive
!
interface FastEthernet0/1
  no ip address
  shutdown
  duplex auto
  speed auto
!
interface Serial0/2/0:23
  no ip address
  isdn switch-type primary-net5
  isdn incoming-voice voice
  isdn supp-service mcid
  isdn T-Activate 5000
  no cdp enable
!
ip classless
!
ip http server
!
disable-eadi
!
!
control-plane
!
!
voice-port 0/2/0:23
!
ccm-manager music-on-hold
!
!
dial-peer voice 500 pots
  service mcid
  destination-pattern 111111....
  incoming called-number 555555....
  direct-inward-dial
  port 0/2/0:23
  prefix 111111

```

```

!
dial-peer voice 600 voip
 destination-pattern 555555....
 session target ipv4:9.1.1.0.2
 incoming called-number 111111....
 playout-delay minimum low
 codec g711ulaw
 no vad
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
end

```

Configuring MCID in Cisco IOS Release 12.3(11)T (Cisco 3745): Example

```

Current configuration : 1492 bytes
!
version 12.3
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname router_3745
!
!
voice-card 3
 dspfarm
!
no aaa new-model
ip subnet-zero
!
!
ip domain name cisco.com
mpls ldp logging neighbor-changes
no ftp-server write-enable
isdn switch-type primary-4ess
no scripting tcl init
no scripting tcl encdir
!
!
no voice hpi capture buffer
no voice hpi capture destination
!
!
controller T1 3/0
 framing esf
 linecode b8zs
 pri-group timeslots 1-24
!
controller T1 3/1
 framing sf
 linecode ami
!
!
interface FastEthernet0/0
 ip address 10.4.175.116 255.255.0.0
 duplex auto

```

```
speed auto
!
interface FastEthernet0/1
 shutdown
 duplex auto
 speed auto
!
interface Serial3/0:23
 no logging event link-status
 isdn switch-type primary-net5
 isdn incoming-voice voice
 isdn supp-service mcid
 no cdp enable
!
ip default-gateway 10.4.0.1
ip classless
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
!
ip http server
!
!
control-plane
!
!
call application voice mcid flash:app_mcid.2.0.0.40.tcl
call application voice mcid mcid-release-timer 10
!
voice-port 3/0:23
!
mgcp call-agent 10.4.175.2 service-type mgcp version 0.1
!
mgcp profile default
!
!
dial-peer voice 1 pots
 application mcid
 destination-pattern 2010
 incoming called-number 2000
 direct-inward-dial
 port 3/0:23
 forward-digits all
!
dial-peer voice 2 voip
 destination-pattern 2000
 session target ipv4:10.4.175.2
!
!
line con 0
line aux 0
line vty 0 4
 login
!
end
```

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.

Additional References

- [“Cisco Unified Communications Manager and Cisco IOS Interoperability Features Roadmap”](#) on page 9—Describes how to access Cisco Feature Navigator; also lists and describes, by Cisco IOS release, Cisco Unified Communications Manager and Cisco IOS interoperability features.
- [“Malicious Call Identification”](#) chapter in the *Cisco Unified Communications Manager Features and Services Guide*—Describes how to configure MCID in Cisco Unified Communications Manager 4.0 (formerly known as Cisco CallManager 4.0).

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0711R)

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

© 2007 Cisco Systems, Inc. All rights reserved.



Configuring RSVP Agent

The RSVP Agent feature implements a Resource Reservation Protocol (RSVP) agent on Cisco IOS voice gateways that support Cisco Unified Communications Manager Version 5.0.1. The RSVP agent enables Cisco Unified Communications Manager to provide resource reservation for voice and video media to ensure QoS and call admission control (CAC). Cisco Unified Communications Manager controls the RSVP agent through Skinny Client Control Protocol (SCCP). This signaling is independent of the signaling protocol used for the call so SCCP, SIP, H.323, and MGCP calls can all use the RSVP agent.

Benefits of this feature include the following:

- Improves flexibility and scalability of bandwidth management in a meshed network by decentralizing call admission control
- Provides method of managing unpredictable bandwidth requirements of video media
- Enables RSVP across WAN for Cisco IP phones and other devices that do not support RSVP

Feature History for RSVP Agent

Release	Modification
12.4(6)T	This feature was introduced.

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.

Contents

- [Prerequisites for RSVP Agent, page 2](#)
- [Restrictions for RSVP Agent, page 2](#)
- [Information About RSVP Agent, page 2](#)
- [How to Enable the RSVP Agent on the Voice Gateway, page 4](#)
- [Configuration Examples for RSVP Agent, page 10](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

- [Additional References, page 13](#)

Prerequisites for RSVP Agent

Cisco IOS Voice Gateway

- Cisco IOS Release 12.4(4)T or a later release.
- Transcoder and MTP services must be configured on the voice gateway. See “[Configuring Enhanced Conferencing and Transcoding for Voice Gateway Routers](#)” on page 67.
- SCCP must be enabled on the local interface that the voice gateway uses to register with Cisco Unified Communications Manager. See the “[Enabling SCCP on the Cisco Unified Communications Manager Interface](#)” section on page 81.
- The **ip rsvp bandwidth** command must be enabled on all interfaces.
- The **ip rsvp policy preempt** command must be enabled.
- The **ccm** command must use the keyword **version 5.0.1**.

Cisco Unified Communications Manager

- Cisco Unified Communications Manager 5.0.1 or a later release.
- Transcoder and MTP services must be configured in Cisco Unified Communications Manager. See the following chapters in the *Cisco Unified Communications Manager Administration Guide*:
 - “[Media Termination Point Configuration](#)”
 - “[Transcoder Configuration](#)”
- RSVP policy level must be configured in Cisco Unified Communications Manager. See the “[Service Parameters Configuration](#)” chapter in the *Cisco Unified Communications Manager Administration Guide*.

Restrictions for RSVP Agent

- RSVP agent is not supported by conference devices.
- RSVP agent is not supported by a hardware MTP or transcoder device using the NM-HDV.
- RSVP agent is supported by a software MTP using the NM-HDV only if the **dsp services dspfarm** command is not enabled for the voice card.
- Lip-sync for video calls is not supported.

Information About RSVP Agent

To configure the RSVP agent on a Cisco IOS voice gateway, you should understand the following concept:

- [RSVP Agent, page 3](#)

RSVP Agent

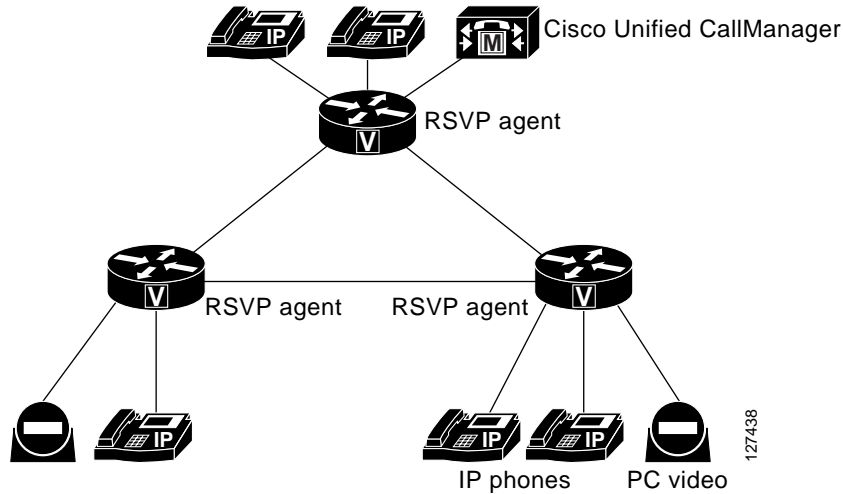
Resource Reservation Protocol (RSVP) is the IP service that allows applications to request end-to-end QoS guarantees from the network. Cisco VoIP applications use RSVP for call admission control, limiting the accepted voice load on the IP network to guarantee the QoS levels of calls. In networks that include both voice and video media, bandwidth requirements can vary considerably over any given time. Cisco Unified Communications Manager ensures resource reservation for voice and video media by using RSVP.

The RSVP agent is a transcoding or MTP device on the Cisco IOS gateway that registers with Cisco Unified Communications Manager as RSVP-capable. The RSVP agent is controlled by Cisco Unified Communications Manager which communicates with the RSVP agent using SCCP.

Cisco Unified Communications Manager consults its policy configuration to determine if RSVP is required for a voice or video call. If the configured QoS level for a call is optional or mandatory, and the RSVP agent is enabled on the voice gateway, Cisco Unified Communications Manager inserts a pair of RSVP agents into the media path to provide RSVP support. The RSVP agent on the Cisco IOS gateway creates the RSVP reservation for the two endpoints and bridges the media connection so that resources are reserved for the media path, providing QoS for the call.

Figure 13 shows where the RSVP agent fits in a Cisco Unified Communications Manager meshed network.

Figure 13 *RSVP Agent in Cisco Unified Communications Manager Meshed Network*



To support video calls, MTP and transcoding resources can process multiple streams in a single session, including audio, video and data, one-way or two-way, using a pass-through mode. In pass-through mode, a SCCP device processes streams using a pure software MTP, regardless of the type of stream, so it can be used for any stream type. Video and data streams are processed using pass-through mode. Audio streams can be processed with or without pass-through mode.

How to Enable the RSVP Agent on the Voice Gateway

This section contains the following procedures:

- [Enabling RSVP in a DSP Farm Profile, page 4](#) (required)
- [Verifying RSVP Agent Configuration, page 6](#) (optional)
- [Troubleshooting the RSVP Agent, page 7](#) (optional)



Note

This document does not contain details about configuring Cisco Unified Communications Manager. See the documentation and online help for Cisco Unified Communications Manager for configuration instructions.

Enabling RSVP in a DSP Farm Profile

Perform this procedure to enable the RSVP agent on an MTP or transcoder device.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dspfarm profile** *profile-identifier* {**mtp** | **transcode**}
4. **codec pass-through**
5. **maximum sessions** *number*
or
maximum sessions {**hardware** | **software**} *number*
6. **associate application sccp**
7. **rsvp**
8. **no shutdown**
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code> Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	<code>configure terminal</code> Example: Router# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	<pre>dspfarm profile profile-identifier {mtp transcode}</pre> <p>Example: Router(config)# dspfarm profile 20 transcode</p>	<p>Enters DSP farm profile configuration mode to define a profile for DSP farm services.</p> <p>Note The <i>profile-identifier</i> and service type uniquely identifies a profile. If the service type and <i>profile-identifier</i> pair is not unique, you are prompted to choose a different <i>profile-identifier</i>.</p>
Step 4	<pre>codec pass-through</pre> <p>Example: Router(config-dspfarm-profile)# codec pass-through</p>	<p>Enables codec pass-through mode for the DSP farm profile.</p> <ul style="list-style-type: none"> Codec pass-through must be enabled for the RSVP agent to support Cisco Unified Communications Manager. Transcoder profiles support multiple codecs. MTP profiles support only one codec in addition to pass-through mode. You must define a separate MTP profile for each additional codec.
Step 5	<pre>maximum sessions number</pre> <p>or</p> <pre>maximum sessions {hardware software} number</pre> <p>Example: Router(config-dspfarm-profile)# maximum sessions 4</p>	<p>Specifies the maximum number of sessions that are supported by the profile.</p> <ul style="list-style-type: none"> <i>number</i>—Range is determined by the available registered DSP resources. Default is 0. <p>Note The hardware and software keywords apply only to MTP profiles.</p>
Step 6	<pre>associate application sccp</pre> <p>Example: Router(config-dspfarm-profile)# associate application sccp</p>	<p>Associates the SCCP protocol to the DSP farm profile.</p>
Step 7	<pre>rsvp</pre> <p>Example: Router(config-dspfarm-profile)# rsvp</p>	<p>Enables RSVP support in the DSP farm profile.</p>
Step 8	<pre>no shutdown</pre> <p>Example: Router(config-dspfarm-profile)# no shutdown</p>	<p>Enables the profile, allocates DSP farm resources, and associates the application.</p>
Step 9	<pre>end</pre> <p>Example: Router(config-dspfarm-profile)# end</p>	<p>Exits to privileged EXEC mode.</p>

What to Do Next

Assign the DSP-farm profile to the appropriate Cisco Unified Communications Manager group. See the [“Associating a DSP Farm Profile to a Cisco Unified Communications Manager Group”](#) section on page 85.

Verifying RSVP Agent Configuration

Perform this procedure to verify the RSVP Agent configuration on the voice gateway.

SUMMARY STEPS

1. **show running-config**
2. **show dspfarm profile** *profile-number*
3. **show sccp ccm group** *group-number*

DETAILED STEPS

Step 1 **show running-config**

Use the **show running-config** command to verify that the RSVP agent is enabled on the SCCP device and that the device is assigned to a Cisco Unified Communications Manager group:

```
Router# show running-config
!
sccp ccm group 1
  bind interface FastEthernet0/0
  associate ccm 2 priority 3
  associate ccm 1 priority 2
  associate profile 10 register mtp_A1
  associate profile 120 register xcoder_A2
  associate profile 110 register mtp_A2
  associate profile 20 register xcoder_A1
!
dspfarm profile 20 transcode
  codec g711ulaw
  codec gsmfr
  codec g711alaw
  codec g729r8
  codec g729ar8
  codec g729br8
  codec g729abr8
  codec pass-through
  rsvp
  maximum sessions 5
  associate application SCCP
!
```

Step 2 **show dspfarm profile** *profile-number*

Use the **show dspfarm profile** command to verify the configuration and status of the resource:

```
Router# show dspfarm profile 20

Dspfarm Profile Configuration

Profile ID = 20, Service = TRANSCODING, Resource ID = 1
Profile Description :
Profile Admin State : UP
Profile Operation State : ACTIVE
Application : SCCP   Status : ASSOCIATED
Resource Provider : FLEX_DSPRM   Status : UP
Number of Resource Configured : 5
Number of Resource Available : 5
Codec Configuration
Codec : gsmfr, Maximum Packetization Period : 20
Codec : g729abr8, Maximum Packetization Period : 60
```

```
Codec : g711alaw, Maximum Packetization Period : 30
Codec : g711lulaw, Maximum Packetization Period : 30
Codec : g729r8, Maximum Packetization Period : 60
Codec : g729ar8, Maximum Packetization Period : 60
Codec : g729br8, Maximum Packetization Period : 60
Codec : pass-through, Maximum Packetization Period : 0
RSVP : ENABLED
```

Step 3 `show sccp ccm group group-number`

Use the `show sccp ccm group` command to verify the DSP farm profiles that are assigned to the Cisco Unified Communications Manager group and the registration names of the SCCP devices.

```
Router# show sccp ccm group 1
```

```
CCM Group Identifier: 1
Description: None
Binded Interface: NONE, IP Address: NONE
Associated CCM Id: 1, Priority in this CCM Group: 2
Associated CCM Id: 2, Priority in this CCM Group: 3
Associated Profile: 10, Registration Name: mtp_A1
Associated Profile: 20, Registration Name: xcoder_A1
Associated Profile: 110, Registration Name: mtp_A2
Associated Profile: 120, Registration Name: xcoder_A2
Registration Retries: 3, Registration Timeout: 10 sec
Keepalive Retries: 3, Keepalive Timeout: 30 sec
CCM Connect Retries: 3, CCM Connect Interval: 10 sec
Switchover Method: GRACEFUL, Switchback Method: GRACEFUL_GUARD
Switchback Interval: 10 sec, Switchback Timeout: 7200 sec
Signaling DSCP value: default, Audio DSCP value: default
```

Troubleshooting the RSVP Agent

You can troubleshoot the performance of the RSVP agent by performing any of the following steps.

SUMMARY STEPS

1. `show sccp`
2. `show sccp connections`
3. `show sccp connections details`
4. `show sccp connections rsvp`
5. `show ip rsvp installed`
6. `show sccp statistics`
7. `debug sccp all`
8. `debug call rsvp-sync [events | func-trace]`
9. `debug voip ccapi inout`

DETAILED STEPS

Step 1 show sccp

Before the start of a call, use the **show sccp** command to verify that the MTP or transcoder device is successfully registered with Cisco Unified Communications Manager:

```
Router# show sccp

SCCP Admin State: UP
Gateway IP Address: 192.168.20.1, Port Number: 0
IP Precedence: 5
User Masked Codec list: None
Call Manager: 192.168.20.11, Port Number: 2000
                Priority: N/A, Version: 5.0.1, Identifier: 3
Call Manager: 192.168.20.12, Port Number: 2000
                Priority: N/A, Version: 5.0.1, Identifier: 1
Call Manager: 192.168.20.13, Port Number: 2000
                Priority: N/A, Version: 5.0.1, Identifier: 2

....

Software MTP Oper State: ACTIVE - Cause Code: NONE
Active Call Manager: 192.168.20.12, Port Number: 2000
TCP Link Status: CONNECTED, Profile Identifier: 10
Reported Max Streams: 1004, Reported Max OOS Streams: 0
Supported Codec: pass-thru, Maximum Packetization Period: N/A
Supported Codec: g711ulaw, Maximum Packetization Period: 30
Supported Codec: rfc2833 dtmf, Maximum Packetization Period: 30
RSVP : ENABLED
```

Step 2 show sccp connections

During the call, use the **show sccp connections** command to display information about the active SCCP connections established for the call, the DSP farm service type (MTP or transcoding), codec (for example, pass-through or g711ulaw), and remote end information:

```
Router# show sccp connections

sess_id   conn_id   stype mode   codec  ripaddr      rport sport
-----
17537646  19438263  mtp   sendrcv pass_th 192.168.20.5 35548 16576
17537646  19438260  mtp   sendrcv pass_th 192.168.22.1 16832 19164

Total number of active session(s) 1, and connection(s) 2
```

Step 3 show sccp connections details

Use the **show sccp connections details** command to display details about active SCCP connections, including the internal call leg ID:

```
Router# show sccp connections details

bridge-info(bid, cid) - Normal bridge information(Bridge id, Calleg id)
mmbridge-info(bid, cid) - Mixed mode bridge information(Bridge id, Calleg id)

sess_id   conn_id   call-id   codec  pkt-period type          bridge-info(bid, cid)
mmbridge-info(bid, cid)
-----
17537646  -        326      N/A   N/A      swmtmpsp All RTPSPI Callegs  N/A
17537646  19438263  324      pass_th 20      rtpspi   (221,326)          N/A
17537646  -        326      N/A   N/A      swmtmpsp All RTPSPI Callegs  N/A
```

```
17537646 19438260 325 pass_th 20 rtpspi (222,326) N/A
```

Total number of active session(s) 1, connection(s) 2, and callees 4

Step 4 show sccp connections rsvp

Use the **show sccp connections rsvp** command to display information about the active RSVP reservations for the call:

```
Router# show sccp connections rsvp
```

sess_id	conn_id	rsvp_id	dir	local ip	:port	remote ip	:port
17537646	19438260	-244	SEND	192.168.20.1	:19164	192.168.22.1	:16832
17537646	19438260	-245	RECV	192.168.20.1	:19164	192.168.22.1	:16832

Total active sessions 1, connections 2, rsvp sessions 2

Step 5 show ip rsvp installed

Use the **show ip rsvp installed** command to see that the RSVP reservation is successfully made and to display the reserved bandwidth for the call:

```
Router# show ip rsvp installed
```

```
RSVP: Loopback0 has no installed reservations
RSVP: FastEthernet0/0 has no installed reservations
RSVP: Serial0/0
BPS    To                From                Protoc DPort  Sport  Weight Conversation
80K    192.168.22.1       192.168.20.1       UDP    16832 19164 25      265
RSVP: FastEthernet0/1 has no installed reservations
RSVP: Serial0/1 has no installed reservations
```

Step 6 show sccp statistics

Use the **show sccp statistics** command to display the SCCP messages exchanged between the RSVP agent and Cisco Unified Communications Manager:

```
Router# show sccp statistics
```

```
SCCP Application Service(s) Statistics:

Profile Identifier: 10, Service Type: Software MTP
TCP packets rx 9, tx 6
Unsupported pkts rx 0, Unrecognized pkts rx 0
Register tx 0, successful 0, rejected 0, failed 0
KeepAlive tx 1, successful 1, failed 0
OpenReceiveChannel rx 2, successful 2, failed 0
CloseReceiveChannel rx 0, successful 0, failed 0
StartMediaTransmission rx 2, successful 2, failed 0
StopMediaTransmission rx 0, successful 0, failed 0
PortReq rx 1
PortRes tx 1, successful 1, failed 0
PortClose rx 0
QosListen rx 1
QosPath rx 1
QosTearDown rx 0, send 0, recv 0, sendrecv 0
QosResvNotify tx 2, send 2, recv 0, sendrecv 0
QosErrorNotify tx 0, send 0, recv 0, sendrecv 0
    err0 0, err1 0, err2 0, err3 0, err4 0, err5 0,
    err6 0, err7 0, err8 0, err9 0, err10 0, err11 0,
QosModify rx 1, send 0, recv 1, sendrecv 0
UpdateDscp rx 0
```

```
Reset rx 0, successful 0, failed 0
MediaStreamingFailure rx 0
Switchover 0, Switchback 0
```

Step 7 debug sccp all

Use the **debug sccp all** command to display the sequence of the SCCP messages. The message sequence may be different if the RSVP policy defined in Cisco Unified Communications Manager is not set to mandatory.

```
Router# show sccp statistics
Router# show log | incl (rcvd | txed)

Feb  4 20:28:41.791: sccp_parse_control_msg: rcvd KeepAliveAckMessage msg
Feb  4 20:28:41.803: sccp_parse_control_msg: rcvd KeepAliveAckMessage msg
Feb  4 20:28:41.815: sccp_parse_control_msg: rcvd KeepAliveAckMessage msg
Feb  4 20:28:55.647: sccp_parse_control_msg: rcvd PortReq msg:
Feb  4 20:28:55.647: sccp_send_port_res: PortRes msg txed in hex(including header) - len
36
Feb  4 20:28:55.651: sccp_parse_control_msg: rcvd QosPath msg:
Feb  4 20:28:55.651: sccp_parse_control_msg: rcvd QosListen msg:
Feb  4 20:28:55.675: sccp_send_qos_resv_notify: QosResvNotify txed in hex(including
header) - len 36
Feb  4 20:28:57.706: OpenReceviceChannel msg rcvd in hex -
Feb  4 20:28:57.710: sccp_open_receive_chnl_ack: OpenRecvChnlAck msg txed in hex(including
header) - len 32
Feb  4 20:28:57.714: OpenReceviceChannel msg rcvd in hex -
Feb  4 20:28:57.718: StartMediaTrans msg rcvd in hex -
Feb  4 20:28:57.726: sccp_open_receive_chnl_ack: OpenRecvChnlAck msg txed in hex(including
header) - len 32
Feb  4 20:28:57.866: StartMediaTrans msg rcvd in hex -
Feb  4 20:28:57.870: sccp_parse_control_msg: rcvd QosModify msg:
Feb  4 20:28:57.878: sccp_send_qos_resv_notify: QosResvNotify txed in hex(including
header) - len 36
```

Step 8 debug call rsvp-sync {events | func-trace}

Use the **debug call rsvp-sync event** and **debug call rsvp-sync func-trace** with the **debug sccp all** command to show how SCCP messages and RSVP events trigger each other.

Step 9 debug voip ccapi inout

Use the **debug voip ccapi inout** command to trace the execution path through the call control application programming interface (API).

Configuration Examples for RSVP Agent

This section contains the following configuration example:

- [RSVP Agent, page 3](#)

RSVP Agent: Example

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
```

```
hostname Router
!
boot-start-marker
boot-end-marker
!
logging buffered 5000000 debugging
no logging console
enable password lab
!
no network-clock-participate slot 2
no network-clock-participate aim 0
no network-clock-participate aim 1
no aaa new-model
ip subnet-zero
ip cef
!
!
no ip domain lookup
no ftp-server write-enable
voice-card 2
  dspfarm
  dsp services dspfarm
!
!
!
interface Loopback0
  ip address 192.168.26.1 255.255.255.255
  max-reserved-bandwidth 100
  ip rsvp bandwidth
!
interface FastEthernet0/0
  ip address 192.168.20.1 255.255.255.0
  max-reserved-bandwidth 100
  duplex auto
  speed auto
  fair-queue 64 256 1000
  ip rsvp bandwidth
!
interface Serial0/0
  ip address 192.168.25.2 255.255.255.252
  max-reserved-bandwidth 100
  fair-queue 64 256 37
  ip rsvp bandwidth
!
interface FastEthernet0/1
  ip address 192.168.24.1 255.255.255.0
  max-reserved-bandwidth 100
  shutdown
  duplex auto
  speed auto
  fair-queue 64 256 1000
  ip rsvp bandwidth
!
interface Serial0/1
  ip address 192.168.25.69 255.255.255.252
  max-reserved-bandwidth 100
  shutdown
  fair-queue 64 256 37
  ip rsvp bandwidth
!
router ospf 10
  log-adjacency-changes
  network 192.168.0.0 0.0.255.255 area 0
!
```

```

ip classless
ip http server
ip rsvp policy preempt
!
!
!
control-plane
!
!
!
voice-port 2/0/0
!
voice-port 2/0/1
!
!
sccp local FastEthernet0/0
sccp ccm 192.168.20.11 identifier 3 version 4.0
sccp ccm 192.168.20.13 identifier 2 version 5.1
sccp ccm 192.168.20.12 identifier 1 version 5.1
sccp
!
sccp ccm group 1
bind interface FastEthernet0/0
associate ccm 2 priority 3
associate ccm 1 priority 2
associate profile 10 register mtp_A1
associate profile 120 register xcoder_A2
associate profile 110 register mtp_A2
associate profile 20 register xcoder_A1
!
dspfarm profile 20 transcode
codec g711ulaw
codec gsmfr
codec pass-through
codec g711alaw
codec g729r8
codec g729ar8
codec g729br8
codec g729abr8
rsvp
maximum sessions 5
associate application SCCP
!
dspfarm profile 120 transcode
codec g729abr8
codec gsmfr
codec g711alaw
codec g711ulaw
codec g729r8
codec g729ar8
codec g729br8
codec pass-through
rsvp
maximum sessions 5
associate application SCCP
!
dspfarm profile 30 conference
codec g711ulaw
codec g711alaw
codec g729ar8
codec g729abr8
codec g729r8
codec g729br8
!

```

```
dspfarm profile 10 mtp
  codec g711ulaw
  codec pass-through
  rsvp
  maximum sessions hardware 2
  maximum sessions software 10
  associate application SCCP
!
dspfarm profile 110 mtp
  codec pass-through
  codec g711ulaw
  rsvp
  maximum sessions hardware 2
  maximum sessions software 10
  associate application SCCP
!
!
!
line con 0
  exec-timeout 0 0
line aux 0
line vty 0 4
  exec-timeout 0 0
  no login
!
ntp clock-period 17175018
ntp server 192.168.20.12
end
```

Additional References

- [Cisco Unified Communications Manager Administration Guide](#), Release 5.0(1)
- [Cisco Unified Communications Manager System Guide](#), Release 5.0(1)
- [Cisco Unified Communications Manager Features and Services Guide](#), Release 5.0(1)

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0711R)

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

© 2007 Cisco Systems, Inc. All rights reserved.

