



## **Cisco Unified Border Element Configuration Guide**

Release 12.4T

### **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 Border Element Configuration 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 <b>^D</b> or <b>Ctrl-D</b> 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
<b>bold</b>	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.
<b>Courier font</b>	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](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"> <li>• Transparent and source-route transparent (SRT) bridging, source-route bridging (SRB), Token Ring Inter-Switch Link (TRISL), and token ring route switch module (TRRSM).</li> <li>• 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.</li> </ul>
<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>	<p>Point-to-Point Protocol (PPP) over ATM (PPPoA) and PPP over Ethernet (PPPoE).</p>
<p><i>Cisco IOS Carrier Ethernet Configuration Guide</i></p> <p><i>Cisco IOS Carrier Ethernet Command Reference</i></p>	<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>
<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>	<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>
<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>	<p>DECnet protocol.</p>
<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>	<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>
<p><i>Cisco IOS Flexible NetFlow Configuration Guide</i></p> <p><i>Cisco IOS Flexible NetFlow Command Reference</i></p>	<p>Flexible NetFlow.</p>



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

<b>Configuration Guide and Command Reference Titles</b>	<b>Features/Protocols/Technologies</b>
<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)**

<b>Configuration Guide and Command Reference Titles</b>	<b>Features/Protocols/Technologies</b>
<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:  <a href="http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-roadmap.html">http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-roadmap.html</a>
<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)

<b>Configuration Guide and Command Reference Titles</b>	<b>Features/Protocols/Technologies</b>
<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)**

<b>Configuration Guide and Command Reference Titles</b>	<b>Features/Protocols/Technologies</b>
<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).  <b>Note</b> 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 <b>debug</b> 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: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>
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: <a href="http://www.rfc-editor.org/">http://www.rfc-editor.org/</a>

## 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 <b>logout</b> or <b>exit</b> command.	<ul style="list-style-type: none"> <li>• Change terminal settings.</li> <li>• Perform basic tests.</li> <li>• Display device status.</li> </ul>
Privileged EXEC	From user EXEC mode, issue the <b>enable</b> command.	Router#	Issue the <b>disable</b> command or the <b>exit</b> command to return to user EXEC mode.	<ul style="list-style-type: none"> <li>• Issue <b>show</b> and <b>debug</b> commands.</li> <li>• Copy images to the device.</li> <li>• Reload the device.</li> <li>• Manage device configuration files.</li> <li>• Manage device file systems.</li> </ul>
Global configuration	From privileged EXEC mode, issue the <b>configure terminal</b> command.	Router(config)#	Issue the <b>exit</b> command or the <b>end</b> command to return to privileged EXEC mode.	Configure the device.
Interface configuration	From global configuration mode, issue the <b>interface</b> command.	Router(config-if)#	Issue the <b>exit</b> command to return to global configuration mode or the <b>end</b> command to return to privileged EXEC mode.	Configure individual interfaces.
Line configuration	From global configuration mode, issue the <b>line vty</b> or <b>line console</b> command.	Router(config-line)#	Issue the <b>exit</b> command to return to global configuration mode or the <b>end</b> 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 <b>reload</b> command. Press the <b>Break</b> 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 <b>continue</b> command.	<ul style="list-style-type: none"> <li>Run as the default operating mode when a valid image cannot be loaded.</li> <li>Access the fall-back procedure for loading an image when the device lacks a valid image and cannot be booted.</li> <li>Perform password recovery when a CTRL-Break sequence is issued within 60 seconds of a power-on or reload event.</li> </ul>
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"> <li>A user-configured access policy was configured using the <b>transport-map</b> command, which directed the user into diagnostic mode.</li> <li>The router was accessed using an RP auxiliary port.</li> <li>A break signal (<b>Ctrl-C</b>, <b>Ctrl-Shift-6</b>, or the <b>send break</b> command) was entered, and the router was configured to enter diagnostic mode when the break signal was received.</li> </ul>	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"> <li>Inspect various states on the router, including the Cisco IOS state.</li> <li>Replace or roll back the configuration.</li> <li>Provide methods of restarting the Cisco IOS software or other processes.</li> <li>Reboot hardware, such as the entire router, an RP, an ESP, a SIP, a SPA, or possibly other hardware components.</li> <li>Transfer files into or off of the router using remote access methods such as FTP, TFTP, and SCP.</li> </ul>

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
<b>help</b>	Provides a brief description of the help feature in any command mode.
<b>?</b>	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](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
<b>h</b>	help
<b>lo</b>	logout
<b>p</b>	ping
<b>s</b>	show
<b>u</b> or <b>un</b>	undebug
<b>w</b>	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](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](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](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](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.





# Overview of Cisco Unified Border Element

---

**Revised: August 5, 2009,**  
**First Published: June 19, 2006**  
**Last Updated: August 5, 2009**

This Cisco Unified Border Element (previously known as the Cisco Multiservice IP-to-IP Gateway) is a special Cisco IOS software image that runs on Cisco multiservice gateway platforms. It provides a network-to-network interface point for billing, security, call admission control, quality of service, and signaling interworking. This chapter describes basic gateway functionality, software images, topology, and summarizes supported features.

## Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Cisco Unified Border Element Features Roadmap](#)” chapter of this guide.

## Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

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



## Activation

---

**Cisco Product Authorization Key (PAK)**—A Product Authorization Key (PAK) is required to configure some of the features described in this guide. Please register your products and activate your PAK at <http://www.cisco.com/go/license> before starting your configuration process.

---

For more information about Cisco IOS voice features, see the entire Cisco IOS Voice Configuration Library—including library preface and glossary, feature documents, and troubleshooting information—at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124tcg/vcl.htm>.



---

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

© 2009 Cisco Systems, Inc. All rights reserved.

# Contents

- Prerequisites for Cisco Unified Border Element Configuration, page 15
- Restrictions for Cisco Unified Border Element Configuration, page 16
- Information About Cisco Unified Border Element, page 17
- Toll Fraud Prevention, page 32
- Where to Go Next, page 33
- Additional References, page 34
- Feature Information for Cisco Unified Border Element Configuration Guide, page 39

## Prerequisites for Cisco Unified Border Element Configuration

### Cisco Unified Border Element Hardware

- Install the routers that will serve as session border controllers in your VoIP network.

### Cisco Unified Border Element Software

- Obtain the appropriate feature license for each router on which you will install an image that supports the Unified Border Element feature. Additional information on obtaining a feature license can be found at:

[http://www.cisco.com/en/US/products/sw/voicesw/ps5640/products\\_data\\_sheet09186a00801da698.html](http://www.cisco.com/en/US/products/sw/voicesw/ps5640/products_data_sheet09186a00801da698.html)



#### Activation

**Cisco Product Authorization Key (PAK)**—A Product Authorization Key (PAK) is required to configure some of the features described in this guide. Please register your products and activate your PAK at <http://www.cisco.com/go/license> before starting your configuration process.

- Install the appropriate Cisco IOS image on each router and configure a working VoIP network. Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

**Table 1** provides additional information on image and feature sets that support the Cisco Unified Border Element.

**Table 1** Cisco IOS Image and Feature Sets for the Cisco Unified Border Element Feature

Platform	Software Image Name	Software Feature Set
Cisco 2601XM	c2600-adventerprisek9_ivs-mz	Cisco 2600 INT VOICE/VIDEO, IPIPGW, TDMIP GW AES
Cisco 2611XM	c2600-ipvoice_ivs-mz	Cisco 2600 INT VOICE/VIDEO, IPIPGW, TDMIP GW
Cisco 2620XM		
Cisco 2621XM	c2600-ipvoice_ivs-mz	Cisco 2600 INT VOICE/VIDEO, IPIPGW, TDMIP GW
Cisco 2650XM		
Cisco 2651XM		

**Table 1** Cisco IOS Image and Feature Sets for the Cisco Unified Border Element Feature (continued)

Platform	Software Image Name	Software Feature Set
Cisco 2691	c2691-adventerprisek9_ivs-mz c2691-ipvoice_ivs-mz	Cisco 2600 INT VOICE/VIDEO, IPIPGW, TDMIP GW AES Cisco 2600 INT VOICE/VIDEO, IPIPGW, TDMIP GW
Cisco 2811 Cisco 2821 Cisco 2851	c2800nm-adventerprisek9_ivs-mz c2800nm-ipvoice_ivs-mz	Cisco 2800 INT VOICE/VIDEO, IPIPGW, TDMIP GW AES Cisco 2800 INT VOICE/VIDEO, IPIPGW, TDMIP GW
Cisco 2801	c2801-adventerprisek9_ivs-mz c2801-ipvoice_ivs-mz	Cisco 2801 INT VOICE/VIDEO, IPIPGW, TDMIP GW AES Cisco 2801 INT VOICE/VIDEO, IPIPGW, TDMIP GW
Cisco 3725	c3725-adventerprisek9_ivs-mz c3725-ipvoice_ivs-mz	Cisco 3725 INT VOICE/VIDEO, IPIPGW, TDMIP GW AES Cisco 3725 INT VOICE/VIDEO, IPIPGW, TDMIP GW
Cisco 3745	c3745-adventerprisek9_ivs-mz c3745-ipvoice_ivs-mz	Cisco 3745 INT VOICE/VIDEO, IPIPGW, TDMIP GW AES Cisco 3745 INT VOICE/VIDEO, IPIPGW, TDMIP GW
Cisco 3825	c3825-adventerprisek9_ivs-mz c3825-ipvoice_ivs-mz	Cisco 3825 INT VOICE/VIDEO, IPIPGW, TDMIP GW AES Cisco 3825 INT VOICE/VIDEO, IPIPGW, TDMIP GW
Cisco 3845	c3845-adventerprisek9_ivs-mz c3845-ipvoice_ivs-mz	Cisco 3845 INT VOICE/VIDEO, IPIPGW, TDMIP GW AES Cisco 3845 INT VOICE/VIDEO, IPIPGW, TDMIP GW
Cisco AS5350XM	c5350-jk9su2_ivs-mz c5350-js_ivs-mz	Cisco AS5350 Series IOS INT Voice/Video IPIPGW, TDMIP GW LI Cisco AS5350 Series IOS INT Voice/Video IPIPGW, TDMIP GW EPLUS
Cisco AS5400XM	c5400-jk9su2_ivs-mz c5400-js_ivs-mz	Cisco AS5400 Series IOS INT VOICE/VIDEO IPIPGW, TDMIP GW LI Cisco AS5400 Series IOS INT VOICE/VIDEO IPIPGW, TDMIP GW EPLUS
Cisco 7200	c7200-adventerprisek9-mz c7200-adipservicesk9li-mz	Cisco 7200 Series IOS Advanced Enterprise Services Cisco 7200 Series IOS ADV IP Services w/ Lawful Intercept
Cisco 7301	c7301-adventerprisek9-mz c7301-adipservicesk9li-mz	Cisco 7301 Series IOS Advanced Enterprise Services Cisco 7301 Series IOS ADV IP Services w/ Lawful Intercept

## Restrictions for Cisco Unified Border Element Configuration

- Cisco Unified Border Elements that require the Registration, Admission, and Status (RAS) protocol must have a via-zone-enabled gatekeeper or equivalent.
- Cisco Unified Border Elements interoperate with Cisco ATA 186, Cisco ATA 188, Cisco Unified Communications Manager, Cisco CallManager Express 3.1, Cisco IOS gateways, NetMeeting, and Polycom ViewStation.
- Cisco fax relay is reported as a voice call on an Cisco Unified Border Element. Fax relay is enabled by default for all systems. No further configuration is needed.
- Fax calls are reported as a modem plus fax call when modem CLI are present.
- Cisco Unified Border Element supports T.38 fax relay (H.323 Annex D). However, endpoints configured with Named Signaling Events (NSE) may result in reduced fax transmission quality and are not supported.
- Codec filtering must be based on codec types; filtering based on byte size is not supported.

- When a Tcl script is running on an Cisco Unified Border Element, the Cisco Unified Border Element does not support ringback tone generation.
- Transcoding is not supported on the Cisco AS5350XM, AS5400XM, Cisco 7200 and the Cisco 7301.

## Information About Cisco Unified Border Element

A Cisco Unified Border Element (Cisco UBE), in this guide also called an IP-to-IP gateway (IPIPGW), border element (BE), or session border controller, facilitates connectivity between independent VoIP networks by enabling H.323 VoIP and videoconferencing calls from one IP network to another. This gateway performs most of the same functions of a PSTN-to-IP gateway, but typically joins two IP call legs, rather than a PSTN and an IP call leg. Media packets can flow either through the gateway (thus hiding the networks from each other) or around the border element, if so configured.

Cisco Unified Border Element is a special Cisco IOS software image that runs on Cisco Unified Border Element platforms. It provides a network-to-network interface point for billing, security, call admission control, quality of service, and signaling interworking.

Cisco Unified Border Element is designed to meet the interconnection needs of Internet telephony service providers (ITSPs) and of enterprises. One set of images provides basic interconnection and a second set provides interconnection through an Open Settlement Protocol (OSP) provider, enabling ITSPs to gain the benefits of the Cisco Unified Border Element while making use of the routing, billing, and settlement capabilities offered by OSP-based clearinghouses.

For the most effective and scalable results, use the Cisco Unified Border Element concurrently with a Cisco gatekeeper

Feature benefits include the following:

- Capacity control and improved call routing control using carrier-based routing with the Cisco Unified Border Element feature and routing traffic through the gateways.
- Improved billing and settlement capabilities.
- Provides key services at the edge of the network for scalability.

To configure the Cisco Unified Border Element Feature, you should understand the following concepts:

- [Gateway Functionality, page 17](#)
- [Cisco Unified Border Element Network Topology, page 18](#)
- [Features Supported by the Cisco Unified Border Element, page 20](#)

## Gateway Functionality

Gateways are responsible for the following tasks.

- Media stream handling and speech path integrity
- DTMF relay
- Fax relay and passthrough
- Digit translation and call processing
- Dial peers and codec filtering
- Carrier ID handling



- Gateway-based billing
- Termination and re-origination of signaling and media

## Cisco Unified Border Element Network Topology

In the current VoIP market, ITSPs who provide wholesale VoIP services use their own IP-to-TDM gateways to exchange calls with the PSTN. Problems occur when a wholesaler receives a call from an originating ITSP and decides to terminate the call to another ITSP. Because it does not own the PSTN gateways, the wholesaler does not receive call setup or release information and therefore cannot bill for the call. Wholesalers are forced either to forbid these connections, thereby foregoing a potential revenue source, or to set up the call through a combination of back-to-back IP-to-TDM gateways. This solution results in reduced quality due to double media coding and decoding, and it wastes TDM port resources.

Cisco Unified Border Element allows the wholesaler to terminate the call from the originating ITSP and then reoriginate it, thereby providing a point at which accurate call detail records (CDRs) can be collected for billing.

The superior interconnect capability provided by the Cisco Unified Border Element enables service providers to conceal their internal network and business relationships while improving call admission control, flexible routing, and protocol interworking capabilities.

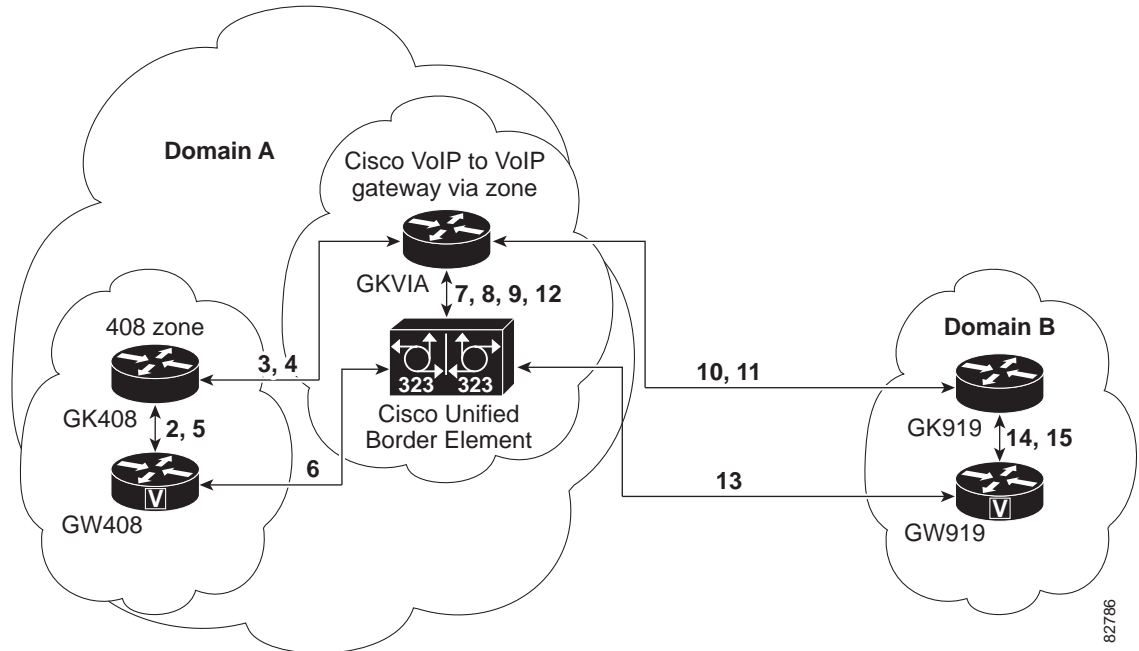
The Cisco Unified Border Element includes the following changes to gateways and gatekeepers to allow Cisco UBE call legs:

- Support for H.323-to-H.323, H.323-to-SIP, and SIP-to-SIP connection types
- Support for transparent codec on H.323-to-H.323 connection types
- Support for H.323 call capacities
- Introduction of gatekeeper via-zones. *Via-zone* is a Cisco term for a zone that contains Cisco Unified Border Elements and via-zone-enabled gatekeepers. A via-zone-enabled gatekeeper is capable of recognizing via-zones and sending traffic to via-zone gateways. Cisco via-zone-enabled gatekeepers include a via-zone command-line interface (CLI) command.

Via-zones are usually located on the edge of an ITSP network and are like a VoIP transfer point, or tandem zone, where traffic passes through on the way to the remote zone destination. Gateways in this zone terminate requested calls and reoriginate traffic to its final destination. Via-zone gatekeepers operate as usual for applications that are not Cisco UBE gatekeepers in via-zones support resource management (for example, gateway selection and load balancing) using the Capacities field in the H.323 Version 4 RAS messages.

Figure 1 shows a simple topology example of the Cisco Unified Border Element using via-zone gatekeepers.

**Figure 1** Cisco Unified Border Element Feature Sample Topology



The gatekeeper in Domain A and the gatekeeper in Domain B are connected to the via-zone gatekeeper, GK408 and the via-zone gatekeeper exchange Registration, Admission, and Status (RAS) messages for the originating side. Then the connection is made between the originating gateway and the Cisco Unified Border Element. The via-zone gatekeeper exchanges RAS messages with GK919 for the terminating side. If the call is accepted, the Cisco Unified Border Element completes the connection from GW408 to GW919, and the media flows through the Cisco Unified Border Element.

In a basic call scenario, on receiving a location request (LRQ) message from the originating gatekeeper (GK408), the via-zone-enabled gatekeeper (GKVIA) processes the message and determines that the call should be set up using the Cisco Unified Border Element. After the originating gateway receives its admission confirmation (ACF) message, it sets up the call.

With the Cisco Unified Border Element feature, instead of the originating gateway signaling the terminating gateway directly, the Cisco Unified Border Element controls the call set-up both the signaling and media channel. The Cisco Unified Border Element is terminating the signaling and media channels, but the information associated with the media is propagated through to the opposite call leg. This process allows the endpoints to determine what media channel capabilities to use for the call. When the call is established, the audio stream flows through the Cisco Unified Border Element, meaning that the gateway terminates the audio channel on one call leg and then reoriginates it to the other leg.

The following scenario illustrates a basic call from the originating gateway to the terminating gateway, using the Cisco Unified Border Element and gatekeepers.

1. GW408 (the originating gateway) calls someone in the 919 area code, which is serviced by GW919 (the terminating gateway).
2. GW408 sends an ARQ with the called number having the 919 area code to a gatekeeper in its zone (GK408).

3. GK408 resolves 919 to belong to a via-zone gatekeeper (GKVIA). GK408 then sends an LRQ to GKVIA.
4. GKVIA receives the LRQ for the 919 number. GKVIA resolves the 919 prefix to belong to the Cisco Unified Border Element. GKVIA is configured to route requests for 919 prefix calls through its Cisco Unified Border Element. GKVIA sends an LCF to GK408.
5. GK408 returns an ACF specifying Cisco Unified Border Element to GW408.
6. GW408 sends a SETUP message to Cisco Unified Border Element for the 919 number.
7. Cisco Unified Border Element consults GKVIA with an ARQ message with the **answerCall=true** parameter to admit the incoming call.
8. GKVIA responds with an ACF to admit the call. From the perspective of the gatekeeper, the first call leg has been established.
9. Cisco Unified Border Element has a dial peer specifying that RAS messages should be sent to GKVIA for all prefixes. Cisco Unified Border Element initiates the resending of the call by sending the ARQ message with the **answerCall** parameter set to, false to GKVIA for 919.
10. GKVIA knows that prefix 919 belongs to GK919, and since the source zone is the via-zone, the GKVIA sends an LRQ to GK919.
11. GK919 sees prefix 919 as a local zone and sends an LCF pointing to GW919.
12. GKVIA returns an ACF specifying GW919.
13. Cisco Unified Border Element sends a SETUP message to GW919 for the 919 call.
14. GW919 sends an ARQ to GK919 to request admission for the call.
15. GK919 sends an ACF with the **answerCall=true** parameter.

All other messages (for example, Proceeding, Alerting, and Connect) are created as two legs between GW408, and GW919, with the Cisco Unified Border Element acting as an intermediate gateway.

## Features Supported by the Cisco Unified Border Element

This section contains lists of the following types of supported features:

- [Gateway Call-Signaling Features, page 21](#)
- [Cisco Unified Border Element Protocol Features, page 25](#)
- [Protocol Interworking, page 26](#)
- [Billing Features, page 27](#)
- [Application and Tcl Script Features, page 27](#)
- [Interoperability Features, page 27](#)
- [IVR Features, page 28](#)
- [Lawful Intercept Support, page 28](#)
- [QoS Features, page 29](#)
- [Tcl Objects Supported by the Cisco Unified Border Element, page 29](#)

## Gateway Call-Signaling Features

Table 2 is a list of supported gateway call-signaling features.

**Table 2 Cisco Unified Border Element Call Signaling Features**

Feature	Details	H.323-to-H.323 Support?	H.323-to-SIP Support?	SIP-to-SIP Support?	Additional Information
<b>Accounting</b>					
	Calling/called name and number RADIUS call accounting records	Yes	Yes	Yes	—
	Conference ID for call relating the two call legs	Yes	Yes	Yes	—
<b>Address Hiding</b>					
	Address hiding	Yes	Yes	Yes	—
<b>Call Admission Control</b>					
	Call Admission Control	Yes	Yes	Yes	CPU, memory utilization, total calls, Max connections, RSVP and IP Circuits for all the protocol combinations (H.323-to-H.323, H.323-to-SIP, and SIP-to-SIP).
	RSVP nonsynchronized	Yes	No	No	Video only
	RSVP synchronized	Yes	No	No	Video only
<b>Cause Codes</b>					
	SIP Cause Codes	No	No	Yes	—
<b>Cisco CallManager Connections</b>					
	Interoperability with Cisco Unified Communications Manager 5.0 and Cisco Unified Communications Manager 4.1.3	Yes	Yes	Yes	—
	No MTP for Cisco Unified Communications Manager Trunks to Cisco Unified BE	Yes	No	No	—
<b>Codec Support</b>					
	Audio Codecs	Yes	Yes	Yes	G.711u, G.711a, G.723, G.726, G.729r8, G.728, AMR-NB, iLBC.
	Codec Transparent Support	Yes	Yes	No	—
	Video Codecs	Yes	No	No	H.261, H.263, H.264.
<b>Codec Transcoding</b>					

Table 2 Cisco Unified Border Element Call Signaling Features

Feature	Details	H.323-to-H.323 Support?	H.323-to-SIP Support?	SIP-to-SIP Support?	Additional Information
	Codec bytes payload value negotiation	Yes	No	No	Payload size is passed transparently and negotiated between the endpoints. Codec bytes configuration on the Cisco Unified Border Element is ignored.
	Codec transcoding (G.711-G.729)	Yes	Yes	No	—
	DTMF Transcoding with the Cisco AS5xxx platforms	Yes	Yes	Yes	—
<b>DTMF</b>					
	DTMF	Yes	Yes	Yes	Configuration must be consistent between the originating and terminating gateways. DTMF configuration is needed at the Cisco Unified Border Element.
	KPML	No	Yes	Yes	—
	DTMF relay and hookflash relay	Yes	No	No	H.245 alphanumeric, H.245 signal, RFC 2833, and Cisco RTP DTMF relay types supported. Configuration not needed on Cisco Unified Border Element.
	G.711 Inband DTMF to RFC 2833	Yes	Yes	Yes	—
<b>ENUM Support- RFC-2916</b>					
	ENUM support	Yes	Yes	Yes	—
<b>Fax/Modem</b>					
	Cisco-proprietary fax relay	Yes	Yes	Yes	Fax relay is enabled by default for all systems. No further configuration is needed.
	Fax pass-through	Yes	Yes	Yes	—
	Modem passthrough	Yes	Yes	Yes	The Cisco Unified Border Element display may not display the codec upshift (G.729 to G.711).
	Modem relay	No	No	No	—
	Fax with Transcoding	Yes	Yes	No	—

**Table 2** Cisco Unified Border Element Call Signaling Features

Feature	Details	H.323-to-H.323 Support?	H.323-to-SIP Support?	SIP-to-SIP Support?	Additional Information
	T.38 fax relay (flow-through)	Yes	Yes	Yes	<ul style="list-style-type: none"> <li>TCP/UDP like-to-like transport: Yes</li> <li>Standards OLC: Yes</li> <li>Cisco Proprietary NSE: No</li> </ul>
<b>Lawful Intercept</b>					
	Lawful intercept	Yes	Yes	Yes	See <a href="#">Table 9</a> and <a href="#">Table 10</a> in this chapter for a list of supported platforms.
<b>Media Inactivity Timer</b>					
	RTCP media inactivity timer	Yes	Yes	Yes	—
<b>Media Modes</b>					
	Media Flow Through	Yes	Yes	Yes	—
	Media Flow Around	Yes	No	Yes	<b>Note</b> SIP-to-SIP support is limited to basic audio calls.
<b>Other Features</b>					
	IP address bind	Yes	Yes	Yes	Interface can be bound to only one protocol type.
	Session refresh with OPTIONS	No	No	Yes	—
	Media Statistics on an Cisco UBE	Yes	Yes	Yes	—
	SIP Error Message Pass Through	No	No	Yes	—
<b>Protocol Compliance</b>					
	H.323 v4	Yes	Yes	No	—
	SIP v2	No	Yes	Yes	—
<b>Quality of Service</b>					
	ToS/DSCP marking support	Yes	Yes	Yes	—
<b>Rotary Support</b>					
	Call Failure Recovery (Rotary)	Yes	No	Yes	SIP-to-SIP calls must have same codec.
	EmptyCapability (TCS=0)	Yes	No	No	TCS=0 message is transparently transferred from leg to leg.
<b>Security</b>					
	CryptoToken - IRR	Yes	No	No	—
	H235CallSecurity	Yes	No	No	Tokens are not transferred from leg to leg. A security token cannot be generated for only one leg (for example, only on the outgoing leg).

**Table 2 Cisco Unified Border Element Call Signaling Features**

Feature	Details	H.323-to-H.323 Support?	H.323-to-SIP Support?	SIP-to-SIP Support?	Additional Information
	IPSEC	Yes	Yes	Yes	—
	Secure RTP with IPSEC for Signaling	Yes	No	No	—
	SRTP	Yes	No	No	—
	Transport Layer Security (TLS)	No	Yes	Yes	—
<b>Signaling Interworking</b>					
	Delayed Media to Delayed Media	No	No	Yes	—
	Delayed Media to Slow Start	No	No	No	—
	Early Media to Early Media	n/a	n/a	Yes	Invite with SDP parameters.
	Fast Start to Delay Media	No	No	No	—
	Fast Start to Fast Start	Yes	n/a	n/a	Fast start elements are sent in PROG or ALERT and not in CALLPROC.
	Slow Start to Delayed Media	No	Yes	No	—
	Slow Start to Early Media	No	No	No	—
	Slow Start to Fast Start	Yes	No	No	Support for basic calls
	Slow Start to Slow Start	Yes	No	No	—
	Progress indicator interworking for media cut-through	Yes	No	No	—
	Tunneled H.245 traffic	Yes	No	No	—
<b>Supplementary Services (Including Cisco Unified Communications Manager)</b>					
	Call Forward	Yes	No	Yes	H323:H450.3, SIP:302
	Call Hold/Resume	Yes	No	Yes	SIP: Reinvite
	ECS to ReINVITE on the Cisco IOS SBC.	No	Yes	Yes	—
	ECS to REFER on the Cisco IOS SBC.	No	Yes	Yes	—
	Call Transfer	Yes	No	Yes	H323:H450.2, SIP:Refer
	Call Waiting	No	No	Yes	—
	Distinctive Ringing	No	No	Yes	—
	Message Waiting Indication (MWI)	Yes	No	Yes	—
	Music on Hold	Yes	Yes	Yes	Not locally generated on Cisco Unified Border Element.

TCL IVR

**Table 2** Cisco Unified Border Element Call Signaling Features

Feature	Details	H.323-to-H.323 Support?	H.323-to-SIP Support?	SIP-to-SIP Support?	Additional Information
	IVR with DTMF SIP NOTIFY, RFC 2833	No	Yes	Yes	—
	IVR with H.245 alphanumeric, H.245 signal, RFC 2833	Yes	Yes	n/a	—
<b>Timeouts</b>					
	H.225 configurable timeout	Yes	No	No	—
<b>Transport Protocols</b>					
	UDP	Yes	Yes	Yes	H.323-to-H.323 and H.323-to-SIP connections require a GK.
	TCP	Yes	Yes	Yes	—
	Interworking UDP and TCP Transport	No	No	Yes	—
<b>Voice and Video Calls</b>					
	Voice	Yes	Yes	Yes	—
	Video	Yes	No	No	—
<b>VoiceXML</b>					
	VXML standard 3.x support	No	Yes	No	—
	VXML with DTMF SIP NOTIFY, RFC 2833	n/a	Yes	Yes	—
	VXML with H.245 alphanumeric H.245 signal, RFC 2833	Yes	Yes	n/a	—

## Cisco Unified Border Element Protocol Features

Table 3 provides an at-a-glance guide to Cisco Unified Border Element Protocol features and the Cisco Border Element Software version the features are introduced.

**Table 3** Cisco UBE Feature List and Software Release Version

Protocol	Feature	Cisco Unified Border Element Software Version
SIP	Session Refresh via REINVITE	Cisco Unified BE 1.1
	SIP Trunk Register	Cisco Unified BE 1.1
	Configurable SIP Listen Port	Cisco Unified BE 1.1
	Delayed Offer to Early Offer — Audio	Cisco Unified BE 1.1
	Delayed Offer to Early Offer — Video	Cisco Unified BE 1.2
	SIP Video support in SDP— Flow-through	Cisco Unified BE 1.1
	SIP Video support in SDP— Flow-around	Cisco Unified BE 1.2



**Table 3** Cisco UBE Feature List and Software Release Version (continued)

Protocol	Feature	Cisco Unified Border Element Software Version
SIP continued	SIP-SIP Call Parameter Changes via REINVITES	Cisco Unified BE 1.2
	Bandwidth per dial-peer (b=AS:xx) support in SDP	Cisco Unified BE 1.2
	SIP Profiles (Header Manipulation)	Cisco Unified BE 1.2
	Map ISDN Facility to SIP INFO	Cisco Unified BE 1.2
	Adjustable Timers for Registration Refresh and Retries	Cisco Unified BE 1.3
	Configurable SIP Parameters via DHCP	Cisco Unified BE 1.3
	Forced Update of SIP Parameters via DHCP	Cisco Unified BE 1.3
	Out-of-dialog OPTIONS Ping to Monitor Dial-peers to Specified SIP Servers and Endpoints	Cisco Unified BE 1.3
	PAID, PPID, Privacy, PCPID, and PAURI Headers on the Cisco Unified Border Element	Cisco Unified BE 1.3
	Preloaded Routes in Outgoing INVITE Messages Based on REGISTER Information	Cisco Unified BE 1.3
	Selective Filtering of Outgoing Provisional Response	Cisco Unified BE 1.3
	Selectively Using sip: URI or tel: URL Formats on Individual SIP Headers	Cisco Unified BE 1.3
	SRTP-RTP Internetworking	Cisco Unified BE 1.3
	Unsupported Content Pass-through	Cisco Unified BE 1.3
H.323	H.235 CryptoToken Passthrough	Cisco Unified BE 1.1
	H.239 Passthrough (PIP)	Cisco Unified BE 1.1
	GK ARQ, RRQ and AAA Security Enhancements	Cisco Unified BE 1.1
	GK LRQ Multicast	Cisco Unified BE 1.1
	GK IZCT Enhancement	Cisco Unified BE 1.2

## Protocol Interworking

Table 4 shows a list of protocol interworking support.

**Table 4** Supported protocol Interworking

Protocol	In Leg	Out Leg	Support
H.323-to-H.323	Fast Start	Fast Start	Bi-Directional
	Slow Start	Slow Start	Bi-Directional
	Fast Start	Slow Start	Bi-Directional
H.323-to-SIP	Fast Start	Early Offer	Bi-Directional
	Slow Start	Delayed Offer	Bi-Directional
SIP-to-SIP	Early Offer	Early Offer	Bi-Directional

**Table 4** Supported protocol Interworking (continued)

Protocol	In Leg	Out Leg	Support
	Delayed Offer	Delayed Offer	Bi-Directional
	Delayed Offer	Early Offer	Uni-Directional

## Billing Features

Table 5 shows a list of supported billing features.

**Table 5** Supported Billing Features

Feature	Supported?	Additional Information
AAA accounting on gateway	Yes	AAA accounting supported on Cisco Unified Border Element. Authentication and authorization supported using available call information (ANI or DNIS) or fixed passwords only. Digit collection for prepaid calling card applications is not supported.
Billing token in unsolicited IRR	Yes	—
Call start time in IRR	Yes	—
Open Settlement Protocol (OSP)	Yes	Cisco Unified Border Element with OSP requires a separate feature license and a separate Cisco IOS image with encryption capabilities.
Per-interface billing	Yes	—

## Application and Tcl Script Features

Table 6 shows a list of supported application and Tcl script features.

**Table 6** Supported Application and Tcl Script Features

Feature	Supported?	Additional Information
IP call leg IVR	Yes	—
Tcl scripts	Yes	—
VXML session application	Yes	—

## Interoperability Features

Table 7 shows a list of supported interoperability features.

**Table 7** Supported Interoperability Features

Feature	Supported?	Additional Information
BroadSoft	Yes	First supported in 12.4(6)T images.
Cisco ATA 186	Yes	—

**Table 7** Supported Interoperability Features

Feature	Supported?	Additional Information
Cisco ATA 188	Yes	First supported in 12.3(7)T images.
Cisco Unified Communications Manager	Yes	—
Cisco CallManager Express	Yes	—
Cisco gateways	Yes	Compatible with H.323 version 2 and above.
Cisco MCM Proxy	Yes	Cannot register proxy in the same zone as an Cisco Unified Border Element.
Third-party gatekeepers	Yes	Third-party gatekeepers must support the equivalent of via-zone functionality.
Third-party gateways	Partially	First supported in 12.3(7)T images.

## IVR Features

Table 8 shows a list of supported IVR features.

**Table 8** Supported IVR Features

Feature	Supported?	Additional Information
TCL IP-IP	Partially	<ul style="list-style-type: none"> <li>TCL Verbs: Yes</li> <li>TDM related: No</li> </ul>
VXML IP-IP	Partially	<ul style="list-style-type: none"> <li>TCL Verbs: Yes</li> <li>TDM related: No</li> </ul>

## Lawful Intercept Support

Lawful Intercept (LI) is the term used to describe the process by which law enforcement agencies conduct electronic surveillance of circuit communications as authorized by judicial or administrative order. Cisco Service Independent Intercept (SII) supports voice and data intercept and intercept requests are initiated by MD using SNMPv3.

Table 9 and Table 10 provide quick reference to platforms and images that support lawful intercept

**Table 9** TDM Gateway Lawful Intercept Support and Related Images

Platform	H.323	SIP	Dial	First Cisco IOS Release	Image
AS5350	Yes	Yes	Yes	12.3(14)T	c5350-ik9su2-mz
AS5400	Yes	Yes	Yes	12.3(14)T	c5400-jk9su2-mz
C2851	Yes	Yes	No	12.4(11)XJ2	c2800nm-adventerprisek9_ivs_li-mz
C3845	Yes	Yes	No	12.4(11)XJ2	c3845-adventerprisek9_ivs_li-mz
C72xx	Yes	Yes	Yes	12.4(6)T	c7200-advipservicesk9_li-mz
C73xx	Yes	Yes	Yes	12.4(6)T	c7300-advipservicesk9_li-mz

**Table 10** Cisco Unified Border Element Gateway Lawful Intercept Support and Related Images

Platform	H.323	SIP	Dial	First Cisco IOS Release	Image
AS5350	Yes	Yes	Yes	12.3(14)T	c5350-ik9su2_ivs-mz
AS5400	Yes	Yes	No	12.3(14)T	c5400_jk9su2_ivs-mz
C2851	Yes	Yes	Yes	12.4(11)XJ2	c2800nm-adventerprisek9_ivs_li-mz
C3825	Yes	Yes	Yes	12.4(15)XY	c3825-adventerprisek9_ivs_li-mz
C3845	Yes	Yes	Yes	12.4(11)XJ2	c3845-adventerprisek9_ivs_li-mz
C72xx	Yes	Yes	Yes	12.4(6)T	c7200-advipservicesk9_li-mz
C73xx	Yes	Yes	Yes	12.4(6)T	c7300-advipservicesk9_li-mz

## QoS Features

Table 11 shows a list of supported quality-of-service (QoS) features.

**Table 11** Supported Quality of Service Features

Feature	Supported?
Class-based weighted fair queueing (LLQ)	Yes
Custom queueing	Yes
Differentiated services code point (DSCP)	Yes
IP precedence	Yes
Link fragmentation and interleaving (LFI)	Yes
Priority-queue weighted fair queueing (PQWFQ)	Yes
RTP header compression	Yes

## Tcl Objects Supported by the Cisco Unified Border Element

The Cisco Unified Border Element supports all current Cisco IOS Tcl functions except those that are required to support IVR as defined: Tone generation

Table 12 through Table 15 list the Tcl commands, information tags, events, and status codes, respectively, that are supported by the Cisco Unified Border Element. Those listed as unsupported may function partially or incorrectly, and therefore their use is not recommended.



### Note

For a complete list of Tcl commands, see the *Tcl IVR API Version 2.0 Programming Guide* at [http://www.cisco.com/en/US/products/sw/voicesw/ps2192/products\\_programming\\_reference\\_guide\\_book09186a00800de1de.html](http://www.cisco.com/en/US/products/sw/voicesw/ps2192/products_programming_reference_guide_book09186a00800de1de.html)

**Table 12** Tcl Commands Supported by the Cisco Unified Border Element

Command	Supported?	Command	Supported?
aaa accounting	Yes	aaa authenticate	Yes
aaa authorize	Yes	call close	Yes
clock	Yes	command terminate	Yes
connection create	Yes	connection destroy	Yes
fsm define	Yes	fsm setstate	Yes
handoff appl	Yes	handoff callappl	Yes
handoff return	Yes	infotag get	Yes
infotag set	Yes	leg collectdigits	Yes
leg connect	Yes	leg disconnect	Yes
leg proceeding	Yes	leg setup	Yes
leg setupack	Yes	leg vxmldialog	No
leg vxmlsend	No	media pause	No
media play	Yes	media resume	No
media seek	No	media stop	No
playtone	Yes	puts	Yes
requiredversion	Yes	set avsend	Yes
set callinfo	Yes	timer left	Yes
timer start	Yes	timer stop	Yes

**Table 13** Tcl Events Supported by the Cisco Unified Border Element

Event	Supported?	Event	Supported?
ev_any_event	Yes	ev_authorize_done	Yes
ev_authenticate_done	Yes	ev_call_timer0	Yes
ev_collectdigits_done	Yes	ev_create_done	Yes
ev_destroy_done	Yes	ev_digit_end	Yes
ev_disconnect_done	Yes	ev_disconnected	Yes
ev_grab	Yes	ev_hookflash	No
ev_handoff	Yes	ev_leg_timer	Yes
ev_media_done	Yes	ev_returned	Yes
ev_setup_done	Yes	ev_setup_indication	Yes
ev_vxmldialog_done	No	ev_vxmlsend_event	No

**Table 14** Tcl Information Tags Supported by the Cisco Unified Border Element

Information Tag	Supported?	Information Tag	Supported?
aaa_avpair	Yes	aaa_avpair_exists	Yes
aaa_new_guid	Yes	cfg_avpair	Yes
cfg_avpair_exists	Yes	con_all	Yes
con_ofleg	Yes	evt_connections	Yes
evt_dcdigits	Yes	evt_digit	Yes
evt_digit_duration	Yes	evt_event	Yes
evt_handoff_string	Yes	evt_iscommand_done	Yes
evt_legs	Yes	evt_status	Yes
evt_vxml_params	No	evt_vxmlelement	No
last_command_handle	Yes	leg_all	Yes
leg_ani	Yes	leg_ani_pi	Yes
leg_ani_si	Yes	leg_cdi_nso	Yes
leg_cdi_rr	Yes	leg_chn_noa	Yes
leg_chn_npi	Yes	leg_chn_num	Yes
leg_cid_cid	Yes	leg_cid_ton	Yes
leg_cnn_noa	Yes	leg_cnn_npi	Yes
leg_cnn_num	Yes	leg_cnn_pi	Yes
leg_cnn_si	Yes	leg_cpc	Yes
leg_dnis	Yes	leg_fdc_dat	Yes
leg_fdc_fname	Yes	leg_fdc_instr	Yes
leg_fdc_param	Yes	leg_gea_cni	Yes
leg_gea_noa	Yes	leg_gea_npi	Yes
leg_gea_num	Yes	leg_gea_pi	Yes
leg_gea_si	Yes	leg_gea_type	Yes
leg_guid	Yes	leg_incoming	Yes
leg_incomming_guid	Yes	leg_inconnection	Yes
leg_isdid	Yes	leg_ocn_noa	Yes
leg_ocn_npi	Yes	leg_ocn_pi	Yes
leg_oli	Yes	leg_outgoing	Yes
leg_password	Yes	leg_pci_dat	Yes
leg_pci_instr	Yes	leg_pci_tri	Yes
leg_rdn_pi	Yes	leg_rdn_si	Yes
leg_redirect_cnt	Yes	leg_redirect_cnt	Yes
leg_remoteipaddress	Yes	leg_rgn_noa	Yes
leg_rgn_npi	Yes	leg_rgn_num	Yes
leg_rgn_pi	Yes	leg_rgn_si	Yes

**Table 14** Tcl Information Tags Supported by the Cisco Unified Border Element (continued)

Information Tag	Supported?	Information Tag	Supported?
leg_rni_orr	Yes	leg_rni_rc	Yes
leg_rni_ri	Yes	leg_rni_rr	Yes
leg_rnn_inn	Yes	leg_rnn_noa	Yes
leg_rnn_npi	Yes	leg_rnn_num	Yes
leg_rnr	Yes	leg_settlement_time	Yes
leg_suppress_outgoing_auto_acct	Yes	leg_tns_cc	Yes
leg_tns_ton	Yes	leg_username	Yes
med_backup_server	No	med_language	No
med_language_map	No	med_location	No
med_total_languages	No	sys_version	Yes

**Table 15** Tcl Status Codes Supported by the Cisco Unified Border Element

Status Code	Supported?	Status Code	Supported?
Authentication Status	Yes	Authorization Status	Yes
Media Status	Yes	Leg Setup Status	Yes
Digit Collection Status	Yes	Disconnect Cause	Yes
VoiceXML Dialog Completion	No		

## 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.

## Where to Go Next

- [Fundamental Cisco Unified Border Element Configuration](#)



## Additional References


The following sections provide additional references related to the Cisco Unified Border Element feature.



### Note

- In addition to the references listed below, each chapter provides additional references related to Cisco Unified Border Element.
- Some of the products and services mentioned in this guide may have reached end of life, end of sale, or both. Details are available at [http://www.cisco.com/en/US/products/prod\\_end\\_of\\_life.html](http://www.cisco.com/en/US/products/prod_end_of_life.html).
- The preface and glossary for the entire voice-configuration library suite of documents is listed below.

## Related Documents

Related Topic	Document Title
Cisco IOS Release 12.4	<ul style="list-style-type: none"> <li>• <a href="#">Cisco IOS Release 12.4 Configuration Guides</a></li> <li>• <a href="#">Cisco IOS Release 12.4T Configuration Guides</a></li> <li>• <a href="#">Cisco IOS Release 12.4 Command References</a></li> <li>• <a href="#">Cisco IOS Voice Configuration Library</a> <a href="http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/cisco_ios_voice_configuration_library_glossary/vcl.htm">http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/cisco_ios_voice_configuration_library_glossary/vcl.htm</a></li> </ul>  <p><b>Note</b> This website contains the library preface and glossary.</p>
Cisco IOS Release 12.3	<ul style="list-style-type: none"> <li>• <a href="#">Cisco IOS Release 12.3 documentation</a></li> <li>• <a href="#">Cisco IOS voice commands</a></li> <li>• <a href="#">Cisco IOS Voice Troubleshooting and Monitoring Guide</a></li> <li>• <a href="#">Tel IVR Version 2.0 Programming Guide</a></li> </ul>
Cisco IOS Release 12.2	<ul style="list-style-type: none"> <li>• <i>Cisco IOS Voice, Video, and Fax Configuration Guide</i>, Release 12.2 at <a href="http://www.cisco.com/en/US/docs/ios/12_2/voice/configuration/guide/fvfax_c.html">http://www.cisco.com/en/US/docs/ios/12_2/voice/configuration/guide/fvfax_c.html</a></li> </ul>
DSP documentation	<p>High-Density Packet Voice Feature Card for Cisco AS5350XM and AS5400XM Universal Gateways</p> <p><a href="http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124lmit/124x/124xc4/vfc_dsp.htm">http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124lmit/124x/124xc4/vfc_dsp.htm</a></p>
GKTMP (GK API) Documents	<ul style="list-style-type: none"> <li>• <i>GKTMP Command Reference</i>: <a href="http://www.cisco.com/en/US/docs/ios/12_2/gktmp/gktmpv4_2/gk_cli.htm">http://www.cisco.com/en/US/docs/ios/12_2/gktmp/gktmpv4_2/gk_cli.htm</a></li> <li>• <i>GKTMP Messages</i>: <a href="http://www.cisco.com/en/US/docs/ios/12_2/gktmp/gktmpv4_2/gk_tmp.html">http://www.cisco.com/en/US/docs/ios/12_2/gktmp/gktmpv4_2/gk_tmp.html</a></li> </ul>

Related Topic	Document Title
internet Low Bitrate Codec (iLBC) Documents	<ul style="list-style-type: none"> <li>• Codecs section of the Dial Peer Configuration on Voice Gateway Routers Guide <a href="http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/int_c/dpeer_c/dp_ovrvw.htm#1035124">http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/int_c/dpeer_c/dp_ovrvw.htm#1035124</a></li> <li>• Dial Peer Features and Configuration section of the Dial Peer Configuration on Voice Gateway Routers Guide <a href="http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/int_c/dpeer_c/dp_config.htm">http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/int_c/dpeer_c/dp_config.htm</a></li> </ul>
Cisco Unified Border Element Configuration Examples	<ul style="list-style-type: none"> <li>• Local-to-remote network using the IPIPGW <a href="http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a00801b0803.shtml">http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a00801b0803.shtml</a></li> <li>• Remote-to-local network using the IPIPGW: <a href="http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a0080203edc.shtml">http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a0080203edc.shtml</a></li> <li>• Remote-to-remote network using the IPIPGW: <a href="http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a0080203edd.shtml">http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a0080203edd.shtml</a></li> <li>• Remote-to-remote network using two IPIPGWs: <a href="http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a0080203edb.shtml">http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a0080203edb.shtml</a></li> <li>• <i>Cisco Unified Border Element SIP TLS Configuration Example</i></li> <li>• <i>Cisco Unified Border Element Transcoding Configuration Example</i></li> </ul>
Related Application Guides	<ul style="list-style-type: none"> <li>• Cisco Unified Communications Manager and Cisco IOS Interoperability Guide</li> <li>• Cisco IOS Fax, Modem, and Text Support over IP Configuration Guide</li> <li>• “Configuring T.38 Fax Relay” chapter</li> <li>• Cisco IOS SIP Configuration Guide</li> <li>• Cisco Unified Communications Manager (CallManager) Programming Guides at: <a href="http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_programming_reference_guides_list.html">http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_programming_reference_guides_list.html</a></li> <li>• <i>Quality of Service for Voice over IP</i> at <a href="http://www.cisco.com/en/US/docs/ios/solutions_docs/qos_solutions/QoSVoIP/QoSVoIP.html">http://www.cisco.com/en/US/docs/ios/solutions_docs/qos_solutions/QoSVoIP/QoSVoIP.html</a></li> </ul>
Related Platform Documents	<ul style="list-style-type: none"> <li>• Cisco 2600 Series Multiservice Platforms</li> <li>• Cisco 2800 Series Integrated Services Routers</li> <li>• Cisco 3600 Series Multiservice Platforms</li> <li>• Cisco 3700 Series Multiservice Access Routers</li> <li>• Cisco 3800 Series Integrated Services Routers</li> <li>• Cisco 7200 Series Routers</li> <li>• Cisco 7301</li> </ul>

Related Topic	Document Title
Related gateway configuration documentation	Media and Signaling Authentication and Encryption Feature for Cisco IOS H.323 Gateways. <a href="http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/htsecure.htm">http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/htsecure.htm</a>
Cisco IOS NAT Configuration Guide, Release 12.4T	<ul style="list-style-type: none"> <li>• <i>Configuring Cisco IOS Hosted NAT Traversal for Session Border Controller</i> <a href="http://www.cisco.com/en/US/docs/ios/12_4t/ip_addr/configuration/guide/htnatsbc.html">http://www.cisco.com/en/US/docs/ios/12_4t/ip_addr/configuration/guide/htnatsbc.html</a></li> </ul>
Troubleshooting and Debugging guides	<ul style="list-style-type: none"> <li>• Cisco IOS Debug Command Reference, Release 12.4 at <a href="http://www.cisco.com/en/US/docs/ios/debug/command/reference/db_book.html">http://www.cisco.com/en/US/docs/ios/debug/command/reference/db_book.html</a></li> <li>• <i>Troubleshooting and Debugging VoIP Call Basics</i> at <a href="http://www.cisco.com/en/US/tech/tk1077/technologies_tech_note09186a0080094045.shtml">http://www.cisco.com/en/US/tech/tk1077/technologies_tech_note09186a0080094045.shtml</a></li> <li>• <i>VoIP Debug Commands</i> at <a href="http://www.cisco.com/en/US/docs/routers/access/1700/1750/software/configuration/guide/debug.html">http://www.cisco.com/en/US/docs/routers/access/1700/1750/software/configuration/guide/debug.html</a></li> </ul>

## Standards

Standards	Title
H.323 Version 4 and earlier	<i>H.323 (ITU-T VOIP protocols)</i>

## MIBs

MIBs	MIBs Link
IP-TAP-MIB	Provisioning the IP intercept.
TAP2-MIB	Provisioning gateway with mediation device info.
USER-CONNECTION-TAP-MIB	Mediation device automatically provisions the intercepts when the target call is setup and removes the intercept when the target call is disconnected.

## RFCs

RFCs	Title
RFC 1889	<i>RTP: A Transport Protocol for Real-Time Applications</i>
RFC 2131	<i>Dynamic Host Configuration Protocol</i>
RFC 2132	<i>DHCP Options and BOOTP Vendor Extensions</i>
RFC 2833	<i>RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals</i>
RFC 3203	<i>DHCP reconfigure extension</i>

<b>RFCs</b>	<b>Title</b>
RFC 3261	<i>SIP: Session Initiation Protocol</i>
RFC 3262	<i>Reliability of Provisional Responses in Session Initiation Protocol (SIP)</i>
RFC 3323	<i>A Privacy Mechanism for the Session Initiation Protocol (SIP)</i>
RFC 3325	<i>Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks</i>
RFC 3361	<i>Dynamic Host Configuration Protocol (DHCP-for-IPv4) Option for Session Initiation Protocol (SIP) Servers</i>
RFC 3455	<i>Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)</i>
RFC 3608	<i>Session Initiation Protocol (SIP) Extension Header Field for Service Route Discovery During Registration</i>
RFC 3711	<i>The Secure Real-time Transport Protocol (SRTP)</i>
RFC 3925	<i>Vendor-Identifying Vendor Options for Dynamic Host Configuration Protocol version 4 (DHCPv4)</i>

## 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><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></p>

# Feature Information for Cisco Unified Border Element Configuration Guide

Table 16 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.2(13)T3 or a later release appear in the table.


**Note**

Table 16 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 16** Feature Information for Cisco Unified Border Element Overview

Feature Name	Release	Feature Information
ATA-188 Interoperability	12.3(7)T	This feature was introduced.
Cisco UBE Image Consolidation	12.3(7)T	This feature was introduced.
H.323 Video Calls Support for H.235 Security	12.4(15)XY	This feature was introduced.
H.323 Video Calls Support for H.239 Signaling	12.4(15)XY	This feature was introduced.
Interworking of Secure RTP calls for SIP and H.323	12.4(15)XY	This feature was introduced.
Lawful Intercept	12.4(6)T 12.4(11)XJ2 12.4(15)XY	12.3(14)T—Support for lawful intercept was introduced on the Cisco AS5350 and Cisco AS5400  12.4(6)T—Support was added for the Cisco 7200 and Cisco 7300.  12.4(11)XJ2—Support was added for the Cisco 2851 and Cisco 3845.  12.4(15)XY—Support was added for the Cisco 3825.
Support for Cisco 7200 and Cisco 7301	12.3(8)T	This feature was introduced.
Support for the Cisco 2801	12.4(4)T	This feature was introduced.
Support for the Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3825, and Cisco 3845	12.3(11)T	This feature was introduced.

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.

© 2009 Cisco Systems, Inc. All rights reserved.







# Cisco Unified Border Element Features Roadmap

---

**Revised: February 27, 2009**  
**First Published: March 18, 2005**  
**Last Updated: February 27, 2009**

This roadmap lists the features documented in the *Cisco Unified Border Element Configuration guide* (previously known as the *Cisco Multiservice IP-to-IP Gateway Application Guide*) and maps them to the chapters in which they appear.

## Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

**Table 1** lists Cisco Unified Border Element feature support for the following Cisco IOS software release trains:

- Cisco IOS Releases 12.2T, 12.3, 12.3T, 12.4, and 12.4T

Only features that were introduced or modified in Cisco IOS Release Cisco IOS Releases 12.2(13)T or later or a later release appear in the table.

## Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS 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.



**Note**

---

**Table 1** lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

---



---

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

© 2009 Cisco Systems, Inc. All rights reserved.

**Table 1** Supported Cisco Unified Border Element Configuration Guide Features

Release	Feature Name	Feature Description	Where Documented
<b>Cisco IOS Releases 12.2T, 12.3, 12.3T, 12.4, and 12.4T</b>			
12.4(24)T	SIP Registration Message	Provides the ability to send a SIP Registration Message from Cisco Unified Border Element using the <b>credentials</b> command.	<a href="#">“Configuring Cisco Unified Border Element for Unsupported Content Pass-through”</a> in the <a href="#">“SIP-to-SIP Connections on a Cisco Unified Border Element”</a> Chapter of this guide.
12.4(22)YB	Selective Filtering of Outgoing Provisional Response on the Cisco Unified Border Element	Supports selective filtering of outgoing provisional responses, including 180 - Alerting, and 183-Session In Progress responses. Selective filtering can be further based on the availability of media information in the received provisional response.	<a href="#">“Configuring Selective Filtering of Outgoing Provisional Response on the Cisco Unified Border Element”</a> in the <a href="#">“SIP-to-SIP Connections on a Cisco Unified Border Element”</a> Chapter of this guide.
	Unsupported Content Pass-through	The feature introduces the ability to configure the Cisco UBE to pass through end to end headers at a global or dial-peer level, that are not processed or understood in a SIP trunk to SIP trunk scenario. The pass through functionality includes all or only a configured list of unsupported or non-mandatory SIP headers, and all unsupported content/MIME types.	<a href="#">“Configuring Cisco Unified Border Element for Unsupported Content Pass-through”</a> in the <a href="#">“SIP-to-SIP Connections on a Cisco Unified Border Element”</a> Chapter of this guide.
12.4(22)YB continued	Adjustable Timers for Registration Refresh and Retries	This feature provides the ability for IOS software to: <ul style="list-style-type: none"> <li>Refresh the REGISTER at a configurable fraction of the expiry timer .</li> <li>Retransmit REGISTER upon failure responses per the min-expires value in a “423 interval too brief” response, or retry-after if present and terminal re-registration interval if retry-after value is absent in 4xx/5xx/6xx responses.</li> <li>Retransmit REGISTER per Timer E up to 32 seconds, and at a user defined random interval thereafter.</li> </ul>	<a href="#">“Configuring Adjustable Timers for Registration Refresh and Retries”</a> in the <a href="#">“SIP-to-SIP Connections on a Cisco Unified Border Element”</a> Chapter of this guide.
	Cisco Unified Border Element Support for SRTP-RTP Internetworking	This feature allows secure enterprise-to-enterprise calls. Support for SRTP-RTP internetworking between one or multiple Cisco Unified Border Elements is enabled for SIP-SIP audio calls.	<a href="#">“Cisco Unified Border Element Support for SRTP-RTP Internetworking”</a> in the <a href="#">“SIP-to-SIP Connections on a Cisco Unified Border Element”</a> Chapter of this guide

**Table 1 Supported Cisco Unified Border Element Configuration Guide Features (continued)**

Release	Feature Name	Feature Description	Where Documented
12.4(22)YB continued	Configurable SIP Parameters via DHCP	The Configurable SIP Parameters via DHCP feature introduces the configuring of SIP parameters via DHCP.	<a href="#">“Configurable SIP Parameters via DHCP”</a> in the <a href="#">“SIP-to-SIP Connections on a Cisco Unified Border Element”</a> Chapter of this guide.
	Forced Update to SIP Parameters via DHCP updated in FTS.	The Configurable SIP Parameters via DHCP feature introduces the configuring of SIP parameters via DHCP.  The following sections provide information about this feature:	<a href="#">“Enabling Forced Update of SIP Parameters via DHCP”</a> in the <a href="#">“SIP-to-SIP Connections on a Cisco Unified Border Element”</a> Chapter of this guide.
	Out-of-dialog OPTIONS Ping to Monitor Dial-peers to Specified SIP Servers and Endpoints	This feature provides a keepalive mechanism at the SIP level between any number of destinations. The generic heartbeat mechanism allows Cisco UBE to monitor the status of SIP servers or endpoints and provide the option of busying-out associated dial-peer upon total heartbeat failure.	<a href="#">“Configuring Cisco UBE Out-of-dialog OPTIONS Ping for Specified SIP Servers or Endpoints”</a> in the <a href="#">“SIP-to-SIP Connections on a Cisco Unified Border Element”</a> Chapter of this guide.
	Preloaded Routes in Outgoing INVITE Messages Based on REGISTER Information	This feature supports the use of preloaded routes for outgoing INVITE messages. The system routes INVITE messages based on REGISTER message information, such as the path: and Service-Route values	<a href="#">“Support for Preloaded Routes in Outgoing INVITE Messages Based on REGISTER Information”</a> in the <a href="#">“SIP-to-SIP Connections on a Cisco Unified Border Element”</a> Chapter of this guide.
	Selectively Using sip: URI or tel: URL Formats on Individual SIP Headers	This feature supports the construction of request URIs in tel: format. The system supports this format for both the To: header and the Request-Line. The system also supports appending the phone-context to the tel: URL.	<a href="#">“Selectively Using sip: URI or tel: URL Formats on Individual SIP Headers”</a> in the <a href="#">“SIP-to-SIP Connections on a Cisco Unified Border Element”</a> Chapter of this guide.
	Support for PAID, PPID, Privacy, PCPID, and PAURI Headers on the Cisco Unified Border Element	This feature provides the ability to: <ul style="list-style-type: none"> <li>Translate P-headers from one type to another.</li> <li>configure the privacy header and the use of the PCPID header to route INVITE messages.</li> <li>Supports multiple PAURI headers in the response messages (200 OK) it receives to REGISTER messages.</li> </ul>	<a href="#">“Support for PAID, PPID, Privacy, PCPID, and PAURI Headers on the Cisco Unified Border Element”</a> in the <a href="#">“SIP-to-SIP Connections on a Cisco Unified Border Element”</a> Chapter of this guide.

**Table 1** Supported Cisco Unified Border Element Configuration Guide Features (continued)

Release	Feature Name	Feature Description	Where Documented
12.4(20)T1	Delayed offer to Early offer for SIP Video Calls	Forces a Cisco Unified Border Element to send a SIP invite with Early-Offer (EO) on the Out-Leg (OL).	“Configuring Delayed-Offer to Early-Offer for SIP Video Calls” in the “Configuring Cisco Unified Border Element Videoconferencing” Chapter of this guide
12.4(20)T	Configurable SIP Listening Port	Allows users the ability to configure the port that SIP messages are listened on.	“Configuring SIP Listening Port” in the “SIP-to-SIP Connections on a Cisco Unified Border Element” Chapter of this guide
	Configuring Bandwidth Parameters for SIP Calls	This features provides the ability to manually configure the bandwidth that is signaled in the outbound SIP invite.	“Configuring Bandwidth Parameters for SIP Calls” in the “SIP-to-SIP Connections on a Cisco Unified Border Element” Chapter of this guide
	Product Authorization Key (PAK)	Requires users to register products and activate a Product Authorization Key (PAK) before starting the configuration process.  <b>Note</b> Register Products and activate your PAK at the following URL <a href="http://www.cisco.com/go/license">http://www.cisco.com/go/license</a> .	—
	H.323 Calling Name Display	Provides a configurable option on the Cisco Gateway to send and interpret the calling name information received in Q931 Facility messages so that the Cisco Unified Communications Manager can display the calling name on the Cisco IP Phones.	“Configuring H.323 Calling Name Display” in the “Cisco Unified Border Element for H.323 Cisco Unified Communications Manager to H.323 Service Provider Connectivity” Chapter of this guide

**Table 1** Supported Cisco Unified Border Element Configuration Guide Features (continued)

Release	Feature Name	Feature Description	Where Documented
	Session Border Controller Enhancements for H.323-to-SIP and SIP-to-SIP Supplementary Services, Transcoding Optimization and Firewall Integration.	<p>New H.323-to-SIP features offered in this release include:</p> <ul style="list-style-type: none"> <li>Supplementary Services specifically mapping ECS to ReINVITE and ECS to REFER on the Cisco IOS SBC.</li> </ul> <p>New SIP-to-SIP features offered in this release include:</p> <ul style="list-style-type: none"> <li>Supplementary Services mapping ReINVITE to ReINVITE are on the Cisco IOS SBC.</li> </ul> <p>New features offered in this release include:</p> <ul style="list-style-type: none"> <li>Also available are enhancements in Transcoding Performance and support for Universal Transcoding Support</li> <li>RAS message enhancements</li> </ul>	<p>“Overview of Cisco Unified Border Element”, “H.323-to-SIP Connections on a Cisco Unified Border Element”, and “SIP-to-SIP Connections on a Cisco Unified Border Element” chapters of this guide</p>
	Session Refresh with reinvites	This feature expands the ability of the Cisco Unified BE to receive a REINVITE that contains either a session refresh parameter or a change in media via a new SDP and ensure the session does not time out.	<p>“Configuring Support for Session Refresh with Reinvites” in the “SIP-to-SIP Connections on a Cisco Unified Border Element” Chapter of this guide</p>
	SIP Video Calls with Flow Around Media	Allows SIP video calls where the media flows around the Cisco Unified Border Element.	<p>“SIP-to-SIP Connections on a Cisco Unified Border Element” Chapter of this guide</p>
12.4(15)XZ	Configurable SIP Parameters	Allows users to change the standard SIP messages sent from the Cisco SIP stack for better interworking with different SIP entities.	<p>“Configuring SIP Parameters” in the “SIP-to-SIP Connections on a Cisco Unified Border Element” Chapter of this guide</p>
	Product Authorization Key (PAK)	<p>Requires users to register products and activate a Product Authorization Key (PAK) before starting the configuration process.</p> <p><b>Note</b> Register Products and activate your PAK at the following URL <a href="http://www.cisco.com/go/license">http://www.cisco.com/go/license</a>.</p>	—
	Configurable SIP Listening Port	Allows users the ability to configure the port that SIP messages are listened on.	<p>“Configuring SIP Listening Port” in the “SIP-to-SIP Connections on a Cisco Unified Border Element” Chapter of this guide</p>

**Table 1** Supported Cisco Unified Border Element Configuration Guide Features (continued)

Release	Feature Name	Feature Description	Where Documented
12.4(15)XZ continued	Configuring Bandwidth Parameters for SIP Calls	This feature provides the ability to manually configure the bandwidth that is signaled in the outbound SIP invite.	<a href="#">“Configuring Bandwidth Parameters for SIP Calls”</a> in the <a href="#">“SIP-to-SIP Connections on a Cisco Unified Border Element”</a> Chapter of this guide
	Session Refresh with reinvites	This feature expands the ability of the Cisco Unified BE to receive a REINVITE that contains either a session refresh parameter or a change in media via a new SDP and ensure the session does not time out.	<a href="#">“Configuring Support for Session Refresh with Reinvites”</a> in the <a href="#">“SIP-to-SIP Connections on a Cisco Unified Border Element”</a> Chapter of this guide
	Delayed offer to Early offer for SIP Video Calls	Forces a Cisco Unified Border Element to send a SIP invite with Early-Offer (EO) on the Out-Leg (OL).	<a href="#">“Configuring Delayed-Offer to Early-Offer for SIP Video Calls”</a> in the <a href="#">“Configuring Cisco Unified Border Element Videoconferencing”</a> Chapter of this guide
	Session Border Controller Enhancements for H.323-to-SIP and SIP-to-SIP Supplementary Services, Transcoding Optimization and Firewall Integration.	<p>New H.323-to-SIP features offered in this release include:</p> <ul style="list-style-type: none"> <li>Supplementary Services specifically mapping ECS to ReINVITE and ECS to REFER on the Cisco IOS SBC.</li> </ul> <p>New SIP-to-SIP features offered in this release include:</p> <ul style="list-style-type: none"> <li>Supplementary Services mapping ReINVITE to ReINVITE are on the Cisco IOS SBC.</li> </ul> <p>New features offered in this release include:</p> <ul style="list-style-type: none"> <li>Also available are enhancements in Transcoding Performance and support for Universal Transcoding Support</li> <li>RAS message enhancements</li> </ul>	<a href="#">“Overview of Cisco Unified Border Element”</a> , <a href="#">“H.323-to-SIP Connections on a Cisco Unified Border Element”</a> , and <a href="#">“SIP-to-SIP Connections on a Cisco Unified Border Element”</a> chapters of this guide
	Ability to Send a SIP Registration Message on a Cisco Unified Border Element	This feature introduces a new command that allows the Cisco Unified Border Element to send a REGISTRATION command to a SIP REGISTRAR.	<a href="#">“Configuring SIP Listening Port”</a> in the <a href="#">“SIP-to-SIP Connections on a Cisco Unified Border Element”</a> Chapter of this guide
12.4(15)XY	—	The official marketing name of Cisco Multiservice IP-to-IP Gateway was changed to Cisco Unified Border Element (Cisco UBE).	—

**Table 1** Supported Cisco Unified Border Element Configuration Guide Features (continued)

Release	Feature Name	Feature Description	Where Documented
<b>12.4(15)XY</b> continued	Interworking of Secure RTP calls for SIP and H323	New features offered in this release include: <ul style="list-style-type: none"> <li>• CUCM SIP Trunks</li> </ul>	<a href="#">“Overview of Cisco Unified Border Element”</a>
	H.323 Video Calls Support for H.239 Signalling	New features offered in this release include: <ul style="list-style-type: none"> <li>• Business to Business Telepresence calls</li> </ul>	<a href="#">“Overview of Cisco Unified Border Element”</a>
	H323 Video Calls Support for H.235 Security	New features offered in this release include: <ul style="list-style-type: none"> <li>• Enhanced Security for France Telecom and Video calls to 3rd party endpoints.</li> </ul>	<a href="#">“Overview of Cisco Unified Border Element”</a>
	Delayed offer to Early offer for SIP Audio Calls	Forces a Cisco Unified Border Element to send a SIP invite with Early-Offer (EO) on the Out-Leg (OL).	<a href="#">“Configuring Delayed-Offer to Early-Offer for SIP Audio Calls”</a> in the <a href="#">“SIP-to-SIP Connections on a Cisco Unified Border Element”</a> Chapter of this guide
	Lawful Intercept for Cisco 3825	Adds Lawful Intercept support on the Cisco 3825.	<a href="#">“Overview of Cisco Unified Border Element”</a> Chapter of this guide.
<b>12.4(11)XW</b>	H.323 Calling Name Display	Provides a configurable option on the Cisco Gateway to send and interpret the calling name information received in Q931 Facility messages so that the Cisco Unified Communications Manager can display the calling name on the Cisco IP Phones.	<a href="#">“Configuring H.323 Calling Name Display”</a> in the <a href="#">“Cisco Unified Border Element for H.323 Cisco Unified Communications Manager to H.323 Service Provider Connectivity”</a> Chapter of this guide

Table 1 Supported Cisco Unified Border Element Configuration Guide Features (continued)

Release	Feature Name	Feature Description	Where Documented
12.4(11)XJ2	Enhanced Hosted NAT Traversal and IP Call Leg Statistics for Session Border Controller (SBC)	<p>Provides enhanced termination and re-origination of signaling and media between VoIP and Video Networks in conformance with RFC3261.</p> <p>New features offered in this release include:</p> <ul style="list-style-type: none"> <li>• Lawful Intercept for 2851 and 3845</li> <li>• DTMF Transcoding and Interworking: <ul style="list-style-type: none"> <li>– Transcoding with AS5xxx platforms</li> </ul> </li> </ul> <p>New H.323-to-H.323 features offered in this release on the Cisco 28xx, 38xx, 5350XM and 5400XM include:</p> <ul style="list-style-type: none"> <li>• Media Statistics on an Cisco Unified Border Element</li> </ul> <p>New H.323-to-SIP features offered in this release on the Cisco 28xx, 38xx, 5350XM and 5400XM include:</p> <ul style="list-style-type: none"> <li>• Media Statistics on a Cisco UBE</li> <li>• H323 to SIP Codec Transparent Support</li> <li>• SIP to H323 Interworking</li> <li>• DTMF Transcoding and Interworking: <ul style="list-style-type: none"> <li>– H245 to KPML</li> </ul> </li> </ul> <p>New SIP-to-SIP features offered in this release on the Cisco 28xx, 38xx, 5350XM and 5400XM include:</p> <ul style="list-style-type: none"> <li>• Media Statistics on an Cisco UBE</li> <li>• SIP Error Message Pass Through</li> <li>• DTMF Transcoding and Interworking: <ul style="list-style-type: none"> <li>– SIP to KPML</li> </ul> </li> </ul>	<p>“<a href="#">Overview of Cisco Unified Border Element</a>”, “<a href="#">H.323-to-H.323 Connections on a Cisco Unified Border Element</a>”, “<a href="#">H.323-to-SIP Connections on a Cisco Unified Border Element</a>”, “<a href="#">SIP-to-SIP Connections on a Cisco Unified Border Element</a>” chapters of this guide</p>
12.4(11)T	H.323-to-SIP Supplementary Feature Interworking for Session Border Controller (SBC)	<p>New H.323-to-H.323 features offered in this release include:</p> <ul style="list-style-type: none"> <li>• G.711 Inband DTMF to RFC 2833</li> <li>• iLBC Codec Support</li> </ul> <p>New H.323-to-SIP features offered in this release include:</p> <ul style="list-style-type: none"> <li>• H.323 RFC 2833 to SIP NOTIFY</li> <li>• iLBC Codec Support</li> <li>• VXML support with SIP NOTIFY DTMF</li> <li>• TCL IVR support with SIP NOTIFY DTMF</li> </ul> <p>New SIP-to-SIP features offered in this release include:</p> <ul style="list-style-type: none"> <li>• iLBC Codec</li> <li>• Session refresh</li> </ul>	<p>“<a href="#">Fundamental Cisco Unified Border Element Configuration</a>”, “<a href="#">H.323-to-H.323 Connections on a Cisco Unified Border Element</a>”, “<a href="#">H.323-to-SIP Connections on a Cisco Unified Border Element</a>”, “<a href="#">SIP-to-SIP Connections on a Cisco Unified Border Element</a>” chapters of this guide</p>



**Table 1 Supported Cisco Unified Border Element Configuration Guide Features (continued)**

Release	Feature Name	Feature Description	Where Documented
	DTMF Relay Digit-Drop on an Cisco Unified Border Element with Cisco Unified Communications Manager	This feature passes DTMF tones out-of-band and drops in-band digits to avoid sending both tones to the outgoing leg on an H.323-to-SIP Cisco UBE.	“Cisco Unified Border Element for H.323 Cisco Unified Communications Manager to H.323 Service Provider Connectivity” chapter of this guide.
12.4(6)XE	H.323-to-SIP Supplementary Feature Interworking for Session Border Controller (SBC)	<p>New H.323-to-SIP features available include:</p> <ul style="list-style-type: none"> <li>• Support H.323-to-SIP Supplementary services for Cisco Unified Communications Manager with MTP on the H.323 Trunk.</li> <li>• G.711 Inband DTMF to RFC 2833</li> <li>• VXML 3.x support</li> <li>• VXML support with SIP Notify</li> </ul> <p>New SIP-to-SIP features offered in this release include:</p> <ul style="list-style-type: none"> <li>• G.711 Inband DTMF to RFC 2833</li> </ul>	“H.323-to-SIP Connections on a Cisco Unified Border Element” and “SIP-to-SIP Connections on a Cisco Unified Border Element” chapters of this guide
12.4(9)T	GSMAMR-NB Codec support on a Cisco Unified Border Element	Support for the complexity multimode codec that supports eight narrowband speech encoding modes with bit rates between 4.75 and 12.2 kbps.	“Fundamental Cisco Unified Border Element Configuration”, chapter of this guide
	SIP-to-SIP Supplementary Services for Session Border Controller (SBC)	<p>New SIP-to-SIP features available include:</p> <ul style="list-style-type: none"> <li>• SIP-to-SIP supplementary services using Refer</li> <li>• Hosted NAT Traversal for SIP</li> <li>• Provides integrated voice and video services on the Cisco AS5350XM and Cisco AS5400XM.</li> </ul>	“SIP-to-SIP Connections on a Cisco Unified Border Element” chapter of this guide
	—	<p>The Gatekeeper content from the Cisco Multiservice IP-to-IP Gateway Application guide was moved to a separate book located at the following</p> <p><a href="http://cisco.com/en/US/docs/ios/voice/cubegk/configuration/guide/ve_book/ve_book.html">http://cisco.com/en/US/docs/ios/voice/cubegk/configuration/guide/ve_book/ve_book.html</a></p>	<i>Cisco Multiservice IP-to-IP Gateway with Gatekeeper Application Guide</i>

**Table 1 Supported Cisco Unified Border Element Configuration Guide Features (continued)**

Release	Feature Name	Feature Description	Where Documented
12.4(6)T	SIP-to-SIP Extended Feature Functionality for Session Border Controller (SBC)	Enables the SIP-to-SIP functionality to conform with RFC 3261 to interoperate with SIP UAs. New SIP-to-SIP features available include: <ul style="list-style-type: none"> <li>• Call Admission Control (based on CPU, memory, total calls)</li> <li>• Delayed Media Call</li> <li>• Media Inactivity</li> <li>• Modem passthrough</li> <li>• TCP and UDP interworking</li> <li>• Tcl scripts with SIP NOTIFY VoiceXML with SIP-to-SIP</li> <li>• Transport Layer Security (TLS)</li> <li>• ENUM support</li> <li>• Lawful Intercept</li> <li>• Interoperability with Cisco Unified Communications Manager 5.0 and BroadSoft</li> </ul>	<a href="#">“SIP-to-SIP Connections on a Cisco Unified Border Element”</a> chapter of this guide
	H.323-to-SIP Extended Call Interworking for Session Border Controller (SBC)	New H.323-to-SIP features available include: <ul style="list-style-type: none"> <li>• Call Admission Control (based on CPU, memory, total calls)</li> </ul>	<a href="#">“H.323-to-SIP Connections on a Cisco Unified Border Element”</a> chapter of this guide
	H.323-to-H.323 Extended Call Interworking for Session Border Controller (SBC)	New H.323-to-H.323 features available include: <ul style="list-style-type: none"> <li>• Secure RTP with IPSEC for Signaling</li> <li>• No MTP for Cisco Unified Communications Manager Trunks to Cisco UBE</li> <li>• Call Admission Control (based on CPU, memory, total calls)</li> </ul>	<a href="#">“H.323-to-H.323 Connections on a Cisco Unified Border Element”</a> chapter of this guide
12.4(4)T	Interoperability Enhancements to the Cisco Unified Border Element	Enables operation of Cisco Unified Border Element features concurrently on the same router with H.323 gatekeeper and TDM-IP voice-gateway features.	<a href="#">“Fundamental Cisco Unified Border Element Configuration”</a> chapter of this guide
	SIP-to-H.323 Extended Call Interworking for Session Border Controller (SBC)	Enables the Cisco UBE to bridge calls between networks that support different VoIP call-signaling protocols (SIP and H.323).	<a href="#">“H.323-to-SIP Connections on a Cisco Unified Border Element”</a> chapter of this guide
	SIP-to-SIP Basic Functionality for Session Border Controller (SBC)	Enables the Cisco UBE to bridge calls between SIP networks.	<a href="#">“SIP-to-SIP Connections on a Cisco Unified Border Element”</a> chapter of this guide
	Support for Cisco UBE and Gatekeeper Features on the Cisco 2801	Provides integrated voice and video services on the Cisco 2801.	<a href="#">“Fundamental Cisco Unified Border Element Configuration”</a> chapter of this guide

**Table 1** Supported Cisco Unified Border Element Configuration Guide Features (continued)

Release	Feature Name	Feature Description	Where Documented
12.3(11)T	Scalability Enhancements for the Cisco 7301 + 7200 NPE-G1 (Extended Socket Boundary)	Increases the call capacity of the Cisco UBE by extending the total number of sockets supported on the Cisco 7301 and Cisco 7200 NPE-G1 routers.	Integrated into Cisco IOS software. No configuration is required.
	Support for Cisco Unified Border Element and Gatekeeper Features on the Cisco 2800 Series and Cisco 3800 Series	Provides integrated voice and video services on the Cisco 2800 series and Cisco 3800 series.	<a href="#">“Fundamental Cisco Unified Border Element Configuration”</a> and chapter of this guide (see also <a href="#">Table 1</a> in the <a href="#">Overview of Cisco Unified Border Element</a> chapter in this guide)
	SIP-to-H.323 Basic Call Interworking for Session Border Controller (SBC)	Enables the Cisco Unified Border Element to bridge calls between networks that support different VoIP call-signaling protocols (SIP and H.323).	<a href="#">“H.323-to-SIP Connections on a Cisco Unified Border Element”</a> chapter of this guide
	SIP-to-H.323 Dual Tone Multifrequency Relay Digit-Drop	Passes DTMF tones out-of-band and drops in-band digits to avoid sending both tones to the outgoing leg on H.323-to-SIP Cisco UBE.	<a href="#">“H.323-to-SIP Connections on a Cisco Unified Border Element”</a> chapter of this guide
	Call Failure Recovery (Rotary) on the Cisco Unified Border Element	Eliminates codec restrictions and enables the Cisco UBE to restart codec negotiation with the originating endpoint based on the codec capabilities of the next dial peer in the rotary group for H.323-to-H.323 interconnections.	<a href="#">“H.323-to-H.323 Connections on a Cisco Unified Border Element”</a> chapter of this guide
	H.323-to-H.323 Interworking Between FastStart and Normal H.245 Signaling	Enables the Cisco UBE to bridge calls between VoIP endpoints that support only H.323 FastStart procedures and endpoints that support only normal H.245 signaling (SlowStart).	<a href="#">“H.323-to-H.323 Connections on a Cisco Unified Border Element”</a> chapter of this guide
	Transcoding G.711-G.729	Supports transcoding (compression and decompression of voice streams to match endpoint-device capabilities) between G.711 and G.729 codecs when the router chassis is equipped with DSP resources (H.323-H.323 and H.323-SIP).	<a href="#">“Fundamental Cisco Unified Border Element Configuration”</a> chapter of this guide
12.3(7)T	Interoperability Enhancements to the Cisco Unified Border Element	Enables operation of Cisco UBE features concurrently on the same router with H.323 gatekeeper and TDM-IP voice-gateway features. Supports interoperability with the Cisco ATA-188 and with Microsoft NetMeeting.	<a href="#">“Fundamental Cisco Unified Border Element Configuration”</a> chapter of this guide
12.3(4)T	Videoconferencing for the Cisco Unified Border Element Feature	Adds video capabilities and improved QoS, allowing increased scalability and control for IP telephony and IP videoconferencing networks.	<a href="#">“Configuring Cisco Unified Border Element Videoconferencing”</a> chapter of this guide
12.3(1)	Cisco Unified Border Element for H.323 Cisco Unified Communications Manager to H.323 Service Provider Connectivity	Provides interoperability with Cisco Unified Communications Manager for basic calls, caller-ID services, supplementary services, and RSVP synchronization with audio.	<a href="#">“H.323-to-H.323 Connections on a Cisco Unified Border Element”</a> chapter of this guide

**Table 1** Supported Cisco Unified Border Element Configuration Guide Features (continued)

Release	Feature Name	Feature Description	Where Documented
	Cisco Unified Border Element with Media Flow-Around	Adds media flow-around capability on the Cisco UBE by supporting the processing of call setup and teardown requests (VoIP call signaling) and for media streams (flow-through and flow-around). Improves scalability and performance when network-topology hiding and bearer-level interworking features are not required.	How to Configuring Media Flow-Around sections of the, <a href="#">“H.323-to-H.323 Connections on a Cisco Unified Border Element”</a> , <a href="#">“H.323-to-SIP Connections on a Cisco Unified Border Element”</a> , and <a href="#">“SIP-to-SIP Connections on a Cisco Unified Border Element”</a> chapters of this guide.
12.2(13)T3	H.323 Cisco Unified Border Element	Provides a network-to-network demarcation point between independent VoIP and video networks by for billing, security, call-admission control, QoS, and signaling interworking. Performs most of the functions of a PSTN-to-IP gateway but joins two H.323 VoIP call legs.	<a href="#">“Fundamental Cisco Unified Border Element Configuration”</a> chapter of this guide

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 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.

© 2009 Cisco Systems, Inc. All rights reserved.





# Fundamental Cisco Unified Border Element Configuration

---

**Revised: July 11, 2008**

**First Published: June 19, 2006**

**Last Updated: July 11, 2008**

This chapter describes fundamental configuration tasks required for Fundamental Cisco Unified Border Element functionality. A Cisco Unified Border Element, in this guide also called an IP-to-IP gateway (IPIPGW), border element (BE), or session border controller, facilitates connectivity between independent VoIP networks by enabling H.323 VoIP and videoconferencing calls from one IP network to another. This gateway performs most of the same functions of a PSTN-to-IP gateway, but typically joins two IP call legs, rather than a PSTN and an IP call leg.

## **Finding Feature Information in This Module**

*Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for Cisco Unified Border Element Configuration Guide](#)” section on [page 45](#).*

## **Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images**

Use Cisco Feature Navigator to find information about platform support and Cisco IOS 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.

## Contents

- [Prerequisites for Fundamental Cisco Unified Border Element Configuration, page 41](#)
- [Restrictions for Fundamental Cisco Unified Border Element Configuration, page 41](#)
- [Information About Cisco Unified Border Element Features, page 41](#)
- [How to Configure Fundamental Cisco Unified Border Element, page 42](#)
- [Configuration Examples for Fundamental Cisco Unified Border Element, page 71](#)



---

**Americas Headquarters:**

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

© 2009 Cisco Systems, Inc. All rights reserved.

- [Additional References, page 79](#)
- [Feature Information for Cisco Unified Border Element Configuration Guide, page 835](#)
- [Glossary, page 84](#)

## Prerequisites for Fundamental Cisco Unified Border Element Configuration

- Perform the prerequisites listed in the “Prerequisites for Cisco Unified Border Element Configuration” section in this guide.
- Perform basic H.323 gateway configuration.
- Perform basic H.323 gatekeeper configuration.

**Note**

For configuration instructions, see the “[Configuring H.323 Gateways](#)” and “[Configuring H.323 Gatekeepers](#)” chapters of the *Cisco IOS Voice, Video, and Fax Configuration Guide*, Release 12.2.

## Restrictions for Fundamental Cisco Unified Border Element Configuration

- Cisco Unified Border Elements that require the Registration, Admission, and Status (RAS) protocol must have a via-zone-enabled gatekeeper or equivalent.
- Cisco Unified Border Elements interoperate with Cisco ATA 186, Cisco ATA 188, Cisco CallManager, Cisco CallManager Express 3.1, Cisco IOS gateways, NetMeeting, and Polycom ViewStation.
- Cisco fax relay is reported as a voice call on an Cisco Unified Border Element.
- Fax calls are reported as a modem plus fax call when modem CLI are present.
- Slow-start to fast-start interworking is supported only for H.32-to-H.323 calls.
- DTMF Interworking rtp-nte to out of band is not supported when high density transcoder is enabled. Use normal transcoding for rtp-nte to out of band DTMF interworking.
- The transcoding process on the Cisco Unified Border Element will always drop fast-start calls down to slow-start between H.323 endpoints even when the H.323 terminating endpoints support fast-start calls.
- Cisco Unified Border Element supports T.38 fax relay (H.323 Annex D). However, endpoints configured with Named Signaling Events (NSE) may result in reduced fax transmission quality and are not supported.

## Information About Cisco Unified Border Element Features

Gateway feature benefits include the following:

- Codec filtering by restricting codecs advertised on outbound call legs. For example, restriction of high-bandwidth codecs is possible on the reorigination side of the Cisco Unified Border Element outbound dial peer.
- Support for changing codecs during rotary dial peer selection.
- Network privacy by hiding the internal network structure from other administrative domains.
- Ability to create interconnections between different VoIP network types (such as SIP-to-H.323, H.323-to-SIP, and SIP-to-SIP protocol interworking).
- Better voice quality, cost and space savings (including rack density), and feature set compared with back-to-back gateways.
- Support for TDM voice.
- Support for Cisco ATA188 and third-party endpoints.
- More control of calls routed between ITSPs.

## How to Configure Fundamental Cisco Unified Border Element

This section contains the following tasks:

- [Configuring an Ethernet Interface, page 42](#)
- [Configuring a RTP Loopback Interface, page 44](#)
- [Configuring Codec Transparency on a Cisco Unified Border Element, page 46](#)
- [Configuring the GSMAMR-NB Codec on a Cisco Unified Border Element, page 49](#)
- [Configuring iLBC Codec on a Cisco Unified Border Element, page 51](#)
- [Configuring QoS for a Cisco Unified Border Element, page 52](#)
- [Configuring Cisco Unified Border Element for High Utilization, page 53](#)
- [Configuring Cisco Unified Border Element with OSP, page 56](#)
- [Media Statistics on a Cisco Unified Border Element, page 60](#)
- [Troubleshooting and Verifying Fundamental Cisco Unified Border Element Configuration and Operation, page 69](#)

### Configuring an Ethernet Interface

You can configure the Cisco Unified Border Element feature to operate with either a single Ethernet interface for all incoming, outgoing, and via-zone gatekeeper traffic or two Ethernet interfaces for signaling and media streams (optional but highly recommended for single-interface configurations). To configure an Ethernet interface, perform the steps in this section.

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot/port*
4. **ip route-cache same-interface**



## 5. exit

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<code>configure terminal</code>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<code>interface type slot/port</code>  <b>Example:</b> Router(config)# interface fastethernet 0/1	Selects the Ethernet interface that you want to configure.
Step 4	<code>ip route-cache same-interface</code>  <b>Example:</b> Router(config-if)# ip route-cache same-interface	Controls the use of high-speed switching caches for IP routing by enabling fast-switching packets to back out on the same interface on which they arrived.
Step 5	<code>exit</code>  <b>Example:</b> Router(config-if)# exit	Exits the current mode.

## Examples

The following example shows a configuration that uses a single Ethernet interface for all traffic:

```
interface FastEthernet0/1
 ip address 10.16.8.6 255.255.0.0
 no ip redirects
 ip route-cache same-interface
 speed auto
 full-duplex
 h323-gateway voip interface
 h323-gateway voip id 7206-vgk1 ipaddr 10.16.8.71 1719
 h323-gateway voip h323-id 3660-hud1
 h323-gateway voip tech-prefix 1#
 h323_gateway voip bind srcaddr 10.16.8.6
```

## Configuring a RTP Loopback Interface

The Cisco Unified Border Element supports configuration of an RTP loopback dial peer for use in verifying and troubleshooting H.323 networks. When a call encounters an RTP loopback dial peer, the gateway automatically signals call connect and loops all voice data back to the source. In contrast to normal calls through the VoIP-to-VoIP gateway, RTP loopback calls consist of only one call leg.

To configure a RTP loopback interface, perform the steps in this section.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice *number* voip**
4. **incoming called-number *string***
5. **destination-pattern *string***
6. **codec *codec***
7. **session target loopback:rtp**
8. **exit**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>dial-peer voice <i>number</i> voip</b>  <b>Example:</b> Router(config)# dial-peer voice 2 voip	Enters dial-peer configuration mode for the specified VoIP dial peer.
Step 4	<b>incoming called-number <i>string</i></b>  <b>Example:</b> Router(config-dial-peer)# incoming called-number 555.+	Associates a prefix with the dial peer for incoming call legs. This enables a specific codec to be applied to incoming call legs.
Step 5	<b>destination-pattern <i>string</i></b>  <b>Example:</b> Router(config-dial-peer)# destination-pattern 555.+	Associates the called number prefix with this dial peer for outgoing call legs.

	Command or Action	Purpose
Step 6	<pre>codec codec</pre> <p><b>Example:</b> Router(config-dial-peer)# codec g711ulaw </p>	<p>Assigns a codec to the dial peer.</p> <p><b>Note</b> The assigned codec must be supported by the incoming call. A codec preference list can be used in place of the specific codec. The specific codec will cause the IP-to-IP mode to be disabled for these calls. The transparent codec option cannot be used for RTP loopback.</p>
Step 7	<pre>session target loopback:rtp</pre> <p><b>Example:</b> Router(config-dial-peer)# session target loopback:rtp </p>	<p>Specifies the RTP loopback option for all calls using this dial peer.</p>
Step 8	<pre>exit</pre> <p><b>Example:</b> Router(config-dial-peer)# exit </p>	<p>Exits the current mode.</p>

## Examples

### Using a Single Dial Peer on a Cisco Unified Border Element

```
Router(config)# dial-peer voice 5550199 voip
Router(config-dial-peer)# incoming called-number 5550199
Router(config-dial-peer)# destination-pattern 5550199
Router(config-dial-peer)# codec g711ulaw
Router(config-dial-peer)# session target loopback:rtp
```

### Using Separate Dial Peers on a Cisco Unified Border Element

```
dial-peer voice 5550188 voip
incoming called-number 5550188
session target ras
codec g711ulaw
!
dial-peer voice 5550182 voip
destination-pattern 5550188
session target loopback:rtp
```

### Using a Codec Preference List to Support Additional Codecs

```
voice class codec 1
codec preference 1 g711ulaw
codec preference 2 g729r8

dial-peer voice 5429999 voip
incoming called-number 5550199
destination-pattern 5550199
voice-class codec 1
session target loopback:rtp
```

## Configuring Codec Transparency on a Cisco Unified Border Element

Codec transparency enables the Cisco Unified Border Element to pass codec capabilities between endpoints. If you configure transparency, the Cisco Unified Border Element uses the codec that was specified by the endpoints for setting up a call.

To configure codec transparency on an Cisco Unified Border Element, perform the steps in this section. This section contains the following subsections:

- [Configuring Codec Transparency for All Dial Peers in a Voice Class, page 46](#)
- [Configuring Codec Transparency for an Individual Dial Peer, page 47](#)

### Restrictions

- Codec transparency is only supported for H.323-to-H.323 calls.
- Codec filtering must be based on codec types; filtering based on byte size is not supported.
- Codec transparency is not supported when call start interwork is configured.
- For video calls, you must configure codec transparency in both incoming and outgoing dial peers. Codec filtering may not be possible for video calls.

### Configuring Codec Transparency for All Dial Peers in a Voice Class

To configure codec transparency for all dial peers in a voice class, perform the steps in this section.

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice class codec** *tag*
4. **codec preference** *value codec-type*
5. **exit**
6. **dial-peer voice** *number voip*
7. **voice class codec** *tag*
8. **exit**

#### DETAILED STEPS

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

	Command or Action	Purpose
Step 3	<code>voice class codec tag</code>  <b>Example:</b> Router(config)# <code>voice class codec 1</code>	Enters voice-class configuration mode for the specified codec voice class.
Step 4	<code>codec preference value codec-type</code>  <b>Example:</b> Router(config-class)# <code>codec preference 1 transparent</code>	Specifies a list of preferred codecs to use on a dial peer. In this case, specifies that the transparent codec (1 transparent) is to be used so that codec capabilities are passed transparently between endpoints.
Step 5	<code>exit</code>  <b>Example:</b> Router(config-class)# <code>exit</code>	Exits the current mode.
Step 6	<code>dial-peer voice number voip</code>  <b>Example:</b> Router(config)# <code>dial-peer voice 1 voip</code>	Enters dial peer configuration mode for the specified VoIP dial peer.
Step 7	<code>voice-class codec tag</code>  <b>Example:</b> Router(config-dial-peer)# <code>voice-class codec 1</code>	Assigns the previously configured codec-selection preference list (codec voice class) to the specified voice class. The tag number maps to the tag number created by means of the <b>voice class codec</b> command.
Step 8	<code>exit</code>  <b>Example:</b> Router(config-dial-peer)# <code>exit</code>	Exits the current mode.

## Configuring Codec Transparency for an Individual Dial Peer

To configure codec transparency for an individual dial peer, perform the steps in this section.

### Restrictions

If you plan to configure both incoming and outgoing dial peers, you must specify the transparent codec on the incoming dial peer.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `dial-peer voice number voip`
4. `codec codec-type`
5. `exit`

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> <code>Router&gt; enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<code>configure terminal</code>  <b>Example:</b> <code>Router# configure terminal</code>	Enters global configuration mode.
Step 3	<code>dial-peer voice <i>number</i> voip</code>  <b>Example:</b> <code>Router(config)# dial-peer voice 2 voip</code>	Enters dial-peer configuration mode for the specified VoIP dial peer.
Step 4	<code>codec <i>codec-type</i></code>  <b>Example:</b> <code>Router(config-dial-peer)# codec transparent</code>	Specifies the transparent codec for this dial peer.
Step 5	<code>exit</code>  <b>Example:</b> <code>Router(config-dial-peer)# exit</code>	Exits the current mode.

## Examples

The following example shows an inbound and outbound dial peer on the same tag in which the inbound dial peer is configured with the transparent codec, and the outbound dial peer is configured with the filter codec:

```
dial-peer voice 1 voip
  incoming called-number .T
  destination-pattern .T
  session target ras
  codec transparent
```

The following example shows separate tags for the inbound and outbound dial peers:

```
dial-peer voice 1 voip
  destination-pattern .T
  session target ras
  codec transparent

dial-peer voice 2 voip
  incoming called-number .T
  codec transparent
  destination-pattern .T
  session target ras
```

The following example shows filtering of high-bandwidth codecs applied to dial peer 1. With this configuration, codecs other than those specified are disallowed.

```
voice class codec 1
  codec preference 1 g729br8
```

```

codec preference 2 g723r53
codec preference 3 g723r68

dial-peer voice 1 voip
voice-class codec 1

```

The following shows a different filtering configuration. With this configuration, codecs other than g729r8 are disallowed.

```

dial-peer voice 1 voip
  destination-pattern .T
  session target ras

```

## Configuring the GSMAMR-NB Codec on a Cisco Unified Border Element

The Adaptive Multirate Narrow Band (AMR-NB) codec is a high complexity multimode codec that supports eight narrowband speech encoding modes with bit rates between 4.75 and 12.2 kbps. The sampling frequency used in AMR-NB is 8000 Hz and the speech encoding is performed on 20 ms speech frames. Therefore, each encoded AMR-NB speech frame represents 160 samples of the original speech.

The AMR-NB codec was originally developed and standardized by the European Telecommunications Standards Institute (ETSI) for Groupe Speciale Mobile (GSM) cellular systems, and chosen by the Third Generation Partnership Project (3GPP) as the mandatory codec for third generation (3G) cellular systems.

[Table 1](#) Contains codec mode and bit rate information for the AMR-NB codec.

**Table 1** *AMR Codec Modes and Bit Rates*

Codec Mode	Bit Rate (kbps)
0	4.75
1	5.15
2	5.90
3	6.70
4	7.40
5	7.95
6	10.2
7	12.2
8 <sup>1</sup>	1.80

1. Used for Silence Indication Detection (SID) frames.

To configure GSMAMR-NB Codec on an Cisco Unified Border Element from a live feed, perform the steps in this section.

### Prerequisites

- You must install an IP Plus image (minimum) of Cisco IOS Release 12.4(9)T or a later release.

## Restrictions

The following restrictions apply when configuring H323-to-SIP, and SIP-to-SIP Cisco Unified Border Element connections:

- Codec filtering is supported only based on codec type.
- Transcoding and conferencing are not supported
- Codec transparent is not supported
- Codec parameters such as pkt period, encap, frame format and modes should be explicitly configured.

The following restrictions apply when configuring H.323-to-H.323 Cisco Unified Border Element connections:

- Codec filtering is supported only based on codec type.
- Transcoding and conferencing are not supported
- Codec transparent is supported
- Configuring codec parameters such as pkt period, encap, frame format and modes is not needed. If configured, they will be ignored as the negotiation of the parameters is left to the endpoints.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice tag {pots | mmoip | voip}**
4. **codec gsmamr-nb [packetization-period 20][encap rfc3267][frame-format {bandwidth-efficient | octet-aligned [crc | no-crc]}] [modes modes-value]**
5. **exit**
6. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> <code>Router&gt; enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<code>configure terminal</code>  <b>Example:</b> <code>Router# configure terminal</code>	Enters global configuration mode.
Step 3	<code>dial-peer voice tag voip</code>  <b>Example:</b> <code>Router(config)# dial-peer voice tag voip</code>	Defines a particular dial peer, specifies the method of voice encapsulation, and enters dial peer configuration mode: <ul style="list-style-type: none"><li>• <b>voip</b>—Indicates that this is a VoIP peer that uses voice encapsulation on the POTS network.</li></ul>



	Command or Action	Purpose
Step 4	<pre>codec gsmamr-nb [packetization-period 20][encap rfc3267] [frame-format {bandwidth-efficient   octet-aligned [crc   no-crc]}] [modes modes-value]</pre> <p><b>Example:</b>  Router(config-dial-peer)# codec gsmamr-nb  packetization-period 20 encap rfc3267  frame-format octet-aligned crc modes  0-2,4,6-7</p>	<p>Specifies the GSMAMR-NB codec for a dial peer:</p> <ul style="list-style-type: none"> <li>• <b>packetization-period 20</b>—Sets the packetization period to 20 ms.</li> <li>• <b>encap rfc3267</b>—Sets the encapsulation value to comply with RFC 3267.</li> <li>• <b>frame-format</b>—Specifies a frame format. Supported values are octet-aligned and bandwidth-efficient. The default is octet-aligned.</li> <li>• <b>crc   no-crc</b>—CRC is applicable only for octet-aligned frame format. If you enter bandwidth-efficient frame format, the <code>crc   no-crc</code> options will not be available because they are inapplicable.</li> <li>• <b>modes</b>—Valid values are from 0 to 7. You can specify modes as a range (for example, 0-2), or individual modes separated by commas (for example, 2,4,6), or a combination of the two (for example, 0-2,4,6-7). Applicable only to GSMAMR-NB codec support.</li> </ul>
Step 5	<pre>exit</pre> <p><b>Example:</b>  Router (config-dial-peer)# exit</p>	<p>Exits dial-peer voice configuration mode and returns to global configuration mode</p>
Step 6	<pre>end</pre> <p><b>Example:</b>  Router&gt; end</p>	<p>Exits global configuration mode and returns to privileged EXEC mode.</p>

## Configuring iLBC Codec on a Cisco Unified Border Element

The internet Low Bitrate Codec (iLBC) is a standard, high-complexity speech codec that is suitable for robust voice communication over IP. iLBC has built-in error correction functionality that helps the codec perform in networks with a high-packet loss.



### Note

H.323-to-SIP calls, the iLBC codec configuration must be the same across all the call legs in the call. i.e. originating gateway, Cisco Unified Border Element(s) and terminating gateway.

Additional information and configuration of the iLBC code on an Cisco Unified Border Element can be found at the following links:

- Codecs section of the Dial Peer Configuration on Voice Gateway Routers Guide  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax\\_c/int\\_c/dpeer\\_c/dp\\_ovrww.htm#1035124](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/int_c/dpeer_c/dp_ovrww.htm#1035124)
- Dial Peer Features and Configuration section of the Dial Peer Configuration on Voice Gateway Routers Guide  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax\\_c/int\\_c/dpeer\\_c/dp\\_config.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/int_c/dpeer_c/dp_config.htm)

## Configuring QoS for a Cisco Unified Border Element

To assign QoS differentiated services code points (DSCP) for H.323 calls through the Cisco Unified Border Element, perform the steps in this section.



### Note

With the exception of RSVP, all VoIP QoS options supported by TDM-to-IP gateways are supported by Cisco Unified Border Elements. See the following documents for details and configuration instructions:

- The “[Configuring Quality of Service for Voice](#)” chapter in *Cisco IOS Voice, Video, and Fax Configuration Guide*, Release 12.2
- [Quality of Service for Voice over IP](#)

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice *number* voip**
4. **ip qos dscp ef media**
5. **ip qos dscp af31 signaling**
6. **exit**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<code>configure terminal</code>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<code>dial-peer voice <i>number</i> voip</code>  <b>Example:</b> Router(config)# dial-peer voice 2 voip	Enters dial peer configuration mode for the specified VoIP dial peer.
Step 4	<code>ip qos dscp ef media</code>  <b>Example:</b> Router(config-dial-peer)# ip qos dscp ef media	Configures express forwarding for RTP packets.

	Command or Action	Purpose
Step 5	<code>ip qos dscp af31 signaling</code>  <b>Example:</b> Router(config-dial-peer)# ip qos dscp af31 signaling	Configures assured forwarding af31 for H.323 signaling.
Step 6	<code>exit</code>  <b>Example:</b> Router(config-dial-peer)# exit	Exits the current mode.

## Configuring Cisco Unified Border Element for High Utilization

For high-utilization configurations, the Cisco Unified Border Element may require a higher percentage of memory than that which is made available by default during bootup. Additionally, high-utilization configurations may experience an increase in dropped packets.

To configure Cisco Unified Border Element for high utilization, perform the steps in this section. This section contains the following subsections:

- [Increase I/O Memory for High Utilization, page 53](#)
- [Manage Ethernet Hold Queue for High Utilization, page 54](#)

### Increase I/O Memory for High Utilization

To increase the amount of memory available to the Cisco Unified Border Element, perform the steps in this section.

#### Prerequisites

Determine if sufficient I/O memory is available by using the **show memory** command:



#### Note

If peak utilization is consistently more than 80 percent of the total I/O memory allocated, use the **memory-size iomem** command to set the I/O memory percentage to use less than 80 percent of the allocation.

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **show version**
4. **memory-size iomem**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> <code>Router&gt; enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<code>configure terminal</code>  <b>Example:</b> <code>Router# configure terminal</code>	Enters global configuration mode.
Step 3	<code>show version</code>  <b>Example:</b> <code>Router# show version</code>	Displays memory statistics.
Step 4	<code>memory-size iomem i/o-memory-percentage</code>  <b>Example:</b> <code>Router(config)# memory-size iomem 20</code>	Reallocates the percentage of DRAM to use for I/O memory and processor memory. The argument is as follows: <ul style="list-style-type: none"> <li><i>i/o-memory-percentage</i>—Valid values:10, 15, 20, 25, 30, 40, and 50. A minimum of 15 MB of memory is required for I/O memory.</li> </ul>

## Manage Ethernet Hold Queue for High Utilization

Some traffic patterns and network environments may produce bursts of packets on the Ethernet interfaces used for Cisco Unified Border Element signaling and media. In some cases, these bursts can result in dropped packets when the Ethernet input queue overflows. Similarly, momentary congestion on the local network could inhibit the Cisco Unified Border Element feature, also resulting in dropped packets when the Ethernet output queue overflows.

Because H.323 uses UDP for media transport and RAS signaling, dropped packets have a negative impact on call signaling integrity and voice quality. Packet drops due to momentary, occasional Ethernet queue overflows in bursty networks can be reduced or eliminated by increasing the Ethernet hold queue sizes.

**Caution**

A consistently overloaded Ethernet hold queue may increase latency. You may be required to upgrade the Cisco Unified Border Element feature to a higher-performance platform or distribute traffic to an additional gateway.

To increase the Ethernet input hold queue, perform the steps in this section.

## SUMMARY STEPS

- `enable`
- `configure terminal`
- `interface type slot/port`
- `hold-queue length in`

5. **hold-queue** *length out*
6. **exit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>interface</b> <i>type slot/port</i>  <b>Example:</b> Router(config)# interface ethernet 0/1	Selects the Ethernet interface that you want to configure.
Step 4	<b>hold-queue</b> <i>length in</i>  <b>Example:</b> Router(config)# hold-queue 1024 in	Sets the Ethernet interface input queue.
Step 5	<b>hold-queue</b> <i>length out</i>  <b>Example:</b> Router(config)# hold-queue 1024 out	Sets the Ethernet interface output queue.
Step 6	<b>exit</b>  <b>Example:</b> Router(config)# exit	Exits the current mode.

## Examples

In general, set the queue size to the smallest value that resolves the packet drops. Monitor the network using the **show interfaces ethernet** command to confirm that the queue occupancy and drops are both close to zero. For example:

```
Router(config)# interface f0/1
Router(config)# hold-queue 1024 in
Router(config)# hold-queue 1024 out
```

```
Router# show interface f0/1 | include queue
Input queue: 17/1024/0/0 (size/max/drops/flushes); Total output drops: 0
Output queue :0/1024 (size/max)
```

```
Router# show interface f0/1
```

```
FastEthernet0/1 is up, line protocol is up
Hardware is AmdFE, address is 0002.b950.5181 (bia 0002.b950.5181)
Description: archived via cfg file p8.cfg on Wed May 1 09:46:33 EDT 2002
Internet address is 10.3.2.63/16
```

```

MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
    reliability 255/255, txload 104/255, rxload 97/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 100Mb/s, 100BaseTX/FX
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:00, output 00:00:00, output hang never
Last clearing of "show interface" counters never
Input queue: 7/1024/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue :0/1024 (size/max)
5 minute input rate 38335000 bits/sec, 24068 packets/sec
5 minute output rate 40897000 bits/sec, 24019 packets/sec
  112943349 packets input, 1022884421 bytes
    Received 405 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog
    0 input packets with dribble condition detected
  113081187 packets output, 2612108380 bytes, 0 underruns
    0 output errors, 0 collisions, 2 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out

```

```
Router# show running-config interface f0/1
```

```
Building configuration...
```

```

Current configuration : 420 bytes
!
interface FastEthernet0/1
 ip address 10.3.2.63 255.255.0.0
 no ip redirects
 ip route-cache same-interface
 speed auto
 full-duplex
 h323-gateway voip interface
 h323-gateway voip id 3640-vgk2 ipaddr 10.3.2.72 1719 priority 1
 h323-gateway voip h323-id 3660-hud3
 h323-gateway voip tech-prefix 1#
 h323-gateway voip bind srcaddr 10.3.2.63
 hold-queue 1024 in
 hold-queue 1024 out

```

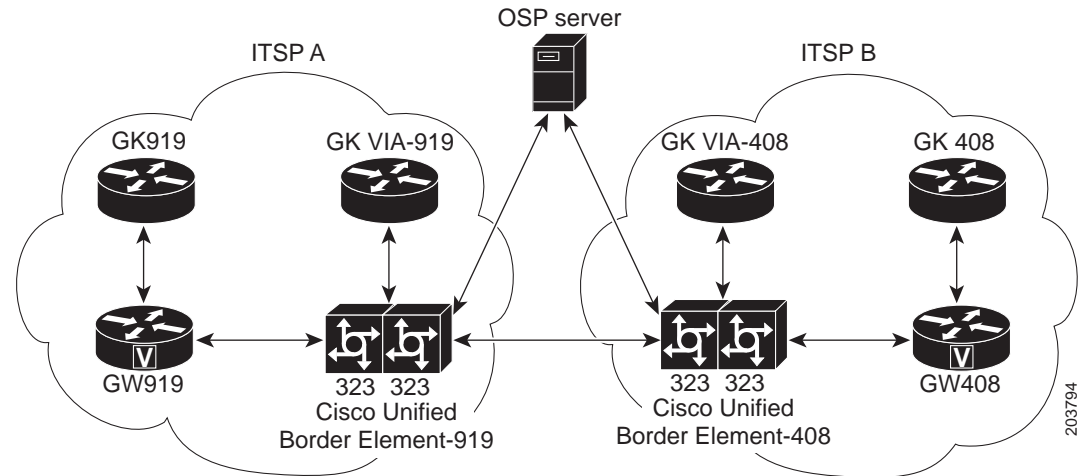
## Configuring Cisco Unified Border Element with OSP

The Cisco Unified Border Element with Open Settlement Protocol (OSP) feature enables VoIP service providers to gain the benefits of the Cisco Unified Border Element and to make use of routing, billing, and settlement capabilities offered by OSP-based clearinghouses.

Open Settlement Protocol is a client-server protocol used to establish authenticated connections between gateways. OSP provides for the secure transfer of accounting and routing information between Cisco Unified Border Elements.

[Figure 1](#) shows a sample topology that uses the Cisco Unified Border Element feature with OSP. With the exception of the authentication and accounting messages that are exchanged between the Cisco Unified Border Element and the OSP server, the exchange of messages between the gateways and gatekeepers is similar to the process illustrated in [Figure 4 on page 74](#).

**Figure 1 Cisco Unified Border Element with OSP Configuration Topology**



**Note**

For details on configuring and using OSP applications, see the “[Configuring Settlement Applications](#)” chapter of the *Cisco IOS Voice, Video and Fax Configuration Guide*, Release 12.2.

To configure the Cisco Unified Border Element with OSP, perform the steps in this section.

## Prerequisites

- Obtain the required feature license for each platform on which you will configure the Cisco Unified Border Element with OSP feature.
- Install a Cisco IOS image that supports the Cisco Unified Border Element and encryption. See [Figure 3 on page 72](#) for a list of Cisco IOS image requirements.
- Configure OSP on the Cisco Unified Border Element. For detailed instructions on configuring OSP, see the [Configuring Settlement Applications](#) chapter of the *Cisco IOS Voice, Video and Fax Configuration Guide*, Release 12.2.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice *number* voip**
4. **application *application-name***
5. **exit**

## DETAILED STEPS

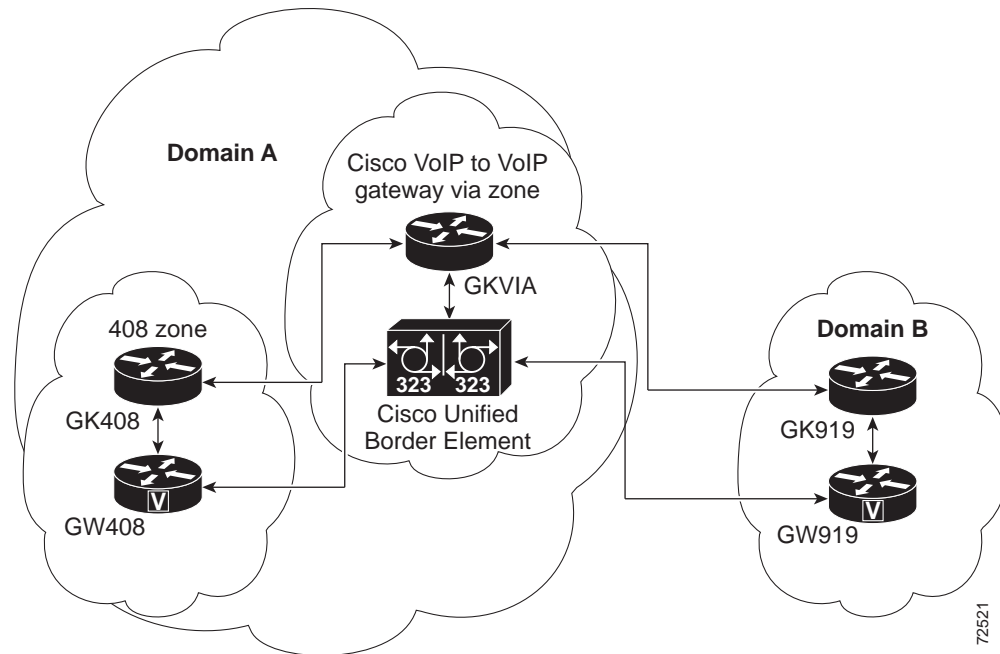
	Command or Action	Purpose
Step 1	<p><code>enable</code></p> <p><b>Example:</b> Router&gt; enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<p><code>configure terminal</code></p> <p><b>Example:</b> Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p><code>dial-peer voice <i>number</i> voip</code></p> <p><b>Example:</b> Router(config)# dial-peer voice 11 voip</p>	<p>Enters dial peer configuration mode for the specified VoIP dial peer.</p> <p><b>Note</b> You need to configure only incoming dial peers for OSP.</p>
Step 4	<p><code>application <i>application-name</i></code></p> <p><b>Example:</b> Router(config-dial-peer)# application session</p>	<p>Configure the dial peer to use a Tcl application that supports OSP.</p> <p><b>Note</b> Unless you have configured a Tcl application for OSP, use the default “session” application.</p>
Step 5	<p><code>exit</code></p> <p><b>Example:</b> Router(config-dial-peer)# exit</p>	<p>Exits the current mode.</p>



## Examples

Figure 2 shows two ITSPs using Cisco Unified Border Element and OSP to connect calls passing between the two networks. The examples that follow are based on this illustration.

**Figure 2 Cisco Unified Border Element with OSP Feature Topology**



### Sample Configuration for the Cisco Unified Border Element with OSP Feature

The following example shows the dial peer configuration necessary to complete calls using the configuration shown in Figure 3 on page 72:

#### Cisco Unified Border Element-919 Dial Peers

The following dial peer is used for incoming calls from GW919:

```
dial-peer voice 11 voip
  application session
  incoming called-number 408....
  session target ras
  codec transparent
!
```

The following dial peer is used for outgoing calls to Cisco Unified Border Element-408:

```
dial-peer voice 12 voip
  destination-pattern 408....
  session target settlement
  codec transparent
!
```

The following dial peer is used for incoming calls from Cisco Unified Border Element-408:

```
dial-peer voice 13 voip
  application session
  incoming called-number 919....
  session target settlement
```

```

codec transparent
!
```

The following dial peer is used for outgoing calls to GW919:

```

dial-peer voice 14 voip
 destination-pattern 919....
 session target ras
 codec transparent
!
```

### Cisco Unified Border Element-408 Dial Peers

The following dial peer is used for incoming calls from Cisco Unified Border Element-919:

```

dial-peer voice 21 voip
 application session
 incoming called-number 408....
 session target settlement
 codec transparent
!
```

The following dial peer is used for outgoing calls to GW408:

```

dial-peer voice 22 voip
 destination-pattern 408....
 session target ras
 codec transparent
!
```

The following dial peer is used for outgoing calls to Cisco Unified Border Element-919:

```

dial-peer voice 23 voip
 destination-pattern 919....
 session target settlement
 codec transparent
!
```

The following dial peer is used for incoming calls from GW408:

```

dial-peer voice 24 voip
 application session
 incoming called-number 919....
 session target ras
 codec transparent
!
```

## Media Statistics on a Cisco Unified Border Element

This chapter describes the media statistics feature. The **media statistics** command allows you to estimate the values of the packet loss, jitter, and the Round Trip Time (RTT) statistics based on RFC-3550.

To enable media statistics on an Cisco Unified Border Element, perform the steps in this section. This section contains the following subsections:

- [Restrictions, page 61](#)
- [Information About Media Statistics in an Cisco Unified Border Element, page 61](#)
- [Configuring Media Statistics in a Cisco Unified Border Element, page 61](#)
- [Verifying Fundamental Cisco Unified Border Element Configurations, page 70](#)

## Restrictions

- Integrated TDM-IP and Cisco Unified Border Element is not supported.
- Estimating media statistics feature on Cisco Unified Border Element is available if the **media statistics** command is configured. The feature is disabled by default.
- Cisco Unified Border Element does not initiate RTCP it only passes the received RTCP packet from incoming leg to Outgoing leg.
- Voice quality may be impacted by per-packet touching of an RTP stream for generating the required voice statistics.

## Information About Media Statistics in an Cisco Unified Border Element

The Voip RTP library estimates the values based on RTCP packets received on the Cisco Unified Border Element. This feature adds the capability to generate the media statistics in Cisco Unified Border Element and estimate the values of packet loss, jitter, and Round Trip Time (RTT)

### Packet Loss

Packet loss is estimated on Cisco Unified Border Element based on RFC 3550. Packet loss calculation is done based on RTP stream and the computation is done in VOIP RTP library by checking the sequence Number.

- The Packet loss value computed is filled in variable cvVoIPCallActiveLostPackets in the CISCO-VOICE-DIAL-CONTROL-MIB
- Packet loss value will be estimated even if the End-End RTCP is not present for the call.

### Jitter

Packet jitter is defined as an estimate of the statistical variance of the RTP data packet interarrival time, measured in timestamp units. Jitter is estimated on Cisco Unified Border Elements based on RFC 3550. Jitter is computed in VOIP RTP library.

- The Jitter value computed is filled in variable cvCallActivePlayDelayJitter in CISCO-VOICE-DIAL-CONTROL-MIB.

### Round Trip Time

The Round Trip Time (RTT) value computed is filled in variable cvVoIPCallActiveRoundTripDelay in CISCO-VOICE-DIAL-CONTROL-MIB.

- Cisco Unified Border Element handles signaling and Media without DSP and establishes calls with protocols H.323, SIP and also does interworking between H.323 and SIP protocols. As the calls are handled DSP less currently the values populated on Cisco Unified Border Element for voice statistics are displayed as zero.

**Note**

A sub-rtcp message is similar to a rtcp message except the payload type is different. A sub-rtcp message is a cisco proprietary message initiated by the Cisco Unified Border Element.

## Configuring Media Statistics in a Cisco Unified Border Element

The media statistics feature can be configured in global, or dial peer configuration mode, perform the steps in this section. This section contains the following subsections:

- [Configuring Media Statistics in Voice-Service Configuration Mode, page 62](#)
- [Configuring Media Statistics on Dial Peer Configuration Mode, page 63](#)
- [Monitoring Media Statistics in a Cisco Unified Border Element, page 64 \(optional\)](#)
- [Verifying Fundamental Cisco Unified Border Element Configurations, page 70](#)

**Note**

- Before you perform a procedure, familiarize yourself with the following information:
  - [“Restrictions” section on page 61](#)
- For help with a procedure, see the monitoring and verifying sections listed above.

## Configuring Media Statistics in Voice-Service Configuration Mode

To globally enable media statistics in voice-service configuration mode to estimate the values for packet loss, jitter, and RTT, perform the steps in this section.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **media statistics**
5. **exit**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>voice service voip</b>  <b>Example:</b> Router(config)# voice service voip	Enters VoIP voice-service configuration mode.

	Command or Action	Purpose
Step 4	<b>media statistics</b>  <b>Example:</b> Router(conf-voi-serv)# media statistics	Estimates the values of packet loss, jitter, and Round Trip Time (RTT) statistics. <ul style="list-style-type: none"> <li>• The statistics are displayed using the <b>show voice history</b> and <b>show call active voice</b> command.</li> <li>• If the media statistics command is disabled the values will be zero.</li> </ul>
Step 5	<b>exit</b>  <b>Example:</b> Router(conf-voi-serv)# exit	Exits the current mode.

## Configuring Media Statistics on Dial Peer Configuration Mode

To enable media statistics in on a dial peer voice-service configuration mode to estimate the values for packet loss, jitter, and RTT, perform the steps in this section.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **media statistics**
5. **exit**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>voice service voip</b>  <b>Example:</b> Router(config)# voice service voip	Enters VoIP voice-service configuration mode.

	Command or Action	Purpose
Step 4	<b>media statistics</b>  <b>Example:</b> Router(conf-voi-serv)# media statistics	Estimates the values of packet loss, jitter, and Round Trip Time (RTT) statistics. <ul style="list-style-type: none"> <li>• The statistics are displayed using the <b>show voice history</b> and <b>show call active voice</b> command.</li> <li>• If the media statistics command is disabled the values will be zero.</li> </ul>
Step 5	<b>exit</b>  <b>Example:</b> Router(config-voice-service)# exit	Exits the current mode.

## Monitoring Media Statistics in a Cisco Unified Border Element

Monitor the **media statistics** with the **show call active voice** look for following variables:

- LostPackets
- PlayDelayJitter
- RoundTripDelay

### SUMMARY STEPS

1. **show call active voice**
2. **show call active voice | i LostPackets**
3. **show call active voice | i RoundTripDelay**
4. **show call active voice | i PlayDelayJitter**
5. **show voip rtp connections**
6. **show call history voice last 2 | i RoundTripDelay**
7. **show call history voice last 2 | i LostPackets**

### DETAILED STEPS

#### Step 1 **show call active voice**

Use this command to display media statistics information and indicate whether the media statistic feature is enabled.

```
c3745-ipipgw#show call active voice
Telephony call-legs: 0
SIP call-legs: 2
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 2
GENERIC:
SetupTime=525050 ms
Index=1
PeerAddress=6662
```

```
PeerSubAddress=
PeerId=0
PeerIfIndex=54
LogicalIfIndex=0
ConnectTime=527550 ms
CallDuration=00:00:04 sec
CallState=4
CallOrigin=2
ChargedUnits=0
InfoType=speech
TransmitPackets=112
TransmitBytes=2240
ReceivePackets=318
ReceiveBytes=6360
VOIP:
ConnectionId[0xA6008E71 0xA8FE11D6 0x800B000D 0x2970B190]
IncomingConnectionId[0xA6008E71 0xA8FE11D6 0x800B000D 0x2970B190]
CallID=5
RemoteIPAddress=1.3.7.16
RemoteUDPPort=19512
RemoteSignallingIPAddress=1.3.7.16
RemoteSignallingPort=52111
RemoteMediaIPAddress=1.3.7.16
RemoteMediaPort=19512
RoundTripDelay=0 ms
SelectedQoS=best-effort
tx_DtmfRelay=rtp-nte
FastConnect=FALSE
AnnexE=FALSE
Separate H245 Connection=FALSE
H245 Tunneling=FALSE
SessionProtocol=sipv2
ProtocolCallId=A601C6C1-A8FE11D6-8029B65F-D48EEF95@1.3.7.16
SessionTarget=1.3.7.16
OnTimeRvPlayout=0
GapFillWithSilence=0 ms
GapFillWithPrediction=0 ms
GapFillWithInterpolation=0 ms
GapFillWithRedundancy=0 ms
HiWaterPlayoutDelay=0 ms
LoWaterPlayoutDelay=0 ms
TxPakNumber=0
TxSignalPak=0
TxComfortNoisePak=0
TxDuration=0
TxVoiceDuration=0
RxPakNumber=0
RxSignalPak=0
RxComfortNoisePak=0
RxDuration=0
RxVoiceDuration=0
RxOutOfSeq=0
RxLatePak=0
RxEarlyPak=0
RxBadProtocol=0
PlayDelayCurrent=0
PlayDelayMin=0
PlayDelayMax=0
PlayDelayClockOffset=0
PlayDelayJitter=0
PlayErrPredictive=0
PlayErrInterpolative=0
PlayErrSilence=0
PlayErrBufferOverflow=0
```

```
PlayErrRetroactive=0
PlayErrTalkspurt=0
OutSignalLevel=0
InSignalLevel=0
LevelTxPowerMean=0
LevelRxPowerMean=0
LevelBgNoise=0
ERLLevel=0
ACOMLevel=0
ErrRxDrop=0
ErrTxDrop=0
ErrTxControl=0
ErrRxControl=0
ReceiveDelay=0 ms
LostPackets=0
EarlyPackets=0
LatePackets=0
SRTP = off
TextRelay = off
VAD = disabled
CoderTypeRate=g729r8
CodecBytes=20
Media Setting=flow-through
CallerName=
CallerIDBlocked=False
OriginalCallingNumber=6662
OriginalCallingOctet=0x0
OriginalCalledNumber=6661
OriginalCalledOctet=0x0
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0x80
TranslatedCallingNumber=6662
TranslatedCallingOctet=0x0
TranslatedCalledNumber=6661
TranslatedCalledOctet=0x0
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0x80
GwReceivedCalledNumber=6661
GwReceivedCalledOctet3=0x0
GwReceivedCallingNumber=6662
GwReceivedCallingOctet3=0x0
GwReceivedCallingOctet3a=0x80
MediaInactiveDetected=no
MediaInactiveTimestamp=
MediaControlReceived=
LongDurationCallDetected=no
LongDurCallTimestamp=
LongDurcallDuration=
Username=6662
GENERIC:
SetupTime=525050 ms
Index=2
PeerAddress=6661
PeerSubAddress=
PeerId=6661
PeerIfIndex=54
LogicalIfIndex=0
ConnectTime=527550 ms
CallDuration=00:00:06 sec
CallState=4
CallOrigin=1
ChargedUnits=0
InfoType=speech
TransmitPackets=432
```



```
TransmitBytes=8640
ReceivePackets=112
ReceiveBytes=2240
VOIP:
ConnectionId[0xA6008E71 0xA8FE11D6 0x800B000D 0x2970B190]
IncomingConnectionId[0xA6008E71 0xA8FE11D6 0x800B000D 0x2970B190]
CallID=6
RemoteIPAddress=1.3.7.112
RemoteUDPPort=18958
RemoteSignallingIPAddress=1.3.7.112
RemoteSignallingPort=5060
RemoteMediaIPAddress=1.3.7.112
RemoteMediaPort=18958
RoundTripDelay=0 ms
SelectedQoS=best-effort
tx_DtmfRelay=rtp-nte
FastConnect=FALSE
AnnexE=FALSE
Separate H245 Connection=FALSE
H245 Tunneling=FALSE
SessionProtocol=sipv2
ProtocolCallId=D0445D00-62B611D6-800DB698-E7A6FDDD@1.3.7.9
SessionTarget=1.3.7.112
OnTimeRvPlayout=0
GapFillWithSilence=0 ms
GapFillWithPrediction=0 ms
GapFillWithInterpolation=0 ms
GapFillWithRedundancy=0 ms
HiWaterPlayoutDelay=0 ms
LoWaterPlayoutDelay=0 ms
TxPakNumber=0
TxSignalPak=0
TxComfortNoisePak=0
TxDuration=0
TxVoiceDuration=0
RxPakNumber=0
RxSignalPak=0
RxComfortNoisePak=0
RxDuration=0
RxVoiceDuration=0
RxOutOfSeq=0
RxLatePak=0
RxEarlyPak=0
RxBadProtocol=0
PlayDelayCurrent=0
PlayDelayMin=0
PlayDelayMax=0
PlayDelayClockOffset=0
PlayDelayJitter=0
PlayErrPredictive=0
PlayErrInterpolative=0
PlayErrSilence=0
PlayErrBufferOverflow=0
PlayErrRetroactive=0
PlayErrTalkspurt=0
OutSignalLevel=0
InSignalLevel=0
LevelTxPowerMean=0
LevelRxPowerMean=0
LevelBgNoise=0
ERLLevel=0
ACOMLevel=0
ErrRxDrop=0
ErrTxDrop=0
```

```

ErrTxControl=0
ErrRxControl=0
ReceiveDelay=0 ms
LostPackets=0
EarlyPackets=0
LatePackets=0
S RTP = off
TextRelay = off
VAD = disabled
CoderTypeRate=g729r8
CodecBytes=20
Media Setting=flow-through
CallerName=
CallerIDBlocked=False
OriginalCallingNumber=6662
OriginalCallingOctet=0x0
OriginalCalledNumber=6661
OriginalCalledOctet=0x0
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0x80
TranslatedCallingNumber=6662
TranslatedCallingOctet=0x0
TranslatedCalledNumber=6661
TranslatedCalledOctet=0x0
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0x80
GwReceivedCalledNumber=6661
GwReceivedCalledOctet3=0x0
GwOutputPulsedCalledNumber=6661
GwOutputPulsedCalledOctet3=0x0
GwReceivedCallingNumber=6662
GwReceivedCallingOctet3=0x0
GwReceivedCallingOctet3a=0x80
GwOutputPulsedCallingNumber=6662
GwOutputPulsedCallingOctet3=0x0
GwOutputPulsedCallingOctet3a=0x80
MediaInactiveDetected=no
MediaInactiveTimestamp=
MediaControlReceived=
LongDurationCallDetected=no
LongDurCallTimestamp=
LongDurcallDuration=
Username=6662
Telephony call-legs: 0
SIP call-legs: 2
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 2

```

**Step 2 Router# show call active voice | i LostPackets**

```

LostPackets=0
LostPackets=126

```

**Step 3 Router# show call active voice | i RoundTripDelay**

```

RoundTripDelay=0 ms
RoundTripDelay=4 ms

```

**Step 4 Router# show call active voice | i PlayDelayJitter**

```
PlayDelayJitter=0
PlayDelayJitter=24
```

### Step 5 Router# show voip rtp connections

```
VoIP RTP active connections :
No. CallId      dstCallId  LocalRTP  RmtRTP  LocalIP      RemoteIP
1   5          6          17892    17794    15.5.34.5    15.5.34.158
2   6          5          16990    18744    15.5.34.5    15.5.34.6
Found 2 active RTP connections
```

## Troubleshooting and Verifying Fundamental Cisco Unified Border Element Configuration and Operation

To troubleshoot or verify connections in an Cisco Unified Border Element, perform the steps in this section. This section contains the following subsections:

- [Troubleshooting Tips, page 69](#)
- [Verifying Fundamental Cisco Unified Border Element Configurations, page 70](#)

### Troubleshooting Tips



#### Caution

Under moderate traffic loads, these **debug** commands produce a high volume of output.

- Use the **debug voip ipipgw** command to debug the Cisco Unified Border Element feature
- The Sub-RTCP sender report (SR) and receiver report (RR) packets are feedback packets of RTP Senders and RTP Receivers respectively.
- The SR includes a 20-byte sender information section for use by active senders.
- Both the SR and RR forms include zero or more reception report blocks and each reception report block provides statistics about the data received from the particular source.
- Use the **debug voip rtcp sub-rtcp** command to debug for LostPackets in the Media Statistics feature.

```
Router# debug voip rtcp sub-rtcp
```

```
VOIP RTCP Subrtcp debugging is on
Oct 16 19:35:26.870: SUBRTCP:tx SR (15.5.34.5-17893)->(15.5.34.158,17795)
rtcp-intv(5002 ms)
Oct 16 19:35:26.870: SUBRTCP Sender Report dump Length - 32:
80 FA 00 07 0F 25 22 05 80 C8 00 05 C8 DE 5D 7E DE C6 2A 6D 00 00 00 00 00 00 00 00
00 00 00 00
Oct 16 19:35:26.878: SUBRTCP:tx SR (15.5.34.5-16991)->(15.5.34.6,18745) rtcp-intv(5005
ms)
Oct 16 19:35:26.878: SUBRTCP Sender Report dump Length - 32:
80 FA 00 07 05 CD 22 05 80 C8 00 05 C8 DE 5D 7E E0 D2 59 C1 00 00 00 00 00 00 00 00
00 00 00 00
```

- Use the **debug voip statistics** command to debug the Media Statistics feature in the Cisco Unified Border Element.

```
Router# debug voip rtp statistics
```

```

VOIP RTP Statistics debugging is on
Oct 16 19:38:20.000: RTP[15.5.34.6-0x1B5B2298]: loss(0) jitter(5 ms, 5992 us)
Oct 16 19:38:22.556: RTP[15.5.34.6-0x1B5B2298]: loss(0) jitter(8 ms, 8054 us)

```

For additional examples of **show** and **debug** command output and details on interpreting the output, see the following resources:

- [Cisco IOS Debug Command Reference](#), Release 12.4T
- [Cisco IOS Voice Troubleshooting and Monitoring Guide](#)
- [Troubleshooting and Debugging VoIP Call Basics](#)
- [Voice Gateway Error Decoder for Cisco IOS](#)
- [VoIP Debug Commands](#)

## Verifying Fundamental Cisco Unified Border Element Configurations

To verify Cisco Unified Border Element feature configuration and operation, perform the following steps (listed alphabetically) as appropriate.



### Note

The word “calls” refers to call legs in some commands and output.

## SUMMARY STEPS

1. **show call active video**
2. **show call active voice**
3. **show call history fax**
4. **show call history video**
5. **show call history voice**
6. **show crm**
7. **show dial-peer voice**
8. **show running-config**
9. **show voip rtp connections**

## DETAILED STEPS

- 
- Step 1** **show call active video**  
Use this command to display the active video H.323 call legs.
- Step 2** **show call active voice**  
Use this command to display call information for voice calls that are in progress.
- Step 3** **show call active fax**  
Use this command to display the fax transmissions that are in progress.
- Step 4** **show call history video**  
Use this command to display the history of video H.323 call legs.
- Step 5** **show call history voice**

Use this command to display the history of voice call legs.

**Step 6** **show call history fax**

Use this command to display the call history table for fax transmissions that are in progress.

**Step 7** **show crm**

Use this command to display the carrier ID list or IP circuit utilization.

**Step 8** **show dial-peer voice**

Use this command to display information about voice dial peers.

**Step 9** **show running-config**

Use this command to verify which H.323-to-H.323, H.323-to-SIP, or SIP-to-SIP connection types are supported.

**Step 10** **show voip rtp connections**

Use this command to display active Real-Time Transport Protocol (RTP) connections.

---

## Configuration Examples for Fundamental Cisco Unified Border Element

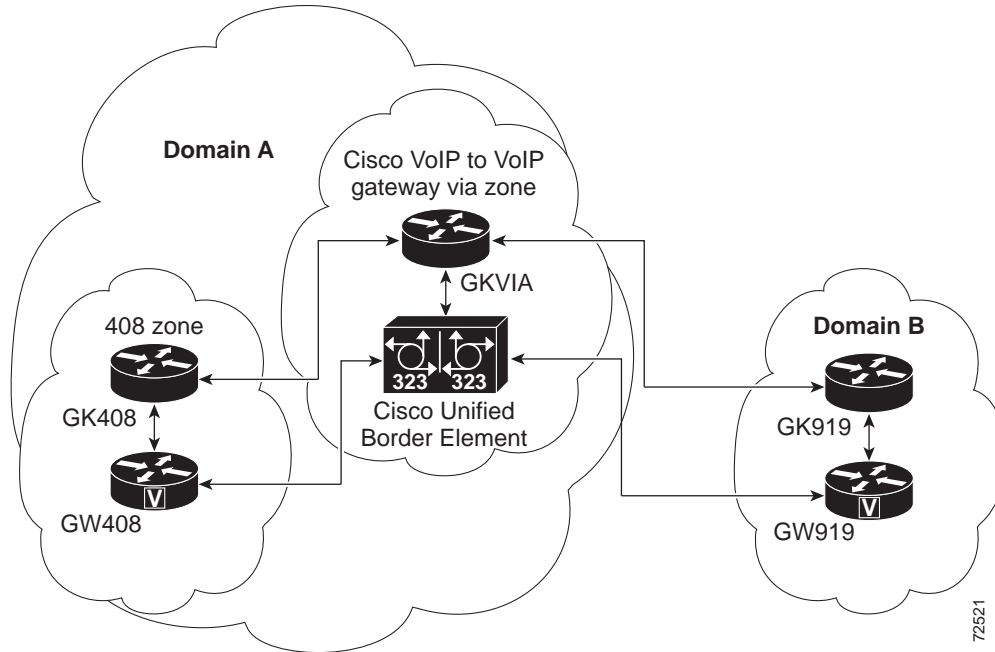
This chapter includes the following configuration examples:

- [Cisco Unified Border Element: Example, page 72](#)
- [Local-to-Remote Network Using the Cisco Unified Border Element: Example, page 74](#)
- [Remote-to-Local Network Using the Cisco Unified Border Element: Example, page 75](#)
- [Remote-to-Remote Network Using a Cisco Unified Border Element: Example, page 76](#)
- [Remote-to-Remote Network Using Two Cisco Unified Border Elements: Example, page 77](#)

## Cisco Unified Border Element: Example

Figure 3 shows an example configuration of the Cisco Unified Border Element feature.

Figure 3 Cisco Unified Border Element Feature Topology



For a detailed description of the actions that occur during a call, see [Figure 1 on page 57](#). The following examples show gateway and gatekeeper configuration.

### Originating Gateway Configuration: Example

```
interface Ethernet0/0
 ip address 10.16.8.132 255.255.255.0
 half-duplex
 h323-gateway voip interface
 h323-gateway voip id GK408 ipaddr 10.16.8.123 1718
 h323-gateway voip h323-id GW408
!
```

```
dial-peer voice 919 voip
 destination-pattern 919.....
 session target ras
!
gateway
```

### Originating Gatekeeper Configuration: Example

```
gatekeeper
 zone local GK408 usa 10.16.8.123
 zone remote GKVIA usa 10.16.8.24 1719
 zone prefix GKVIA 919*
 gw-type-prefix 1#*
 no shutdown
```

### Cisco Unified Border Element Configuration: Example

```
!
voice service voip
 no allow-connections any to pots
 no allow-connections pots to any
 allow-connections h323 to h323
 h323
 ip circuit max-calls 1000
 ip circuit default only
!
!
interface FastEthernet0/0
 ip address 10.16.8.145 255.255.255.0
 ip route-cache same-interface
 duplex auto
 speed auto
 h323-gateway voip interface
 h323-gateway voip id GKVIA ipaddr 10.16.8.24 1718
 h323-gateway voip h323-id IPIPGW
 h323-gateway voip tech-prefix 1#
!
!
dial-peer voice 919 voip
 incoming called-number 919.....
 destination-pattern 919.....
 session target ras
 codec transparent
!
gateway
```

### Via Zone Gatekeeper Configuration: Example

```
gatekeeper
 zone local GKVIA usa 10.16.8.24
 zone remote GK919 usa 10.16.8.146 1719 invia GKVIA outvia GKVIA
 zone prefix GK919 919*
 no shutdown
```

### Terminating Gateway: Example

```
interface Ethernet0/0
 ip address 10.16.8.134 255.255.255.0
 half-duplex
 h323-gateway voip interface
 h323-gateway voip id GK919 ipaddr 10.16.8.146 1718
 h323-gateway voip h323-id GW919
 h323-gateway voip tech-prefix 919
!
```

```
dial-peer voice 919 pots
 destination-pattern 919.....
 port 1/0:1
 !
 gateway
```

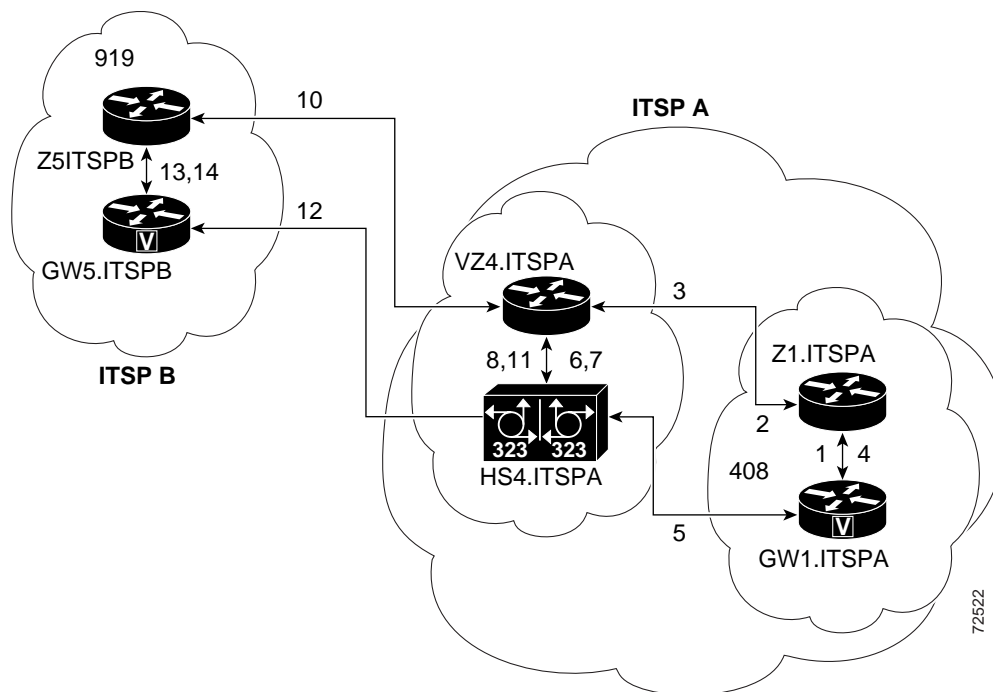
### Terminating Gatekeeper Configuration: Example

```
gatekeeper
 zone local GK919 usa 10.16.8.146
 gw-type-prefix 1#* default-technology
 no shutdown
```

## Local-to-Remote Network Using the Cisco Unified Border Element: Example

Figure 4 shows a local-to-remote network using the Cisco Unified Border Element feature.

**Figure 4** Local-to-Remote Network Using the Cisco Unified Border Element Feature Topology



### Note

For a detailed configuration example of a local-to-remote network using the Cisco Unified Border Element, see the following website:

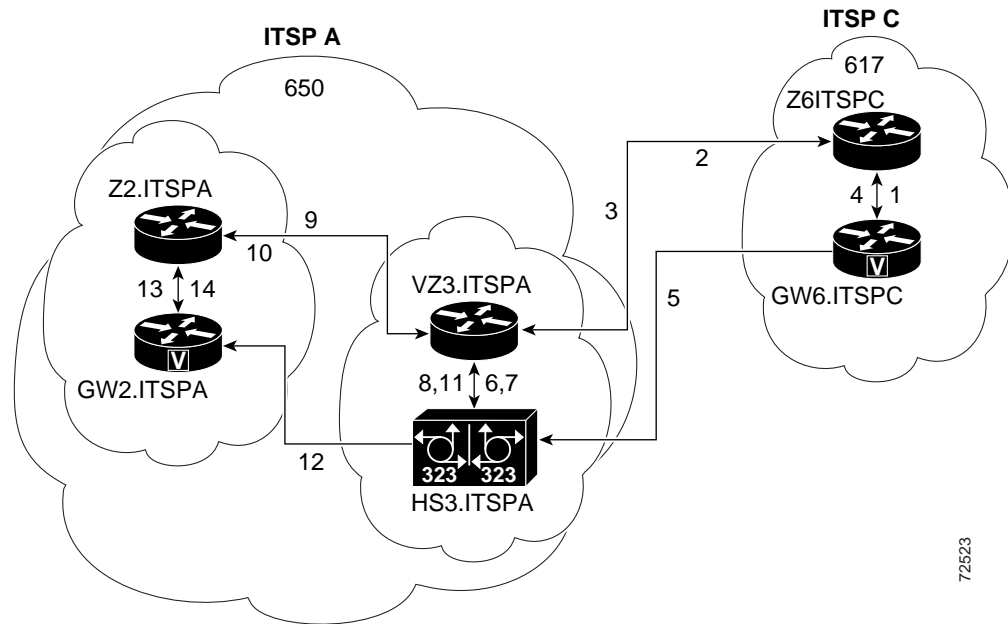
[http://www.cisco.com/en/US/tech/tk1077/technologies\\_configuration\\_example09186a00801b0803.shtml](http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a00801b0803.shtml)



# Remote-to-Local Network Using the Cisco Unified Border Element: Example

Figure 5 shows a remote-to-local network using the Cisco Unified Border Element feature.

**Figure 5** Remote-to-Local Network Using the Cisco Unified Border Element Feature Topology



**Note**

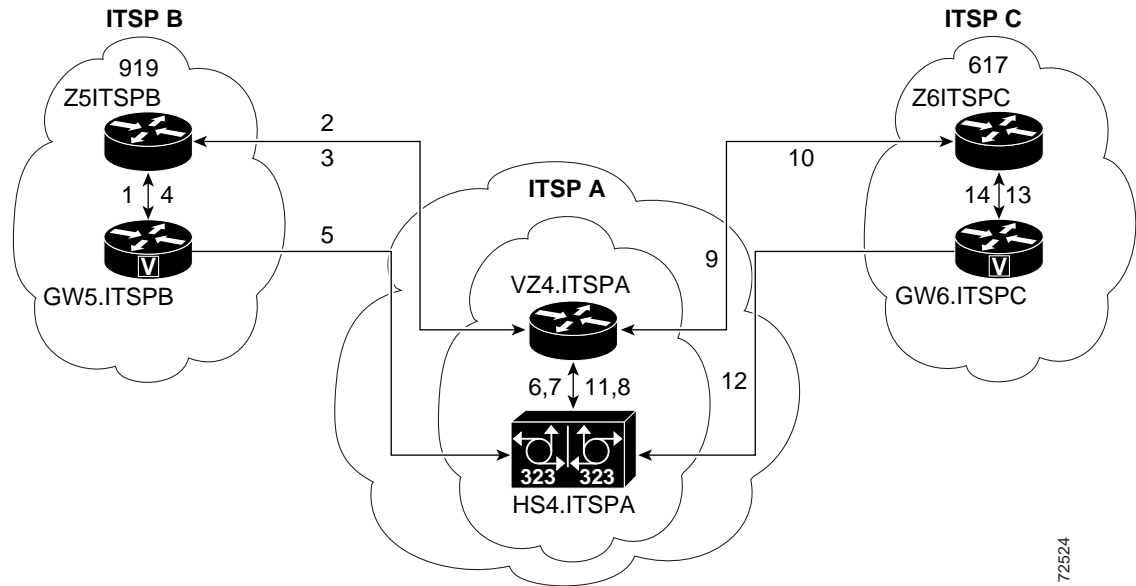
For a detailed configuration example of a remote-to-local network using the Cisco Unified Border Element, see the following website:

[http://www.cisco.com/en/US/tech/tk1077/technologies\\_configuration\\_example\\_09186a0080203edc.shtml](http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example_09186a0080203edc.shtml).

## Remote-to-Remote Network Using a Cisco Unified Border Element: Example

Figure 6 shows a remote-to-remote network using an Cisco Unified Border Element.

**Figure 6** Remote-to-Remote Network Using a Cisco Unified Border Element Topology



### Note

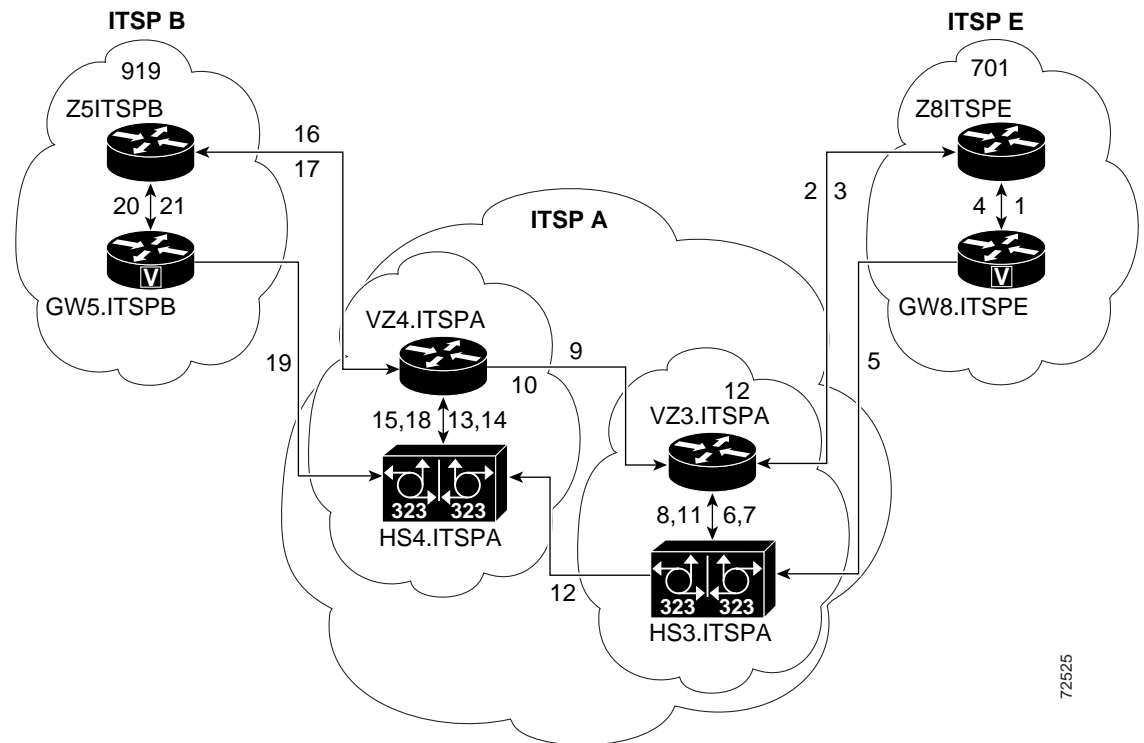
For a detailed configuration example of a remote-to-remote network using the Cisco Unified Border Element, see the following website:

[http://www.cisco.com/en/US/tech/tk1077/technologies\\_configuration\\_example\\_09186a0080203edd.shtml](http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example_09186a0080203edd.shtml).

## Remote-to-Remote Network Using Two Cisco Unified Border Elements: Example

Figure 7 shows a remote-to-remote network using two Cisco Unified Border Elements.

Figure 7 Remote-to-Remote Network Using Two Cisco Unified Border Elements Topology



### Note

For a detailed configuration example of a remote-to-remote network using two Cisco Unified Border Elements, see the following website:

[http://www.cisco.com/en/US/tech/tk1077/technologies\\_configuration\\_example\\_09186a0080203edb.shtml](http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example_09186a0080203edb.shtml).

### Using the Cisco Unified Border Element to Assign DSCP Code Points to Gateway Traffic

The following example configures the Cisco Unified Border Element to assign DSCP code points to traffic that passes through the gateway:

```
dial-peer voice 1 voip
  incoming called-number .T
  destination-pattern .T
  ip qos dscp ef media
  ip cos dscp af31 signaling
  session target ras
  codec transparent
```

### Using Class and Policy Maps to Control Bandwidth Allocation

The following example uses class and policy maps to control bandwidth allocation based on matching received DSCP code points:

```
class-map match-all Silver-Data
  match ip dscp af11
  match ip dscp af12
  match ip dscp af13
class-map match-all Voice-Control
  match ip dscp af31
class-map match-all Gold-Data
  match ip dscp af21
  match ip dscp af22
  match ip dscp af23
class-map match-all Voice
  match ip dscp ef
!
!
policy-map LLQ
  class Voice
    priority percent 40
  class Voice-Control
    bandwidth remaining percent 5
  class Gold-Data
    bandwidth remaining percent 45
  class Silver-Data
    bandwidth remaining percent 35
  class class-default
    bandwidth remaining percent 5
    random-detect dscp-based
    random-detect dscp 2 70 128 10
    random-detect dscp 4 58 128 10
    random-detect dscp 6 44 128 10
policy-map FairQueue
  class class-default
```


## Where to Go Next

- [H.323-to-H.323 Connections on a Cisco Unified Border Element](#)
- [H.323-to-SIP Connections on a Cisco Unified Border Element](#)
- [SIP-to-SIP Connections on a Cisco Unified Border Element](#)
- [Cisco Unified Border Element for H.323 Cisco Unified Communications Manager to H.323 Service Provider Connectivity](#)
- [Configuring Cisco Unified Border Element Videoconferencing](#)

# Additional References

The following sections provide references related to the Cisco Unified Border Element with Gatekeeper.

## Related Documents

Related Topic	Document Title
Cisco IOS Release 12.4	<ul style="list-style-type: none"> <li>• <a href="#">Cisco IOS Release 12.4 Configuration Guides</a></li> <li>• <a href="#">Cisco IOS Release 12.4T Configuration Guides</a></li> <li>• <a href="#">Cisco IOS Release 12.4 Command References</a></li> <li>• <a href="#">Cisco IOS Voice Configuration Library</a></li> </ul> <p><a href="http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/cisco_ios_voice_configuration_library_glossary/vcl.htm">http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/cisco_ios_voice_configuration_library_glossary/vcl.htm</a></p>  <p><b>Note</b> This website contains the library preface and glossary.</p>
Cisco IOS Release 12.3	<ul style="list-style-type: none"> <li>• <a href="#">Cisco IOS Release 12.3 documentation</a></li> <li>• <a href="#">Cisco IOS voice commands</a></li> <li>• <a href="#">Cisco IOS Voice Troubleshooting and Monitoring Guide</a></li> <li>• <a href="#">Tcl IVR Version 2.0 Programming Guide</a></li> </ul>
Cisco IOS Release 12.2	<ul style="list-style-type: none"> <li>• <i>Cisco IOS Voice, Video, and Fax Configuration Guide</i>, Release 12.2 at <a href="http://www.cisco.com/en/US/docs/ios/12_2/voice/configuration/guide/fvfax_c.html">http://www.cisco.com/en/US/docs/ios/12_2/voice/configuration/guide/fvfax_c.html</a></li> </ul>
DSP documentation	<p>High-Density Packet Voice Feature Card for Cisco AS5350XM and AS5400XM Universal Gateways</p> <p><a href="http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/1241imit/124x/124xc4/vfc_dsp.htm">http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/1241imit/124x/124xc4/vfc_dsp.htm</a></p>
GKTMP (GK API) Documents	<ul style="list-style-type: none"> <li>• <i>GKTMP Command Reference</i>: <a href="http://www.cisco.com/en/US/docs/ios/12_2/gktmp/gktmpv4_2/gk_cli.htm">http://www.cisco.com/en/US/docs/ios/12_2/gktmp/gktmpv4_2/gk_cli.htm</a></li> <li>• <i>GKTMP Messages</i>: <a href="http://www.cisco.com/en/US/docs/ios/12_2/gktmp/gktmpv4_2/gk_tmp.html">http://www.cisco.com/en/US/docs/ios/12_2/gktmp/gktmpv4_2/gk_tmp.html</a></li> </ul>
internet Low Bitrate Codec (iLBC) Documents	<ul style="list-style-type: none"> <li>• Codecs section of the Dial Peer Configuration on Voice Gateway Routers Guide <a href="http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vfax_c/int_c/dpeer_c/dp_ovrvw.htm#1035124">http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vfax_c/int_c/dpeer_c/dp_ovrvw.htm#1035124</a></li> <li>• Dial Peer Features and Configuration section of the Dial Peer Configuration on Voice Gateway Routers Guide <a href="http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vfax_c/int_c/dpeer_c/dp_config.htm">http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vfax_c/int_c/dpeer_c/dp_config.htm</a></li> </ul>

Related Topic	Document Title
Cisco Unified Border Element Configuration Examples	<ul style="list-style-type: none"> <li>• Local-to-remote network using the IPIPGW <a href="http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a00801b0803.shtml">http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a00801b0803.shtml</a></li> <li>• Remote-to-local network using the IPIPGW: <a href="http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a0080203edc.shtml">http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a0080203edc.shtml</a></li> <li>• Remote-to-remote network using the IPIPGW: <a href="http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a0080203edd.shtml">http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a0080203edd.shtml</a></li> <li>• Remote-to-remote network using two IPIPGWs: <a href="http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a0080203edb.shtml">http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a0080203edb.shtml</a></li> </ul>
Related Application Guides	<ul style="list-style-type: none"> <li>• <a href="#">Cisco Unified Communications Manager and Cisco IOS Interoperability Guide</a></li> <li>• <a href="#">Cisco IOS Fax, Modem, and Text Support over IP Configuration Guide</a></li> <li>• “Configuring T.38 Fax Relay” chapter</li> <li>• <a href="#">Cisco IOS SIP Configuration Guide</a></li> <li>• Cisco Unified Communications Manager (CallManager) Programming Guides at: <a href="http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_programming_reference_guides_list.html">http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_programming_reference_guides_list.html</a></li> <li>• <i>Quality of Service for Voice over IP</i> at <a href="http://www.cisco.com/en/US/docs/ios/solutions_docs/qos_solutions/QoSVoIP/QoSVoIP.html">http://www.cisco.com/en/US/docs/ios/solutions_docs/qos_solutions/QoSVoIP/QoSVoIP.html</a></li> </ul>
Related Platform Documents	<ul style="list-style-type: none"> <li>• <a href="#">Cisco 2600 Series Multiservice Platforms</a></li> <li>• <a href="#">Cisco 2800 Series Integrated Services Routers</a></li> <li>• <a href="#">Cisco 3600 Series Multiservice Platforms</a></li> <li>• <a href="#">Cisco 3700 Series Multiservice Access Routers</a></li> <li>• <a href="#">Cisco 3800 Series Integrated Services Routers</a></li> <li>• <a href="#">Cisco 7200 Series Routers</a></li> <li>• <a href="#">Cisco 7301</a></li> </ul>
Related gateway configuration documentation	<p>Media and Signaling Authentication and Encryption Feature for Cisco IOS H.323 Gateways.</p> <p><a href="http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/htsecure.htm">http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/htsecure.htm</a></p>
Cisco IOS NAT Configuration Guide, Release 12.4T	<ul style="list-style-type: none"> <li>• <i>Configuring Cisco IOS Hosted NAT Traversal for Session Border Controller</i> <a href="http://www.cisco.com/en/US/docs/ios/12_4t/ip_addr/configuration/guide/htnatsbc.html">http://www.cisco.com/en/US/docs/ios/12_4t/ip_addr/configuration/guide/htnatsbc.html</a></li> </ul>

Related Topic	Document Title
Troubleshooting and Debugging guides	<ul style="list-style-type: none"> <li>• Cisco IOS Debug Command Reference, Release 12.4 at <a href="http://www.cisco.com/en/US/docs/ios/debug/command/reference/db_book.html">http://www.cisco.com/en/US/docs/ios/debug/command/reference/db_book.html</a></li> <li>• <i>Troubleshooting and Debugging VoIP Call Basics</i> at <a href="http://www.cisco.com/en/US/tech/tk1077/technologies_tech_note09186a0080094045.shtml">http://www.cisco.com/en/US/tech/tk1077/technologies_tech_note09186a0080094045.shtml</a></li> <li>• <i>VoIP Debug Commands</i> at <a href="http://www.cisco.com/en/US/docs/routers/access/1700/1750/software/configuration/guide/debug.html">http://www.cisco.com/en/US/docs/routers/access/1700/1750/software/configuration/guide/debug.html</a></li> </ul>

## Standards

Standard	Title
H.323 Version 4 and earlier	<i>H.323 (ITU-T VOIP protocols)</i>
H.323 - H.245 Version 12, Annex R	<i>H.323 (ITU-T VOIP protocols)</i>

## MIBs

MIB	MIBs Link
<ul style="list-style-type: none"> <li>• None</li> </ul>	<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><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p>

## RFCs

RFC	Title
RFC 2833	RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals
RFC 3261	SIP: Session Initiation Protocol
RFC 3267	Real-Time Transport Protocol (RTP) Payload Format and File Storage Format for the Adaptive Multi-Rate (AMR) and Adaptive Multi-Rate Wide band (AMR-WB) Audio Codecs.

## 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. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.</p>	<p><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></p>



# Feature Information for Cisco Unified Border Element Configuration Guide

Table 2 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.3(1) or a later release appear in the table.

For information on a feature in this technology that is not documented here, see the “Cisco Unified Border Element Features Roadmap.”


**Note**

Table 2 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 2** Feature Information for fundamental Cisco Unified Border Element Configuration

Feature Name	Releases	Feature Information
Cisco Unified Border Element with OSP	12.2(13)T3	Enables VoIP service providers to gain the benefits of the Cisco Unified Border Element and to make use of routing, billing, and settlement capabilities offered by OSP-based clearinghouses.
Codec support	12.2(13)T3 12.4(9)T 12.4(11)T	12.2(13)T3—Codec Transparency on an Cisco Unified Border Element. Enables the Cisco Unified Border Element to pass codec capabilities between endpoints. 12.4(9)T—GSMAMR-NB Codec on an Cisco Unified Border Element. Supports the complexity multimode codec that supports eight narrowband speech encoding modes with bit rates between 4.75 and 12.2 kbps. 12.4(11)T—iLBC Codec on an Cisco Unified Border Element. Supports robust voice communication over IP using the iLBC codec in Cisco Unified Border Element networks.
Ethernet Interface	12.2(13)T3	Configures Cisco Unified Border Element feature to operate with either a single Ethernet interface for all incoming, outgoing, and via-zone gatekeeper traffic or two Ethernet interfaces for signaling and media streams.
Hosted NAT Traversal Enhancements	12.4(11)XJ2	This feature was introduced.
Identify Alternate endpoint Call Attempts in RADIUS Call Accounting Records	12.4(4)T	This feature was introduced.
Interoperability Enhancements to the Cisco Unified Border Element	12.4(4)T	This feature was introduced.
IP Call Leg Statistics (Delay, Jitter and Return Trip Time)	12.4(11)XJ2	This feature was introduced.
Media Modes	12.3(1)	Cisco Unified Border Element with Media Flow-Around
Microsoft NetMeeting Interoperability	12.3(7)T	This feature was introduced.

**Table 2** Feature Information for fundamental Cisco Unified Border Element Configuration

Feature Name	Releases	Feature Information
QoS for an Cisco Unified Border Element	12.2(13)T3	Assigns differentiated services code points (DSCP) for H.323 calls through the Cisco Unified Border Element,
Rotary Support	12.3(11)T	12.3(11)T—Call-Failure Recovery (rotary)
RTP Loopback Interface	12.2(13)T3	The Cisco Unified Border Element supports configuration of an RTP loopback dial peer for use in verifying and troubleshooting H.323 networks.
Signaling Interworking	12.3(11)T	Slow-Start to Fast-Start Interworking
Tcl+IVR in an IP-Only Environment	12.3(7)T	This feature was introduced.
Transcoding and Interworking:	12.3(11)T 12.4(11)XJ2	12.3(11)T—Voice-Codec Transcoding 12.4(11)XJ2—DTMF Transcoding and Interworking: <ul style="list-style-type: none"> <li>• H245 &lt;--&gt; KPML</li> <li>• T.38 Fax using NSE</li> <li>• Transcoding with AS5x platforms</li> </ul>

## Glossary

**AMR-NB**—Adaptive Multi-rate Narrow Band

**ETSI**—European Telecommunications Standards Institute

**GSM**—Groupe Speciale Mobile

**3GPP**—Third Generation Partnership Project

**3G**—Third generation



### Note

See [Internetworking Terms and Acronyms](#) for terms not included in this glossary.

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 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.

© 2009 Cisco Systems, Inc. All rights reserved.





# H.323-to-H.323 Connections on a Cisco Unified Border Element

---

**Revised:** July 11, 2008,  
**First Published:** June 19, 2006  
**Last Updated:** July 11, 2008

This chapter describes how to configure and enable features for H.323-to-H.323 connections in an Cisco Unified Border Element topology.

## Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for H.323-to-H.323 Cisco Unified Border Element Connections” section on page 24](#).

## Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS 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.

## Contents

- [Prerequisites for H.323-to-H.323 Connections on a Cisco Unified Border Element, page 87](#)
- [Restrictions for H.323-to-H.323 Connections on a Cisco Unified Border Element, page 87](#)
- [Information About H.323-to-H.323 Connections on a Cisco Unified Border Element, page 87](#)
- [How to Configure H.323-to-H.323 Connections on a Cisco Unified Border Element, page 88](#)
- [Verifying H.323-to-H.323 Cisco Unified Border Element Configuration and Operation, page 103](#)
- [Additional References, page 105](#)
- [Where to Go Next, page 104](#)
- [Feature Information for H.323-to-H.323 Cisco Unified Border Element Connections, page 108](#)



---

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

© 2009 Cisco Systems, Inc. All rights reserved.

## Prerequisites for H.323-to-H.323 Connections on a Cisco Unified Border Element

- Perform the prerequisites listed in the “Prerequisites for Cisco Unified Border Element Configuration” section on page 20.
- Perform fundamental gateway configuration listed in the [Prerequisites for Fundamental Cisco Unified Border Element Configuration](#), page 41.
- Perform basic H.323 gateway configuration.
- Perform basic H.323 gatekeeper configuration.

**Note**

For configuration instructions, see the “[Configuring H.323 Gateways](#)” and “[Configuring H.323 Gatekeepers](#)” chapters of the *Cisco IOS Voice, Video, and Fax Configuration Guide*, Release 12.2.

## Restrictions for H.323-to-H.323 Connections on a Cisco Unified Border Element

- Connections are disabled by default in Cisco IOS images that support the Cisco Unified Border Element.
- Slow-start to fast-start interworking is supported only for H.323-to-H.323 calls.
- Transcoding in fast-start to slow-start interworking is not supported.
- Supplementary services with transcoding is not supported.
- DTMF Interworking rtp-nte to out of band is not supported when high density transcoder is enabled. Use normal transcoding for rtp-nte to out of band DTMF interworking.

## Information About H.323-to-H.323 Connections on a Cisco Unified Border Element

H.323-to-H.323 Gateway configuration provides a network-to-network demarcation point between independent VoIP and video networks by for billing, security, call-admission control, QoS, and signaling interworking. Performs most of the functions of a PSTN-to-IP gateway but joins two H.323 VoIP call legs.

**Note**

When you configure H.323-to-H.323 connections on a Cisco UBE, the ports on all its interfaces are open by default. This makes the Cisco UBE vulnerable to malicious attackers who can execute toll fraud across the gateway if the Cisco UBE has a public IP address and a PSTN connection. To eliminate the threat, you should bind an interface to private IP address that is not accessible by untrusted hosts. In addition, you should protect any public or untrusted interface by configuring a firewall or an access control list (ACL) to prevent unwanted traffic from traversing the router.

# How to Configure H.323-to-H.323 Connections on a Cisco Unified Border Element

This section contains the following tasks:

- [Configuring H.323-to-H.323 Connections on a Cisco Unified Border Element, page 88](#) (required)
- [Enabling H.323-to-H.323 Interworking Between Fast Start and Slow Start, page 89](#)
- [Configuring Media Flow-Around, page 92](#)
- [Configuring H.323-to-H.323 Call Failure Recovery \(Rotary\) on a Cisco Unified Border Element, page 95](#)
- [Managing H.323 IP Group Call Capacities, page 96](#)
- [Configuring Overlap Signaling for H.323-to-H.323 Connections on a Cisco Unified Border Element, page 101](#)

## Configuring H.323-to-H.323 Connections on a Cisco Unified Border Element

To configure H.323-to-H.323 connections on a Cisco UBE, perform the steps in this section.

### Restrictions

Connections are disabled by default in Cisco IOS images that support the Cisco Unified Border Element.

### SUMMARY STEPS

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

### DETAILED STEPS

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

	Command or Action	Purpose
Step 3	<code>voice service voip</code>	Enters VoIP voice-service configuration mode.
	<b>Example:</b> <code>Router(config)# voice service voip</code>	
Step 4	<code>allow-connections from-type to-type</code>	Allows connections between specific types of endpoints in an Cisco Unified Border Element. Arguments are as follows: <ul style="list-style-type: none"> <li><i>from-type</i>—Type of connection. Valid values: <b>h323</b>, <b>sip</b>.</li> <li><i>to-type</i>—Type of connection. Valid values: <b>h323</b>, <b>sip</b>.</li> </ul> <b>Note</b> H.323-to-H.323: By default, H.323-to-H.323 connections are disabled and POTS-to-any and any-to-POTS connections are enabled.
	<b>Example:</b> <code>Router(config-voi-serv)# allow-connections h323 to h323</code>	
Step 5	<code>exit</code>	Exits the current mode.
	<b>Example:</b> <code>Router(config-voi-serv)# exit</code>	

## Enabling H.323-to-H.323 Interworking Between Fast Start and Slow Start

Slow-start to fast-start interworking prevents the Cisco Unified Border Element from dropping a call down to slow-start when it detects different call signaling on the incoming and outgoing legs of H.323 to H.323 calls. Configuration may be done at either the dial-peer level or the global level.

To enable H.323-to-H.323 interworking perform the steps in this section. This section contains the following subsections:

- [Enabling Slow-Start to Fast-Start Interworking at the Global Level, page 89](#)
- [Enabling Slow-Start to Fast-Start Interworking at the Dial Peer Level, page 90](#)

### Enabling Slow-Start to Fast-Start Interworking at the Global Level

To configure slow-start to fast-start interworking on an Cisco Unified Border Element at the global level, perform the steps in this section.

#### Prerequisites

Configure **call start interwork** on both the incoming and outgoing legs.

#### Restrictions

The **call start interwork** command only supports interwork between fast-start and slow-start. It should not be used in situations where fast-start to fast-start or slow-start to slow-start calls are possible.

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **h323**
5. **call start interwork**
6. **exit**

**DETAILED STEPS**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<code>enable</code>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<code>configure terminal</code>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<code>voice service voip</code>  <b>Example:</b> Router(config)# voice service voip	Enters VoIP voice-service configuration mode.
<b>Step 4</b>	<code>h323</code>  <b>Example:</b> Router(conf-voi-serv)# h323	Enters H.323 voice-service configuration mode.
<b>Step 5</b>	<code>call start interwork</code>  <b>Example:</b> Router(conf-voi-serv)# call start interwork	Enables slow-start to fast-start interworking.
<b>Step 6</b>	<code>exit</code>  <b>Example:</b> Router(conf-voi-serv)# exit	Exits the current mode.

**Enabling Slow-Start to Fast-Start Interworking at the Dial Peer Level**

To configure slow-start to fast-start interworking on an Cisco Unified Border Element at the dial-peer level, perform the steps in this section.

**Prerequisites**

- Configure **call start interwork** on both the incoming and outgoing legs.



- Specify the codec on both the incoming and outgoing dial-peer.

## Restrictions

- The **call start interwork** command only supports interwork between fast-start and slow-start. It should not be used in situations where fast-start to fast-start or slow-start to slow-start calls are possible.
- When **call start interwork** is configured, both incoming and outgoing dial-peer need to have a specific codec configured.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice-class h323**
4. **call start interwork**
5. **exit**
6. Repeat as needed.

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>voice class h323 tag</b>  <b>Example:</b> Router(config)# voice class h323 4	Creates an H.323 voice class that is independent of a dial peer and can be used on multiple dial peers.
Step 4	<b>call start interwork</b>  <b>Example:</b> Router(config-class)# call start interwork	Enables slow-start to fast-start interworking.
Step 5	<b>exit</b>  <b>Example:</b> Router(config-class)# exit	Exits the current mode.
Step 6	Repeat for both incoming and outgoing legs.	—

## Configuring Media Flow-Around

This feature adds media flow-around capability on the Cisco UBE by supporting the processing of call setup and teardown requests (VoIP call signaling) and for media streams (flow-through and flow-around). Media flow-around can be configured the global level or it must be configured on both incoming and outgoing dial peers. If configured only on either the incoming or outgoing dialpeer, the call will become a flow-through call.

Media flow-around is a good choice to improve scalability and performance when network-topology hiding and bearer-level interworking features are not required

With the default configuration, the Cisco Unified Border Element receives media packets from the inbound call leg, terminates them, and then reoriginates the media stream on an outbound call leg. Media flow-around enables media packets to be passed directly between the endpoints, without the intervention of the Cisco Unified Border Element. The Cisco Unified Border Element continues to handle routing and billing functions.

**Note**

---

The Cisco Unified Border Element must be running Cisco IOS Release 12.3(1) or a later release to support media flow-around.

---

To specify media flow-around for voice class, all VoIP calls, or individual dial peers perform the steps in this section. This section contains the following subsections:

- [Configuring Media Flow-Around for a Voice Class, page 92](#)
- [Configuring Media Flow-Around at the Global Level, page 93](#)
- [Configuring Media Flow-Around for a Dial Peer, page 94](#)

## Configuring Media Flow-Around for a Voice Class

To configure media flow-around for a voice class, perform the steps in this section.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice class media 1tag**
4. **media flow-around**
5. **dial-peer voice 2 voip**
6. **voice-class media tag**
7. **exit**

**DETAILED STEPS**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<code>enable</code>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
<b>Step 2</b>	<code>configure terminal</code>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<code>voice class media tag</code>  <b>Example:</b> Router(config)# voice class media 1	Enters voice-class configuration mode and assign an identification tag for a media voice class.
<b>Step 4</b>	<code>media flow-around</code>  <b>Example:</b> Router(config-class)# media flow-around	Enables media flow around.
<b>Step 5</b>	<code>dial-peer voice 2 voip</code>  <b>Example:</b> Router(config-class)# dial-peer voice 2 voip	Enters dial-peer configuration mode and assign an identification tag for VoIP.
<b>Step 6</b>	<code>voice class media tag</code>  <b>Example:</b> Router(config-dial-peer)# voice class media 1	Assign an identification tag for a media voice class.
<b>Step 7</b>	<code>exit</code>  <b>Example:</b> Router(config-class)# exit	Exit voice class-configuration mode.

**Configuring Media Flow-Around at the Global Level**

To configure media flow-around at the global level, perform the steps in this section.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `voice service voip`
4. `media flow-around`
5. `exit`

**DETAILED STEPS**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<code>enable</code>  <b>Example:</b> <code>Router&gt; enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
<b>Step 2</b>	<code>configure terminal</code>  <b>Example:</b> <code>Router# configure terminal</code>	Enters global configuration mode.
<b>Step 3</b>	<code>voice service voip</code>  <b>Example:</b> <code>Router(config)# voice service voip</code>	Enters VoIP voice-service configuration mode.
<b>Step 4</b>	<code>media flow-around</code>  <b>Example:</b> <code>Router(config-voi-serv) media flow-around</code>	Enables media flow-around.
<b>Step 5</b>	<code>exit</code>  <b>Example:</b> <code>Router(config-voi-serv) exit</code>	Exits the current mode.

**Configuring Media Flow-Around for a Dial Peer**

To configure media flow-around for an individual dial-peer, perform the steps in this section.

**Restrictions**

If you plan to configure both incoming and outgoing dial peers, you must specify the transparent codec on the incoming dial peer.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `dial-peer voice number voip`
4. `media flow-around`
5. `exit`

**DETAILED STEPS**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<code>enable</code>  <b>Example:</b> <code>Router&gt; enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<code>configure terminal</code>  <b>Example:</b> <code>Router# configure terminal</code>	Enters global configuration mode.
<b>Step 3</b>	<code>dial-peer voice number voip</code>  <b>Example:</b> <code>Router(config)# dial-peer voice 2 voip</code>	Enters dial-peer configuration mode for the specified VoIP dial peer.
<b>Step 4</b>	<code>media flow-around</code>  <b>Example:</b> <code>Router(config-dial-peer) media flow-around</code>	Enables media flow-around.
<b>Step 5</b>	<code>exit</code>  <b>Example:</b> <code>Router(config-dial-peer)# exit</code>	Exits the current mode.

**Configuring H.323-to-H.323 Call Failure Recovery (Rotary) on a Cisco Unified Border Element**

- Call failure recovery (Rotary) on the Cisco Unified Border Element eliminates the need for identical codec capabilities for all dial peers in the rotary group, and allows the Cisco Unified Border Element to restart the codec negotiation end-to-end.
- Call failure recovery will continue until “voice hunt stop” is reached.

To configure H.323-to-H.323 call failure recovery (rotary) on an Cisco Unified Border Element, perform the steps in this section.

**Restrictions**

If extended caps (DTMF or T.38) are configured on the outgoing gateway or the trunking gateway, extended caps must be configured in both places.

**SUMMARY STEPS**

- `enable`
- `configure terminal`
- `voice service voip`
- `h323`

5. `emptycapability`
6. `exit`

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> <code>Router&gt; enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<code>configure terminal</code>  <b>Example:</b> <code>Router# configure terminal</code>	Enters global configuration mode.
Step 3	<code>voice service voip</code>  <b>Example:</b> <code>Router(config)# voice service voip</code>	Enters VoIP voice-service configuration mode.
Step 4	<code>h323</code>  <b>Example:</b> <code>Router(conf-voi-serv)# h323</code>	Enters H.323 voice-service configuration mode.
Step 5	<code>emptycapability</code>  <b>Example:</b> <code>Router(conf-serv-h323)# emptycapability</code>	Enables call failure recovery (TCS=0).
Step 6	<code>exit</code>  <b>Example:</b> <code>Router(conf-serv-h323)# exit</code>	Exits the current mode.

## Managing H.323 IP Group Call Capacities

Managing maximum capacity for the IP group is done with carrier IDs created on an IP trunk group. If you do not configure specific carrier IDs, you can use the **ip circuit default only** command to create a single carrier. However, if you want to use carrier ID-based routing, or if you need extra control for load and resource balancing, you must configure carrier IDs in conjunction with the **voice source-group** command.

The Cisco UBE feature works with the **voice source-group** command to provide matching criteria for incoming calls. The **voice source-group** command assigns a name to a set of source IP group characteristics. The terminating gateway uses these characteristics to identify and translate the incoming VoIP call. If there is no voice source group match, the default carrier ID is used, any source carrier ID on the incoming message is transmitted without change, and no destination carrier is available. Call-capacity information is reported to the gatekeeper, but carrier routing information is not.

If the voice source group matches, the matched source carrier ID is used and the target carrier ID defined in the voice source group is used for the destination carrier ID.

To manage H.323 IP group call capacities, perform the steps in this section.

## Restrictions

You can use the commands that follow only when no calls are active. If you try to use these commands with active calls present, the commands are rejected.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **h323**
5. **ip circuit max-calls**
6. **ip circuit carrier-id**
7. **ip circuit default only**
8. **ip circuit default name**
9. **exit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<code>configure terminal</code>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<code>voice service voip</code>  <b>Example:</b> Router(config)# voice service voip	Enters VoIP voice-service configuration mode.
Step 4	<code>h323</code>  <b>Example:</b> Router(conf-voi-serv)# h323	Enters H.323 voice-service configuration mode.

	Command or Action	Purpose
Step 5	<pre>ip circuit max-calls maximum-calls</pre> <p><b>Example:</b>  Router(config-serv-h323)# ip circuit max-calls 1500</p>	<p>(Required only if reserved calls are to exceed 1000) Sets the maximum number of aggregate H.323 IP circuit carrier call legs.</p> <p>If you do not configure this value, the default maximum value is 1000 reserved call legs. You may need to configure a lower value to obtain overload behavior. You can also configure a higher value.</p> <p><b>Note</b> After you set a maximum number of call legs for defined circuits, any aggregate capacity left over is available for default circuits. For example, if you specify 1000 as the maximum number of call legs and then reserve 200 call legs for defined circuits, 800 call legs are available for use by default circuits.</p> <p><b>Note</b> The Cisco Unified Border Element prevents you from allocating all of the capacity to specified carriers; at least one available circuit is required, which can be the default.</p>
Step 6	<pre>ip circuit carrier-id carrier-name [reserved-calls reserved]</pre> <p><b>Example:</b>  Router(config-serv-h323)# ip circuit carrier-id AA reserved-calls 500</p>	<p>(Optional) Defines an IP circuit using the specified name as the circuit ID.</p> <p><b>Note</b> The <b>reserved</b> keyword for this command is optional. Using this keyword creates a specified maximum number of calls for that circuit ID. The default value is 200 call legs.</p>
Step 7	<pre>ip circuit default only</pre> <p><b>Example:</b>  Router(config-serv-h323)# ip circuit default only</p>	<p>(Optional) Creates a single carrier to use all of the call capacity available to the Cisco Unified Border Element.</p> <p><b>Note</b> If you use the <b>ip circuit default only</b> command, you cannot use the <b>ip circuit carrier-id</b> command to configure more circuits. Using the <b>ip circuit default only</b> command creates a single carrier using the default carrier name.</p>

## Examples

The following examples show a default carrier with no voice source group configured:

### Default Carrier with No Voice Source Group

```
voice service voip
  allow-connections h323 to h323
  h323
  ip circuit max-calls 1000
  ip circuit default only
```

If there is no incoming source carrier ID:

- Capacity only is reported to the gatekeeper using the default circuit (two call legs).
- No source or destination carrier information is reported.

If there is an incoming source carrier ID:



- Two call legs are counted against the default circuit and reported to the GK.
- The source carrier ID is passed through the gateway to the terminating leg.

The following examples show a configuration with more reserved calls than the default value for the **max-calls** argument (1000):

#### Configuration with Default Calls in Excess of 1000

This example assigns 1100 calls to other carriers, leaving 400 calls available to the default carrier:

```
voice service voip
  allow-connections h323 to h323
  h323
    ip circuit max-calls 1000
    ip circuit carrier-id AA reserved-calls 500
    ip circuit carrier-id bb reserved-calls 500
    ip circuit carrier-id cc reserved-calls 100
```

The following examples show the default carrier configured with an incoming source carrier but no voice source group configured.



#### Note

In this example, 800 call legs are implicitly reserved for the default circuit.

#### Default Carrier and Incoming Source Carrier with No Voice Source Group



#### Note

A gatekeeper is required with carrier-id routing.

```
voice service voip
  allow-connections h323 to h323
  h323
    ip circuit max-calls 1000
    ip circuit carrier-id AA reserved-calls 200
```

If there is no incoming source carrier ID:

- Capacity only is reported to the GK using the default circuit (two call legs).
- No source or destination carrier information is reported.

If there is an incoming source carrier ID called “AA”:

- One call leg is counted against circuit “AA”.
- One call leg (outbound) is counted against the default circuit.
- The source carrier ID is passed through the gateway to the terminating leg.

If there is an incoming source carrier ID called “BB” (for example) or anything other than “AA”:

- Two call legs are counted against the default circuit.
- The source carrier ID “BB” is passed through the gateway to the terminating leg.

The following examples show the first voice source-group match case:

#### Voice Source-Group Match Case 1

```
voice service voip
  allow-connections h323 to h323
  h323
    ip circuit max-calls 1000
    ip circuit carrier-id AA reserved-calls 200
```

```
!
voice source-group 1
  carrier-id source AA
  carrier-id target AA
```

If there is no incoming source carrier ID, the default circuit is used because there is no match in the voice source group.

If there is an incoming source carrier ID called “AA,” the following are in effect:

- The voice source group matches.
- Both call legs are counted against circuit “AA”.
- The source carrier ID is passed through the gateway to the terminating leg.
- The destination carrier ID is “AA”.

The following examples show the second voice source group match case:

### Voice Source-Group Match Case 2

```
voice service voip
  allow-connections h323 to h323
  h323
    ip circuit max-calls 1000
    ip circuit carrier-id AA reserved-calls 200
    ip circuit carrier-id BB reserved-calls 200
!
voice source-group 1
  carrier-id source AA
  carrier-id target BB
```

If there is no incoming source carrier ID, the default circuit is used because there is no match in the voice source group.

If there is an incoming source carrier ID called “AA”:

- The voice source-group matches.
- One leg is counted against circuit “AA”.
- One leg is counted against circuit “BB”.
- The source carrier ID is passed through the gateway to the terminating leg.
- The destination carrier ID is “BB”.

The following examples show the third voice source-group match case:

### Voice Source-Group Match Case 3

```
voice service voip
  allow-connections h323 to h323
  h323
    ip circuit max-calls 1000
    ip circuit carrier-id AA reserved-calls 200
    ip circuit carrier-id BB reserved-calls 200
!
voice source-group 1
  access-list 1
  carrier-id source BB
```

If the access-list matches, the following apply:

- One leg is counted against circuit “BB”.
- One leg is counted against the default circuit (for the destination circuit).

- The source carrier ID is synthesized to “BB” and used to report to the gatekeeper. It is also used on the outgoing setup.

If a source carrier ID is received on the incoming setup, it is overridden with the synthesized carrier ID

## Configuring Overlap Signaling for H.323-to-H.323 Connections on a Cisco Unified Border Element

The terminating gateway is responsible for collecting all the called number digits. Overlap signaling is implemented by matching destination patterns on the dial peers. When H.225 signal overlap is configured on the originating gateway, it sends the SETUP to the terminating gateway once a dial-peer match is found. The originating gateway sends all further digits received from the user to the terminating gateway using INFO messages until it receives a sending complete message from the user. The terminating gateway receives the digits in SETUP and subsequent INFO messages and does a dial-peer match. If a match is found, it sends a SETUP with the collected digits to the PSTN. All subsequent digits are sent to the PSTN using INFO messages to complete the call.

To configure overlap signaling in an Cisco Unified Border Element, perform the steps in this section.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **h323**
5. **h225 signal overlap**
6. **h225 timeout t302**
7. **exit**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<code>configure terminal</code>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<code>voice service voip</code>  <b>Example:</b> Router(config)# voice service voip	Enters VoIP voice-service configuration mode.

	Command or Action	Purpose
Step 4	<pre>h323</pre> <p><b>Example:</b> Router(conf-voi-serv)# h323</p>	Enters H.323 voice-service configuration mode.
Step 5	<pre>h225 signal overlap</pre> <p><b>Example:</b> Router(conf-serv-h323)# h225 signal overlap</p>	Activates overlap signaling to the destination gateway.
Step 6	<pre>h225 timeout t302 seconds</pre> <p><b>Example:</b> Router(conf-serv-h323)# h225 timeout t302 15</p>	Sets the t302 timer timeout value. The argument is as follows: <ul style="list-style-type: none"> <li><i>seconds</i>— Number of seconds for timeouts. Range: 1 to 30.</li> </ul>
Step 7	<pre>exit</pre> <p><b>Example:</b> Router(conf-serv-h323)# exit</p>	Exits the current mode.

## Troubleshooting Tips



### Caution

Under moderate traffic loads, these **debug** commands produce a high volume of output.

- Use the **debug voip ipipgw** command to debug the Cisco Unified Border Element feature.
- Use any of the following additional **debug** commands on the gateway as appropriate:

#### H.323 Call-Type Scenarios

- **debug cch323 all**
- **debug h225 asn1**
- **debug h225 events**
- **debug h225 q931**
- **debug h245 asn1**
- **debug h245 events**
- **debug voip ipipgw**
- **debug voip ccapi inout**

**Note**

For examples of **show** and **debug** command output and details on interpreting the output, see the following resources:

- [Cisco IOS Debug Command Reference](#), Release 12.4T
- [Cisco IOS Voice Troubleshooting and Monitoring Guide](#)
- [Troubleshooting and Debugging VoIP Call Basics](#)
- [Voice Gateway Error Decoder for Cisco IOS](#)
- [VoIP Debug Commands](#)

## Verifying H.323-to-H.323 Cisco Unified Border Element Configuration and Operation

To verify Cisco Unified Border Element feature configuration and operation, perform the following steps (listed alphabetically) as appropriate.

**Note**

The word “calls” refers to call legs in some commands and output.

### SUMMARY STEPS

1. **show call active video**
2. **show call active voice**
3. **show call history fax**
4. **show call history video**
5. **show call history voice**
6. **show crm**
7. **show dial-peer voice**
8. **show running-config**
9. **show voip rtp connections**

### DETAILED STEPS

- 
- |               |   |
|---------------|---|
| <b>Step 1</b> | <b>show call active video</b><br>Use this command to display the active video H.323 call legs.                      |
| <b>Step 2</b> | <b>show call active voice</b><br>Use this command to display call information for voice calls that are in progress. |
| <b>Step 3</b> | <b>show call active fax</b><br>Use this command to display the fax transmissions that are in progress.              |
| <b>Step 4</b> | <b>show call history video</b>  |

Use this command to display the history of video H.323 call legs.

**Step 5 show call history voice**

Use this command to display the history of voice call legs.

**Step 6 show call history fax**

Use this command to display the call history table for fax transmissions that are in progress.

**Step 7 show crm**

Use this command to display the carrier ID list or IP circuit utilization.

**Step 8 show dial-peer voice**

Use this command to display information about voice dial peers.

**Step 9 show running-config**

Use this command to verify which H.323-to-H.323, H.323-to-SIP, or SIP-to-SIP connection types are supported.

**Step 10 show voip rtp connections**

Use this command to display active Real-Time Transport Protocol (RTP) connections.

---

## Where to Go Next

- [H.323-to-SIP Connections on a Cisco Unified Border Element](#)
- [SIP-to-SIP Connections on a Cisco Unified Border Element](#)
- [Cisco Unified Border Element for H.323 Cisco Unified Communications Manager to H.323 Service Provider Connectivity](#)
- [Configuring Cisco Unified Border Element Videoconferencing](#)

# Additional References

The following sections provide references related to H.323-to-H.323 Cisco UBE Connections:

## Related Documents

Related Topic	Document Title
Cisco IOS Release 12.4	<ul style="list-style-type: none"> <li>• <a href="#">Cisco IOS Release 12.4 Configuration Guides</a></li> <li>• <a href="#">Cisco IOS Release 12.4T Configuration Guides</a></li> <li>• <a href="#">Cisco IOS Release 12.4 Command References</a></li> <li>• <a href="#">Cisco IOS Voice Configuration Library</a></li> </ul> <p><a href="http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/cisco_ios_voice_configuration_library_glossary/vcl.htm">http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/cisco_ios_voice_configuration_library_glossary/vcl.htm</a></p>  <p><b>Note</b> This website contains the library preface and glossary.</p>
Cisco IOS Release 12.3	<ul style="list-style-type: none"> <li>• <a href="#">Cisco IOS Release 12.3 documentation</a></li> <li>• <a href="#">Cisco IOS voice commands</a></li> <li>• <a href="#">Cisco IOS Voice Troubleshooting and Monitoring Guide</a></li> <li>• <a href="#">Tcl IVR Version 2.0 Programming Guide</a></li> </ul>
Cisco IOS Release 12.2	<ul style="list-style-type: none"> <li>• <i>Cisco IOS Voice, Video, and Fax Configuration Guide</i>, Release 12.2 at <a href="http://www.cisco.com/en/US/docs/ios/12_2/voice/configuration/guide/fvfvfax_c.html">http://www.cisco.com/en/US/docs/ios/12_2/voice/configuration/guide/fvfvfax_c.html</a></li> </ul>
DSP documentation	<p>High-Density Packet Voice Feature Card for Cisco AS5350XM and AS5400XM Universal Gateways</p> <p><a href="http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/1241imit/124x/124xc4/vfc_dsp.htm">http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/1241imit/124x/124xc4/vfc_dsp.htm</a></p>
GKTMP (GK API) Documents	<ul style="list-style-type: none"> <li>• <i>GKTMP Command Reference</i>: <a href="http://www.cisco.com/en/US/docs/ios/12_2/gktmp/gktmpv4_2/gk_cli.htm">http://www.cisco.com/en/US/docs/ios/12_2/gktmp/gktmpv4_2/gk_cli.htm</a></li> <li>• <i>GKTMP Messages</i>: <a href="http://www.cisco.com/en/US/docs/ios/12_2/gktmp/gktmpv4_2/gk_tmp.html">http://www.cisco.com/en/US/docs/ios/12_2/gktmp/gktmpv4_2/gk_tmp.html</a></li> </ul>
internet Low Bitrate Codec (iLBC) Documents	<ul style="list-style-type: none"> <li>• Codecs section of the Dial Peer Configuration on Voice Gateway Routers Guide <a href="http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vfax_c/int_c/dpeer_c/dp_ovrvw.htm#1035124">http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vfax_c/int_c/dpeer_c/dp_ovrvw.htm#1035124</a></li> <li>• Dial Peer Features and Configuration section of the Dial Peer Configuration on Voice Gateway Routers Guide <a href="http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vfax_c/int_c/dpeer_c/dp_config.htm">http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vfax_c/int_c/dpeer_c/dp_config.htm</a></li> </ul>

Related Topic	Document Title
Cisco Unified Border Element Configuration Examples	<ul style="list-style-type: none"> <li>• Local-to-remote network using the IPIPGW <a href="http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a00801b0803.shtml">http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a00801b0803.shtml</a></li> <li>• Remote-to-local network using the IPIPGW: <a href="http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a0080203edc.shtml">http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a0080203edc.shtml</a></li> <li>• Remote-to-remote network using the IPIPGW: <a href="http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a0080203edd.shtml">http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a0080203edd.shtml</a></li> <li>• Remote-to-remote network using two IPIPGWs: <a href="http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a0080203edb.shtml">http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a0080203edb.shtml</a></li> </ul>
Related Application Guides	<ul style="list-style-type: none"> <li>• <a href="#">Cisco Unified Communications Manager and Cisco IOS Interoperability Guide</a></li> <li>• <a href="#">Cisco IOS Fax, Modem, and Text Support over IP Configuration Guide</a></li> <li>• “Configuring T.38 Fax Relay” chapter</li> <li>• <a href="#">Cisco IOS SIP Configuration Guide</a></li> <li>• Cisco Unified Communications Manager (CallManager) Programming Guides at: <a href="http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_programming_reference_guides_list.html">http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_programming_reference_guides_list.html</a></li> <li>• <i>Quality of Service for Voice over IP</i> at <a href="http://www.cisco.com/en/US/docs/ios/solutions_docs/qos_solutions/QoSVoIP/QoSVoIP.html">http://www.cisco.com/en/US/docs/ios/solutions_docs/qos_solutions/QoSVoIP/QoSVoIP.html</a></li> </ul>
Related Platform Documents	<ul style="list-style-type: none"> <li>• <a href="#">Cisco 2600 Series Multiservice Platforms</a></li> <li>• <a href="#">Cisco 2800 Series Integrated Services Routers</a></li> <li>• <a href="#">Cisco 3600 Series Multiservice Platforms</a></li> <li>• <a href="#">Cisco 3700 Series Multiservice Access Routers</a></li> <li>• <a href="#">Cisco 3800 Series Integrated Services Routers</a></li> <li>• <a href="#">Cisco 7200 Series Routers</a></li> <li>• <a href="#">Cisco 7301</a></li> </ul>
Related gateway configuration documentation	<p>Media and Signaling Authentication and Encryption Feature for Cisco IOS H.323 Gateways.</p> <p><a href="http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/htsecure.htm">http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/htsecure.htm</a></p>



Related Topic	Document Title
Cisco IOS NAT Configuration Guide, Release 12.4T	<ul style="list-style-type: none"> <li>• <i>Configuring Cisco IOS Hosted NAT Traversal for Session Border Controller</i> at <a href="http://www.cisco.com/en/US/docs/ios/12_4t/ip_addr/configuration/guide/htnatsbc.html">http://www.cisco.com/en/US/docs/ios/12_4t/ip_addr/configuration/guide/htnatsbc.html</a></li> </ul>
Troubleshooting and Debugging guides	<ul style="list-style-type: none"> <li>• Cisco IOS Debug Command Reference, Release 12.4 at <a href="http://www.cisco.com/en/US/docs/ios/debug/command/reference/db_book.html">http://www.cisco.com/en/US/docs/ios/debug/command/reference/db_book.html</a></li> <li>• <i>Troubleshooting and Debugging VoIP Call Basics</i> at <a href="http://www.cisco.com/en/US/tech/tk1077/technologies_tech_note09186a0080094045.shtml">http://www.cisco.com/en/US/tech/tk1077/technologies_tech_note09186a0080094045.shtml</a></li> <li>• <i>VoIP Debug Commands</i> at <a href="http://www.cisco.com/en/US/docs/routers/access/1700/1750/software/configuration/guide/debug.html">http://www.cisco.com/en/US/docs/routers/access/1700/1750/software/configuration/guide/debug.html</a></li> </ul>

## Standards

Standards	Title
H.323 Version 4 and earlier	<i>H.323 (ITU-T VOIP protocols)</i>

## MIBs

MIBs	MIBs Link
None.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

RFCs	Title
RFC 2833	<i>RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals</i>
RFC 3261	<i>SIP: Session Initiation Protocol</i>

## 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><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></p>

## Feature Information for H.323-to-H.323 Cisco Unified Border Element Connections

Table 1 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.3(1) or a later release appear in the table.

For information on a feature in this technology that is not documented here, see the “[Cisco Unified Border Element Features Roadmap](#)”



### Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for H.323-to-H.323 Gateway Connections

Feature Name	Releases	Feature Information
Call Admission Control.	12.4(6)T	This feature was introduced.
Cisco Unified Communications Manager Connections	12.4(6)T	No MTP for Cisco Unified Communications Manager Trunks to Cisco Unified Border Element.
Codec Support	12.4(11)T	Configuring iLBC Codec on an Cisco Unified Border Element
DTMF	12.4(11)T	G.711 Inband DTMF to RFC 283.
H.323-to-H.323 Connections on a Cisco Unified Border Element	12.3(1)	H.323-to-H.323 Gateway configuration provides a network-to-network demarcation point between independent VoIP and video networks by for billing, security, call-admission control, QoS, and signaling interworking.

**Table 1** Feature Information for H.323-to-H.323 Gateway Connections (continued)

Feature Name	Releases	Feature Information
Managing H.323 IP Group Call Capacities	12.2(13)T	Creates a maximum capacity for the IP group providing extra control for load and resource balancing.
Media Modes	12.3(1)	Media Flow-Around. Adds media flow-around capability on the Cisco UBE by supporting the processing of call set-up and teardown request (VoIP call signaling) and for media streams (flow-through and flow-around) Improves scalability and performance when network-topology hiding and bearer-level interworking features are not required.
Overlap Signaling for H.323-to-H.323 Connections on a Cisco Unified Border Element	12.3(11)T	The terminating gateway is responsible for collecting all the called number digits. Overlap signaling is implemented by matching destination patterns on the dial peers.
Rotary Support	12.3(11)T 12.4(6)T	12.3(11)T—H.323-to-H.323 Call Failure Recovery (Rotary) on a Cisco Unified Border Element. Eliminates codec restrictions and enables the Cisco UBE to restart codec negotiation with the originating endpoint based on the codec capabilities of the next dial peer in the rotary group for H.323-to-H.323 interconnections.  12.4(6)T—Secure RTP with IPSEC for Signaling.
Signal Interworking	12.3(11)T	H.323-to-H.323 Interworking Between Fast Start and Slow Start. This feature enables the Cisco UBE to bridge calls between VoIP endpoints that support only H.323 FastStart procedures and endpoints that support only normal H.245 signaling (SlowStart).

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 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.

© 2009 Cisco Systems, Inc. All rights reserved.





# H.323-to-SIP Connections on a Cisco Unified Border Element

---

**Revised:** July 11, 2008,  
**First Published:** June 19, 2006  
**Last Updated:** July 11, 2008

This chapter describes how to configure and enable features for H.323-to-SIP connections in a Cisco Unified Border Element topology.

## Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for H.323-to-SIP Connections on a Cisco Unified Border Element, page 129](#)”

## Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS 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.

## Contents

- [Prerequisites for Configuring H.323-to-SIP Connection on a Cisco Unified Border Element, page 112](#)
- [Restrictions for H.323-to-SIP Connections on a Cisco Unified Border Element, page 112](#)
- [Information About H.323-to-SIP Connections on a Cisco Unified Border Element, page 113](#)
- [How to Configure H.323-to-SIP Connections on a Cisco Unified Border Element, page 113](#)
- [Where to Go Next, page 125](#)
- [Additional References, page 126](#)
- [Feature Information for H.323-to-SIP Connections on a Cisco Unified Border Element, page 129](#)



---

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

© 2009 Cisco Systems, Inc. All rights reserved.

## Prerequisites for Configuring H.323-to-SIP Connection on a Cisco Unified Border Element

- Perform the prerequisites listed in the “Prerequisites for Cisco Unified Border Element Configuration” section on page 20 in this guide.
- Perform fundamental gateway configuration listed in the “Prerequisites for Fundamental Cisco Unified Border Element Configuration” section on page 44 in this guide.
- Perform basic H.323 gateway configuration.
- Perform basic H.323 gatekeeper configuration.

**Note**

For configuration instructions, see the “[Configuring H.323 Gateways](#)” and “[Configuring H.323 Gatekeepers](#)” chapters of the *Cisco IOS Voice, Video, and Fax Configuration Guide*, Release 12.2.

## Restrictions for H.323-to-SIP Connections on a Cisco Unified Border Element

- Changing codecs during rotary dial peer selection is not supported.
- Codec preference order in voice class should be the same in all dial peers.
- Configure extended capabilities on dial peers for fast start-to-early media scenarios.
- Delayed Offer to Slow-Start is not supported for SRTP-to-SRTP H.323-to-SIP calls.
- During a triggered INVITE scenario the Cisco UBE always generates a delayed offer INVITE.
- Fast-start to delayed-media signal interworking is not supported.
- Fast Start to Early Offer Supplementary Service will not work without extended capabilities configured under dial-peer.
- GSMFR and GSMEFR codecs are not supported.
- H450.2 & H450.3 are enabled & invisible under dial peers by default. H.450 cannot be enabled at the dial peer level if they are globally disabled.
- Media flow-around is not supported.
- Passing multiple diversion headers or multiple contact header in 302 to the H.323 leg is not supported.
- RSVP for supplementary scenarios is not supported.
- Session refresh is not supported.
- SIP-to-H.323 Supplementary Services based on H.450 is not supported.
- Slow-start to early media signal interworking is not supported.
- Supplementary services are Empty Capability Set (ECS) based supplementary services from the H.323 perspective, not H.450 supplementary services.
- Transcoding for supplementary calls is not supported.

- DTMF Interworking rtp-nte to out of band is not supported when high density transcoder is enabled. Use normal transcoding for rtp-nte to out of band DTMF interworking.

**Cisco IOS Release 12.4(15)XY and earlier releases:**

- SRTP Passthrough is not supported.

**Cisco IOS Release 12.4(11)XJ2 and earlier releases:**

- Delayed-media to slow-start signal interworking is not supported.
- H323-SIP Supplementary Services is not supported (ECS based).

**Cisco IOS Release 12.4(11)T and earlier releases:**

- Codec Transparent is not supported.

**Cisco IOS Release 12.4(2)T and earlier releases:**

- Extended codec support and codec filtering is not supported.

**Cisco IOS Release 12.3(8)T and earlier releases:**

- Basic call is not supported.

## Information About H.323-to-SIP Connections on a Cisco Unified Border Element

- All codecs using static payload are supported.
- Fast-start to early media signal interworking is supported.
- H.323-to-SIP Supplementary Services are supported in Cisco IOS Release 12.4(15)XY and later.
- Supported codecs using dynamic payload are g726r16 and g726r24.
- Slow-start to delayed-media signal interworking is supported.
- One or multiple codes may configured on the incoming and out-going dial-peer.
- SRTP-to-SRTP for SIP-to-H.323 calls is supported:
  - Supported signal interworking include: Fast-Start to Early Offer, Early Offer to Fast-Start, and Slow-Start to Delayed Offer.

## How to Configure H.323-to-SIP Connections on a Cisco Unified Border Element

The section contains the following tasks:

- [H.323-to-SIP Basic Call Interworking for Session Border Controller \(SBC\)](#), page 114
- [H.323-to-SIP Supplementary Feature Interworking for Session Border Controller \(SBC\)](#), page 114
- [H.323-to-SIP Supplementary Service Enhancements for Session Border Controller \(SBC\)](#), page 115
- [Configuring H.323-to-SIP Connections on a Cisco Unified Border Element](#), page 115
- [Configuring DTMF Relay Digit-Drop on a Cisco Unified Border Element](#), page 116

- [Configuring H.323-to-SIP Call Failure Recovery \(Rotary\) on a Cisco Unified Border Element, page 118](#)
- [Managing H.323 IP Group Call Capacities, page 119](#)
- [Troubleshooting and Verifying H.323-to-SIP connections on a Cisco Unified Border Element, page 123](#)

## H.323-to-SIP Basic Call Interworking for Session Border Controller (SBC)

This feature enables the IP-to-IP gateway to bridge calls between networks that support different VoIP call-signaling protocols (SIP and H.323). The SIP-to-H.323 protocol interworking capabilities of the Cisco Unified Border Element support the following:

- Basic voice calls (G.711 and G.729 codecs)
- UDP and TCP transport
- Interworking between H.323 Fast-Start and SIP early-media signaling
- Interworking between H.323 Slow-Start and SIP delayed-media signaling
- DTMF relay interworking:
  - H.245 alpha/signal <--> SIP RFC 2833
  - H.245 alpha/signal <--> SIP Notify
- Codec transcoding (G.711-G.729)
- Calling/called name and number
- T.38 fax relay and Cisco fax relay
- RADIUS call-accounting records
- RSVP synchronized with call signaling
- TCL IVR 2.0 for SIP, including media playout and digit collection (RFC 2833 DTMF relay)

## H.323-to-SIP Supplementary Feature Interworking for Session Border Controller (SBC)

Provides enhanced termination and re-origination of signaling and media between VoIP and Video Networks in conformance with RFC3261. New features offered in this release on the Cisco 28xx, 38xx, 5350XM and 5400XM include:

- Support H.323-to-SIP Supplementary services for Cisco Unified Communications Manager with MTP on the H.323 Trunk.
- ILBC Codec Support
- Interworking between G.711 inband DTMF to RFC2833
- VXML 3.x support
- VXML support with SIP Notify



## Restrictions

- H450.2 & H450.3 are enabled & invisible under dialpeers by default. H.450 cannot be enabled at the dial peer level if they are globally disabled.
- RSVP for supplementary scenarios is not supported.
- Transcoding for supplementary calls is not supported.

## H.323-to-SIP Supplementary Service Enhancements for Session Border Controller (SBC)

H.323-to-SIP features offered in this release include:

- Mapping ECS to ReINVITE and ECS to REFER on the Cisco IOS SBC.

## Configuring H.323-to-SIP Connections on a Cisco Unified Border Element

To configure H.323-to-SIP connections on a Cisco Unified Border Element, perform the steps in this section.

### Restrictions

Connections are disabled by default in Cisco IOS images that support the Cisco Unified Border Element

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `voice service voip`
4. `allow-connections`
5. `exit`

### DETAILED STEPS

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

	Command or Action	Purpose
Step 3	<code>voice service voip</code>  <b>Example:</b> <code>Router(config)# voice service voip</code>	Enters VoIP voice-service configuration mode.
Step 4	<code>allow-connections from-type to to-type</code>  <b>Example:</b> <code>Router(conf-voi-serv)# allow-connections h323 to sip</code>	Allows connections between specific types of endpoints in an Cisco Unified Border Element. Arguments are as follows: <ul style="list-style-type: none"> <li><i>from-type</i>—Type of connection. Valid values: <b>h323, sip</b>.</li> <li><i>to-type</i>—Type of connection. Valid values: <b>h323, sip</b>.</li> </ul> <b>Note</b> H.323-to-H.323: By default, H.323-to-H.323 connections are disabled and POTS-to-any and any-to-POTS connections are enabled.
Step 5	<code>exit</code>  <b>Example:</b> <code>Router(conf-voi-serv)# exit</code>	Exits the current mode.

## Configuring DTMF Relay Digit-Drop on a Cisco Unified Border Element

To avoid sending both in-band and out-of band tones to the outgoing leg when sending Cisco Unified Border Element calls in-band (rtp-nte) to out-of band (h245-alphanumeric). Configure the **dtmf-relay rtp-nte digit-drop** command on the incoming SIP dial-peer. On the H.323 side configure either **dtmf-relay h245-alphanumeric** or **dtmf-relay h245-signal**. This may also be used for H.323-to-SIP calls.

To configure DTMF relay digit drop on an Cisco Unified Border Element, perform the steps in this section.

### Restrictions

The debug output will show that the H245 out of band messages are sent to the TGW. However, the digits are not heard on the phone.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice tag voip**
4. **dtmf-relay [cisco-rtp] [h245-alphanumeric] [rtp-nte [digit-drop]]**
5. **exit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<pre>enable</pre> <p><b>Example:</b> Router&gt; enable </p>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<pre>configure terminal</pre> <p><b>Example:</b> Router# configure terminal </p>	Enters global configuration mode.
Step 3	<pre>dial-peer voice number voip</pre> <p><b>Example:</b> Router(config)# dial-peer voice 2 voip </p>	Enters dial-peer configuration mode for the specified VoIP dial peer.
Step 4	<pre>dtmf-relay [cisco-rtp] [h245-alphanumeric] [rtp-nte] [digit-drop]</pre> <p><b>Example:</b> Router (config-dial-peer)# dtmf-relay rtp-nte digit-drop h245-alphanumeric </p>	Forwards DTMF tones. Keywords are as follows: <ul style="list-style-type: none"> <li>• <b>cisco-rtp</b>—Forwards DTMF tones by using RTP with a Cisco-proprietary payload type.</li> <li>• <b>h245-alphanumeric</b>—Forwards DTMF tones by using the H.245 alphanumeric method.</li> <li>• <b>h245-signal</b>—Forwards DTMF tones by using the H.245 signal UII method.</li> <li>• <b>rtp-nte</b>—Forwards DTMF tones by using Real-Time Transport Protocol (RTP) with the Named Telephone Event (NTE) payload type.</li> <li>• <b>digit-drop</b>—Passes digits out-of-band, and in-band digits are dropped.</li> </ul> <p><b>Note</b> The <b>digit-drop</b> keyword is only seen when the <b>rtp-nte</b> keyword is configured.</p>
Step 5	<pre>exit</pre> <p><b>Example:</b> Router(config-dial-peer)# exit </p>	Exits the current mode.

## Examples

The following example shows DTMF-Relay digits configured to avoid sending both in-band and out-of-band tones to the outgoing leg in an Cisco Unified Border Element:

```
.
.
.
dial-peer voice 1 voip
  voice-class codec 2
  dtmf-relay rtp-nte digit-drop h245-alphanumeric
.
.
.
```

## Configuring H.323-to-SIP Call Failure Recovery (Rotary) on a Cisco Unified Border Element

Call failure recovery (Rotary) on the Cisco Unified Border Element eliminates the need for identical codec capabilities for all dial peers in the rotary group, and allows the Cisco Unified Border Element to restart the codec negotiation end-to-end. Call failure recovery will continue until “voice hunt stop” is reached.

To configure H.323-to-SIP call failure recovery (rotary) on an Cisco Unified Border Element, perform the steps in this section.

### Restrictions

If extended caps (DTMF or T.38) are configured on the outgoing gateway or the trunking gateway, extended caps must be configured in both places.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **h323**
5. **emptycapability**
6. **exit**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> <code>Router&gt; enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<code>configure terminal</code>  <b>Example:</b> <code>Router# configure terminal</code>	Enters global configuration mode.
Step 3	<code>voice service voip</code>  <b>Example:</b> <code>Router(config)# voice service voip</code>	Enters VoIP voice-service configuration mode.
Step 4	<code>h323</code>  <b>Example:</b> <code>Router(conf-voi-serv)# h323</code>	Enters H.323 voice-service configuration mode.

	Command or Action	Purpose
Step 5	<code>emptycapability</code>  <b>Example:</b> <code>Router(conf-serv-h323)# emptycapability</code>	Enables call failure recovery (TCS=0).
Step 6	<code>exit</code>  <b>Example:</b> <code>Router(conf-serv-h323)# exit</code>	Exits the current mode.

## Managing H.323 IP Group Call Capacities

The Cisco Unified Border Element feature works with the **voice source-group** command to provide matching criteria for incoming calls. The **voice source-group** command assigns a name to a set of source IP group characteristics. The terminating gateway uses these characteristics to identify and translate the incoming VoIP call. If there is no voice source group match, the default carrier ID is used, any source carrier ID on the incoming message is transmitted without change, and no destination carrier is available. Call-capacity information is reported to the gatekeeper, but carrier routing information is not.

If the voice source group matches, the matched source carrier ID is used and the target carrier ID defined in the voice source group is used for the destination carrier ID.

To configure H.323 IP call capabilities, perform the steps in this section.

### Restrictions

You can use the commands that follow only when no calls are active. If you try to use these commands with active calls present, the commands are rejected.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **h323**
5. **ip circuit max-calls**
6. **ip circuit carrier-id**
7. **ip circuit default only**
8. **ip circuit default name**
9. **exit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<pre>enable</pre> <p><b>Example:</b> Router&gt; enable </p>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<pre>configure terminal</pre> <p><b>Example:</b> Router# configure terminal </p>	Enters global configuration mode.
Step 3	<pre>voice service voip</pre> <p><b>Example:</b> Router(config)# voice service voip </p>	Enters VoIP voice-service configuration mode.
Step 4	<pre>h323</pre> <p><b>Example:</b> Router(config-voice-service)# h323 </p>	Enters H.323 voice-service configuration mode.
Step 5	<pre>ip circuit carrier-id carrier-name [reserved-calls reserved]</pre> <p><b>Example:</b> Router(config-serv-h323)# ip circuit carrier-id AA reserved-calls 500 </p>	(Optional) Defines an IP circuit using the specified name as the circuit ID.  <b>Note</b> The <b>reserved</b> keyword for this command is optional. Using this keyword creates a specified maximum number of calls for that circuit ID. The default value is 200 call legs.
Step 6	<pre>ip circuit default only</pre> <p><b>Example:</b> Router(config-serv-h323)# ip circuit default only </p>	(Optional) Creates a single carrier to use all of the call capacity available to the Cisco Unified Border Element.  <b>Note</b> If you use the <b>ip circuit default only</b> command, you cannot use the <b>ip circuit carrier-id</b> command to configure more circuits. Using the <b>ip circuit default only</b> command creates a single carrier using the default carrier name.
Step 7	<pre>ip circuit default name carrier-name</pre> <p><b>Example:</b> Router(config-serv-h323)# ip circuit default name AA </p>	(Optional) Changes the default circuit name.
Step 8	<pre>exit</pre> <p><b>Example:</b> Router(config-serv-h323)# exit </p>	Exits the current mode.

## Examples

The following examples show a default carrier with no voice source group configured:

**Default Carrier with No Voice Source Group**

```
voice service voip
  allow-connections h323 to h323
  h323
    ip circuit max-calls 1000
    ip circuit default only
```

If there is no incoming source carrier ID:

- Capacity only is reported to the gatekeeper using the default circuit (two call legs).
- No source or destination carrier information is reported.

If there is an incoming source carrier ID:

- Two call legs are counted against the default circuit and reported to the GK.
- The source carrier ID is passed through the gateway to the terminating leg.

The following examples show a configuration with more reserved calls than the default value for the **max-calls** argument (1000):

**Configuration with Default Calls in Excess of 1000**

This example assigns 1100 calls to other carriers, leaving 400 calls available to the default carrier:

```
voice service voip
  allow-connections h323 to h323
  h323
    ip circuit max-calls 1000
    ip circuit carrier-id AA reserved-calls 500
    ip circuit carrier-id bb reserved-calls 500
    ip circuit carrier-id cc reserved-calls 100
```

The following examples show the default carrier configured with an incoming source carrier but no voice source group configured.

**Note**


---

In this example, 800 call legs are implicitly reserved for the default circuit.

---

**Default Carrier and Incoming Source Carrier with No Voice Source Group****Note**


---

A gatekeeper is required with carrier-id routing.

---

```
voice service voip
  allow-connections h323 to h323
  h323
    ip circuit max-calls 1000
    ip circuit carrier-id AA reserved-calls 200
```

If there is no incoming source carrier ID:

- Capacity only is reported to the GK using the default circuit (two call legs).
- No source or destination carrier information is reported.

If there is an incoming source carrier ID called “AA”:

- One call leg is counted against circuit “AA”.
- One call leg (outbound) is counted against the default circuit.

- The source carrier ID is passed through the gateway to the terminating leg.

If there is an incoming source carrier ID called “BB” (for example) or anything other than “AA”:

- Two call legs are counted against the default circuit.
- The source carrier ID “BB” is passed through the gateway to the terminating leg.

The following examples show the first voice source-group match case:

#### Voice Source-Group Match Case 1

```
voice service voip
  allow-connections h323 to h323
  h323
    ip circuit max-calls 1000
    ip circuit carrier-id AA reserved-calls 200
  !
voice source-group 1
  carrier-id source AA
  carrier-id target AA
```

If there is no incoming source carrier ID, the default circuit is used because there is no match in the voice source group.

If there is an incoming source carrier ID called “AA,” the following are in effect:

- The voice source group matches.
- Both call legs are counted against circuit “AA”.
- The source carrier ID is passed through the gateway to the terminating leg.
- The destination carrier ID is “AA”.

The following examples show the second voice source group match case:

#### Voice Source-Group Match Case 2

```
voice service voip
  allow-connections h323 to h323
  h323
    ip circuit max-calls 1000
    ip circuit carrier-id AA reserved-calls 200
    ip circuit carrier-id BB reserved-calls 200
  !
voice source-group 1
  carrier-id source AA
  carrier-id target BB
```

If there is no incoming source carrier ID, the default circuit is used because there is no match in the voice source group.

If there is an incoming source carrier ID called “AA”:

- The voice source-group matches.
- One leg is counted against circuit “AA”.
- One leg is counted against circuit “BB”.
- The source carrier ID is passed through the gateway to the terminating leg.
- The destination carrier ID is “BB”.

The following examples show the third voice source-group match case:



### Voice Source-Group Match Case 3

```
voice service voip
  allow-connections h323 to h323
  h323
    ip circuit max-calls 1000
    ip circuit carrier-id AA reserved-calls 200
    ip circuit carrier-id BB reserved-calls 200
  !
voice source-group 1
  access-list 1
  carrier-id source BB
```

If the access-list matches, the following apply:

- One leg is counted against circuit “BB”.
- One leg is counted against the default circuit (for the destination circuit).
- The source carrier ID is synthesized to “BB” and used to report to the gatekeeper. It is also used on the outgoing setup.
- If a source carrier ID is received on the incoming setup, it is overridden with the synthesized carrier ID.

## Troubleshooting and Verifying H.323-to-SIP connections on a Cisco Unified Border Element

To troubleshoot or verify connections in an Cisco Unified Border Element, perform the steps in this section. This section contains the following subsections:

- [Troubleshooting Tips, page 123](#)
- [Verifying Cisco Unified Border Element Configuration and Operation, page 124](#)

### Troubleshooting Tips



#### Caution

---

Under moderate traffic loads, these **debug** commands produce a high volume of output.

---

- Use the **debug voip ipipgw** command to debug the Cisco Unified Border Element feature.
- Use any of the following additional **debug** commands on the gateway as appropriate:
  - **debug cch323 all**
  - **debug ccsip all**
  - **debug h225 asn1**
  - **debug h225 events**
  - **debug h245 asn1**
  - **debug h245 events**
  - **debug voip ipipgw**
  - **debug voip ccapi inout**

**Note**

For examples of **show** and **debug** command output and details on interpreting the output, see the following resources:

- [Cisco IOS Debug Command Reference](#), Release 12.4T
- [Cisco IOS Voice Troubleshooting and Monitoring Guide](#)
- [Troubleshooting and Debugging VoIP Call Basics](#)
- [Voice Gateway Error Decoder for Cisco IOS](#)
- [VoIP Debug Commands](#)

## Verifying Cisco Unified Border Element Configuration and Operation

To verify Cisco Unified Border Element IP-to-IP feature configuration and operation, perform the following steps (listed alphabetically) as appropriate.

**Note**

The word “calls” refers to call legs in some commands and output.

### SUMMARY STEPS

1. **show call active video**
2. **show call active voice**
3. **show call history fax**
4. **show call history video**
5. **show call history voice**
6. **show crm**
7. **show dial-peer voice**
8. **show running-config**
9. **show voip rtp connections**

### DETAILED STEPS

- 
- Step 1** **show call active video**  
Use this command to display the active video H.323 call legs.
- Step 2** **show call active voice**  
Use this command to display call information for voice calls that are in progress.
- Step 3** **show call active fax**  
Use this command to display the fax transmissions that are in progress.
- Step 4** **show call history video**  
Use this command to display the history of video H.323 call legs.
- Step 5** **show call history voice**  
Use this command to display the history of voice call legs.

**Step 6 show call history fax**

Use this command to display the call history table for fax transmissions that are in progress.

**Step 7 show crm**

Use this command to display the carrier ID list or IP circuit utilization.

**Step 8 show dial-peer voice**

Use this command to display information about voice dial peers.

**Step 9 show running-config**

Use this command to verify which H.323-to-H.323, H.323-to-SIP, or SIP-to-SIP connection types are supported.

**Step 10 show voip rtp connections**

Use this command to display active Real-Time Transport Protocol (RTP) connections.

---


## Where to Go Next

- [H.323-to-H.323 Connections on a Cisco Unified Border Element](#)
- [SIP-to-SIP Connections on a Cisco Unified Border Element](#)
- [Cisco Unified Border Element for H.323 Cisco Unified Communications Manager to H.323 Service Provider Connectivity](#)
- [Configuring Cisco Unified Border Element Videoconferencing](#)

# Additional References

The following sections provide references related to H.323-to-SIP IP-to-IP Gateway Connections

## Related Documents

Related Topic	Document Title
Cisco IOS Release 12.4	<ul style="list-style-type: none"> <li>• <a href="#">Cisco IOS Release 12.4 Configuration Guides</a></li> <li>• <a href="#">Cisco IOS Release 12.4T Configuration Guides</a></li> <li>• <a href="#">Cisco IOS Release 12.4 Command References</a></li> <li>• <a href="#">Cisco IOS Voice Configuration Library</a> <a href="http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/cisco_ios_voice_configuration_library_glossary/vcl.htm">http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/cisco_ios_voice_configuration_library_glossary/vcl.htm</a></li> </ul>  <p><b>Note</b> This website contains the library preface and glossary.</p>
Cisco IOS Release 12.3	<ul style="list-style-type: none"> <li>• <a href="#">Cisco IOS Release 12.3 documentation</a></li> <li>• <a href="#">Cisco IOS voice commands</a></li> <li>• <a href="#">Cisco IOS Voice Troubleshooting and Monitoring Guide</a></li> <li>• <a href="#">Tel IVR Version 2.0 Programming Guide</a></li> </ul>
Cisco IOS Release 12.2	<ul style="list-style-type: none"> <li>• <i>Cisco IOS Voice, Video, and Fax Configuration Guide</i>, Release 12.2 at <a href="http://www.cisco.com/en/US/docs/ios/12_2/voice/configuration/guide/fvfax_c.html">http://www.cisco.com/en/US/docs/ios/12_2/voice/configuration/guide/fvfax_c.html</a></li> </ul>
DSP documentation	<p>High-Density Packet Voice Feature Card for Cisco AS5350XM and AS5400XM Universal Gateways</p> <p><a href="http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124imit/124x/124xc4/vfc_dsp.htm">http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124imit/124x/124xc4/vfc_dsp.htm</a></p>
GKTMP (GK API) Documents	<ul style="list-style-type: none"> <li>• <i>GKTMP Command Reference</i>: <a href="http://www.cisco.com/en/US/docs/ios/12_2/gktmp/gktmpv4_2/gk_cli.htm">http://www.cisco.com/en/US/docs/ios/12_2/gktmp/gktmpv4_2/gk_cli.htm</a></li> <li>• <i>GKTMP Messages</i>: <a href="http://www.cisco.com/en/US/docs/ios/12_2/gktmp/gktmpv4_2/gk_tmp.html">http://www.cisco.com/en/US/docs/ios/12_2/gktmp/gktmpv4_2/gk_tmp.html</a></li> </ul>
internet Low Bitrate Codec (iLBC) Documents	<ul style="list-style-type: none"> <li>• Codecs section of the Dial Peer Configuration on Voice Gateway Routers Guide <a href="http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgr/vfax_c/int_c/dpeer_c/dp_ovrvw.htm#1035124">http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgr/vfax_c/int_c/dpeer_c/dp_ovrvw.htm#1035124</a></li> <li>• Dial Peer Features and Configuration section of the Dial Peer Configuration on Voice Gateway Routers Guide <a href="http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgr/vfax_c/int_c/dpeer_c/dp_config.htm">http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgr/vfax_c/int_c/dpeer_c/dp_config.htm</a></li> </ul>

Related Topic	Document Title
Cisco Unified Border Element Configuration Examples	<ul style="list-style-type: none"> <li>• Local-to-remote network using the IPIPGW <a href="http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a00801b0803.shtml">http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a00801b0803.shtml</a></li> <li>• Remote-to-local network using the IPIPGW: <a href="http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a0080203edc.shtml">http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a0080203edc.shtml</a></li> <li>• Remote-to-remote network using the IPIPGW: <a href="http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a0080203edd.shtml">http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a0080203edd.shtml</a></li> <li>• Remote-to-remote network using two IPIPGWs: <a href="http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a0080203edb.shtml">http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a0080203edb.shtml</a></li> </ul>
Related Application Guides	<ul style="list-style-type: none"> <li>• <a href="#">Cisco Unified Communications Manager and Cisco IOS Interoperability Guide</a></li> <li>• <a href="#">Cisco IOS Fax, Modem, and Text Support over IP Configuration Guide</a></li> <li>• <a href="#">“Configuring T.38 Fax Relay” chapter</a></li> <li>• <a href="#">Cisco IOS SIP Configuration Guide</a></li> <li>• Cisco Unified Communications Manager (CallManager) Programming Guides at: <a href="http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_programming_reference_guides_list.html">http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_programming_reference_guides_list.html</a></li> <li>• <i>Quality of Service for Voice over IP</i> at <a href="http://www.cisco.com/en/US/docs/ios/solutions_docs/qos_solutions/QoSVoIP/QoSVoIP.html">http://www.cisco.com/en/US/docs/ios/solutions_docs/qos_solutions/QoSVoIP/QoSVoIP.html</a></li> </ul>
Related Platform Documents	<ul style="list-style-type: none"> <li>• <a href="#">Cisco 2600 Series Multiservice Platforms</a></li> <li>• <a href="#">Cisco 2800 Series Integrated Services Routers</a></li> <li>• <a href="#">Cisco 3600 Series Multiservice Platforms</a></li> <li>• <a href="#">Cisco 3700 Series Multiservice Access Routers</a></li> <li>• <a href="#">Cisco 3800 Series Integrated Services Routers</a></li> <li>• <a href="#">Cisco 7200 Series Routers</a></li> <li>• <a href="#">Cisco 7301</a></li> </ul>
Related gateway configuration documentation	<p>Media and Signaling Authentication and Encryption Feature for Cisco IOS H.323 Gateways.</p> <p><a href="http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/htsecure.htm">http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/htsecure.htm</a></p>
Cisco IOS NAT Configuration Guide, Release 12.4T	<ul style="list-style-type: none"> <li>• <i>Configuring Cisco IOS Hosted NAT Traversal for Session Border Controller</i> <a href="http://www.cisco.com/en/US/docs/ios/12_4t/ip_addr/configuration/guide/htnatsbc.html">http://www.cisco.com/en/US/docs/ios/12_4t/ip_addr/configuration/guide/htnatsbc.html</a></li> </ul>

Related Topic	Document Title
Troubleshooting and Debugging guides	<ul style="list-style-type: none"> <li>• Cisco IOS Debug Command Reference, Release 12.4 at <a href="http://www.cisco.com/en/US/docs/ios/debug/command/reference/db_book.html">http://www.cisco.com/en/US/docs/ios/debug/command/reference/db_book.html</a></li> <li>• <i>Troubleshooting and Debugging VoIP Call Basics</i> at <a href="http://www.cisco.com/en/US/tech/tk1077/technologies_tech_note09186a0080094045.shtml">http://www.cisco.com/en/US/tech/tk1077/technologies_tech_note09186a0080094045.shtml</a></li> <li>• <i>VoIP Debug Commands</i> at <a href="http://www.cisco.com/en/US/docs/routers/access/1700/1750/software/configuration/guide/debug.html">http://www.cisco.com/en/US/docs/routers/access/1700/1750/software/configuration/guide/debug.html</a></li> </ul>

## Standards

Standards	Title
H.323 Version 4 and earlier	<i>H.323 (ITU-T VOIP protocols)</i>

## MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

RFCs	Title
RFC 2833	<i>RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals</i>
RFC 3261	<i>SIP: Session Initiation Protocol</i>

## 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>	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>

## Feature Information for H.323-to-SIP Connections on a Cisco Unified Border Element

Table 1 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.3(1) or a later release appear in the table.

For information on a feature in this technology that is not documented here, see the “[Cisco Unified Border Element Features Roadmap](#).”



### Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for H.323-to-SIP Connections on a Cisco Unified Border Element

Feature Name	Releases	Feature Information
Accounting	12.3(11)T	RADIUS call-accounting records, calling/called name and number.
Call Admission Control	12.3(11)T	RSVP synchronized with call signaling.
Cisco Unified Communications Manager Connections	12.4(6)XE	H.323-to-SIP Supplementary services for Cisco Unified Communications Manager with MTP on the H.323 Trunk
Codec Support	12.4(11)T	iLBC Codec Support
Codec Transcoding	12.3(11)T	Codec transcoding (G.711-G.729)—This feature enables the IP-to-IP gateway to bridge calls between networks that support different VoIP call-signaling protocols (SIP and H.323)

**Table 1** Feature Information for H.323-to-SIP Connections on a Cisco Unified Border Element (continued)

Feature Name	Releases	Feature Information
DTMF	12.3(11)T 12.4(6)XE	12.3(11)T—DTMF relay <ul style="list-style-type: none"> <li>H.245 alpha/signal &lt;--&gt; SIP RFC 2833</li> <li>H.245 alpha/signal &lt;--&gt; SIP Notify</li> </ul> 12.4(6)XE—G.711 Inband DTMF to RFC 2833
Fax/Modem	12.3(11)T	T.38 fax relay and Cisco fax relay
Managing H.323 IP Group Call Capacities	12.2(13)T	Creates a maximum capacity for the IP group providing extra control for load and resource balancing.
Mapping ECS to ReINVITE and ECS to REFER on the Cisco IOS SBC.	12.4(20)T	H.323-to-SIP Supplementary Service Enhancements for Session Border Controller (SBC)
Media Modes	12.3(1)	Media flow-around capability on the IP-to-IP gateway by supporting the processing of call set-up and teardown request (VoIP call signaling) and for media streams (flow-through and flow-around)
Rotary Support	12.3(11)T	H.323-to-H.323 Call Failure Recovery (Rotary) on a Cisco Unified Border Element. Eliminates codec restrictions and enables the Cisco UBE to restart codec negotiation with the originating endpoint based on the codec capabilities of the next dial peer in the rotary group for H.323-to-H.323 interconnections.
Signaling Interworking	12.3(11)T 12.4(4)T	12.3(11)T—This feature enables SIP-to-H.323 protocol interworking capabilities of the Cisco Unified Border Element: <ul style="list-style-type: none"> <li>Interworking between H.323 Fast-Start and SIP early-media signaling</li> <li>Interworking between H.323 Slow-Start and SIP delayed-media signaling</li> </ul> 12.4(4)T—Extended SIP-to-H.323 Call Interworking for Session Border Controller (SBC)
TCL IVR	12.3(11)T 12.4(11)T	12.3(11)T—TCL IVR 2.0 for SIP, including media playout and digit collection (RFC 2833 DTMF relay) 12.4(11)T —TCL IVR support with SIP NOTIFY DTMF
Transport Protocols	12.3(11)T	UDP and TCP transport
VXML	12.4(6)XE 12.4(11)T	12.4(6)XE— <ul style="list-style-type: none"> <li>VXML 3.x support</li> <li>VXML support with SIP Notify</li> </ul> 12.4(11)T—VXML support with SIP NOTIFY DTMF



---

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, 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. (0903R)

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.

© 2009 Cisco Systems, Inc. All rights reserved.





# SIP-to-SIP Connections on a Cisco Unified Border Element

---

**Revised: February 27, 2009**  
**First Published: June 19, 2006**  
**Last Updated: February 27, 2009**

This chapter describes how to configure and enable features for SIP-to-SIP connections in an Cisco Unified Border Element topology. A Cisco Unified Border Element (Cisco UBE), in this guide also called an IP-to-IP gateway (IPIPGW), border element (BE), or session border controller, facilitates connectivity between independent VoIP networks by enabling VoIP and videoconferencing calls from one IP network to another.

## Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for SIP-to-SIP Connections on a Cisco Unified Border Element” section on page 231](#).

## Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS 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.

## Contents

This chapter describes how to configure SIP-to-SIP connections in a Cisco Unified Border Element (Cisco UBE). It covers the following features:

- [Prerequisites for Configuring SIP-to-SIP Connections on a Cisco Unified Border Element, page 132](#)
- [Restrictions for Configuring SIP-to-SIP Connections on a Cisco Unified Border Element, page 132](#)
- [Information About Configuring SIP-to-SIP Connections on a Cisco Unified Border Element, page 133](#)
- [How to Configure SIP-to-SIP Gateway Features, page 133](#)



---

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

© 2009 Cisco Systems, Inc. All rights reserved.

- [Configuration Examples for SIP-to-SIP Connections in a Cisco Unified Border Element](#), page 222
- [Additional References](#), page 228
- [Feature Information for SIP-to-SIP Connections on a Cisco Unified Border Element](#), page 231

## Prerequisites for Configuring SIP-to-SIP Connections on a Cisco Unified Border Element

- Perform the prerequisites listed in the “[Prerequisites for Cisco Unified Border Element Configuration](#)” procedure on page -15 in this guide.
- Perform fundamental gateway configuration listed in the “[Prerequisites for Fundamental Cisco Unified Border Element Configuration](#)” procedure on page -41 in this guide.
- Perform basic H.323 gateway configuration.
- Perform basic H.323 gatekeeper configuration.



### Note

For configuration instructions, see the “[Configuring H.323 Gateways](#)” and “[Configuring H.323 Gatekeepers](#)” chapters of the *Cisco IOS Voice, Video, and Fax Configuration Guide*, Release 12.2.

## Restrictions for Configuring SIP-to-SIP Connections on a Cisco Unified Border Element

### Cisco IOS Release 12.4(15)XY and later releases:

- Registration is not supported.

### Cisco IOS Release 12.4(15)T and before:

- Delayed-Offer to Delayed-Offer is not supported.
- Codec T is not supported.
- Registration is not supported.
- Supplementary services are not supported.
- Transcoding is not supported.
- Like-to-like error messages are not passed from the incoming SIP leg to the outgoing SIP leg.

### Cisco IOS Release 12.4(9)T and before:

- Topology and address hiding is not supported.

### Cisco IOS Release 12.4(9)T and later releases:

- Media flow-around for Delayed-Offer to Early-Offer audio and video calls is not supported.
- DTMF Interworking rtp-nte to out of band is not supported when high density transcoder is enabled. Use normal transcoding for rtp-nte to out of band DTMF interworking.

# Information About Configuring SIP-to-SIP Connections on a Cisco Unified Border Element

**Note**

When you configure SIP on a router, the ports on all its interfaces are open by default. This makes the router vulnerable to malicious attackers who can execute toll fraud across the gateway if the router has a public IP address and a public switched telephone network (PSTN) connection. To eliminate the threat, you should bind an interface to private IP address that is not accessible by untrusted hosts. In addition, you should protect any public or untrusted interface by configuring a firewall or an access control list (ACL) to prevent unwanted traffic from traversing the router.

- Delayed-Offer to Early-Offer audio calls are supported.
- Delayed-Offer to Delayed-Offer calls are supported.
- Delayed-Offer to Delayed-Offer video calls are supported in Cisco IOS Release 12.4(15)XY and later.
- Delayed-Offer to Delayed-Offer audio calls are supported in Cisco IOS Release 12.4(15)T and later.
- Early-Offer to Early-Offer for audio calls are supported.
- Early-Offer to Early-Offer, Delayed-Offer to Early-Offer video calls are supported in 12.4(15)XZ and later.
- Fax relay is enabled by default for all systems. No further configuration is needed.
- Like-to-like dtmf, codec and fax are supported.
- Like-to-like error messages are not passed from the incoming SIP leg to the outgoing SIP leg. Error messages are passed through Cisco Unified BE when the **header-passing error-passthru** command is configured in Cisco IOS Release 12.4(15) T and later.
- Media flow-around (except for Delayed-Offer to Early-Offer audio and video calls) in Cisco IOS Release 12.4(9)T and later.
- reINVITE pass-through for Session Refresh is supported.
- SIP-to-SIP Video (including Delayed-Offer to Delayed-Offer, Early-Offer to Early-Offer, Delayed-Offer to Early-Offer calls) are supported.
- SRTP-to-SRTP support for SIP-to-SIP calls is supported.

## How to Configure SIP-to-SIP Gateway Features

The following section provides configuration information for the following SIP-to-SIP features.

- [SIP-to-SIP Basic Functionality for Session Border Controller \(SBC\), page 134](#)
- [SIP-to-SIP Extended Feature Functionality for Session Border Controller \(SBC\), page 135](#)
- [SIP-to-SIP Supplementary Services for Session Border Controller \(SBC\), page 136](#)
- [SIP-to-SIP Supplementary Feature Interworking for Session Border Controller \(SBC\), page 135](#)
- [Configuring IP Address-Hiding, page 136](#)
- [Configuring SIP-to-SIP Connections in a Cisco Unified Border Element, page 137](#)
- [Configuring Delayed-Offer to Early-Offer for SIP Audio Calls, page 138](#)

- [Configuring SIP Error Message Pass Through](#), page 141
- [Configuring Cisco Unified Border Element for Unsupported Content Pass-through](#), page 143
- [Configuring Media Flow-Around](#), page 146
- [Configuring DTMF Relay Digit-Drop on a Cisco Unified Border Element](#), page 149
- [Enabling In-Dialog OPTIONS to Monitor Active SIP Sessions](#), page 152
- [Configuring Cisco UBE Out-of-dialog OPTIONS Ping for Specified SIP Servers or Endpoints](#), page 155
- [Configuring SIP Parameters](#), page 157
- [Configurable SIP Parameters via DHCP](#), page 159
- [Configuring SIP Listening Port](#), page 171
- [Configuring Bandwidth Parameters for SIP Calls](#), page 173
- [Configuring Support for Session Refresh with Reinvites](#), page 173
- [Sending a SIP Registration Message from a Cisco Unified Border Element](#), page 175
- [Configuring Adjustable Timers for Registration Refresh and Retries](#), page 176
- [Configuring Cisco Unified Border Element Support for SRTP-RTP Internetworking](#), page 181
- [Support for PAID, PPID, Privacy, PCPID, and PAURI Headers on the Cisco Unified Border Element](#), page 193
- [Support for Preloaded Routes in Outgoing INVITE Messages Based on REGISTER Information](#), page 208
- [Selectively Using sip: URI or tel: URL Formats on Individual SIP Headers](#), page 213
- [Configuring Selective Filtering of Outgoing Provisional Response on the Cisco Unified Border Element](#), page 218
- [Verifying and Troubleshooting SIP-to-SIP Connections on a Cisco Unified Border Element](#), page 221

## SIP-to-SIP Basic Functionality for Session Border Controller (SBC)

SIP-to-SIP Basic Functionality for SBC for Cisco UBE provides termination and reorigination of both signaling and media between VoIP and video networks using SIP signaling in conformance with RFC3261. The SIP-to-SIP protocol interworking capabilities of the Cisco Unified Border Element (Cisco UBE) support the following:

- Basic voice calls (Supported audio codecs include: G.711, G.729, G.728, G.726, G.723, G.722, gsmamr nb, AAC\_LD, iLBC. Video codecs: H.263, and H.264)
- Codec transcoding
- Calling/called name and number
- DTMF relay interworking
  - SIP RFC 2833 <-> SIP RFC 2833
  - SIP Notify <-> SIP Notify
- Interworking between SIP early-media and SIP early-media signaling
- Interworking between SIP delayed-media and SIP delayed-media signaling

- RADIUS call-accounting records
- RSVP synchronized with call signaling
- SIP-SIP Video calls
- TCL IVR 2.0 for SIP, including media playout and digit collection (RFC 2833 DTMF relay)
- T.38 fax relay and Cisco fax relay
- UDP and TCP transport

## SIP-to-SIP Extended Feature Functionality for Session Border Controller (SBC)

Enables the SIP-to-SIP functionality to conform with RFC 3261 to interoperate with SIP UAs. New SIP-to-SIP features available include:

- Call Admission Control (based on CPU, memory, total calls)
- Delayed Media Call
- ENUM support
- [Configuring SIP Error Message Pass Through, page 141](#)
- Interoperability with Cisco Unified Communications Manager 5.0 and BroadSoft.
- Lawful Intercept
- Media Inactivity
- Modem passthrough
- TCP and UDP interworking
- Tcl scripts with SIP NOTIFY VoiceXML with SIP-to-SIP
- Transport Layer Security (TLS)

## SIP-to-SIP Supplementary Feature Interworking for Session Border Controller (SBC)

Provides enhanced termination and re-origination of signaling and media between VoIP and Video Networks in conformance with RFC3261. New SIP-to-SIP capabilities offered in this release on the Cisco 28xx, 38xx, 5350XM and 5400XM include:

- iLBC Codec
  - Codecs section of the Dial Peer Configuration on Voice Gateway Routers Guide
    - [http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax\\_c/int\\_c/dpeer\\_c/dp\\_ovrvw.htm#1035124](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/int_c/dpeer_c/dp_ovrvw.htm#1035124)
  - Dial Peer Features and Configuration section of the Dial Peer Configuration on Voice Gateway Routers Guide
    - [http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax\\_c/int\\_c/dpeer\\_c/dp\\_config.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/int_c/dpeer_c/dp_config.htm)
- G.711 Inband DTMF to RFC 2833
- Session refresh

- SIP-to-SIP Supplementary Services
  - Refer/302 Based Supplementary Services Supported from 12.4(9)T onwards
  - ReInvite Based Supplementary Services Supported from 12.4(15)XZ

## SIP-to-SIP Supplementary Services for Session Border Controller (SBC)

This chapter describes the SIP-to-SIP supplementary service features for SBC. The SIP-to-SIP supplementary services feature enhances terminating and re-originating both signaling and media between VoIP and Video networks by supporting the following features:

- AMR-NB Codec support
- IP Address Hiding in all SIP messages including supplementary services
- Media
  - Media Flow Around
- Support on Cisco AS5350XM and Cisco AS5400XM
- SIP-to-SIP Supplementary services using REFER/3xx method. The following features are enabled by default.
  - Message Waiting Indication
  - Call Waiting
  - Call Transfer (Blind, Consult, Alerting)
  - Call Forward (All, Busy, No Answer)
  - Distinctive Ringing
  - Call Hold/Resume
  - Music on Hold
- Hosted NAT Traversal for SIP

## Configuring IP Address-Hiding

Configuring address-hiding hides signaling and media peer addresses from the endpoints, especially for supplemental services when the Cisco Unified BE passes REFER/3xx messages from leg to leg. Configuring the address hiding feature ensures that the Cisco Unified BE is the only point of signaling and media entry/exit in all scenarios. To enable address-hiding in all SIP messages, perform the steps in this section.

### Restrictions

When supplementary services are configured the endpoint sends messages to the SBC, this is then forwarded to the peer endpoint. Address-hiding is preserved during this message forwarding



## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **address-hiding**
5. **exit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	<code>configure terminal</code>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<code>voice service voip</code>  <b>Example:</b> Router(config)# voice service voip	Enters VoIP voice-service configuration mode.
Step 4	<code>address-hiding</code>  <b>Example:</b> Router(conf-voi-serv)# address-hiding	Hides signaling and media peer addresses from the endpoints.
Step 5	<code>exit</code>  <b>Example:</b> Router(conf-voi-serv)# exit	Exits the current mode.

## Configuring SIP-to-SIP Connections in a Cisco Unified Border Element

To configure SIP-to-SIP connection types, perform the steps in this section.

### Restrictions

- Connections are disabled by default in Cisco IOS images that support the Cisco UBE.
- This chapter covers only those features that require a unique configuration in order to support the Cisco UBE. For information on those H.323 gateway features not mentioned in this chapter, see the [Cisco IOS Voice, Video, and Fax Configuration Guide](#).

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **allow-connections**
5. **exit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<pre>enable</pre> <p><b>Example:</b> Router&gt; enable </p>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<pre>configure terminal</pre> <p><b>Example:</b> Router# configure terminal </p>	Enters global configuration mode.
Step 3	<pre>voice service voip</pre> <p><b>Example:</b> Router(config)# voice service voip </p>	Enters VoIP voice-service configuration mode.
Step 4	<pre>allow-connections from-type to to-type</pre> <p><b>Example:</b> Router(config-voi-serv)# allow-connections sip to sip </p>	Allows connections between specific types of endpoints in an Cisco UBE. Arguments are as follows: <ul style="list-style-type: none"> <li>• <i>from-type</i>—Type of connection. Valid values: <b>h323</b>, <b>sip</b>.</li> <li>• <i>to-type</i>—Type of connection. Valid values: <b>h323</b>, <b>sip</b>.</li> </ul> <p><b>Note</b> H.323-to-H.323: By default, H.323-to-H.323 connections are disabled and POTS-to-any and any-to-POTS connections are enabled.</p>
Step 5	<pre>exit</pre> <p><b>Example:</b> Router(config-voi-serv)# exit </p>	Exits the current mode.

## Configuring Delayed-Offer to Early-Offer for SIP Audio Calls

This feature alters the default configuration of the Cisco Unified BE from not distinguishing SIP Delayed-Offer to Early-Offer call flows, to forcing the Cisco Unified BE to generate an Early-Offer with the configured codecs for an incoming Delayed-Offer INVITE. To configure a Cisco Unified Border Element to send a SIP invite with Early-Offer (EO) on the Out-Leg (OL) perform the steps in this section.

To Delayed-Offer to Early-Offer for SIP Audio Calls for all VoIP calls, or individual dial peers, perform the steps in this section. This section contains the following subsections:

- [Configuring Delayed-Offer to Early-Offer for SIP Audio Calls at the Global Level, page 139](#)
- [Configuring Delayed-Offer to Early-Offer for SIP Audio Calls for a Dial-Peer, page 140](#)

## Prerequisites

- The **allow-connections sip to sip** command must be configured before you configure media flow-around. For more information and configuration steps see the “[Configuring SIP-to-SIP Connections in a Cisco Unified Border Element](#)” section on [page 137](#) of this chapter.

## Restrictions

- Cisco Unified Communications Manager 5.x supports Early-Offer over SIP trunk for audio calls with MTP
- Support for Cisco Unified Communications Manager Early-Offer for video calls and audio calls without MTP is not supported

[Table 1](#) shows a list of protocol interworking for SIP.

**Table 1** Supported protocol interworking

Protocol	In Leg	Out Leg	Support
H.323-to-SIP	Fast Start	Early-Offer	Bi-Directional
	Slow Start	Delayed-Offer	Bi-Directional
SIP-to-SIP	Early-Offer	Early-Offer	Bi-Directional
	Delayed-Offer	Delayed-Offer	Bi-Directional
	Delayed-Offer	Early-Offer	Uni-Directional

## Configuring Delayed-Offer to Early-Offer for SIP Audio Calls at the Global Level

To configure Delayed-Offer to Early-Offer for SIP Audio Calls at the global level, perform the steps in this section.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **allow-connections sip**
5. **early-offer forced**
6. **exit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<pre>enable</pre> <p><b>Example:</b> Router&gt; enable </p>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<pre>configure terminal</pre> <p><b>Example:</b> Router# configure terminal </p>	Enters global configuration mode.
Step 3	<pre>voice service voip</pre> <p><b>Example:</b> Router(config)# voice service voip </p>	Enters VoIP voice-service configuration mode.
Step 4	<pre>allow-connections from-type to to-type</pre> <p><b>Example:</b> Router(config-voi-serv)# allow-connections sip to sip </p>	Allows connections between specific types of endpoints in an Cisco UBE. Arguments are as follows: <ul style="list-style-type: none"> <li><i>from-type</i>—Type of connection. Valid values: <b>h323</b>, <b>sip</b>.</li> <li><i>to-type</i>—Type of connection. Valid values: <b>h323</b>, <b>sip</b>.</li> </ul> <p><b>Note</b> H.323-to-H.323: By default, H.323-to-H.323 connections are disabled and POTS-to-any and any-to-POTS connections are enabled.</p>
Step 5	<pre>early-offer forced</pre> <p><b>Example:</b> Router(config-voi-serv)# early-offer forced </p>	Enables SIP Delayed-Offer to Early-Offer globally.
Step 6	<pre>exit</pre> <p><b>Example:</b> Router(config-voi-serv)# exit </p>	Exits the current mode.

## Configuring Delayed-Offer to Early-Offer for SIP Audio Calls for a Dial-Peer

To configure Delayed-Offer to Early-Offer for SIP Audio Calls for an individual dial-peer, perform the steps in this section.

## SUMMARY STEPS

- enable
- configure terminal
- dial-peer voice 1 voip
- voice-class sip early-offer forced
- exit

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> <code>Router&gt; enable</code>	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	<code>configure terminal</code>  <b>Example:</b> <code>Router# configure terminal</code>	Enters global configuration mode.
Step 3	<code>dial-peer voice number voip</code>  <b>Example:</b> <code>Router(config)# dial-peer voice 2 voip</code>	Enters dial-peer configuration mode for the specified VoIP dial peer.
Step 4	<code>voice-class sip early-offer forced</code>  <b>Example:</b> <code>Router(config-dial-peer)# voice-class sip early-offer forced</code>	Forcefully send Early-Offer
Step 5	<code>exit</code>  <b>Example:</b> <code>Router(config-dial-peer)# exit</code>	Exits the current mode.

## Configuring SIP Error Message Pass Through

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

SIP error responses that are not supported on the Cisco UBE include: 300—Multiple choices, 301—Moved permanently, and 485—Ambiguous

Pre-leg SIP error responses that are not transparently passed though include:

Error code received	Corresponding error reported on the peer leg
400—Bad request	500—Internal error
401—Unauthorized	503—Service unavailable
406—Not acceptable	500—Internal error
407—Authentication required	503—Service unavailable
413—Request message body too large	500—Internal error
414—Request URI too large	500—Internal error
416—Unsupported URI scheme	500—Internal error
423—Interval too brief	500—Internal error

Error code received	Corresponding error reported on the peer leg
482—Loop detected	500—Internal error
483—Too many hops	500—Internal error
488—Not acceptable media (applicable only when the call is transcoded)	500—Internal error

## Restrictions

- Configuring SIP error header passing in at the dial-peer level is not supported.

## SUMMARY STEPS

- enable**
- configure terminal**
- voice service voice**
- sip**
- header-passing error-pass through**
- exit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<code>configure terminal</code>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<code>voice service voip</code>  <b>Example:</b> Router(config)# voice service voip	Enters VoIP voice-service configuration mode.
Step 4	<code>sip</code>  <b>Example:</b> Router(config-voi-srv)# sip	Enters SIP configuration mode.

	Command or Action	Purpose
Step 5	<pre>header-passing error-pass through</pre> <p><b>Example:</b>  <pre>Router(conf-serv-sip)#header-passing error-pass through</pre></p>	Passes received error responses from one SIP leg to pass transparently to another SIP leg.
Step 6	<pre>exit</pre> <p><b>Example:</b>  <pre>Router(config-serv-sip) exit</pre></p>	Exit SIP configuration mode.

## Configuring Cisco Unified Border Element for Unsupported Content Pass-through

This feature introduces the ability to configure the Cisco UBE to pass through end to end headers at a global or dial-peer level, that are not processed or understood in a SIP trunk to SIP trunk scenario. The pass through functionality includes all or only a configured list of unsupported or non-mandatory SIP headers, and all unsupported content/MIME types.

The Cisco Unified Border Element does not support end-to-end media negotiation between the two endpoints that establish a call session through the Cisco Unified Border Element. This is a limitation when the endpoints intend to negotiate codec/payload types that the Cisco Unified Border Element does not process, because currently, unsupported payload types will never be negotiated by the Cisco Unified Border Element. Unsupported content types include text/plain, image/jpeg and application/resource-lists+xml. To address this problem, SDP is configured to pass through transparently at the Cisco Unified Border Element, so that both the remote ends can negotiate media independently of the Cisco Unified Border Element.

SDP pass-through is addressed in two modes:

- Flow-through: Cisco Unified Border Element plays no role in the media negotiation, it blindly terminates and re-originates the RTP packets irrespective of the content type negotiated by both the ends. This supports address hiding and NAT traversal.
- Flow-around: Cisco Unified Border Element neither plays a part in media negotiation, nor does it terminate and re-originate media. Media negotiation and media exchange is completely end-to-end.

### Prerequisites for Cisco UBE for Unsupported Content Pass-through

- Configuring the **media flow-around** command is required for SDP pass-through. When flow-around is not configured, the flow-through mode of SDP pass-through will be functional.
- When the dial-peer media flow mode is asymmetrically configured, the default behavior is to fallback to SDP pass-through with flow-through.

### Restrictions for Cisco UBE for Unsupported Content Pass-through

When SDP pass-through is enabled, some of interworking that the Cisco Unified Border Element currently performs cannot be activated. These features include:

- Delayed Offer to Early Offer Interworking
- Supplementary Services with triggered Invites

- DTMF Interworking scenarios
- Fax Interworking/QoS Negotiation
- Transcoding

To enable Cisco UBE Unsupported Content Pass-through perform the steps in this section. This section contains the following subsections:

- [Configuring Cisco UBE for Unsupported Content Pass-through at the Global Level, page 144](#)
- [Configuring Cisco UBE for Unsupported Content Pass-through at the Dial Peer Level, page 145](#)

## Configuring Cisco UBE for Unsupported Content Pass-through at the Global Level

To configure Unsupported Content Pass-through on an Cisco Unified Border Element at the global level, perform the steps in this section.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **sip**
5. **pass-thru {content {sdp | unsupported} | headers {unsupported | list tag}}**
6. **exit**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>voice service voip</b>  <b>Example:</b> Router(config)# voice service voip	Enters VoIP voice-service configuration mode.
Step 4	<b>sip</b>  <b>Example:</b> Router(config-voi-srv)# sip	Enters SIP configuration mode.



	Command or Action	Purpose
Step 5	<pre>pass-thru {content {sdp   unSUPP}   headers {unSUPP   list tag}}</pre> <p><b>Example:</b>  Router(conf-serv-sip)# pass-thru {content {sdp   unSUPP}   headers {unSUPP   list &lt;tag&gt;}} </p>	Passes the SDP transparently from in-leg to the out-leg with no media negotiation.
Step 6	<pre>exit</pre> <p><b>Example:</b>  Router(conf-voi-serv)# exit </p>	Exits the current mode.

## Configuring Cisco UBE for Unsupported Content Pass-through at the Dial Peer Level

To configure Unsupported Content Pass-through on an Cisco Unified Border Element at the dial-peer level, perform the steps in this section.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `dial-peer voice number voip`
4. `voice-class sip pass-thru {{headers | content} {content {unSUPP | sdp}}}`
5. `exit`

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<pre>enable</pre> <p><b>Example:</b>  Router&gt; enable </p>	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	<pre>configure terminal</pre> <p><b>Example:</b>  Router# configure terminal </p>	Enters global configuration mode.
Step 3	<pre>dial-peer voice number voip</pre> <p><b>Example:</b>  Router(config)# dial-peer voice 22 voip </p>	Enters dial-peer configuration mode for the specified VoIP dial peer.

	Command or Action	Purpose
Step 4	<b>voice-class sip pass-thru</b> { headers   content } { content { unsumm   sdp }  <b>Example:</b> Router (conf-dial-peer)# voice-class sip pass-thru headers	Passes the SDP transparently from in-leg to the out-leg with no media negotiation.
Step 5	<b>exit</b>  <b>Example:</b> Router(conf-voi-serv)# exit	Exits the current mode.

## Configuring Media Flow-Around

This feature adds media flow-around capability on the Cisco Unified Border Element by supporting the processing of call setup and teardown requests (VoIP call signaling) and for media streams (flow-through and flow-around). Media flow-around can be configured the global level or it must be configured on both incoming and outgoing dial peers. If configured only on either the incoming or outgoing dialpeer, the call will become a flow-through call.

Media flow-around is a good choice to improve scalability and performance when network-topology hiding and bearer-level interworking features are not required

With the default configuration, the Cisco UBE receives media packets from the inbound call leg, terminates them, and then reoriginates the media stream on an outbound call leg. Media flow-around enables media packets to be passed directly between the endpoints, without the intervention of the Cisco UBE. The Cisco UBE continues to handle routing and billing functions.

To specify media flow-around for voice class, all VoIP calls, or individual dial peers, perform the steps in this section. This section contains the following subsections:

- [Configuring Media Flow-Around for a Voice Class, page 147](#)
- [Configuring Media Flow-Around at the Global Level, page 148](#)
- [Configuring Media Flow-Around for a Dial-Peer, page 148](#)

## Prerequisites

- The **allow-connections sip to sip** command must be configured before you configure media flow-around. For more information and configuration steps see the [“Configuring SIP-to-SIP Connections in a Cisco Unified Border Element”](#) section on page 137 of this chapter.

## Configuring Media Flow-Around for a Voice Class

To configure media flow-around for a voice class, perform the steps in this section.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice class media 1**
4. **media flow-around**
5. **dial-peer voice 2 voip**
6. **voice-class media 1**
7. **exit**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	<code>configure terminal</code>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<code>voice class media tag</code>  <b>Example:</b> Router(config)# voice class media 1	Enters voice-class configuration mode and assign an identification tag for a media voice class.
Step 4	<code>media flow-around</code>  <b>Example:</b> Router(config-class)# media flow-around	Enables media flow around.
Step 5	<code>dial-peer voice tag voip</code>  <b>Example:</b> Router(config-class)# dial-peer voice 2 voip	Enters dial-peer configuration mode and assign an identification tag for VoIP.
Step 6	<code>voice class media tag</code>  <b>Example:</b> Router(config-dial-peer)# voice class media 1	Assign an identification tag for a media voice class.
Step 7	<code>exit</code>  <b>Example:</b> Router(config-dial-peer)# exit	Exit dial-peer configuration mode.

## Configuring Media Flow-Around at the Global Level

To configure media flow-around at the global level, perform the steps in this section.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **media flow-around**
5. **exit**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> <code>Router&gt; enable</code>	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	<code>configure terminal</code>  <b>Example:</b> <code>Router# configure terminal</code>	Enters global configuration mode.
Step 3	<code>voice service voip</code>  <b>Example:</b> <code>Router(config)# voice service voip</code>	Enters VoIP voice-service configuration mode.
Step 4	<code>media flow-around</code>  <b>Example:</b> <code>Router(config-voi-serv)# media flow-around</code>	Enables media flow-around.
Step 5	<code>exit</code>  <b>Example:</b> <code>Router(config-voi-serv)# exit</code>	Exits the current mode.

## Configuring Media Flow-Around for a Dial-Peer

To configure media flow-around for an individual dial-peer, perform the steps in this section.

### Restrictions

If you plan to configure both incoming and outgoing dial peers, you must specify the transparent codec on the incoming dial peer.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice 1 voip**
4. **media flow-around**
5. **exit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> <code>Router&gt; enable</code>	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	<code>configure terminal</code>  <b>Example:</b> <code>Router# configure terminal</code>	Enters global configuration mode.
Step 3	<code>dial-peer voice number voip</code>  <b>Example:</b> <code>Router(config)# dial-peer voice 2 voip</code>	Enters dial-peer configuration mode for the specified VoIP dial peer.
Step 4	<code>media flow-around</code>  <b>Example:</b> <code>Router(config-dial-peer)# media flow-around</code>	Enables media flow-around.
Step 5	<code>exit</code>  <b>Example:</b> <code>Router(config-dial-peer)# exit</code>	Exits the current mode.

## Configuring DTMF Relay Digit-Drop on a Cisco Unified Border Element

To avoid sending both in-band and out-of band tones to the outgoing leg when sending Cisco UBE calls in-band (rtp-nte) to out-of band (h245-alphanumeric), configure the **dtmf-relay rtp-nte digit-drop** command on the incoming SIP dial-peer. On the H.323 side configure either **dtmf-relay h245-alphanumeric** or **dtmf-relay h245-signal** command. This feature can also be used for H.323-to-SIP, and H.323-to-H.323 calls.


**Note**

For a SIP (rtp-nte) to H.323 (h245-alphanumeric) via Cisco UBE call, if any RTP-NTE packets are sent before the H.323 Endpoint answers the call, the dual-tone multifrequency (DTMF) signal is not audible on a terminating gateway (TGW)

To configure DTMF relay digit drop on an Cisco UBE with Cisco Unified Communications Manager, perform the steps in this section.

## Restrictions

- You should not configure digit-drop for inband to and from rtp-nte dtmf conversion (this involves transcoder), the digit-drop CLI prevents sending rtp-nte packets from the RTP lib.
- Configuring the **digit-drop** command is required for interworking between OOB and RTP NTE.
- Digit-drop for in-band rtp-nte DTMF conversion requiring a transcoder is not supported.
- IOS MTP should be used when the Cisco UBE does DTMF interworking between inband G.711 voice and RFC2833 with CCM SIP trunk.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice tag voip**
4. **dtmf-relay [cisco-rtp] [h245-alphanumeric] [h245-signal][rtp-nte [digit-drop]]**
5. **exit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>dial-peer voice tag voip</b>  <b>Example:</b> Router(config)# dial-peer voice 2 voip	Enters dial-peer voice configuration mode for the specified VoIP dial peer.

	Command or Action	Purpose
Step 4	<pre>dtmf-relay [cisco-rtp] [h245-alphanumeric][h245-signal] [rtp-nte digit-drop]]</pre> <p><b>Example:</b> Router (config-dial-peer)# dtmf-relay rtp-nte digit-drop</p>	<p>Forwards DTMF tones. Keywords are as follows:</p> <ul style="list-style-type: none"> <li>• <b>cisco-rtp</b>—Forwards DTMF tones by using RTP with a Cisco-proprietary payload type.</li> <li>• <b>h245-alphanumeric</b>—Forwards DTMF tones by using the H.245 alphanumeric method.</li> <li>• <b>h245-signal</b>—Forwards DTMF tones by using the H.245 signal UII method.</li> <li>• <b>rtp-nte</b>—Forwards DTMF tones by using Real-Time Transport Protocol (RTP) with the Named Telephone Event (NTE) payload type.</li> <li>• <b>digit-drop</b>—Passes digits out-of-band; and drops in-band digits.</li> </ul> <p><b>Note</b> The <b>digit-drop</b> keyword is available only when the <b>rtp-nte</b> keyword is configured.</p>
Step 5	<pre>exit</pre> <p><b>Example:</b> Router(config-dial-peer)# exit</p>	<p>Exits the current mode.</p>

## Examples

The following example shows DTMF-Relay digits configured to avoid sending both in-band and out-of-band tones to the outgoing leg in an Cisco Unified BE:

```
.
.
.
dial-peer voice 1 voip
 dtmf-relay h245-alphanumeric rtp-nte digit-drop
.
.
.
```

## Troubleshooting tips

The debug output will show that the H245 out of band messages are sent to the TGW. However, entry of the digits are not audible on the phone.

## Enabling In-Dialog OPTIONS to Monitor Active SIP Sessions

The two common methods to determine whether a SIP session is active; RTP/RTCP media inactivity timer and session timer have limitations when used with the Cisco UBE. The media inactivity (rtp/rtcp) method will not work if flow around mode is configured as the media is sent directly between endpoints without going through the Cisco UBE and session timer cannot be used if the SIP endpoint does not support session timer.

The in-dialog OPTIONS refresh feature introduces a refresh mechanism that addresses these two scenarios, and can be used on SIP-to-SIP and SIP-to-H.323 calls. The refresh with OPTIONS method is meant to only be hop-to-hop, and not end-to-end. Since session timer achieves similar results, the OPTIONS refresh/ping will not take affect when session timer is negotiated. The behavior on the H.323 endpoint is as if it was a TDM-SIP call. The generating in-dialog OPTIONS is enabled at the global level or dialpeer level. The system default setting is disabled. This feature can be use by both a TDM voice gateway and an Cisco UBE.

To enable in-dialog OPTIONS at the global level, or individual dial peers, perform the steps in this section. This section contains the following subsections:

- [Methods to Determine Active SIP Sessions, page 152](#)
- [Enabling In-dialog OPTIONS at the Global Level, page 152](#)
- [Enabling in-dialog OPTIONS for a Dial-Peer, page 154](#)

### Methods to Determine Active SIP Sessions

#### RTP/RTCP

The SIP Media Inactivity Timer enables Cisco gateways to monitor and disconnect VoIP calls if no Real-Time Control Protocol (RTCP) packets are received within a configurable time period.

#### Session Timer

The SIP Session Timer periodically refresh Session Initiation Protocol (SIP) sessions by sending repeated INVITE requests. The repeated INVITE requests are sent during an active call leg to allow user agents (UA) or proxies to determine the status of a SIP session. The re-INVITES ensure that active sessions stay active and completed sessions are terminated.

### Enabling In-dialog OPTIONS at the Global Level

To enable in-dialog OPTIONS at the global level, perform the steps in this section.

**Note**

---

The global system default setting is disable.

---



## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **sip**
5. **options-ping 90**
6. **exit**
7. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<code>configure terminal</code>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<code>voice service voip</code>  <b>Example:</b> Router(config)# voice service voip	Enters VoIP voice-service configuration mode.
Step 4	<code>sip</code>  <b>Example:</b> Router(config-voi-srv)# sip	Enters SIP configuration mode.
Step 5	<code>options-ping</code>  <b>Example:</b> Router(conf-serv-sip)# options-ping 90	Enables in-dialog OPTIONS. OPTIONS transactions are sent, in seconds.
Step 6	<code>exit</code>  <b>Example:</b> Router(conf-serv-sip)# exit	Exits the current mode.
Step 7	<code>end</code>  <b>Example:</b> Router(config-voi-srv)# end	Returns to privileged EXEC mode.

## Enabling in-dialog OPTIONS for a Dial-Peer

To enable in-dialog OPTIONS for an individual dial-peer, perform the steps in this section.

### Restrictions

When configuring in-dialog OPTIONS at the dial-peer level OPTIONS must be configured on both incoming and outgoing dial peers.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice 1 voip**
4. **voice-class sip options-ping**
5. **exit**
6. **end**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> <code>Router&gt; enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<code>configure terminal</code>  <b>Example:</b> <code>Router# configure terminal</code>	Enters global configuration mode.
Step 3	<code>dial-peer voice <i>number</i> voip</code>  <b>Example:</b> <code>Router(config)# dial-peer voice 2 voip</code>	Enters dial-peer configuration mode for the specified VoIP dial peer.
Step 4	<code>voice-class sip options-ping</code>  <b>Example:</b> <code>Router(config-voip-peer)# voice-class sip options-ping 65</code>	Enables intervals OPTIONS transactions to be sent, in seconds.
Step 5	<code>exit</code>  <b>Example:</b> <code>Router(config-dial-peer)# exit</code>	Exits the current mode.
Step 6	<code>end</code>  <b>Example:</b> <code>Router(config-voi-srv)# end</code>	Returns to privileged EXEC mode.

## Configuring Cisco UBE Out-of-dialog OPTIONS Ping for Specified SIP Servers or Endpoints

The Out-of-dialog (OOD) Options Ping feature provides a keepalive mechanism at the SIP level between any number of destinations. A generic heartbeat mechanism allows Cisco Unified Border Element to monitor the status of SIP servers or endpoints and provide the option of busying-out a dial-peer upon total heartbeat failure. When a monitored endpoint heartbeat responses fails, the dial-peer is busied out. If an alternate dial-peer is configured for the same destination pattern, the call is failed over to the next preference dial peer, or the on call is rejected with an error cause code.

The response to options ping will be considered unsuccessful and dial-peer will be busied out for following scenarios:

**Table 2**      **Error Codes that busyout the endpoint**

Error Code	Description
503	service unavailable
505	sip version not supported
no response	i.e. request timeout

All other error codes, including 400 are considered a valid response and the dial peer is not busied out.



### Note

The purpose of this feature is to determine if the SIP session protocol on the endpoint is UP and available to handle calls. It may not handle OPTIONS message but as long as the SIP protocol is available, it should be able to handle calls.

When a dial-peer is busied out, Cisco Unified Border Element resumes the heartbeat mechanism and the dial-peer is reset to active upon receipt of a response.

## Prerequisites

The following are required for OOD Options ping to function. If any are missing, the Out-of-dialog (OOD) Options ping will not be sent and the dial peer is reset to the default active state.

- Dial-peer should not be manually shutdown
- Session protocol must be configured for SIP
- Configure session target or outbound proxy

## Restrictions

- The Cisco Unified Border Element OOD Options ping feature is only configured at the Dial-peer level.
- All dial peers start in an up state on a router reboot.
- If a dial-peer has both an outbound proxy and a session target configured, the OOD options ping is sent to the proxy address first.
- If multiple dial-peers point to the same SIP server IP address, an independent OOD options ping is sent for each dial-peer.

- If a SIP server is configured as a DNS hostname, OOD Options pings are sent to all the returned addresses until a response is received.
- Configuration for Cisco Unified Border Element OOD and TDM Gateway OOD are different, but can co-exist.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice tag voip**
4. **voice-class sip options-keepalive**
5. **exit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> <code>Router&gt; enable</code>	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	<code>configure terminal</code>  <b>Example:</b> <code>Router# configure terminal</code>	Enters global configuration mode.
Step 3	<code>dial-peer voice tag voip</code>  <b>Example:</b> <code>Router(config)# dial-peer voice 200 voip</code>	Enters dial-peer configuration mode for the VoIP peer designated by tag.
Step 4	<code>voice-class sip options-keepalive {up-interval seconds   down-interval seconds   retry retries}</code>  <b>Example:</b> <code>Router(config-dial-peer)# voice-class sip options-keepalive up-interval 12 down-interval 65 retry 3</code>	Monitors connectivity between endpoints.
Step 5	<code>exit</code>  <b>Example:</b> <code>Router(config-dial-peer)# exit</code>	Exits the current mode.

## Troubleshooting Tips

The following commands can help troubleshoot the OOD Options Ping feature:

- **debug ccsip all**—shows all Session Initiation Protocol (SIP)-related debugging.
- **show dial-peer voice x**—shows configuration of keepalive information.

```
Router> show dial-peer voice | in options
```

```
voice class sip options-keepalive up-interval 60 down-interval 30 retry 5
voice class sip options-keepalive dial-peer action = active
```

- **show dial-peer voice summary**—shows Active or Busyout dial-peer status.

```
Router# show dial-peer voice summary
```

TAG	TYPE	AD		PREFIX	PRE PASS	
		MIN	OPER		DEST-PATTERN	KEEPALIVE
111	voip	up	up		0 syst	active
9	voip	up	down		0 syst	busy-out

## Configuring SIP Parameters

The SIP Parameters feature allow customers to add, remove, or modify the SIP parameters in the SIP messages going out of a border element. The SIP message is generated from the standard signaling stack, but runs the message through a parser which can add, delete or modify specific parameters. This allows interoperability with additional third party devices that require specific SIP message formats. All SIP methods and responses are supported, profiles can be added either in dial-peer level or global level. Basic Regular Expression support would be provided for modification of header values. SDP parameters can also be added, removed or modified.

This feature is applicable only for outgoing SIP messages. Changes to the messages are applied just before they are sent out, and the SIP SPI code does not remember the changes. Because there are no restrictions on the changes that can be applied, users must be careful when configuring this feature – for example, the call might fail if a regular expression to change the To tag value is configured.

The **all** keyword is used to apply rules on all requests and responses.

## Restrictions

- This feature applies to outgoing SIP messages.
- This feature is disabled by default.
- Removal of mandatory headers is not supported.
- This feature allows removal of entire MIME bodies from SIP messages. Addition of MIME bodies is not supported.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *number* **voip**
4. **voice-class sip profiles** *group-number*
5. **response** *option* **sip-header** *option* **ADD** *word* **CR**
6. **exit**
7. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<pre>enable</pre> <p><b>Example:</b> Router&gt; enable</p>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<pre>configure terminal</pre> <p><b>Example:</b> Router# configure terminal</p>	Enters global configuration mode.
Step 3	<pre>voice service number voip</pre> <p><b>Example:</b> Router(config)# voice service 1 voip</p>	Enters VoIP voice-service configuration mode.
Step 4	<pre>voice-class sip-profiles group-number</pre> <p><b>Example:</b> Router(config)# voice-class sip profiles 42</p>	Establishes individual sip profiles defined by a group-number. Valid group-numbers are from 1 to 1000.
Step 5	<pre>response option sip-header option ADD word CR</pre> <p><b>Example:</b> Router(config)# request INVITE sip-header supported remove</p>	Add, change, or delete any SIP or SDP header in voice class or sip-profile submenu.
Step 6	<pre>exit</pre> <p><b>Example:</b> Router(config-dial-peer)# exit</p>	Exits the current mode.
Step 7	<pre>end</pre> <p><b>Example:</b> Router(config-voi-srv)# end</p>	Returns to privileged EXEC mode.

## Example

```

!
!
!
voice service voip
allow-connections sip to sip
redirect ip2ip
sip
early-offer forced
midcall-signaling passthru
sip-profiles 1
!
!
!
voice class sip-profiles 1
request INVITE sip-header Supported remove

```

```
request INVITE sip-header Min-SE remove
request INVITE sip-header Session-Expires remove
request INVITE sip-header Unsupported modify "Unsupported:" "timer"
!
!
!
```

## Configurable SIP Parameters via DHCP

The Configurable SIP Parameters via DHCP feature allows a Dynamic Host Configuration Protocol (DHCP) server to provide Session Initiation Protocol (SIP) parameters via a DHCP client. These parameters are used for user registration and call routing.

The DHCP server returns the SIP Parameters via DHCP options 120 and 125. These options are used to specify the SIP user registration and call routing information. The SIP parameters returned are the SIP server address via Option 120, and vendor-specific information such as the pilot, contract or primary number, an additional range of secondary numbers, and the SIP domain name via Option 125.

In the event of changes to the SIP parameter values, this feature also allows a DHCP message called DHCPFORCERENEW to reset or apply a new set of values.

The SIP parameters provisioned by DHCP are stored, so that on reboot they can be reused.

### Prerequisites for Configurable SIP Parameters via DHCP

- A DHCP interface has to be associated with SIP before configurable SIP parameters via DHCP can be enabled.

### Restrictions for Configurable SIP Parameters via DHCP

- DHCP Option 120 is the standard DHCP option (RFC3361) to get a SIP server address, and this can be used by any vendor DHCP server. Only one address is supported, which is in the IPv4 address format. Multiple IPv4 address entries are not supported. Also, there is no support for a DNS name in this or for any port number given behind the IPv4 address.
- DHCP Option 125 (RFC 3925) provides vendor-specific information and its interpretation is associated with the enterprise identity. The primary and secondary phone numbers and domain are obtained using Option 125, which is vendor-specific. As long as other customers use the same format as in the Next Generation Network (NGN) DHCP specification, they can use this feature.
- A primary or contract number is required in suboption 202 of DHCP Option 125. There can be only one instance of the primary number and not multiple instances.
- Multiple secondary or numbers in suboption 203 of DHCP Option 125 are supported. Up to five numbers are accepted and the rest ignored. Also, they have to follow the contract number in the DHCP packet data.
- Authentication is not supported for REGISTER and INVITE messages sent from a Cisco Unified Border Element that uses DHCP provisioning
- The DHCP provisioning of SIP Parameters is supported only over one DHCP interface.
- The DHCP option is available only to be configured for the primary registrar. It will not be available for a secondary registrar.

## Information About Configurable SIP Parameters via DHCP

To perform basic Configurable SIP Parameters via DHCP configuration tasks, you should understand the following concepts:

- [Cisco Unified Border Element Support for Configurable SIP Parameters via DHCP, page 160](#)
- [DHCP to Provision SIP Server, Domain Name, and Phone Number, page 160](#)
- [DHCP-SIP Call Flow, page 161](#)
- [DHCP Message Details, page 162](#)

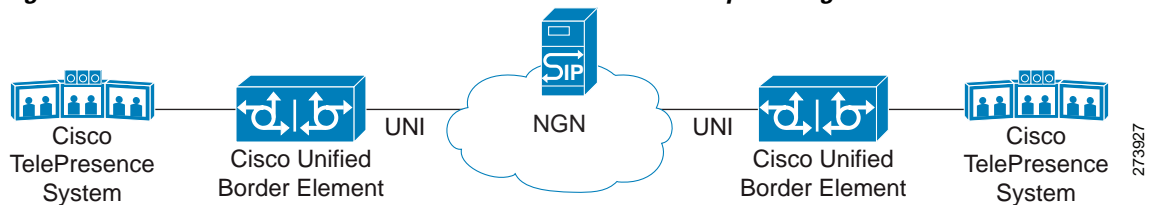
## Cisco Unified Border Element Support for Configurable SIP Parameters via DHCP

The Cisco Unified Border Element provides the support for the DHCP provisioning of the SIP parameters.

The NGN is modeled using SIP as a VoIP protocol. In order to connect to NGN, the User to Network Interface (UNI) specification is used. Cisco TelePresence Systems (CTS), consisting of an IP Phone, a codec, and Cisco Unified Communications Manager, are required to interconnect over the NGN for point-to-point and point-to-multipoint video calls. Because Cisco Unified Communications Manager does not provide a UNI interface, there has to be an entity to provide the UNI interface. The Cisco Unified Border Element provides the UNI interface and has several advantages such as demarcation, delayed offer to early offer, and registration.

Figure 1 shows the Cisco Unified Border Element providing the UNI interface for the NGN.

**Figure 1** Cisco NGN with Cisco Unified Border Element providing UNI interface



## DHCP to Provision SIP Server, Domain Name, and Phone Number

NGN requires Cisco Unified Border Element to support DHCP (RFC 2131 and RFC 2132) to provision the following:

- IP address for Cisco Unified Border Element's UNI interface facing NGN
- SIP server address using option 120
- Option 125 vendor specific information to get:
  - Pilot number (also called primary or contract number), there is only one pilot number in DHCPACK, and REGISTER is done only for the pilot number
  - Additional numbers, or secondary numbers, are in DHCPACK; there is no REGISTER for additional numbers
  - SIP domain name
- DHCPFORCERENEW to reset or apply a new set of SIP parameters (RFC 3203)

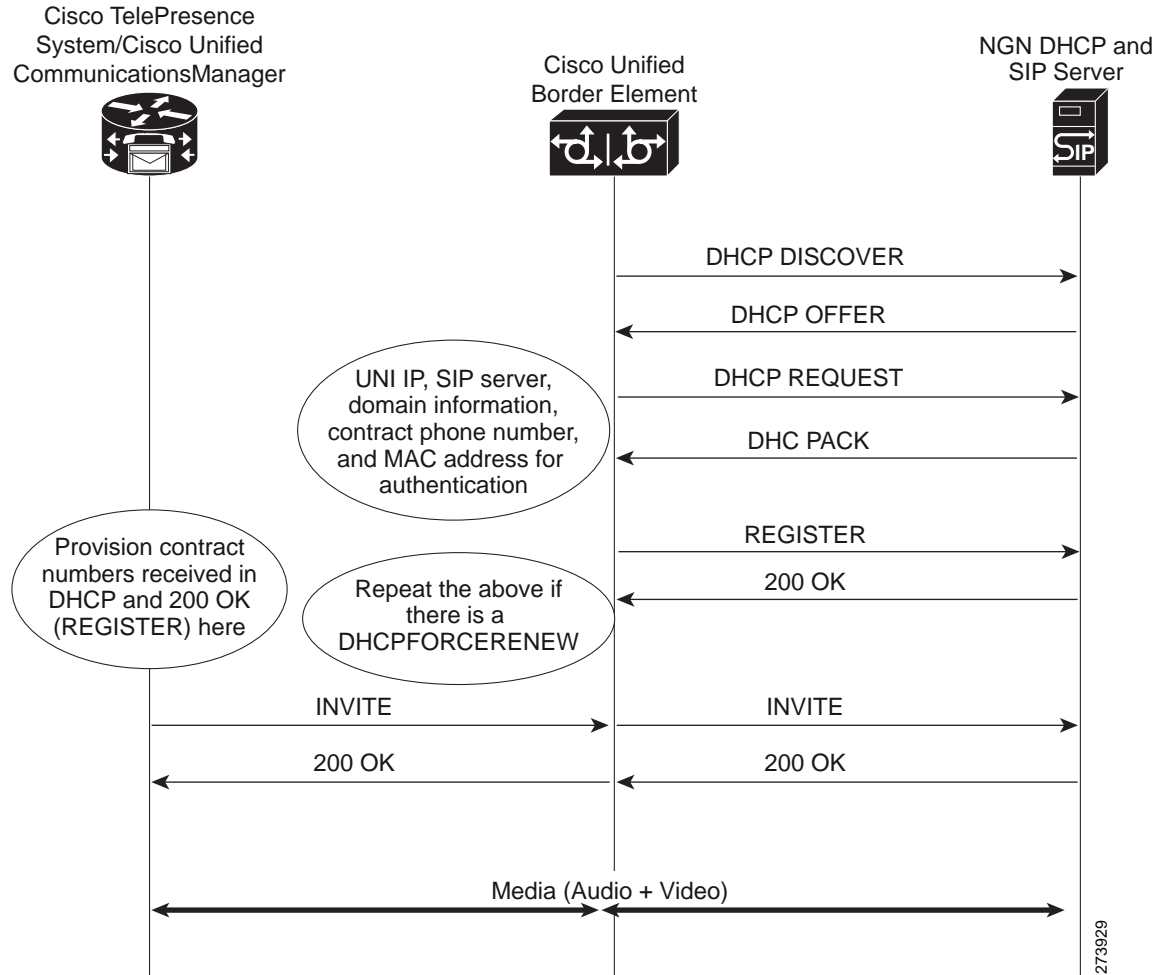


## DHCP-SIP Call Flow

The following scenario shows the DHCP messages involved in provisioning information such as the IP address for UNI interface, and SIP parameters including the SIP server address, phone number, and domain name, along with how SIP messages use the provisioned information.

Figure 2 shows the DHCP and SIP messages involved in obtaining the SIP parameters and using them for REGISTER and INVITE.

**Figure 2 DHCP-SIP Call Flow**

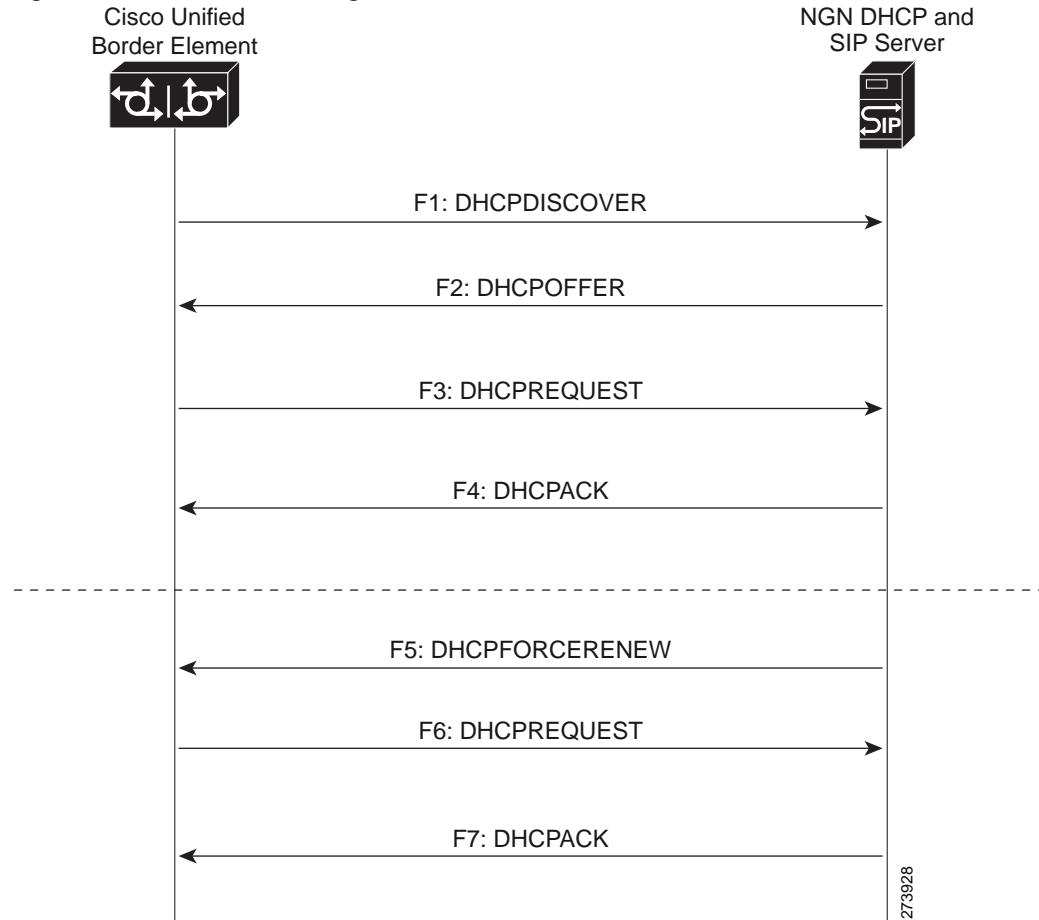


273929

## DHCP Message Details

The DHCP call flow involved in obtaining Cisco Unified Border Element provision information, including the IP address for UNI interface and SIP information such as phone number, domain, and SIP server, is shown in [Figure 2](#).

**Figure 3** *DHCP Message Details*



The DHCP messages involved in provisioning the SIP parameters are described in Steps 1 to 6.

1. F1: The Cisco Unified Border Element DHCP client sends a DHCPDISCOVER message to find the available NGN DHCP servers on the network and obtain a valid IPv4 address. The Cisco Unified Border Element DHCP client identity (computer name) and MAC address are included in this message.
2. F2: The Cisco Unified Border Element DHCP client receives a DHCPOFFER message from each available NGN DHCP server. The DHCPOFFER message includes the offered DHCP server's IPv4 address, the DHCP client's MAC address, and other configuration parameters.
3. F3: The Cisco Unified Border Element DHCP client selects an NGN DHCP server and its IPv4 address configuration from the DHCPOFFER messages it receives, and sends a DHCPREQUEST message requesting its usage. Note that this is where Cisco Unified Border Element requests SIP server information via DHCP Option 120 and vendor-identifying information via DHCP Option 125.

4. F4: The chosen NGN DHCP server assigns its IPv4 address configuration to the Cisco Unified Border Element DHCP client by sending a DHCPACK message to it. The Cisco Unified Border Element DHCP client receives the DHCPACK message. This is where the SIP server address, phone number and domain name information are received via DHCP options 120 and 125. The Cisco Unified Border Element will use the information for registering the phone number and routing INVITE messages to the given SIP server.
5. F5: When NGN has a change of information or additional information (such as changing SIP server address from 1.1.1.1 to 2.2.2.2) for assigning to Cisco Unified Border Element, the DHCP server initiates DHCPFORCERENEW to the Cisco Unified Border Element. If the authentication is successful, the Cisco Unified Border Element DHCP client accepts the DHCPFORCERENEW and moves to the next stage of sending DHCPREQUEST. Otherwise DHCPFORCERENEW is ignored and the current information is retained and used.
6. F6 and F7: In response to DHCPFORCERENEW, similar to steps F3 and F4, the Cisco Unified Border Element requests DHCP Options 120 and 125. Upon getting the response, SIP will apply these parameters if they are different by sending an UN-REGISTER message for the previous phone number and a REGISTER message for the new number. Similarly, a new domain and SIP server address will be used. If the returned information is the same as the current set, it is ignored and hence registration and call routing remains the same.

## How to Configure SIP Parameters via DHCP

To configure SIP parameters via DHCP, perform the following tasks:

- [Configuring the DHCP Client, page 163](#) (Required)
- [Enabling the SIP Configuration, page 165](#) (Required)
- [Configuring a SIP Outbound Proxy Server, page 166](#) (Required)
- [Enabling Forced Update of SIP Parameters via DHCP, page 169](#) (Required)

## Configuring the DHCP Client

To receive the SIP configuration parameters the Cisco Unified Border Element has to act as a DHCP client. This is because in the NGN network, a DHCP server pushes the configuration to a DHCP client. Thus the Cisco Unified Border Element must be configured as a DHCP client.

Perform this task to configure the DHCP client.

## Prerequisites

You must configure the **ip dhcp client** commands before entering the **ip address dhcp** command on an interface to ensure that the DHCPDISCOVER messages that are generated contain the correct option values. The **ip dhcp client** commands are checked only when an IP address is acquired from DHCP. If any of the **ip dhcp client** commands are entered after an IP address has been acquired from DHCP, the DHCPDISCOVER messages' correct options will not be present or take effect until the next time the router acquires an IP address from DHCP. This means that the new configuration will only take effect after either the **ip address dhcp** command or the **release dhcp** and **renew dhcp EXEC** commands have been configured.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address dhcp**
5. **ip dhcp client request sip-server-address**
6. **ip dhcp client request vendor-identifying-specific**
7. **exit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>interface</b> <i>type number</i>  <b>Example:</b> Router(config)# interface gigabitethernet 0/0	Configures an interface type and enters interface configuration mode.
Step 4	<b>ip dhcp client request sip-server-address</b>  <b>Example:</b> Router(config-if)# ip dhcp client request sip-server-address	Configures the DHCP client to request a SIP server address from a DHCP server.
Step 5	<b>ip dhcp client request vendor-identifying-specific</b>  <b>Example:</b> Router(config-if)# ip dhcp client request vendor-identifying-specific	Configures the DHCP client to request vendor-specific information from a DHCP server.
Step 6	<b>ip address dhcp</b>  <b>Example:</b> Router(config-if)# ip address dhcp	Acquires an IP address on the interface from the DHCP.
Step 7	<b>exit</b>  <b>Example:</b> Router(config-if)# exit	Exits the current mode.

## Enabling the SIP Configuration

Enabling the SIP configuration allows the Cisco Unified Border Element to use the SIP parameters received via DHCP for user registration and call routing.

Perform this task to enable the SIP configuration.

### Prerequisites

The **dhcp interface** command has to be entered to declare the interface before the **registrar** and **credential** commands are entered.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **sip-ua**
5. **dhcp interface** *type number*
6. **registrar dhcp expires** *seconds* **random-contact refresh-ratio** *seconds*
7. **credentials dhcp password** [**0** | **7**] *password realm domain-name*
8. **exit**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>interface</b> <i>type number</i>  <b>Example:</b> Router(config)# interface gigabitethernet 0/0	Configures an interface type and enters interface configuration mode.
Step 4	<b>sip-ua</b>  <b>Example:</b> Router(config-if)# sip-ua	Enters SIP user-agent configuration mode.

	Command or Action	Purpose
Step 5	<pre>dhcp interface type number</pre> <p><b>Example:</b> Router(sip-ua)# dhcp interface gigabitethernet 0/0 </p>	<p>Assigns a specific interface for DHCP provisioning of SIP parameters.</p> <ul style="list-style-type: none"> <li>Multiple interfaces on the CUBE can be configured with DHCP—this command specifies the DHCP interface used with SIP.</li> </ul>
Step 6	<pre>registrar dhcp expires seconds random-contact refresh-ratio seconds</pre> <p><b>Example:</b> Router(sip-ua)# registrar dhcp expires 100 random-contact refresh-ratio 90 </p>	<p>Registers E.164 numbers on behalf of analog telephone voice ports (FXS) and IP phone virtual voice ports (EFXS) with an external SIP proxy or SIP registrar server.</p> <ul style="list-style-type: none"> <li><b>expires seconds</b>—Specifies the default registration time, in seconds. Range is 60 to 65535. Default is 3600.</li> <li><b>refresh-ratio seconds</b>—Specifies the refresh-ratio, in seconds. Range is 1 to 100 seconds. Default is 80.</li> </ul>
Step 7	<pre>credentials dhcp password [0   7] password realm domain-name</pre> <p><b>Example:</b> Router(sip-ua)# credentials dhcp password cisco realm cisco.com </p>	<p>Sends a SIP registration message from a Cisco Unified Border Element in the UP state.</p>
Step 8	<pre>exit</pre> <p><b>Example:</b> Router(sip-ua)# exit </p>	<p>Exits the current mode.</p>

## Troubleshooting Tips

To display information on DHCP and SIP interaction when SIP parameters are provisioned by DHCP, use the **debug ccsip dhcp** command in privileged EXEC mode.

## Configuring a SIP Outbound Proxy Server

An outbound-proxy configuration sets the Layer 3 address (IP address) for any outbound REGISTER and INVITE SIP messages. The SIP server can be configured as an outbound proxy server in voice service SIP configuration mode or dial peer configuration mode. When enabled in voice service SIP configuration mode, all the REGISTER and INVITE messages are forwarded to the configured outbound proxy server. When enabled in dial-peer configuration mode, only the messages hitting the defined dial-peer will be forwarded to the configured outbound proxy server.

The configuration tasks in each mode are presented in the following sections:

- [Configuring a SIP Outbound Proxy Server in Voice Service VoIP Configuration Mode, page 167](#)
- [Configuring a SIP Outbound Proxy Server and Session Target in Dial Peer Configuration Mode, page 168](#)

Perform either of these tasks to configure the SIP server as a SIP outbound proxy server.

## Configuring a SIP Outbound Proxy Server in Voice Service VoIP Configuration Mode

Perform this task to configure the SIP server as a SIP outbound proxy server in voice service SIP configuration mode.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **sip**
5. **outbound-proxy dhcp**
6. **exit**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>voice service voip</b>  <b>Example:</b> Router(config)# voice service voip	Enters voice service VoIP configuration mode and specifies VoIP as the voice-encapsulation type.
Step 4	<b>sip</b>  <b>Example:</b> Router(config-voi-srv)# sip	Enters voice service SIP configuration mode.
Step 5	<b>outbound-proxy dhcp</b>  <b>Example:</b> Router(conf-serv-sip)# outbound-proxy dhcp	Configures the DHCP client to request a SIP server address from a DHCP server.
Step 6	<b>exit</b>  <b>Example:</b> Router(config-serv-sip)# exit	Exits the current mode.

## Configuring a SIP Outbound Proxy Server and Session Target in Dial Peer Configuration Mode

Perform this task to configure the SIP server as a SIP outbound proxy server in dial peer configuration mode.

### Restrictions

SIP must be configured on the dial peer before DHCP is configured. Therefore the **session protocol sipv2** command must be executed before the **session target dhcp** command. DHCP is supported only with SIP configured on the dial peer.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice *number* voip**
4. **session protocol sipv2**
5. **voice-class sip outbound-proxy dhcp**
6. **session target dhcp**
7. **exit**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>dial-peer voice <i>number</i> voip</b>  <b>Example:</b> Router(config)# dial-peer voice 10 voip	Defines a dial peer, specifies VoIP as the method of voice encapsulation, and enters dial peer configuration mode.
Step 4	<b>session protocol sipv2</b>  <b>Example:</b> Router(config-dial-peer)# session protocol sipv2	Enters the session protocol type as SIP.
Step 5	<b>voice-class sip outbound-proxy dhcp</b>  <b>Example:</b> Router(config-dial-peer)# voice-class sip outbound-proxy dhcp	Configures the SIP server received from the DHCP server as a SIP outbound proxy server.



	Command or Action	Purpose
Step 6	<pre>session target dhcp</pre> <p><b>Example:</b> Router(config-dial-peer)# session target dhcp</p>	Specifies that the DHCP protocol is used to determine the IP address of the session target.
Step 7	<pre>exit</pre> <p><b>Example:</b> Router(config-dial-peer)# exit</p>	Exits the current mode.

### Enabling Forced Update of SIP Parameters via DHCP

In the event of changes to the SIP parameter values, a DHCP message called DHCPFORCERENEW can reset or apply a new set of values. The NGN can add or change phone number, SIP server address and domain name by sending DHCPFORCERENEW. When the SIP server receives the SIP parameter values, it compares the existing values to see if they are the same or if they have changed. If they are the same, the existing SIP parameters continue to be used. If they are different, the current phone number is unregistered and the new one registered, and the new SIP server address and domain name are used.

Perform this task to enable the forced update of SIP parameters via DHCP.

### Prerequisites

The DHCP provisioning of SIP parameters must be enabled.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `ip dhcp-client forcerenew`
4. `exit`

### DETAILED STEPS

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

	Command or Action	Purpose
Step 3	<code>ip dhcp-client forcerenew</code>  <b>Example:</b> Router(config)# ip dhcp-client forcerenew	Enables the forced update of SIP parameters via DHCP.
Step 4	<code>exit</code>  <b>Example:</b> Router(config)# exit	Exits the current mode.

## Configuration Examples for Configurable SIP Parameters via DHCP

This section contains the following configuration examples:

- [Configuring the DHCP Client: Example, page 170](#)
- [Enabling the SIP Configuration: Example, page 170](#)
- [Configuring a SIP Outbound Proxy Server in Voice Service VoIP Configuration Mode: Example, page 170](#)
- [Configuring a SIP Outbound Proxy Server in Dial Peer Configuration Mode: Example, page 171](#)
- [Enabling Forced Update of SIP Parameters via DHCP: Example, page 171](#)

### Configuring the DHCP Client: Example

The following is an example of how to enable the DHCP client:

```
Router> enable
Router# configure terminal
Router(config)# interface gigabitethernet 1/1
Router(config-if)# ip dhcp client request sip-server-address
Router(config-if)# ip dhcp client request vendor-identifying-specific
Router(config-if)# ip address dhcp
Router(config-if)# exit
```

### Enabling the SIP Configuration: Example

The following is an example of how to enable the SIP configuration:

```
Router> enable
Router# configure terminal
Router(config)# interface gigabitethernet 1/0
Router(config-if)# sip-ua
Router(sip-ua)# dhcp interface gigabitethernet 1/0
Router(sip-ua)# registrar dhcp expires 90 random-contact refresh-ratio 90
Router(sip-ua)# credentials dhcp password cisco realm cisco.com
Router(sip-ua)# exit
```

### Configuring a SIP Outbound Proxy Server in Voice Service VoIP Configuration Mode: Example

The following is an example of how to configure a SIP outbound proxy in voice service SIP configuration mode:

```
Router> enable
Router# configure terminal
Router(config)# voice service voip
Router(config-voi-srv)# sip
Router(conf-serv-sip)# outbound-proxy dhcp
Router(config-serv-if)# exit
```

## Configuring a SIP Outbound Proxy Server in Dial Peer Configuration Mode: Example

The following is an example of how to configure a SIP outbound proxy in dial peer configuration mode:

```
Router> enable
Router# configure terminal
Router(config)# dial-peer voice 11 voip
Router(config-dial-peer)# session protocol sipv2
Router(config-dial-peer)# voice-class sip outbound-proxy dhcp
Router(config-dial-peer)# session target dhcp
Router(config-dial-peer)# exit
```

## Enabling Forced Update of SIP Parameters via DHCP: Example

The following is an example of how to enable forced update of SIP parameters via DHCP:

```
Router> enable
Router# configure terminal
Router(config)# ip dhcp-client forcerenew
Router(config)# exit
```

## Configuring SIP Listening Port

To manually change the SIP listen port for UDP/TCP/TLS calls, perform the steps in this section:

### Prerequisites

- Configure the **shutdown** command in sip configuration mode first. This ensures that there are no active calls when the SIP listen port is changed. If SIP service is not shutdown, the listen-port command flashes an error message saying “shutdown SIP service before changing SIP listen port”.
- This feature is applicable for both incoming and outgoing call SIP.
- The IP-to-IP gateway port number defined in global configuration will be used for both IN leg and OUT leg.

### Restrictions

- Configuring SIP listening port on a dial-peer basis is not supported.
- Configuring the same listening port for both UDP/TCP and TLS is not supported.
- Configuring SIP listen port to a port that is already in use is not supported, and results in an error message.

- Changing the SIP listening port when Transport Process (TCP/UDP/TLS) services are shutdown, will not close or reopen the port. The only result is that the new port number is updated. The new port is bound when transport services (TCP/UDP/TLS) is enabled.
- Both **secure** and **non-secure** keywords are supported on Crypto images
- The **non-secure** keyword is supported on non-Crypto images.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **sip**
5. **listen-port {non-secure | secure} port-number**
6. **exit**
7. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> <code>Router&gt; enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<code>configure terminal</code>  <b>Example:</b> <code>Router# configure terminal</code>	Enters global configuration mode.
Step 3	<code>voice service voip</code>  <b>Example:</b> <code>Router(config)# voice service voip</code>	Enters VoIP voice-service configuration mode.
Step 4	<code>sip</code>  <b>Example:</b> <code>Router(config-voi-srv)# sip</code>	Enters SIP configuration mode.
Step 5	<code>listen-port {non-secure   secure} port-number</code>  <b>Example:</b> <code>Router (config-voip-peer)# listen-port secure 3000</code>	Port number. Range: 1 to 65535. The default for UDP/TCP is 5060, the default for TLS is 5061.  <b>Image Support</b> <ul style="list-style-type: none"> <li>• The <b>secure</b> and <b>non-secure</b> keywords are supported on Crypto images.</li> <li>• The <b>non-secure</b> keyword is supported on non-Crypto images.</li> </ul>

	Command or Action	Purpose
Step 6	<code>exit</code>  <b>Example:</b> Router(config-dial-peer)# <code>exit</code>	Exits the current mode.
Step 7	<code>end</code>  <b>Example:</b> Router(config-voi-srv)# <code>end</code>	Returns to privileged EXEC mode.

## Configuring Bandwidth Parameters for SIP Calls

This feature provides a CLI command that is configured under each dialpeer that is triggered when an outbound SIP call is made using this dialpeer. The configured value for the Bandwidth command overwrite the default bandwidth that is determined by the codec selected. This command is helpful to allow the bandwidth to be signalled independent of the specific codec used

To manually change the SIP listen port for UDP/TCP/TLS calls, perform the steps in this section:

### Prerequisites

- Configure the **shutdown** command in sip configuration mode first. This ensures that there are no active calls when the SIP listen port is changed. If SIP service is not shutdown, the listen-port command flashes an error message saying “shutdown SIP service before changing SIP listen port”.
- This feature is applicable for both incoming and outgoing call SIP.
- The Cisco Unified BE port number defined in global configuration will be used for both IN leg and OUT leg.

### Restrictions

- Configuring SIP listening port on a dial-peer basis is not supported.

## Configuring Support for Session Refresh with Reinvites

Configuring support for session refresh with reinvites expands the ability of the Cisco Unified BE to receive a REINVITE message that contains either a session refresh parameter or a change in media via a new SDP and ensure the session does not time out. The **midcall-signaling** command distinguishes between the way a Cisco Unified Communications Express and Cisco Unified Border Element releases signaling messages. Most SIP-to-SIP video and SIP-to-SIP ReInvite-based supplementary services features require the Configuring Session Refresh with Reinvites feature to be configured.

### Cisco IOS Release 12.4(15)XZ and Earlier Releases

Session refresh support via OPTIONS method. For configuration information, see the [“Enabling In-Dialog OPTIONS to Monitor Active SIP Sessions”](#) section on page 152.

**Cisco IOS Release 12.4(15)XZ and Later Releases**

Cisco Unified BE transparently passes other session refresh messages and parameters so that UAs and proxies can establish keepalives on a call.

**Prerequisites**

- The **allow-connections sip to sip** command must be configured before you configure the Session refresh with Reinvites feature. For more information and configuration steps see the [“Configuring SIP-to-SIP Connections in a Cisco Unified Border Element”](#) section on page 137.

**Restrictions**

- SIP-to-SIP video calls and SIP-to-SIP ReInvite-based supplementary services fail if the **midcall-signaling** command is not configured.



**Note** The following features function if the **midcall-signaling** command is not configured: session refresh, fax, and refer-based supplementary services.

- Configuring Session Refresh with Reinvites is for SIP-to-SIP calls only. All other calls (H323-to-SIP, and H323-to-H323) do not require the **midcall-signaling** command be configured
- Configuring the Session Refresh with Reinvites feature on a dial-peer basis is not supported.

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **sip**
5. **midcall-signaling passthru**
6. **exit**
7. **end**

**DETAILED STEPS**

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

	Command or Action	Purpose
Step 3	<code>voice service voip</code>  <b>Example:</b> <code>Router(config)# voice service voip</code>	Enters VoIP voice-service configuration mode.
Step 4	<code>sip</code>  <b>Example:</b> <code>Router(conf-voi-serv)# sip</code>	Enters SIP configuration mode.
Step 5	<code>midcall-signaling passthru</code>  <b>Example:</b> <code>Router(conf-serv-sip)# midcall-signaling passthru</code>	Passes SIP messages from one IP leg to another IP leg.
Step 6	<code>exit</code>  <b>Example:</b> <code>Router(conf-serv-sip)# exit</code>	Exits the current mode.
Step 7	<code>end</code>  <b>Example:</b> <code>Router(conf-serv-sip) end</code>	Returns to privileged EXEC mode.

## Sending a SIP Registration Message from a Cisco Unified Border Element

The **credentials** command allows you to send a SIP registration message from a Cisco Unified Border Element in the UP state. Registration can include numbers, number ranges (such as E.164-numbers), or text information.

Before Cisco IOS Release 12.4(24)T, a POTS dial peer was required to register numbers from a Cisco Unified Border Element in the UP state. The **credentials** command is modified in Release 12.4(24s)T to allow for registration of the E.164-numbers, if there is no POTS dial peer.

### Prerequisites

Configure a registrar in sip user-agent configuration mode.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `sip-uaF`
4. `credentials username username password password realm domain-name`
5. `exit`
6. `end`

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> <code>Router&gt; enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>
Step 2	<code>configure terminal</code>  <b>Example:</b> <code>Router# configure terminal</code>	Enters global configuration mode.
Step 3	<code>sip-ua</code>  <b>Example:</b> <code>Router(config)# sip-ua</code>	Enters sip user-agent configuration mode.
Step 4	<code>credentials username username password password realm domain-name</code>  <b>Example:</b> <code>Router(config-sip-ua)# credentials username alex password test realm cisco.com</code>	Enters SIP digest credentials in sip-ua configuration mode.
Step 5	<code>exit</code>  <b>Example:</b> <code>Router(config-sip-ua)# exit</code>	Exits the current mode.
Step 6	<code>end</code>  <b>Example:</b> <code>Router(config)# end</code>	Returns to privileged EXEC mode.

## Configuring Adjustable Timers for Registration Refresh and Retries

Configuring Adjustable Timers for Registration Refresh and Retries provides the ability for IOS software to refresh the REGISTER at a configurable fraction of the expiry timer specified in the 200 OK of the REGISTER. The feature also provides the ability to retransmit REGISTER upon failure responses per the min-expires value in a “423 interval too brief” response, or retry-after if present and terminal re-registration interval if retry-after value is absent in 4xx/5xx/6xx responses. Additionally, the ability to retransmit REGISTER per Timer E up to 32 seconds, and at a command line interface controlled random interval thereafter.

This feature addresses the UNI SIP registration specification requirements on Cisco Unified Border Element to interwork CTS over NGN and includes the following are SIP registration enhancements:

### 423 Interval Too Brief Response Handling

Cisco Unified Border Element retransmits the REGISTER with the received Min-Expires value in the 423 response. The retransmit interval is the same as the configured REGISTER refresh ratio.



If the registration response from the REGISTRAR server is a “423 Interval Too Brief” message the configured registration expires time-value sent in the REGISTER message is not acceptable. The 423 header response contains the acceptable expires time value in the Min-Expires header. The newly received time value is then used in the Expires header when the next registration refresh message is sent.

#### **4xx/5xx/6xx Error Response Handling (Except 423)**

If the registration response from the REGISTRAR server is a 4xx/5xx/6xx (except 423) message, an error has occurred. The retransmit interval uses the Retry-After value if present in the 4xx/5xx/6xx response. The only supported Retry-After header format is ‘Retry-After:1800’. If the Retry-After header is not present in the response, the retransmit interval will be refresh interval if **refresh-ratio** keyword is configured else it will be the default retransmit interval.

The error response may contain a time value in the “Retry-After” header which can be then used as the refresh interval of the next REGISTER message. If “Retry-After” header is not present in the error response, the configured refresh ratio and “Expires” time value will be used to calculate the interval between the sending of the next REGISTER message.

#### **Configurable REGISTER Refresh Ratio**

The Cisco Unified Border Element sends REGISTER refresh at 40% to 50% of the expiry time as specified in 200 OK of REGISTER. Use the **refresh-ratio** keyword to configure the REGISTER refresh ratio. If the refresh-ratio option is not configured, the default REGISTER refresh ratio is 80% of the expiry timer. The minimum refresh interval is one minute.

#### **No REGISTER Response Handling**

The Cisco Unified Border Element handles no response to REGISTER by retransmitting at intervals Timer E for up to a maximum of 32 seconds. If no REGISTER response is received from the REGISTRAR server, the REGISTER message will be retransmitted. By configuring the **retry register** command to 10, the Cisco Unified Border Element retransmits the REGISTER (starting at 500 ms) and continues to retransmit at double the rate, to a maximum of 4 seconds. The default REGISTER retransmit count is six retries, after which the Cisco Unified Border Element retransmits at a random interval (5 to 10 minutes).

There is a two minute interval after which the REGISTER retransmits begin again. The **retry register exhausted-random-interval** command allows the user to set a desired interval after the number of REGISTER retransmits have been exhausted. This also allows the user to set a range in which a number (in minutes) is randomly generated and used as the interval between retransmission exhaustion.

#### **REGISTER Refresh, Error and No Response Retransmit**

The default REGISTER refresh ratio is eighty percent (80%) of the expiry time. The default REGISTER error retransmit interval is 5% of the configured expiry time or two minutes, whichever is greater.

#### **Random String in REGISTER Contact**

Cisco Unified Border Element uses a random string in the Contact header of the REGISTER message. The random string consists of alphanumeric characters. A different random string is generated and used for each number registered.

To configure Adjustable Timers for Registration Refresh and Retries, perform the steps in this section:

## **SUMMARY STEPS**

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

3. `sip-ua`
4. `registrar`
5. `retry register retries`
6. `exit`

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<pre>enable</pre> <p><b>Example:</b> Router&gt; enable</p>	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	<pre>configure terminal</pre> <p><b>Example:</b> Router# configure terminal</p>	Enters global configuration mode.
Step 3	<pre>sip-ua</pre> <p><b>Example:</b> Router(config)# sip-ua</p>	Enters the SIP user agent ( <code>sip-ua</code> ) configuration mode to configure SIP-UA related commands.
Step 4	<pre>registrar expires 60 refresh-ratio 45 random-contact</pre> <p><b>Example:</b> Router(config-sip-ua)# expires 60 refresh-ratio 45 random-contact</p>	<p>Configures the SIP registrar for retry attempts. The keywords are as follows:</p> <ul style="list-style-type: none"> <li>• <b>expires</b>—Default registration expires time</li> <li>• <b>refresh-ratio</b>—Registration refresh ratio expressed as a percentage. Valid entries are 1 to 100. The default is 80</li> <li>• <b>random-contact</b>—Random String Contact Header</li> </ul>
Step 5	<pre>retry register retries exhausted-random-interval minimum 4 maximum 5</pre> <p><b>Example:</b> Router(config-sip-ua)# retry register retries exhausted-random-interval minimum 4 maximum 5</p>	<p>Sets the total number of SIP register messages that the gateway should send. The keywords are as follows:</p> <ul style="list-style-type: none"> <li>• <b>retries</b>—Total number of register messages that the gateway should send. The range is from 1 to 10. The default is 10 retries.</li> <li>• <b>exhausted-random-interval</b>—specifies that the register request is generated within the defined time interval.</li> <li>• <b>minimum minutes</b>—Sets the minimum time interval, in minutes.</li> <li>• <b>maximum minutes</b>—Sets the maximum time interval in minutes.</li> </ul>
Step 6	<pre>exit</pre> <p><b>Example:</b> Router(config-sip-ua)# exit</p>	Exits the current mode.

## Cisco Unified Border Element Support for SRTP-RTP Internetworking

The Cisco Unified Border Element Support for SRTP-RTP Internetworking feature allows secure enterprise-to-enterprise calls. The feature also provides operational enhancements for Session Initiation Protocol (SIP) trunks from Cisco Unified Call Manager and Cisco Unified Call Manager Express. Support for Secure Real-Time Transport Protocol (SRTP)-RTP internetworking between one or multiple Cisco Unified Border Elements is enabled for SIP-SIP audio calls.

### Prerequisites for Cisco Unified Border Element Support for SRTP-RTP Internetworking

The Cisco Unified Border Element Support for SRTP-RTP Internetworking feature is supported in Cisco Unified CallManager 7.0 and later releases.

### Restrictions for Cisco Unified Border Element Support for SRTP-RTP Internetworking

The following features are not supported by the Cisco Unified Border Element Support for SRTP-RTP Internetworking feature:

- Voice-class codec
- Call admission control (CAC) support
- Rotary SIP-SIP
- T.38 Fax
- Early offer to delayed offer calls
- Delayed offer to early offer calls

### Information About Cisco Unified Border Element Support for SRTP-RTP Internetworking

To configure support for SRTP-RTP internetworking, you should understand the following concepts:

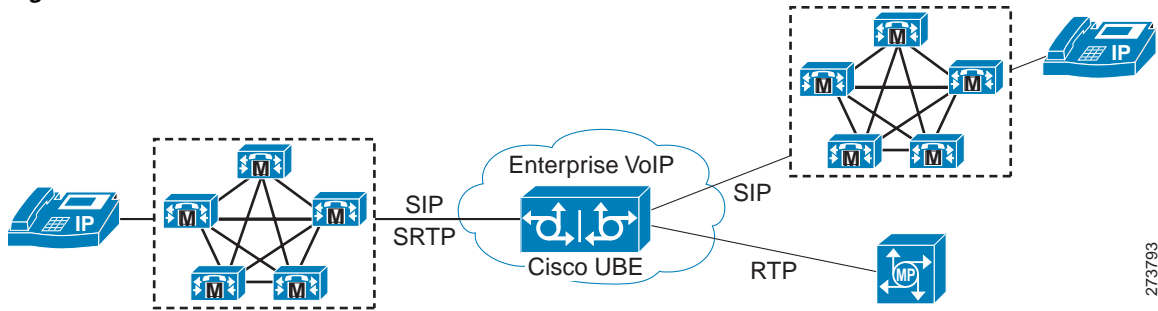
- [Cisco Unified Border Element Support for SRTP-RTP Internetworking, page 179](#)
- [TLS on the Cisco Unified Border Element, page 181](#)

### Cisco Unified Border Element Support for SRTP-RTP Internetworking

The Cisco Unified Border Element Support for SRTP-RTP Internetworking feature connects SRTP Cisco Unified CallManager domains with the following:

- RTP Cisco Unified CallManager domains. Domains that do not support SRTP, or have not been configured for SRTP, as shown in [Figure 4](#).
- RTP Cisco applications or servers. For example, Cisco Unified MeetingPlace, Cisco WebEx, or Cisco Unity, which do not support SRTP, or have not been configured for SRTP, or are resident in a secure data center, as shown in [Figure 4](#).
- RTP to third-party equipment. For example, IP trunks to PBXs or virtual machines, which do not support SRTP.

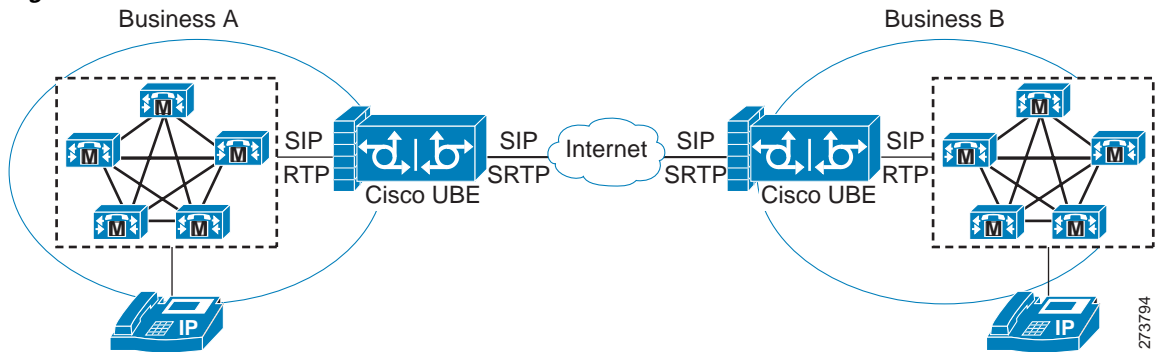
**Figure 4** *SRTP Domain Connections*



273793

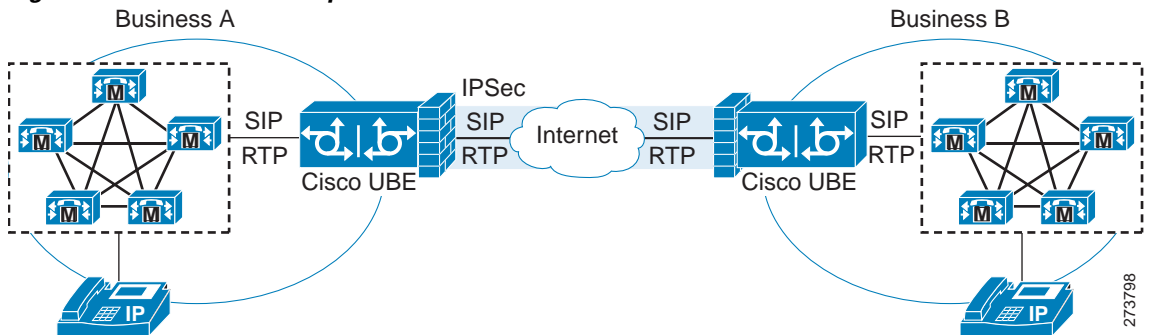
The Cisco Unified Border Element Support for SRTP-RTP Internetworking feature connects SRTP enterprise domains to RTP SIP provider (SP) SIP trunks. SRTP-RTP internetworking connects RTP enterprise networks with SRTP over an external network between businesses. This provides flexible secure business-to-business communications without the need for static IPsec tunnels or the need to deploy SRTP within the enterprise, as shown in [Figure 5](#). SRTP-RTP internetworking also connects SRTP enterprise networks with static IPsec over external networks, as shown in [Figure 6](#).

**Figure 5** *Secure Business-to-Business Communications*



273794

**Figure 6** *SRTP Enterprise Network Connections*



273798

SRTP-RTP internetworking on the Cisco Unified Border Element in a network topology uses single pair key generation. Existing audio and dual-tone multifrequency (DTMF) transcoding is used to support voice calls. SRTP-RTP internetworking support is provided in both flow-through and high-density mode. SRTP-SRTP pass-through is not impacted.

SRTP is configured on one dial peer and RTP is configured on the other dial peer using the **srtp** and **srtp fallback** commands. The dial-peer configuration takes precedence over the global configuration on the Cisco Unified Border Element.

Fallback handling occurs if one of the call endpoints does not support SRTP. The call can fall back to RTP-RTP, or the call can fail, depending on the configuration. Fallback takes place only if the **srtp fallback** command is configured on the respective dial peer. RTP-RTP fall back occurs when no transcoding resources are available for SRTP-RTP internetworking.

## TLS on the Cisco Unified Border Element

The Cisco Unified Border Element Support for SRTP-RTP Internetworking feature allows Transport Layer Security (TLS) to be enabled or disabled between the SCCP server and SCCP client. By default TLS is enabled, which provides added protection at transport level and ensures that SRTP keys are not easily accessible. Once TLS is disabled, the SRTP keys are not protected.

SRTP-RTP internetworking is available with normal and universal transcoders. The transcoder on the Cisco Unified Border Element is invoked using SCCP messaging between the SCCP server and the SCCP client. The SCCP messages carry the SRTP keys to the digital signal processor (DSP) farm at the SCCP client. The transcoder can be within the same router or can be located in a separate router. TLS should be disabled only when the transcoder is located in the same router. To disable TLS, configure the **no** form of the **tls** command in dsp farm profile configuration mode. Disabling TLS improves CPU performance.

## How to Configure Cisco Unified Border Element Support for SRTP-RTP Internetworking

This section contains the following task:

- [Configuring Cisco Unified Border Element Support for SRTP-RTP Internetworking, page 181](#) (required)

## Configuring Cisco Unified Border Element Support for SRTP-RTP Internetworking

Configuring the Cisco Unified Border Element Support for SRTP-RTP Internetworking feature consists of the following tasks:

- [Configuring the Certificate Authority, page 182](#) (required)
- [Configuring a Trustpoint for the Secure Universal Transcoder, page 183](#) (required)
- [Configuring DSP Farm Services, page 184](#) (required)
- [Associating SCCP to the Secure DSP Farm Profile, page 186](#) (required)
- [Registering the Secure Universal Transcoder to the Cisco Unified Border Element, page 189](#) (required)
- [Configuring SRTP-RTP Internetworking Support, page 191](#) (required)

## Configuring the Certificate Authority

Perform the steps described in this section to configure the certificate authority.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip http server**
4. **crypto pki server *cs-label***
5. **database level complete**
6. **grant auto**
7. **no shutdown**
8. **exit**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<code>configure terminal</code>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<code>ip http server</code>  <b>Example:</b> Router(config)# ip http server	Enables the HTTP server on your IP or IPv6 system, including the Cisco web browser user interface.
Step 4	<code>crypto pki server <i>cs-label</i></code>  <b>Example:</b> Router(config)# crypto pki server 3854-cube	Enables a Cisco IOS certificate server and enters certificate server configuration mode. <ul style="list-style-type: none"> <li>• In the example, 3845-cube is specified as the name of the certificate server.</li> </ul>
Step 5	<code>database level complete</code>  <b>Example:</b> Router(cs-server)# database level complete	Controls what type of data is stored in the certificate enrollment database. <ul style="list-style-type: none"> <li>• In the example, each issued certificate is written to the database.</li> </ul>
Step 6	<code>grant auto</code>  <b>Example:</b> Router(cs-server)# grant auto	Specifies automatic certificate enrollment.

	Command or Action	Purpose
Step 7	<pre>no shutdown</pre> <p><b>Example:</b> Router(cs-server)# no shutdown </p>	Reenables the certificate server. <ul style="list-style-type: none"> <li>• Create and enter a new password when prompted.</li> </ul>
Step 8	<pre>exit</pre> <p><b>Example:</b> Router(cs-server)# exit </p>	Exits certificate server configuration mode.

## Configuring a Trustpoint for the Secure Universal Transcoder

Perform the steps in this section to configure, authenticate, and enroll the trustpoint for the secure universal transcoder.

### Prerequisites

Before you configure the trustpoint for the secure universal transcoder, you should configure the certificate authority, as described in the [“Configuring the Certificate Authority”](#) section on page 182.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** *name*
4. **enrollment url** *url*
5. **serial-number**
6. **revocation-check** *method*
7. **rsa** *key-label*
8. **end**
9. **crypto pki authenticate** *name*
10. **crypto pki enroll** *name*
11. **exit**

### DETAILED STEPS

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

	Command or Action	Purpose
Step 3	<code>crypto pki trustpoint name</code>  <b>Example:</b> Router(config)# <code>crypto pki trustpoint secdsp</code>	Declares the trustpoint that the router uses and enters ca-trustpoint configuration mode. <ul style="list-style-type: none"> <li>In the example, the trustpoint is named secdsp.</li> </ul>
Step 4	<code>enrollment url url</code>  <b>Example:</b> Router(ca-trustpoint)# <code>enrollment url http://10.13.2.52:80</code>	Specifies the enrollment parameters of a certification authority (CA). <ul style="list-style-type: none"> <li>In the example, the URL is defined as <code>http://10.13.2.52:80</code></li> </ul>
Step 5	<code>serial-number</code>  <b>Example:</b> Router(ca-trustpoint)# <code>serial-number</code>	Specifies whether the router serial number should be included in the certificate request.
Step 6	<code>revocation-check method</code>  <b>Example:</b> Router(ca-trustpoint)# <code>revocation-check crl</code>	Checks the revocation status of a certificate. <ul style="list-style-type: none"> <li>In the example, the certificate revocation list checks the revocation status.</li> </ul>
Step 7	<code>rsakeypair key-label</code>  <b>Example:</b> Router(ca-trustpoint)# <code>rsakeypair 3845-cube</code>	Specifies which key pair to associate with the certificate. <ul style="list-style-type: none"> <li>In the example, the key pair, 3845-cube generated during enrollment is associated with the certificate.</li> </ul>
Step 8	<code>end</code>  <b>Example:</b> Router(ca-trustpoint)# <code>end</code>	Exits ca-trustpoint configuration mode.
Step 9	<code>crypto pki authenticate name</code>  <b>Example:</b> Router(config)# <code>crypto pki authenticate secdsp</code>	Authenticates the CA. <ul style="list-style-type: none"> <li>Accept the trustpoint CA certificate if prompted.</li> </ul>
Step 10	<code>crypto pki enroll name</code>  <b>Example:</b> Router(config)# <code>crypto pki enroll secdsp</code>	Obtains the certificate for the router from the CA. <ul style="list-style-type: none"> <li>Create and enter a new password if prompted.</li> <li>Request a certificate from the CA if prompted.</li> </ul>
Step 11	<code>exit</code>  <b>Example:</b> Router(config)# <code>exit</code>	Exits global configuration mode.

## Configuring DSP Farm Services

Perform the steps in this section to configure DSP farm services.



## Prerequisites

Before you configure DSP farm services, you should configure the trustpoint for the secure universal transcoder, as described in the [“Configuring a Trustpoint for the Secure Universal Transcoder”](#) section on page 183.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice-card slot**
4. **dspfarm**
5. **dsp services dspfarm**
6. Repeat Steps 3,4, and 5 to configure a second voice card.
7. **exit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<code>configure terminal</code>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<code>voice-card slot</code>  <b>Example:</b> Router(config)# voice-card 0	Configures a voice card and enters voice-card configuration mode. <ul style="list-style-type: none"> <li>• In the example, voice card 0 is configured.</li> </ul>
Step 4	<code>dspfarm</code>  <b>Example:</b> Router(config-voicecard)# dspfarm	Adds a specified voice card to those participating in a DSP resource pool.
Step 5	<code>dsp services dspfarm</code>  <b>Example:</b> Router(config-voicecard)# dsp services dspfarm	Enables DSP farm services for a particular voice network module.
Step 6	Repeat Steps 3, 4, and 5 to configure a second voice card.	—
Step 7	<code>exit</code>  <b>Example:</b> Router(config-voicecard)# exit	Exits voice-card configuration mode.

## Associating SCCP to the Secure DSP Farm Profile

Perform the steps in this section to associate SCCP to the secure DSP farm profile.

### Prerequisites

Before you associate SCCP to the secure DSP farm profile, you should configure DSP farm services, as described in the [“Configuring DSP Farm Services”](#) section on page 184.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **sccp local** *interface-type interface-number*
4. **sccp ccm** *ip-address identifier identifier-number version version-number*
5. **sccp**
6. **associate ccm** *identifier-number priority priority-number*
7. **associate profile** *profile-identifier register device-name*
8. **dspfarm profile** *profile-identifier transcode universal security*
9. **trustpoint** *trustpoint-label*
10. **codec** *codec-type*
11. Repeat Step 10 to configure required codecs.
12. **maximum sessions** *number*
13. **associate application sccp**
14. **no shutdown**
15. **exit**

### DETAILED STEPS

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

	Command or Action	Purpose
Step 3	<p><code>sccp local interface-type interface-number</code></p> <p><b>Example:</b> Router(config)# sccp local GigabitEthernet 0/0</p>	<p>Selects the local interface that SCCP applications (transcoding and conferencing) use to register with Cisco CallManager.</p> <ul style="list-style-type: none"> <li>In the example, the following parameters are set: <ul style="list-style-type: none"> <li>GigabitEthernet is defined as the interface type that the SCCP application uses to register with Cisco CallManager.</li> <li>The interface number that the SCCP application uses to register with Cisco CallManager is specified as 0/0.</li> </ul> </li> </ul>
Step 4	<p><code>sccp ccm ip-address identifier identifier-number version version-number</code></p> <p><b>Example:</b> Router(config)# sccp ccm 10.13.2.52 identifier 1 version 5.0.1</p>	<p>Adds a Cisco Unified Communications Manager server to the list of available servers.</p> <ul style="list-style-type: none"> <li>In the example, the following parameters are set: <ul style="list-style-type: none"> <li>10.13.2.52 is configured as the IP address of the Cisco Unified Communications Manager server.</li> <li>The number 1 identifies the Cisco Unified Communications Manager server.</li> <li>The Cisco Unified Communications Manager version is identified as 5.0.1.</li> </ul> </li> </ul>
Step 5	<p><code>sccp</code></p> <p><b>Example:</b> Router(config)# sccp</p>	<p>Enables the SCCP and its related applications (transcoding and conferencing) and enters SCCP Cisco CallManager configuration mode.</p>
Step 6	<p><code>associate ccm identifier-number priority priority-number</code></p> <p><b>Example:</b> Router(config-sccp-ccm)# associate ccm 1 priority 1</p>	<p>Associates a Cisco Unified CallManager with a Cisco CallManager group and establishes its priority within the group.</p> <ul style="list-style-type: none"> <li>In the example, the following parameters are set: <ul style="list-style-type: none"> <li>The number 1 identifies the Cisco Unified CallManager.</li> <li>The Cisco Unified CallManager is configured with the highest priority within the Cisco CallManager group.</li> </ul> </li> </ul>
Step 7	<p><code>associate profile profile-identifier register device-name</code></p> <p><b>Example:</b> Router(config-sccp-ccm)# associate profile 1 register sxcoder</p>	<p>Associates a DSP farm profile with a Cisco CallManager group.</p> <ul style="list-style-type: none"> <li>In the example, the following parameters are set: <ul style="list-style-type: none"> <li>The number 1 identifies the DSP farm profile.</li> <li>Sxcoder is configured as the user-specified device name in Cisco Unified CallManager.</li> </ul> </li> </ul>

	Command or Action	Purpose
Step 8	<p><code>dspfarm profile <i>profile-identifier</i> transcode universal security</code></p> <p><b>Example:</b>  Router(config-sccp-ccm)# dspfarm profile 1  transcode universal security</p>	<p>Defines a profile for DSP farm services and enters DSP farm profile configuration mode.</p> <ul style="list-style-type: none"> <li>In the example, the following parameters are set: <ul style="list-style-type: none"> <li>Profile 1 is enabled for transcoding.</li> <li>Profile 1 is enabled for secure DSP farm services.</li> </ul> </li> </ul>
Step 9	<p><code>trustpoint <i>trustpoint-label</i></code></p> <p><b>Example:</b>  Router(config-dspfarm-profile)# trustpoint  secdsp</p>	<p>Associates a trustpoint with a DSP farm profile.</p> <ul style="list-style-type: none"> <li>In the example, the trustpoint to be associated with the DSP farm profile is labeled secdsp.</li> </ul>
Step 10	<p><code>codec <i>codec-type</i></code></p> <p><b>Example:</b>  Router(config-dspfarm-profile)# codec g711ulaw</p>	<p>Specifies the codecs that are supported by a DSP farm profile.</p> <ul style="list-style-type: none"> <li>In the example, the g711ulaw codec is specified.</li> </ul>
Step 11	Repeat Step 10 to configure required codecs.	—
Step 12	<p><code>maximum sessions <i>number</i></code></p> <p><b>Example:</b>  Router(config-dspfarm-profile)# maximum  sessions 84</p>	<p>Specifies the maximum number of sessions that are supported by the profile.</p> <ul style="list-style-type: none"> <li>In the example, a maximum of 84 sessions are supported by the profile. The maximum number of sessions depends on the number of DSPs available for transcoding.</li> </ul>
Step 13	<p><code>associate application sccp</code></p> <p><b>Example:</b>  Router(config-dspfarm-profile)# associate  application sccp</p>	<p>Associates SCCP to the DSP farm profile.</p>
Step 14	<p><code>no shutdown</code></p> <p><b>Example:</b>  Router(config-dspfarm-profile)# no shutdown</p>	<p>Allocates DSP farm resources and associates with the application.</p>
Step 15	<p><code>exit</code></p> <p><b>Example:</b>  Router(config-dspfarm-profile)# exit</p>	<p>Exits DSP farm profile configuration mode.</p>

## Registering the Secure Universal Transcoder to the Cisco Unified Border Element

Perform the steps in this section to register the secure universal transcoder to the Cisco Unified Border Element. The Cisco Unified Border Element Support for SRTP-RTP Internetworking feature supports both secure transcoders and secure universal transcoders.

### Prerequisites

Before you register the secure universal transcoder to the Cisco Unified Border Element, you should associate SCCP to the secure DSP farm profile, as described in the [“Associating SCCP to the Secure DSP Farm Profile”](#) section on page 186.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **sdspfarm transcode sessions** *number*
5. **sdspfarm tag** *number device-name*
6. **em logout** *time1 time2 time3*
7. **max-ephones** *max-phones*
8. **max-dn** *max-directory-numbers*
9. **ip source-address** *ip-address*
10. **secure-signaling trustpoint** *label*
11. **tftp-server-credentials trustpoint** *label*
12. **create cnf-files**
13. **no sccp**
14. **sccp**
15. **end**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router> configure terminal	Enters global configuration mode.
Step 3	<b>telephony-service</b>  <b>Example:</b> Router(config)# telephony-service	Enters telephony-service configuration mode.

	Command or Action	Purpose
Step 4	<p><code>sdspfarm transcode sessions number</code></p> <p><b>Example:</b>  Router(config-telephony)# sdspfarm transcode sessions 84</p>	<p>Specifies the maximum number of transcoding sessions allowed per Cisco CallManager Express router.</p> <ul style="list-style-type: none"> <li>In the example, a maximum of 84 DSP farm sessions are specified.</li> </ul>
Step 5	<p><code>sdspfarm tag number device-name</code></p> <p><b>Example:</b>  Router(config-telephony)# sdspfarm tag 1 sxcoder</p>	<p>Permits a DSP farm to be registered to Cisco Unified CallManager Express and associates it with an SCCP client interface's MAC address.</p> <ul style="list-style-type: none"> <li>In the example, DSP farm 1 is associated with the sxcoder device.</li> </ul>
Step 6	<p><code>em logout time1 time2 time3</code></p> <p><b>Example:</b>  Router(config-telephony)# em logout 0:0 0:0 0:0</p>	<p>Configures three time-of-day based timers for automatically logging out all Extension Mobility feature users.</p> <ul style="list-style-type: none"> <li>In the example, all users are logged out from Extension Mobility after 00:00.</li> </ul>
Step 7	<p><code>max-ephones 4</code></p> <p><b>Example:</b>  Router(config-telephony)# max-ephones 4</p>	<p>Sets the maximum number of Cisco IP phones to be supported by a Cisco CallManager Express router.</p> <ul style="list-style-type: none"> <li>In the example, a maximum of four phones are supported by the Cisco CallManager Express router.</li> </ul>
Step 8	<p><code>max-dn max-directory-numbers</code></p> <p><b>Example:</b>  Router(config-telephony)# max-dn 4</p>	<p>Sets the maximum number of extensions (ephone-dns) to be supported by a Cisco Unified CallManager Express router.</p> <ul style="list-style-type: none"> <li>In the example, a maximum of four extensions is allowed.</li> </ul>
Step 9	<p><code>ip source-address ip-address</code></p> <p><b>Example:</b>  Router(config-telephony)# ip source-address 10.13.2.52</p>	<p>Identifies the IP address and port through which IP phones communicate with a Cisco Unified CallManager Express router.</p> <ul style="list-style-type: none"> <li>In the example, 10.13.2.52 is configured as the router IP address.</li> </ul>
Step 10	<p><code>secure-signaling trustpoint label</code></p> <p><b>Example:</b>  Router(config-telephony)# secure-signaling trustpoint secdsp</p>	<p>Specifies the name of the PKI trustpoint with the certificate to use for TLS handshakes with IP phones on TCP port 2443.</p> <ul style="list-style-type: none"> <li>In the example, PKI trustpoint secdsp is configured.</li> </ul>
Step 11	<p><code>tftp-server-credentials trustpoint label</code></p> <p><b>Example:</b>  Router(config-telephony)# tftp-server-credentials trustpoint scme</p>	<p>Specifies the PKI trustpoint that signs the phone configuration files.</p> <ul style="list-style-type: none"> <li>In the example, PKI trustpoint scme is configured.</li> </ul>
Step 12	<p><code>create cnf-files</code></p> <p><b>Example:</b>  Router(config-telephony)# create cnf-files</p>	<p>Builds the XML configuration files that are required for IP phones in Cisco Unified CallManager Express.</p>

	Command or Action	Purpose
Step 13	<code>no sccp</code>  <b>Example:</b> Router(config-telephony)# <code>no sccp</code>	Disables SCCP and its related applications (transcoding and conferencing) and exits telephony-service configuration mode.
Step 14	<code>sccp</code>  <b>Example:</b> Router(config)# <code>sccp</code>	Enables SCCP and its related applications (transcoding and conferencing).
Step 15	<code>end</code>  <b>Example:</b> Router(config)# <code>end</code>	Exits global configuration mode.

## Configuring SRTP-RTP Internetworking Support

Perform the steps in this section to enable SRTP-RTP internetworking support between one or multiple Cisco Unified Border Elements for SIP-SIP audio calls. In this task, RTP is configured on the incoming call leg and SRTP is configured on the outgoing call leg.

### Prerequisites

Before you configure the Cisco Unified Border Element Support for SRTP-RTP Internetworking feature, you should register the secure universal transcoder to the Cisco Unified Border Element, as described in the [“Registering the Secure Universal Transcoder to the Cisco Unified Border Element”](#) section on page 189.

### Restrictions

The Cisco Unified Border Element Support for SRTP-RTP Internetworking feature is available only on platforms that support transcoding on the Cisco Unified Border Element. The feature is also available only on secure Cisco IOS images on the Cisco Unified Border Element.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `dial-peer voice tag voip`
4. `destination-pattern string`
5. `session protocol sipv2`
6. `session target ipv4:destination-address`
7. `incoming called-number string`
8. `codec codec`
9. `end`
10. `dial-peer voice tag voip`

11. Repeat Steps 4, 5, 6, and 7 to configure a second dial peer.
12. `srtplib`
13. `exit`

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<pre>enable</pre> <p><b>Example:</b> Router&gt; enable </p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<pre>configure terminal</pre> <p><b>Example:</b> Router# configure terminal </p>	<p>Enters global configuration mode.</p>
Step 3	<pre>dial-peer voice tag voip</pre> <p><b>Example:</b> Router(config)# dial-peer voice 201 voip </p>	<p>Defines a particular dial peer, to specify the method of voice encapsulation, and enters dial peer voice configuration mode.</p> <ul style="list-style-type: none"> <li>• In the example, the following parameters are set: <ul style="list-style-type: none"> <li>– Dial peer 201 is defined.</li> <li>– VoIP is shown as the method of encapsulation.</li> </ul> </li> </ul>
Step 4	<pre>destination-pattern string</pre> <p><b>Example:</b> Router(config-dial-peer)# destination-pattern 5550111 </p>	<p>Specifies either the prefix or the full E.164 telephone number to be used for a dial peer string.</p> <ul style="list-style-type: none"> <li>• In the example, 5550111 is specified as the pattern for the telephone number.</li> </ul>
Step 5	<pre>session protocol sipv2</pre> <p><b>Example:</b> Router(config-dial-peer)# session protocol sipv2 </p>	<p>Specifies a session protocol for calls between local and remote routers using the packet network.</p> <ul style="list-style-type: none"> <li>• In the example, the <b>sipv2</b> keyword is configured so that the dial peer uses the IETF SIP.</li> </ul>
Step 6	<pre>session target ipv4:destination-address</pre> <p><b>Example:</b> Router(config-dial-peer)# session target ipv4:10.13.25.102 </p>	<p>Designates a network-specific address to receive calls from a VoIP or VoIPv6 dial peer.</p> <ul style="list-style-type: none"> <li>• In the example, the IP address of the dial peer to receive calls is configured as 10.13.25.102.</li> </ul>
Step 7	<pre>incoming called-number string</pre> <p><b>Example:</b> Router(config-dial-peer)# incoming called-number 5550111 </p>	<p>Specifies a digit string that can be matched by an incoming call to associate the call with a dial peer.</p> <ul style="list-style-type: none"> <li>• In the example, 5550111 is specified as the pattern for the E.164 or private dialing plan telephone number.</li> </ul>
Step 8	<pre>codec codec</pre> <p><b>Example:</b> Router(config-dial-peer)# codec g711ulaw </p>	<p>Specifies the voice coder rate of speech for the dial peer.</p> <ul style="list-style-type: none"> <li>• In the example, G.711 mu-law at 64,000 bps, is specified as the voice coder rate for speech.</li> </ul>



	Command or Action	Purpose
Step 9	<code>end</code>  <b>Example:</b> <code>Router(config-dial-peer)# end</code>	Exits dial peer voice configuration mode.
Step 10	<code>dial-peer voice tag voip</code>  <b>Example:</b> <code>Router(config)# dial-peer voice 200 voip</code>	Defines a particular dial peer, to specify the method of voice encapsulation, and enters dial peer voice configuration mode. <ul style="list-style-type: none"> <li>In the example, the following parameters are set: <ul style="list-style-type: none"> <li>Dial peer 200 is defined.</li> <li>VoIP is shown as the method of encapsulation.</li> </ul> </li> </ul>
Step 11	Repeat Steps 4, 5, 6, and 7 to configure a second dial peer.	—
Step 12	<code>srtp</code>  <b>Example:</b> <code>Router(config-dial-peer)# srtp</code>	Specifies that SRTP is used to enable secure calls for the dial peer.
Step 13	<code>codec codec</code>  <b>Example:</b> <code>Router(config-dial-peer)# codec g711ulaw</code>	Specifies the voice coder rate of speech for the dial peer. <ul style="list-style-type: none"> <li>In the example, G.711 mu-law at 64,000 bps, is specified as the voice coder rate for speech.</li> </ul>
Step 14	<code>exit</code>  <b>Example:</b> <code>Router(config-dial-peer)# exit</code>	Exits dial peer voice configuration mode.

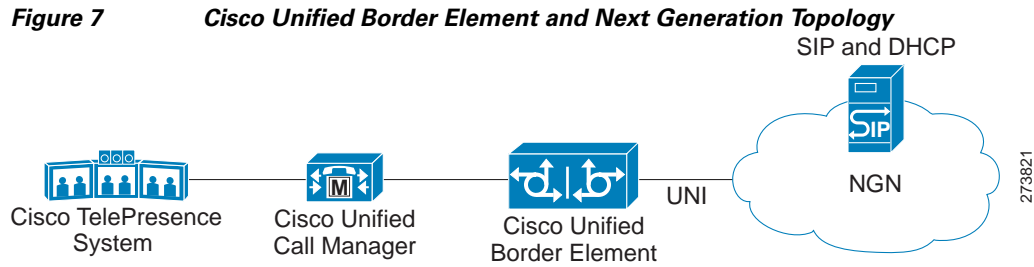
## Troubleshooting Tips

The following commands can help troubleshoot Cisco Unified Border Element support for SRTP-RTP internetworking:

- `show crypto pki certificates`
- `show sccp`
- `show sdsfarm`

## Support for PAID, PPID, Privacy, PCPID, and PAURI Headers on the Cisco Unified Border Element

Figure 7 shows a typical network topology where the Cisco Unified Border Element is configured to route messages between a call manager system (such as the Cisco Unified Call Manager) and a Next Generation Network (NGN).



Devices that connect to an NGN must comply with the User-Network Interface (UNI) specification. The Cisco Unified Call Manager 5.0 does not support the UNI specification. However, the Cisco Unified Border Element supports the NGN UNI specification and can be configured to interconnect the NGN and the Cisco Unified Call Manager 5.0.

The Cisco Unified Border Element supports the following:

- the use of P-Preferred Identity (PPID), P-Asserted Identity (PAID), Privacy, P-Called Party Identity (PCPID), and P-Associated URI (PAURI) headers, collectively known as P-headers, in INVITE messages
- the translation of PAID headers to PPID headers and vice versa
- the translation of From: or RPID headers to PAID or PPID headers and vice versa
- the configuration of the privacy header and the use of the PCPID header to route INVITE messages
- the use of multiple PAURI headers in the response messages (200 OK) it receives to REGISTER messages

## P-Preferred Identity and P-Asserted Identity Headers

NGN servers use the PPID header to identify the preferred number that the caller wants to use. The PPID is part of INVITE messages sent to the NGN. When the NGN receives the PPID, it authorizes the value, uses it as a PAID, and inserts it into the outgoing INVITE message to the Cisco Unified Border Element.

However, some call manager systems, such as Cisco Unified Call Manager 5.0, use the Remote-Party Identity (RPID) value to send calling and called number information. Therefore, the Cisco Unified Border Element must support building the PPID value for an outgoing INVITE message to the NGN, using the RPID value or the From: value received in the incoming INVITE message. In addition, the Cisco Unified Border Element must support building the From: value of the outgoing INVITE message to the call manager system using the PAID received from the NGN.

In non-NGN systems, the Cisco Unified Border Element can be configured to translate between PPID and PAID values, and between From: or RPID values and PAID values, at global and dial-peer levels.

In configurations where all relevant servers support the PPID or PAID headers, the Cisco Unified Border Element can be configured to transparently pass the header.



### Note

If the NGN sets the From: value to anonymous, the PAID is the only value that identifies the caller.

[Table 3](#) describes the types of INVITE message header translations supported by the Cisco Unified Border Element. It also includes information on the configuration commands to use to configure P-header translations.

**Note**

Table 3 shows the P-header translation configuration settings only. In addition to configuring these settings, you must configure other system settings (such as the session protocol).

**Table 3** P-header Configuration Settings

Incoming Header	Outgoing Header	Configuration Notes
From:	PPID	<p>To enable the translation to PPID privacy headers in the outgoing header at a global level, use the <b>asserted-id ppi</b> command in voice service VoIP SIP configuration mode. For example: <code>Router(conf-serv-sip)# asserted-id ppi</code></p> <p>To enable the translation to PPID privacy headers in the outgoing header on a specific dial peer, use the <b>voice-class sip asserted-id ppi</b> command in dial peer voice configuration mode. For example: <code>Router(config-dial-peer)# voice-class sip asserted-id ppi</code></p>
From:	PAID	<p>To enable the translation to PAID privacy headers in the outgoing header at a global level, use the <b>asserted-id pai</b> command in voice service VoIP SIP configuration mode. For example: <code>Router(conf-serv-sip)# asserted-id pai</code></p> <p>To enable the translation to PAID privacy headers in the outgoing header on a specific dial peer, use the <b>voice-class sip asserted-id pai</b> command in dial peer voice configuration mode. For example: <code>Router(config-dial-peer)# voice-class sip asserted-id pai</code></p>
From:	RPID	<p>To enable the translation to RPID headers in the outgoing header, use the <b>remote-party-id</b> command in SIP user-agent configuration mode. For example: <code>Router(config-sip-ua)# remote-party-id</code></p> <p>This is the default system behavior.</p>
PPID	PAID	<p>To enable the translation to PAID privacy headers in the outgoing header at a global level, use the <b>asserted-id pai</b> command in voice service VoIP SIP configuration mode. For example: <code>Router(conf-serv-sip)# asserted-id pai</code></p> <p>To enable the translation to PAID privacy headers in the outgoing header on a specific dial peer, use the <b>voice-class sip asserted-id pai</b> command in dial peer voice configuration mode. For example: <code>Router(config-dial-peer)# voice-class sip asserted-id pai</code></p>
PPID	From:	<p>By default, the translation to RPID headers is enabled and the system translates PPID headers in incoming messages to RPID headers in the outgoing messages. To disable the default behavior and enable the translation from PPID to From: headers, use the <b>no remote-party-id</b> command in SIP user-agent configuration mode. For example: <code>Router(config-sip-ua)# no remote-party-id</code></p>
PPID	RPID	<p>To enable the translation to RPID headers in the outgoing header, use the <b>remote-party-id</b> command in SIP user-agent configuration mode. For example: <code>Router(config-sip-ua)# remote-party-id</code></p> <p>This is the default system behavior.</p>

Table 3 P-header Configuration Settings (continued)

Incoming Header	Outgoing Header	Configuration Notes
PAID	PPID	<p>To enable the translation to PPID privacy headers in the outgoing header at a global level, use the <b>asserted-id ppi</b> command in voice service VoIP SIP configuration mode. For example: <code>Router(conf-serv-sip)# asserted-id ppi</code></p> <p>To enable the translation to PPID privacy headers in the outgoing header on a specific dial peer, use the <b>voice-class sip asserted-id ppi</b> command in dial peer voice configuration mode. For example: <code>Router(config-dial-peer)# voice-class sip asserted-id ppi</code></p>
PAID	From:	<p>By default, the translation to RPID headers is enabled and the system translates PPID headers in incoming messages to RPID headers in the outgoing messages. To disable the default behavior and enable the translation from PPID to From: headers, use the <b>no remote-party-id</b> command in SIP user-agent configuration mode. For example: <code>Router(config-sip-ua)# no remote-party-id</code></p>
PAID	RPID	<p>To enable the translation to RPID headers in the outgoing header, use the <b>remote-party-id</b> command in SIP user-agent configuration mode. For example: <code>Router(config-sip-ua)# remote-party-id</code></p> <p>This is the default system behavior.</p>
RPID	PPID	<p>To enable the translation to PPID privacy headers in the outgoing header at a global level, use the <b>asserted-id ppi</b> command in voice service VoIP SIP configuration mode. For example: <code>Router(conf-serv-sip)# asserted-id ppi</code></p> <p>To enable the translation to PPID privacy headers in the outgoing header on a specific dial peer, use the <b>voice-class sip asserted-id ppi</b> command in dial peer voice configuration mode. For example: <code>Router(config-dial-peer)# voice-class sip asserted-id ppi</code></p>
RPID	PAID	<p>To enable the translation to PAID privacy headers in the outgoing header at a global level, use the <b>asserted-id pai</b> command in voice service VoIP SIP configuration mode. For example: <code>Router(conf-serv-sip)# asserted-id pai</code></p> <p>To enable the translation to PAID privacy headers in the outgoing header on a specific dial peer, use the <b>voice-class sip asserted-id pai</b> command in dial peer voice configuration mode. For example: <code>Router(config-dial-peer)# voice-class sip asserted-id pai</code></p>
RPID	From:	<p>By default, the translation to RPID headers is enabled and the system translates PPID headers in incoming messages to RPID headers in the outgoing messages. To disable the default behavior and enable the translation from PPID to From: headers, use the <b>no remote-party-id</b> command in SIP user-agent configuration mode. For example: <code>Router(config-sip-ua)# no remote-party-id</code></p>

## Privacy

If the user is subscribed to a privacy service, the Cisco Unified Border Element can support privacy using one of the following methods:

- Using prefixes

The NGN dial plan can specify prefixes to enable privacy settings. For example, the dial plan may specify that if the caller dials a prefix of 184, the calling number is not sent to the called party.

The dial plan may also specify that the caller can choose to send the calling number to the called party by dialing a prefix of 186. In this case, the Cisco Unified Border Element transparently passes the prefix as part of the called number in the INVITE message.

The actual prefixes for the network are specified in the dial plan for the NGN, and can vary from one NGN to another.

- Using the Privacy header

If the Privacy header is set to None, the calling number is delivered to the called party. If the Privacy header is set to a Privacy:id value, the calling number is not delivered to the called party.

If the user is not subscribed to a privacy service, the Cisco Unified Border Element can be configured with no Privacy settings.

## P-Called Party Identity

The Cisco Unified Border Element can be configured to use the PCPID header in an incoming INVITE message to route the call, and to use the PCPID value to set the To: value of outgoing INVITE messages.

The PCPID header is part of the INVITE messages sent by the NGN, and is used by Third Generation Partnership Project (3GPP) networks. The Cisco Unified Border Element uses the PCPID from incoming INVITE messages (from the NGN) to route calls to the Cisco Unified Call Manager.



### Note

---

The PCPID header supports the use of E.164 numbers only.

---

## P-Associated URI

The Cisco Unified Border Element supports the use of PAURI headers sent as part of the registration process. After the Cisco Unified Border Element sends REGISTER messages using the configured E.164 number, it receives a 200 OK message with one or more PAURIs. The number in the first PAURI (if present) must match the contract number. The Cisco Unified Border Element supports a maximum of six PAURIs for each registration.



### Note

---

The Cisco Unified Border Element performs the validation process only when a PAURI is present in the 200 OK response.

---

The registration validation process works as follows:

- The Cisco Unified Border Element receives a REGISTER response message that includes PAURI headers that include the contract number and up to five secondary numbers.
- The Cisco Unified Border Element validates the contract number against the E.164 number that it is registering:
  - If the values match, the Cisco Unified Border Element completes the registration process and stores the PAURI value. This allows administration tools to view or retrieve the PAURI if needed.
  - If the values do not match, the Cisco Unified Border Element unregisters and then reregisters the contract number. The Cisco Unified Border Element performs this step until the values match.

## Random Contact Support

The Cisco Unified Border Element can use random-contact information in REGISTER and INVITE messages so that user information is not revealed in the contact header.

To provide random contact support, the Cisco Unified Border Element performs SIP registration based on the random-contact value. The Cisco Unified Border Element then populates outgoing INVITE requests with the random-contact value and validates the association between the called number and the random-contact value. The Cisco Unified Border Element routes calls based on the PCPID, to ensure that the called number remains private.

The default contact header in REGISTER messages is the calling number. The Cisco Unified Border Element can generate a string of 32 random alphanumeric characters to replace the calling number in the REGISTER contact header. A different random character string is generated for each pilot or contract number being registered. All subsequent registration requests will use the same random character string.

The Cisco Unified Border Element uses the random character string in the contact header for INVITE messages that it forwards to the NGN. The NGN sends INVITE messages to the Cisco Unified Border Element with random-contact information in the Request URI in the form sip:random-string. For example: INVITE sip:FefhH3zIHe9i8ImcGjDD1PEc5XfFy51G@10.12.1.46:5060.

The Cisco Unified Border Element cannot use the To: value of the incoming INVITE message to route the call because it might not identify the correct user agent if supplementary services are invoked. Therefore, the Cisco Unified Border Element must use the PCPID to route the call to the Cisco Unified Call Manager. You can configure routing based on the PCPID at global and dial-peer levels.

## Configuring P-Header and Random-Contact Support on the Cisco Unified Border Element

To enable random contact support you must configure the Cisco Unified Border Element to support Session Initiation Protocol (SIP) registration with random-contact information, as described in this section.

To enable the Cisco Unified Border Element to use the PCPID header in an incoming INVITE message to route the call, and to use the PCPID value to set the To: value of outgoing INVITE messages, you must configure P-Header support as described in this section.

This section contains the following tasks:

- [Configuring P-Header Translation on a Cisco Unified Border Element, page 199](#)
- [Configuring P-Header Translation on an Individual Dial Peer, page 200](#)
- [Configuring P-Called-Party-Id Support on a Cisco Unified Border Element, page 201](#)
- [Configuring P-Called-Party-Id Support on an Individual Dial Peer, page 202](#)
- [Configuring Privacy Support on a Cisco Unified Border Element, page 203](#)
- [Configuring Privacy Support on an Individual Dial Peer, page 204](#)
- [Configuring Random-Contact Support on a Cisco Unified Border Element, page 205](#)
- [Configuring Random-Contact Support for an Individual Dial Peer, page 207](#)

## Restrictions

To enable random-contact support, you must configure the Cisco Unified Border Element to support SIP registration with random-contact information. In addition, you must configure random-contact support in VoIP voice-service configuration mode or on the dial peer.

If random-contact support is configured for SIP registration only, the system generates the random-contact information, includes it in the SIP REGISTER message, but does not include it in the SIP INVITE message.

If random-contact support is configured in VoIP voice-service configuration mode or on the dial peer only, no random contact is sent in either the SIP REGISTER or INVITE message.

## Configuring P-Header Translation on a Cisco Unified Border Element

To configure P-Header translations on a Cisco Unified Border Element, perform the steps in this section.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **sip**
5. **asserted-id** *header-type*
6. **exit**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<code>configure terminal</code>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<code>voice service voip</code>  <b>Example:</b> Router(config)# voice service voip	Enters VoIP voice-service configuration mode.
Step 4	<code>sip</code>  <b>Example:</b> Router(conf-voi-serv)# sip	Enters voice service VoIP SIP configuration mode.

	Command or Action	Purpose
Step 5	<code>asserted-id header-type</code>  <b>Example:</b> Router(conf-serv-sip)# asserted-id ppi	Specifies the type of privacy header in the outgoing SIP requests and response messages.
Step 6	<code>exit</code>  <b>Example:</b> Router(conf-serv-sip)# exit	Exits the current mode.

## Configuring P-Header Translation on an Individual Dial Peer

To configure P-Header translation on an individual dial peer, perform the steps in this section.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `dial-peer voice tag voip`
4. `voice-class sip asserted-id header-type`
5. `exit`

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<code>configure terminal</code>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<code>dial-peer voice tag voip</code>  <b>Example:</b> Router(config)# dial-peer voice 2611 voip	Defines the dial peer, specifies the method of voice encapsulation, and enters dial peer voice configuration mode.
Step 4	<code>voice-class sip asserted-id header-type</code>  <b>Example:</b> Router(config-dial-peer)# voice-class sip asserted-id ppi	Specifies the type of privacy header in the outgoing SIP requests and response messages, on this dial peer.
Step 5	<code>exit</code>  <b>Example:</b> Router(config-dial-peer)# exit	Exits the current mode.



## Configuring P-Called-Party-Id Support on a Cisco Unified Border Element

To configure P-Called-Party-Id support on a Cisco Unified Border Element, perform the steps in this section.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **sip**
5. **call-route p-called-party-id**
6. **random-request-uri validate**
7. **exit**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<pre>enable</pre> <p><b>Example:</b> Router&gt; enable</p>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<pre>configure terminal</pre> <p><b>Example:</b> Router# configure terminal</p>	Enters global configuration mode.
Step 3	<pre>voice service voip</pre> <p><b>Example:</b> Router(config)# voice service voip</p>	Enters VoIP voice-service configuration mode.
Step 4	<pre>sip</pre> <p><b>Example:</b> Router(conf-voi-serv)# sip</p>	Enters voice service VoIP SIP configuration mode.
Step 5	<pre>call-route p-called-party-id</pre> <p><b>Example:</b> Router(conf-serv-sip)# call-route p-called-party-id</p>	Enables the routing of calls based on the PCPID header.

	Command or Action	Purpose
Step 6	<code>random-request-uri validate</code>  <b>Example:</b> Router(conf-serv-sip)# random-request-uri validate	Enables the validation of the random string in the Request URI of the INVITE message.
Step 7	<code>exit</code>  <b>Example:</b> Router(conf-serv-sip)# exit	Exits the current mode.

## Configuring P-Called-Party-Id Support on an Individual Dial Peer

To configure P-Called-Party-Id support on an individual dial peer, perform the steps in this section.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `dial-peer voice tag voip`
4. `voice-class sip call-route p-called-party-id`
5. `voice-class sip random-request-uri validate`
6. `exit`

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<code>configure terminal</code>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<code>dial-peer voice tag voip</code>  <b>Example:</b> Router(config)# dial-peer voice 2611 voip	Defines the dial peer, specifies the method of voice encapsulation, and enters dial peer voice configuration mode.
Step 4	<code>voice-class sip call-route p-called-party-id</code>  <b>Example:</b> Router(config-dial-peer)# voice-class sip call-route p-called-party-id	Enables the routing of calls based on the PCPID header on this dial peer.

	Command or Action	Purpose
Step 5	<pre>voice-class sip random-request-uri validate</pre> <p><b>Example:</b> Router(config-dial-peer)# voice-class sip random-request-uri validate </p>	Enables the validation of the random string in the Request URI of the INVITE message on this dial peer.
Step 6	<pre>exit</pre> <p><b>Example:</b> Router(config-dial-peer)# exit </p>	Exits the current mode.

## Configuring Privacy Support on a Cisco Unified Border Element

To configure privacy support on a Cisco Unified Border Element, perform the steps in this section.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **sip**
5. **privacy *privacy-option***
6. **privacy-policy *privacy-policy-option***
7. **exit**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<pre>enable</pre> <p><b>Example:</b> Router&gt; enable </p>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<pre>configure terminal</pre> <p><b>Example:</b> Router# configure terminal </p>	Enters global configuration mode.
Step 3	<pre>voice service voip</pre> <p><b>Example:</b> Router(config)# voice service voip </p>	Enters VoIP voice-service configuration mode.
Step 4	<pre>sip</pre> <p><b>Example:</b> Router(conf-voi-serv)# sip </p>	Enters voice service VoIP SIP configuration mode.

	Command or Action	Purpose
Step 5	<code>privacy <i>privacy-option</i></code>  <b>Example:</b> Router(conf-serv-sip)# <code>privacy id</code>	Enables the privacy settings for the header.
Step 6	<code>privacy-policy <i>privacy-policy-option</i></code>  <b>Example:</b> Router(conf-serv-sip)# <code>privacy-policy passthru</code>	Specifies the privacy policy to use when passing the privacy header from one SIP leg to the next.
Step 7	<code>exit</code>  <b>Example:</b> Router(conf-serv-sip)# <code>exit</code>	Exits the current mode.

## Configuring Privacy Support on an Individual Dial Peer

To configure privacy support on an individual dial peer, perform the steps in this section.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `dial-peer voice tag voip`
4. `voice-class sip privacy privacy-option`
5. `voice-class sip privacy-policy privacy-policy-option`
6. `exit`

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> Router> <code>enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<code>configure terminal</code>  <b>Example:</b> Router# <code>configure terminal</code>	Enters global configuration mode.
Step 3	<code>dial-peer voice <i>tag</i> voip</code>  <b>Example:</b> Router(config)# <code>dial-peer voice 2611 voip</code>	Defines the dial peer, specifies the method of voice encapsulation, and enters dial peer voice configuration mode.

	Command or Action	Purpose
Step 4	<pre>voice-class sip privacy <i>privacy-option</i></pre> <p><b>Example:</b> Router(config-dial-peer)# voice-class sip privacy id</p>	Enables the privacy settings for the header on this dial peer.
Step 5	<pre>voice-class sip privacy-policy <i>privacy-policy-option</i></pre> <p><b>Example:</b> Router(config-dial-peer)# voice-class sip privacy-policy passthru</p>	Specifies the privacy policy to use when passing the privacy header from one SIP leg to the next, on this dial peer.
Step 6	<pre>exit</pre> <p><b>Example:</b> Router(config-dial-peer)# exit</p>	Exits the current mode.

## Configuring Random-Contact Support on a Cisco Unified Border Element

To configure random-contact support on a Cisco Unified Border Element, perform the steps in this section.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **sip-ua**
4. **credentials username *username* password *password* realm *domain-name***
5. **registrar ipv4:*destination-address* random-contact expires *expiry***
6. **exit**
7. **voice service voip**
8. **sip**
9. **random-contact**
10. **exit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<pre>enable</pre> <p><b>Example:</b> Router&gt; enable </p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<pre>configure terminal</pre> <p><b>Example:</b> Router# configure terminal </p>	<p>Enters global configuration mode.</p>
Step 3	<pre>sip-ua</pre> <p><b>Example:</b> Router(config)# sip-ua </p>	<p>Enters SIP user-agent configuration mode.</p>
Step 4	<pre>credentials username username password password realm domain-name</pre> <p><b>Example:</b> Router(config-sip-ua)# credentials username 123456 password cisco realm cisco </p>	<p>Sends a SIP registration message from the Cisco Unified Border Element.</p>
Step 5	<pre>registrar ipv4:destination-address random-contact expires expiry</pre> <p><b>Example:</b> Router(config-sip-ua)# registrar ipv4:10.1.2.2 random-contact expires 200 </p>	<p>Enables the SIP gateways to register E.164 numbers on behalf of analog telephone voice ports (FXS), IP phone virtual voice ports (EFXS), and Skinny Client Control Protocol (SCCP) phones with an external SIP proxy or SIP registrar.</p> <ul style="list-style-type: none"> <li>The <b>random-contact</b> keyword configures the Cisco Unified Border Element to send the random string from the REGISTER message to the registrar.</li> </ul>
Step 6	<pre>exit</pre> <p><b>Example:</b> Router(config-sip-ua)# exit </p>	<p>Exits the current mode.</p>
Step 7	<pre>voice service voip</pre> <p><b>Example:</b> Router(config)# voice service voip </p>	<p>Enters VoIP voice-service configuration mode.</p>
Step 8	<pre>sip</pre> <p><b>Example:</b> Router(conf-voi-serv)# sip </p>	<p>Enters voice service VoIP SIP configuration mode.</p>

	Command or Action	Purpose
Step 9	<code>random-contact</code>  <b>Example:</b> Router(conf-serv-sip)# <code>random-contact</code>	Enables random-contact support on a Cisco Unified Border Element.
Step 10	<code>exit</code>  <b>Example:</b> Router(conf-serv-sip)# <code>exit</code>	Exits the current mode.

## Configuring Random-Contact Support for an Individual Dial Peer

To configure configure random-contact support for an individual dial peer, perform the steps in this section.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `sip-ua`
4. `credentials username username password password realm domain-name`
5. `registrar ipv4:destination-address random-contact expires expiry`
6. `exit`
7. `dial-peer voice tag voip`
8. `voice-class sip random-contact`
9. `exit`

### DETAILED STEPS

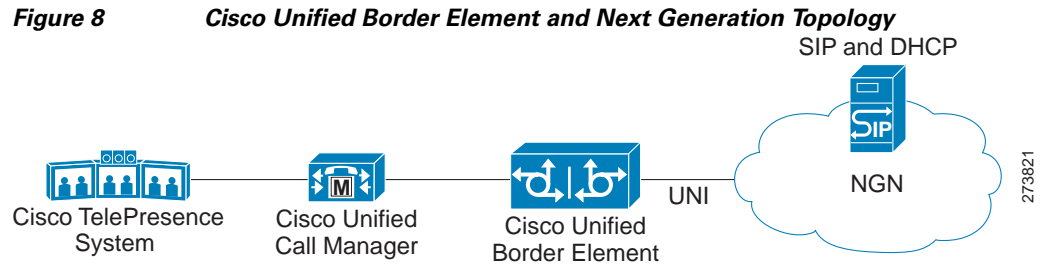
	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> Router> <code>enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<code>configure terminal</code>  <b>Example:</b> Router# <code>configure terminal</code>	Enters global configuration mode.
Step 3	<code>sip-ua</code>  <b>Example:</b> Router(config)# <code>sip-ua</code>	Enters SIP user-agent configuration mode.

	Command or Action	Purpose
Step 4	<b>credentials</b> <i>username username password password realm domain-name</i>  <b>Example:</b> Router(config-sip-ua)# credentials username 123456 password cisco realm cisco	Sends a SIP registration message from the Cisco Unified Border Element.
Step 5	<b>registrar</b> <i>ipv4:destination-address random-contact expires expiry</i>  <b>Example:</b> Router(config-sip-ua)# registrar ipv4:10.1.2.2 random-contact expires 200	Enables the SIP gateways to register E.164 numbers on behalf of FXS, EFXS, and SCCP phones with an external SIP proxy or SIP registrar. <ul style="list-style-type: none"> <li>The <b>random-contact</b> keyword configures the Cisco Unified Border Element to send the random string from the REGISTER message to the registrar.</li> </ul>
Step 6	<b>exit</b>  <b>Example:</b> Router(config-sip-ua)# exit	Exits the current mode.
Step 7	<b>dial-peer</b> <i>voice tag voip</i>  <b>Example:</b> Router(config)# dial-peer voice 2611 voip	Defines the dial peer, specifies the method of voice encapsulation, and enters dial peer voice configuration mode.
Step 8	<b>voice-class</b> <i>sip random-contact</i>  <b>Example:</b> Router(config-dial-peer)# voice-class sip random-contact	Enables random-contact support on this dial peer.
Step 9	<b>exit</b>  <b>Example:</b> Router(config-dial-peer)# exit	Exits the current mode.

## Support for Preloaded Routes in Outgoing INVITE Messages Based on REGISTER Information

Figure 7 shows a typical network topology where the Cisco Unified Border Element is configured to route messages between a call manager system (Cisco Unified Call Manager) and a Next-Generation-Network (NGN).





The Cisco Unified Border Element supports the use of preloaded routes for outgoing INVITE messages. The system routes INVITE messages based on REGISTER message information, such as the path: and Service-Route values.

The Cisco Unified Border Element sends REGISTER messages containing the Supported: path value to the NGN server. In response to the REGISTER message, the NGN server sends a 200 OK REGISTER message to the Cisco Unified Border Element. The 200 OK REGISTER message includes the path: value and the Service-Route value. The Service-Route value can be an IP address or Fully Qualified Domain Name (FQDN).

Depending on the configuration you specify, the Cisco Unified Border Element can send the Service-Route, path: and SIP server values in the Route: header of outgoing INVITE messages. You use the **preloaded-route** command to configure the Route: header in outgoing INVITE messages.

If you configure the Cisco Unified Border Element to include Service-Route information only, then the Route: header in the outgoing INVITE message contains the Service-Route value from the Service-Route header of the 200 OK Register message.

If you configure the Cisco Unified Border Element to include Service-Route and SIP server information, then the Route: header in the outgoing INVITE message contains the Service-Route, path: and SIP server values. The path: and Service-Route values are taken from the Service-Route header of the 200 OK Register message.

If you configure the Cisco Unified Border Element to include Service-Route and SIP server information, but no Service-Route or path: is received in the 200 OK Register message, then the Route: header in the outgoing INVITE message contains the SIP server value only.

If the Cisco Unified Border Element receives a 180 response message that includes the Record-Route header, then it adds the Record-Route value to the Route: header for subsequent requests in the same dialogue.

The INVITE message also contains random-contact information in the Request-Line URI. Therefore, the Cisco Unified Border Element can use the P-Called Party Identify value to route the call to Cisco Unified Call Manager.

In the following examples, the Cisco Unified Border Element receives a 180 Ringing message from the NGN. The message includes the Record-Route value. The Cisco Unified Border Element uses the Record-Route value in the Route: header of a Provisional Response Acknowledgment (PRACK) message.

The following is an example of a 180 Ringing message, including a Record-Route value, that the NGN sends to the Cisco Unified Border Element:

```
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 10.144.54.136:5060;branch=z9hG4bK766e3920d0224243ab6
From: 0311111111 <sip:0311111111@ngn.east.ntt.co.jp>;tag=1255396194
To: <tel:0322222222;phone-context=ngn.east.ntt.co.jp>;tag=1182396213
Call-ID: ff968380-66f179ec-a0284020-87745983@10.144.54.136
Allow: INVITE, BYE, CANCEL, ACK, PRACK
CSeq: 1 INVITE
```

```
Require: 100rel
RSeq: 1130
Contact: <sip:fld4f281Kc@10.144.54.134:5060>
Content-Length: 0
Record-Route: <sip:10.144.54.134:5060;maddr=10.144.54.134;lr>
```

The following is an example of a PRACK message, with the Record-Route value in the Route: header, that the Cisco Unified Border Element sends to the NGN:

```
PRACK sip:fld4f281Kc@10.144.54.134:5060 SIP/2.0
Via: SIP/2.0/UDP 10.144.54.136:5060;branch=z9hG4bK766e3920d0224243ab8
From: 0311111111 <sip:0311111111@ngn.east.ntt.co.jp>;tag=1255396194
To: <tel:0322222222;phone-context=ngn.east.ntt.co.jp>;tag=1182396213
Call-ID: ff968380-66f179ec-a0284020-87745983@10.144.54.136
CSeq: 2 PRACK
RAck: 1130 1 INVITE
Max-Forwards: 70
Content-Length: 0
Route: <sip:10.144.54.134:5060;maddr=10.144.54.134;lr>
```

## Configuring Preloaded Route Support on the Cisco Unified Border Element

To configure preloaded route support on the Cisco Unified Border Element by enabling support for the Service-Route and path: values in the Route header of outgoing INVITE message, perform the steps in this section.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **sip**
5. **support-path-header**
6. **preloaded-route sip-server service-route**
7. **exit**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<code>configure terminal</code>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<code>voice service voip</code>  <b>Example:</b> Router(config)# voice service voip	Enters VoIP voice-service configuration mode.

	Command or Action	Purpose
Step 4	<code>sip</code>  <b>Example:</b> Router(conf-voi-serv)# <code>sip</code>	Enters SIP configuration mode.
Step 5	<code>support-path-header</code>  <b>Example:</b> Router(conf-serv-sip)# <code>support-path-header</code>	Configures the system to include the path: value in the Route: header of outgoing INVITE messages.
Step 6	<code>preloaded-route sip-server service-route</code>  <b>Example:</b> Router(conf-serv-sip)# <code>preloaded-route sip-server service-route</code>	Configures the system to include the SIP server and Service-Route information in the Route header of outgoing INVITE message.
Step 7	<code>exit</code>  <b>Example:</b> Router(conf-serv-sip)# <code>exit</code>	Exits the current mode.

## Configuring Preloaded Route Support on the Cisco Unified Border Element on an Individual Dial Peer

To configure preloaded route support for an individual dial peer on the Cisco Unified Border Element, by enabling support for the Service-Route and path: values in the Route header of outgoing INVITE message, perform the steps in this section.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `voice service voip`
4. `sip`
5. `support-path-header`
6. `exit`
7. `dial-peer voice tag voip`
8. `voice-class sip preloaded-route sip-server service-route`
9. `exit`

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><code>enable</code></p> <p><b>Example:</b> Router&gt; enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<p><code>configure terminal</code></p> <p><b>Example:</b> Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p><code>voice service voip</code></p> <p><b>Example:</b> Router(config)# voice service voip</p>	<p>Enters VoIP voice-service configuration mode.</p>
Step 4	<p><code>sip</code></p> <p><b>Example:</b> Router(conf-voi-serv)# sip</p>	<p>Enters SIP configuration mode.</p>
Step 5	<p><code>support-path-header</code></p> <p><b>Example:</b> Router(conf-serv-sip)# support-path-header</p>	<p>Configures the system to include the path: value in the Route: header of outgoing INVITE messages.</p>
Step 6	<p><code>exit</code></p> <p><b>Example:</b> Router(conf-serv-sip)# exit</p>	<p>Exits the current mode.</p>
Step 7	<p><code>dial-peer voice tag voip</code></p> <p><b>Example:</b> Router(config)# dial-peer voice 2611 voip</p>	<p>Defines the dial peer, specifies the method of voice encapsulation, and enters dial peer voice configuration mode.</p>
Step 8	<p><code>voice-class sip preloaded-route sip-server service-route</code></p> <p><b>Example:</b> Router(config-dial-peer)# voice-class sip preloaded-route sip-server service-route</p>	<p>Enables preloaded route support for SIP calls for this dial-peer, and enables the system to add SIP server and Service-Route information to the Route header in outgoing INVITE messages.</p>
Step 9	<p><code>exit</code></p> <p><b>Example:</b> Router(config-dial-peer)# exit</p>	<p>Exits the current mode.</p>

## Selectively Using sip: URI or tel: URL Formats on Individual SIP Headers

The Cisco Unified Border Element supports the construction of request URIs in tel: format. The system supports this format for both the To: header and the Request-Line. The system also supports appending the phone-context parameter to the tel: URL.

### Phone-context

If the system is configured to use the tel: URL format in the Request-Line or the To: header, then the phone-context is appended to the tel: URL.

The system populates the phone-context parameter with the session target hostname and domain. The system identifies the session target hostname and domain in one of the following ways:

- The session target hostname and domain is manually configured using the **session target** command at the dial-peer level.
- The session target DHCP is configured and the system dynamically retrieves the values from the DHCP server.

The system must populate the phone-context parameter with a domain name. Therefore, if the configured session target is an IP address, the system does not append a phone-context parameter to the tel: URL.

### Request-Line URIs

The Cisco Unified Call Manager uses the sip: format in the Request-Line URIs when it sends INVITE messages to the Cisco Unified Border Element server. However, NGN servers require the tel: format in Request-Line URIs. Therefore, the Cisco Unified Border Element must use the tel: format in the Request-Line URI of INVITE messages sent to the NGN. The tel: format must include the phone-context value.

The NGN server uses the sip: format in the Request-Line URIs of the INVITE messages that it sends to the Cisco Unified Border Element. The Cisco Unified Call Manager also supports the use of the sip: format.

### To: Header

The Cisco Unified Call Manager uses sip: format in the To: header, when it sends INVITE messages to the Cisco Unified Border Element. However, NGN servers require the tel: format in the To: headers. Therefore, the Cisco Unified Border Element must use the tel: format in the To: header of INVITE messages sent to the NGN. The tel: format must include the phone-context value.

The NGN server requires the tel: format in the To: header in the INVITE messages that it sends to the Cisco Unified Border Element. However, the Cisco Unified Call Manager supports the use of the sip: format. Therefore, the Cisco Unified Border Element must use the sip: format in the To: header of INVITE messages sent to the Cisco Unified Call Manager.

## Configuring tel: URL Formats and Phone-Context Parameter

The tasks in this section describe how to send URIs in the Request-Line and the To: header as telephone (TEL) URIs and how to include the phone-context parameter in the headers, at both a system level and on an individual dial peer.

This section contains the following tasks:

- [Configuring tel: URI Formats and Phone-Context Parameter on Individual SIP Headers, page 214](#)
- [Configuring tel: URI Formats and Phone-Context Parameter on Individual SIP Headers on an Individual Dial Peer, page 215](#)
- [Configuring tel: URI Formats on the To: Header, page 216](#)
- [Configuring tel: URI Formats on the To: Header on an Individual Dial Peer, page 217](#)

## Configuring tel: URI Formats and Phone-Context Parameter on Individual SIP Headers

To enable the URIs in the Request-Line and the To: header to be sent as telephone (TEL) URIs and to include the phone-context parameter in the headers, perform the steps in this section.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **sip**
5. **url tel phone-context**
6. **tel-config to-hdr phone-context**
7. **exit**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<code>configure terminal</code>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<code>voice service voip</code>  <b>Example:</b> Router(config)# voice service voip	Enters VoIP voice-service configuration mode.
Step 4	<code>sip</code>  <b>Example:</b> Router(conf-voi-serv)# sip	Enters SIP configuration mode.
Step 5	<code>url tel phone-context</code>  <b>Example:</b> Router(conf-serv-sip)# url tel phone-context	Configures the Request-Line URI to tel: format.

	Command or Action	Purpose
Step 6	<pre>tel-config to-hdr phone-context</pre> <p><b>Example:</b> Router(conf-serv-sip)# tel-config to-hdr phone-context </p>	Configures the To: header Request-URI to tel: format.
Step 7	<pre>exit</pre> <p><b>Example:</b> Router(conf-serv-sip)# exit </p>	Exits the current mode.

## Configuring tel: URI Formats and Phone-Context Parameter on Individual SIP Headers on an Individual Dial Peer

To enable the URIs in the Request-Line and the To: header to be sent as telephone (TEL) URIs on an individual dial peer and to include the phone-context parameter in the headers, perform the steps in this section.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice *tag* voip**
4. **voice-class sip url tel phone-context**
5. **voice-class sip tel-config to-hdr phone-context**
6. **exit**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<pre>enable</pre> <p><b>Example:</b> Router&gt; enable </p>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<pre>configure terminal</pre> <p><b>Example:</b> Router# configure terminal </p>	Enters global configuration mode.
Step 3	<pre>dial-peer voice <i>tag</i> voip</pre> <p><b>Example:</b> Router(config)# dial-peer voice 2611 voip </p>	Defines the dial peer, specifies the method of voice encapsulation, and enters dial peer voice configuration mode.

	Command or Action	Purpose
Step 4	<pre>voice-class sip url tel phone-context</pre> <p><b>Example:</b> Router(config-dial-peer)# voice-class sip url tel phone-context</p>	Configures the Request-Line URI to tel: format and appends the phone-context parameter to the header, on the initial outgoing INVITE associated with this dial peer.
Step 5	<pre>voice-class sip tel-config to-hdr phone-context</pre> <p><b>Example:</b> Router(config-dial-peer)# voice-class sip tel-config to-hdr phone-context</p>	Configures the To: header Request-URI to tel: format and appends the phone-context parameter to the header, on the initial outgoing INVITE associated with this dial peer.
Step 6	<pre>exit</pre> <p><b>Example:</b> Router(config-dial-peer)# exit</p>	Exits the current mode.

## Configuring tel: URI Formats on the To: Header

To enable the URIs in the To: header to be sent as telephone (TEL) URIs, without including the phone-context parameter in the header, perform the steps in this section.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **sip**
5. **tel-config to-hdr**
6. **exit**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<pre>enable</pre> <p><b>Example:</b> Router&gt; enable</p>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<pre>configure terminal</pre> <p><b>Example:</b> Router# configure terminal</p>	Enters global configuration mode.
Step 3	<pre>voice service voip</pre> <p><b>Example:</b> Router(config)# voice service voip</p>	Enters VoIP voice-service configuration mode.



	Command or Action	Purpose
Step 4	<code>sip</code>  <b>Example:</b> Router(conf-voi-serv)# <code>sip</code>	Enters SIP configuration mode.
Step 5	<code>tel-config to-hdr</code>  <b>Example:</b> Router(conf-serv-sip)# <code>tel-config to-hdr</code>	Configures the To: header Request-URI to tel: format.
Step 6	<code>exit</code>  <b>Example:</b> Router(conf-serv-sip)# <code>exit</code>	Exits the current mode.

## Configuring tel: URI Formats on the To: Header on an Individual Dial Peer

To enable the URIs in the To: header to be sent as telephone (TEL) URIs, without including the phone-context parameter in the header, on an individual dial peer, perform the steps in this section.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `dial-peer voice tag voip`
4. `voice-class sip tel-config to-hdr`
5. `exit`

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> Router> <code>enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<code>configure terminal</code>  <b>Example:</b> Router# <code>configure terminal</code>	Enters global configuration mode.
Step 3	<code>dial-peer voice tag voip</code>  <b>Example:</b> Router(config)# <code>dial-peer voice 2611 voip</code>	Defines the dial peer, specifies the method of voice encapsulation, and enters dial peer voice configuration mode.

	Command or Action	Purpose
Step 4	<pre>voice-class sip tel-config to-hdr</pre> <p><b>Example:</b>  Router(config-dial-peer)# voice-class sip  tel-config to-hdr </p>	Configures the To: header Request-URI to tel: format on the initial outgoing INVITE associated with this dial peer.
Step 5	<pre>exit</pre> <p><b>Example:</b>  Router(config-dial-peer)# exit </p>	Exits the current mode.

## Configuring Selective Filtering of Outgoing Provisional Response on the Cisco Unified Border Element

This feature adds support on Cisco UBE for selective filtering of outgoing provisional responses, including 180 - Alerting, and 183-Session In Progress responses. Selective filtering can be further based on the availability of media information in the received provisional response.

Next Generation Network (NGN) restricts the UNI from sending 183 response with SDP towards the NGN network. Cisco Unified CM always sends 183 response with SDP responses. It is necessary for the Cisco UBE to block these responses to allow Cisco Unified CM to interwork within the Next Generation network.

Blocking 180 and 183 responses with or without SDP requirement is to block 183 with SDP only.

To enable Selective Filtering of Outgoing Provisional Response on the Cisco UBE perform the steps in this section. This section contains the following subsections:

- [Configuring Cisco UBE for Unsupported Content Pass-through at the Global Level, page 144](#)
- [Configuring Cisco UBE for Unsupported Content Pass-through at the Dial Peer Level, page 145](#)

## Configuring Selective Filtering of Outgoing Provisional Response on the Cisco UBE at the Global Level

To configure Selective Filtering of Outgoing Provisional Response on the Cisco UBE at the global level, perform the steps in this section:

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **sip**
5. **block 183 sdp absent**
6. **exit**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> <code>Router&gt; enable</code>	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	<code>configure terminal</code>  <b>Example:</b> <code>Router# configure terminal</code>	Enters global configuration mode.
Step 3	<code>voice service voip</code>  <b>Example:</b> <code>Router(config)# voice service voip</code>	Enters VoIP voice-service configuration mode.
Step 4	<code>sip</code>  <b>Example:</b> <code>Router(config-voi-srv)# sip</code>	Enters SIP configuration mode.
Step 5	<code>block 183 sdp absent</code>  <b>Example:</b> <code>Router(conf-serv-sip)# block 183 sdp absent}</code>	Filters outgoing provisional responses, including 180 - Alerting, and 183-Session In Progress responses.
Step 6	<code>exit</code>  <b>Example:</b> <code>Router(conf-voi-serv)# exit</code>	Exits the current mode.

## Configuring Selective Filtering of Outgoing Provisional Response on the Cisco UBE at the Dial Peer Level

To configure Selective Filtering of Outgoing Provisional Response on the Cisco UBE at the dial-peer level, configure the outgoing dial-peer as follows the steps in this section:

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice *number* voip**
4. **voice-class sip block 183 sdp present**
5. **exit**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> <code>Router&gt; enable</code>	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	<code>configure terminal</code>  <b>Example:</b> <code>Router# configure terminal</code>	Enters global configuration mode.
Step 3	<code>dial-peer voice <i>number</i> voip</code>  <b>Example:</b> <code>Router(config)# dial-peer voice 22 voip</code>	Enters dial-peer configuration mode for the specified VoIP dial peer.
Step 4	<code>voice-class sip block 183 sdp present</code>  <b>Example:</b> <code>Router (conf-dial-peer)# voice-class sip block 183 sdp present</code>	Filters outgoing provisional responses, including 180 - Alerting, and 183-Session In Progress responses.
Step 5	<code>exit</code>  <b>Example:</b> <code>Router(conf-voi-serv)# exit</code>	Exits the current mode.

# Verifying and Troubleshooting SIP-to-SIP Connections on a Cisco Unified Border Element

To troubleshoot or verify connections in an Cisco UBE, perform the following task:

- [Troubleshooting Tips, page 221](#)
- [Verifying SIP-to-SIP Connections in an Cisco Unified Border Element, page 221](#)

## Troubleshooting Tips



### Caution

Under moderate traffic loads, these debug commands produce a high volume of output.

- Use the **debug voip ipipgw** command to debug the Cisco Unified Border Element feature.
- Use any of the following additional commands on the gateway as appropriate to troubleshoot SIP-to-SIP call scenarios:
  - **debug ccsip all**
  - **debug voip ccapi inout**



### Note

For examples of **show** and **debug** command output and details on interpreting the output, see the following resources:

- [Cisco IOS Debug Command Reference, Release 12.4T](#)
- [Cisco IOS Voice Troubleshooting and Monitoring Guide](#)
- [Troubleshooting and Debugging VoIP Call Basics](#)
- [Voice Gateway Error Decoder for Cisco IOS](#)
- [VoIP Debug Commands](#)

## Verifying SIP-to-SIP Connections in an Cisco Unified Border Element

To verify SIP-to-SIP feature configuration and operation, perform the following steps (listed alphabetically) as appropriate.

### SUMMARY STEPS

1. **show call active video**
2. **show call active voice**
3. **show call history fax**
4. **show call history video**
5. **show call history voice**
6. **show crm**

7. **show dial-peer voice**
8. **show running-config**
9. **show voip rtp connections**

## DETAILED STEPS

- 
- |                |  |
|----------------|--|
| <b>Step 1</b>  | <b>show call active video</b>  |
|                | Use this command to display the active video H.323 call legs.  |
| <b>Step 2</b>  | <b>show call active voice</b>  |
|                | Use this command to display call information for voice calls that are in progress.                           |
| <b>Step 3</b>  | <b>show call active fax</b>  |
|                | Use this command to display the fax transmissions that are in progress.                                      |
| <b>Step 4</b>  | <b>show call history video</b>   |
|                | Use this command to display the history of video H.323 call legs.  |
| <b>Step 5</b>  | <b>show call history voice</b>   |
|                | Use this command to display the history of voice call legs.  |
| <b>Step 6</b>  | <b>show call history fax</b>   |
|                | Use this command to display the call history table for fax transmissions that are in progress.               |
| <b>Step 7</b>  | <b>show crm</b>  |
|                | Use this command to display the carrier ID list or IP circuit utilization.                                   |
| <b>Step 8</b>  | <b>show dial-peer voice</b>  |
|                | Use this command to display information about voice dial peers.  |
| <b>Step 9</b>  | <b>show running-config</b>   |
|                | Use this command to verify which H.323-to-H.323, H.323-to-SIP, or SIP-to-SIP connection types are supported. |
| <b>Step 10</b> | <b>show voip rtp connections</b>   |
|                | Use this command to display active Real-Time Transport Protocol (RTP) connections.                           |
- 

# Configuration Examples for SIP-to-SIP Connections in a Cisco Unified Border Element

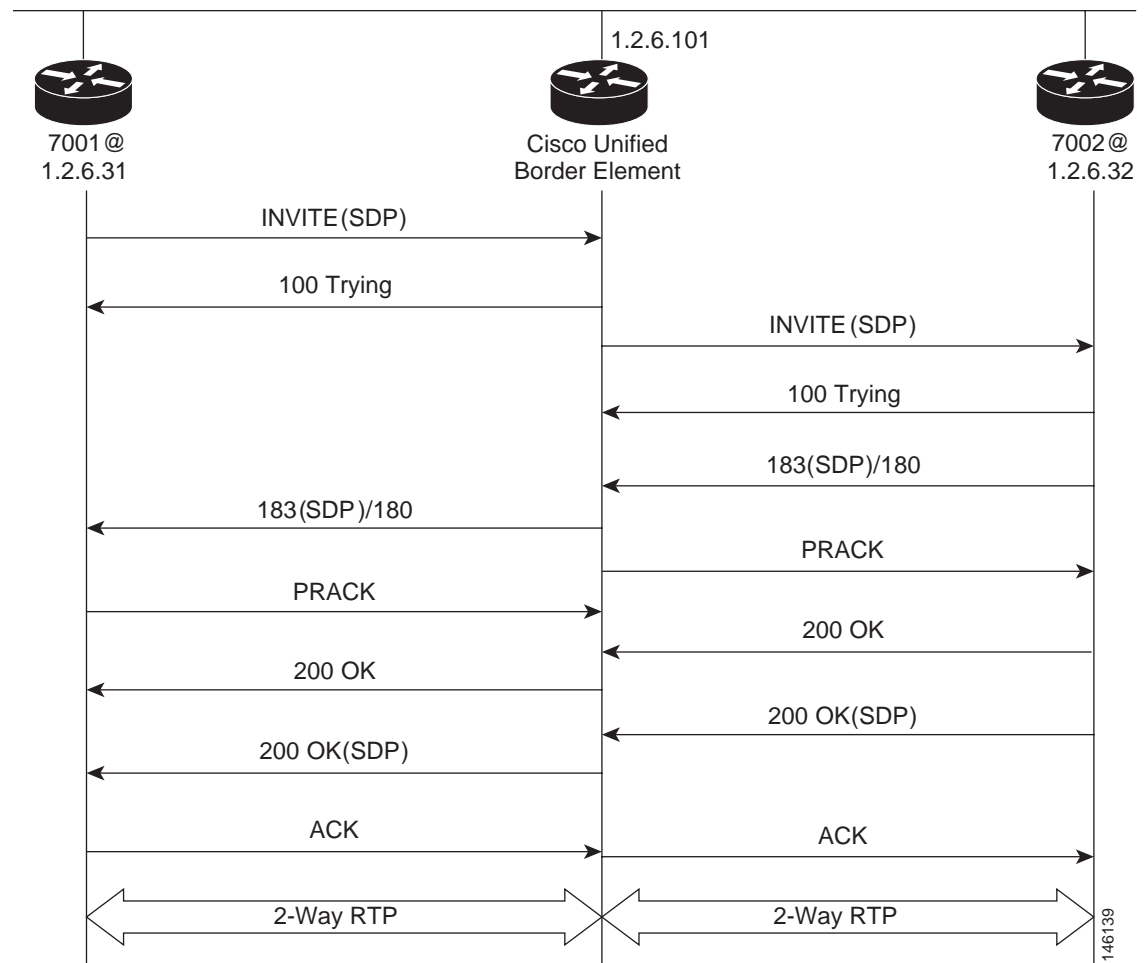
This section contains the following examples:

- [Basic SIP-to-SIP Call Flow: Example, page 223](#)
- [SRTP-RTP Internetworking: Example, page 225](#)

## Basic SIP-to-SIP Call Flow: Example

The following scenario illustrates a basic SIP-to-SIP call flow, using the Cisco Unified Border Element. [Figure 9](#) shows a simple topology example of the SIP-to-SIP gateway topology.

**Figure 9** Cisco Unified Border Element Feature Sample Topology



### Call Flow

- The Cisco UBE receives INVITE with Session Description Protocol (SDP) from the OGW. The SDP contains information about the capabilities the endpoint supports for this call like the Audio Codec's, DTMF etc.
- The Codec and DTMF type received from OGW is matched with the incoming configured or default dial-peer.
- The SGW responds to the INVITE message from the OGW by sending a 100 Trying message to OGW.

- The Matched Capabilities are sent to the application which forwards the Matched Capabilities to the outbound SPI.
- The application receives the Matched Capabilities.
- The Codec Type and DTMF type is selected and SDP is formed based on the outgoing dial-peer configured capabilities, and the capabilities received from the application.
- The Cisco UBE sends an Invite with SDP to the TGW.
- The TGW responds to the Cisco UBE with a 100 Trying message.
- The TGW sends 183 (SDP) if the Phone type on TGW is POTS or 180 if the Phone type on TGW is SIP /SCCP Phone to the Cisco UBE.
- Cisco UBE sends a PRACK Message to the TGW.
- OGW receives 183(SDP)/180 from the Cisco UBE.
- TGW sends 200 Ok to the Cisco UBE.
- Cisco UBE receives a PRACK message from the OGW.
- OGW receives 200 Ok from the Cisco UBE.
- The TGW sends 200 Ok with SDP to the Cisco UBE.
- Cisco UBE sends 200 Ok with SDP to the OGW.
- OGW sends ACK to the Cisco UBE.
- Cisco UBE sends ACK towards TGW only after it receives ACK from the OGW.
- Two-phase exchange provides negotiation capabilities based on simple offer/answer model of SDP exchange
- The Contact header field should always carry the address of Cisco UBE and in none of the messages the IP address on one service provider should be sent to other.

INVITE message received from OGW has Contact: <sip:70005@1.2.6.31:5060>

INVITE message sent from Cisco UBE has Contact: <sip:70005@1.2.6.101:5060>

The same applies to the Contact address when sending response messages towards OGW.

Table 4 shows support for Early Media and their supported Codec and packetization values.

**Table 4** Early Media Codec packetization values

Incoming Leg	Outgoing Leg
711 A/U	711 A/U
723 r53	723 r53
723 r63	723 r63
723 ar53	723 ar53
723 ar63	723 ar63
726 r16	726 r16
726 r24	726 r24
726 ar32	726 ar32
728	728
729r8/729/729ar8	729r8/729/729ar8
729br8/729abr8	729br8/729abr8
gsmfr/gsmefr	gsmfr/gsmefr



**Transparent Codec**

Most video endpoints have proprietary codecs for both audio and video. This makes transparent codecs are most important when handling video calls. If Codec T is configured under the dial-peer all the audio capabilities are transparently passed from one leg to another. Codecs that are not supported by the platform are also passed from incoming leg to outgoing leg.

**Table 5** *Transport Codec*

Incoming Leg	Outgoing Leg	Support
H.323	H.323	Yes

**Note**

If both g79r8 and g729br8 is configured using voice class Codec then g729br8 is only codec sent in INVITE.

INVITE message contains

```
m=audio 19078 RTP/AVP 18 101 19
```

```
c=IN IP4 1.5.5.2
```

```
a=rtpmap:18 G729/8000
```

```
a=fmtp:18 annexb=yes
```

- if TGW sends in session progress G729r8 then G.729r8 is the negotiated codec.
- if TGW sends in session progress G729br8 then G.729br8 is the negotiated codec.

**Packetization**

The packetization values with different codecs are sent to Cisco UBE with attribute “ptime”. The Cisco UBE should ensure that the packetization value received from OGW is sent to TGW.

For example: ptime = 10 is sent when g711ulaw is configured 80 bytes.

## SRTP-RTP Internetworking: Example

The following example shows how to configure Cisco Unified Border Element support for SRTP-RTP internetworking. In this example, the incoming call leg is RTP and the outgoing call leg is SRTP.

```
enable
configure terminal
ip http server
crypto pki server 3845-cube
database level complete
grant auto
no shutdown
%PKI-6-CS_GRANT_AUTO: All enrollment requests will be automatically granted.
% Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key or type Return to exit
Password:
Re-enter password:
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
% SSH-5-ENABLED: SSH 1.99 has been enabled
% Exporting Certificate Server signing certificate and keys...
% Certificate Server enabled.
%PKI-6-CS_ENABLED: Certificate server now enabled.
```

```

!
crypto pki trustpoint secdsp
  enrollment url http://10.13.2.52:80
  serial-number
  revocation-check crl
  rsakeypair 3845-cube
  exit
!
crypto pki authenticate secdsp
Certificate has the following attributes:
  Fingerprint MD5: CCC82E9E 4382CCFE ADA0EB8C 524E2FC1
  Fingerprint SHA1: 34B9C4BF 4841AB31 7B0810AD 80084475 3965F140
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
crypto pki enroll secdsp
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this password to the CA
Administrator in order to revoke your certificate. For security reasons your password will
not be saved in the configuration. Please make a note of it.
Password:
Re-enter password:
% The subject name in the certificate will include: 3845-CUBE
% The serial number in the certificate will be: FHK1212F4MU
% Include an IP address in the subject name? [no]:
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate secdsp verbose' command will show the fingerprint.
CRYPTO_PKI: Certificate Request Fingerprint MD5: 56CE5FC3 B8411CF3 93A343DA 785C2360
CRYPTO_PKI: Certificate Request Fingerprint SHA1: EE029629 55F5CA10 21E50F08 F56440A2
DDC7469D
%PKI-6-CERTRET: Certificate received from Certificate Authority
!
voice-card 0
  dspfarm
  dsp services dspfarm
voice-card 1
  dspfarm
  dsp services dspfarm
  exit
!
sccp local GigabitEthernet 0/0
sccp ccm 10.13.2.52 identifier 1 version 5.0.1
sccp
SCCP operational state bring up is successful.sccp ccm group 1
  associate ccm 1 priority 1
  associate profile 1 register sxcoder
  dspfarm profile 1 transcode universal security
    trustpoint secdsp
    codec g711ulaw
    codec g711alaw
    codec g729ar8
    codec g729abr8
    codec g729r8
    codec ilbc
    codec g729br8
    maximum sessions 84
    associate application sccp
    no shutdown
  exit
!
telephony-service
%LINEPROTO-5-UPDOWN: Line protocol on Interface EDSP0, changed state to upsdspfarm units 1
  sdspfarm transcode sessions 84
  sdspfarm tag 1 sxcoder

```

```
em logout 0:0 0:0 0:0
max-ephones 4
max-dn 4
ip source-address 10.13.2.52
Updating CNF files
CNF-FILES: Clock is not set or synchronized, retaining old versionStamps
CNF files updating complete
  secure-signaling trustpoint secdsp
  tftp-server-credentials trustpoint scme
CNF-FILES: Clock is not set or synchronized, retaining old versionStamps
CNF files update complete (post init)
  create cnf-files
CNF-FILES: Clock is not set or synchronized, retaining old versionStamps
  no sccp
!
sccp
SCCP operational state bring up is successful.
end
%SDSPFARM-6-REGISTER: mtp-1:sxcoder IP:10.13.2.52 Socket:1 DeviceType:MTP has registered.
%SYS-5-CONFIG_I: Configured from console by console
dial-peer voice 201 voip
  destination-pattern 5550111
  session protocol sipv2
  session target ipv4:10.13.25.102
  incoming called-number 5550112
  codec g711ulaw
!
dial-peer voice 200 voip
  destination-pattern 5550112
  session protocol sipv2
  session target ipv4:10.13.2.51
  incoming called-number 5550111
  srtp
  codec g711ulaw
```


## Where to Go Next

- [H.323-to-H.323 Connections on a Cisco Unified Border Element](#)
- [H.323-to-SIP Connections on a Cisco Unified Border Element](#)
- [Cisco Unified Border Element for H.323 Cisco Unified Communications Manager to H.323 Service Provider Connectivity](#)
- [Configuring Cisco Unified Border Element Videoconferencing](#)

# Additional References

The following sections provide references related to SIP-to-SIP Cisco Unified Border Element Connections

## Related Documents

Related Topic	Document Title
Cisco IOS Release 12.4	<ul style="list-style-type: none"> <li>• <a href="#">Cisco IOS Release 12.4 Configuration Guides</a></li> <li>• <a href="#">Cisco IOS Release 12.4T Configuration Guides</a></li> <li>• <a href="#">Cisco IOS Release 12.4 Command References</a></li> <li>• <a href="#">Cisco IOS Voice Configuration Library</a> <a href="http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/cisco_ios_voice_configuration_library_glossary/vcl.htm">http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/cisco_ios_voice_configuration_library_glossary/vcl.htm</a></li> </ul>  <p><b>Note</b> This website contains the library preface and glossary.</p>
Cisco IOS Release 12.3	<ul style="list-style-type: none"> <li>• <a href="#">Cisco IOS Release 12.3 documentation</a></li> <li>• <a href="#">Cisco IOS voice commands</a></li> <li>• <a href="#">Cisco IOS Voice Troubleshooting and Monitoring Guide</a></li> <li>• <a href="#">Tel IVR Version 2.0 Programming Guide</a></li> </ul>
Cisco IOS Release 12.2	<ul style="list-style-type: none"> <li>• <i>Cisco IOS Voice, Video, and Fax Configuration Guide</i>, Release 12.2 at <a href="http://www.cisco.com/en/US/docs/ios/12_2/voice/configuration/guide/fvfax_c.html">http://www.cisco.com/en/US/docs/ios/12_2/voice/configuration/guide/fvfax_c.html</a></li> </ul>
DSP documentation	<p>High-Density Packet Voice Feature Card for Cisco AS5350XM and AS5400XM Universal Gateways</p> <p><a href="http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124imit/124x/124xc4/vfc_dsp.htm">http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124imit/124x/124xc4/vfc_dsp.htm</a></p>
GKTMP (GK API) Documents	<ul style="list-style-type: none"> <li>• <i>GKTMP Command Reference</i>: <a href="http://www.cisco.com/en/US/docs/ios/12_2/gktmp/gktmpv4_2/gk_cli.htm">http://www.cisco.com/en/US/docs/ios/12_2/gktmp/gktmpv4_2/gk_cli.htm</a></li> <li>• <i>GKTMP Messages</i>: <a href="http://www.cisco.com/en/US/docs/ios/12_2/gktmp/gktmpv4_2/gk_tmp.html">http://www.cisco.com/en/US/docs/ios/12_2/gktmp/gktmpv4_2/gk_tmp.html</a></li> </ul>
internet Low Bitrate Codec (iLBC) Documents	<ul style="list-style-type: none"> <li>• Codecs section of the Dial Peer Configuration on Voice Gateway Routers Guide <a href="http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgr/vfax_c/int_c/dpeer_c/dp_ovrvw.htm#1035124">http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgr/vfax_c/int_c/dpeer_c/dp_ovrvw.htm#1035124</a></li> <li>• Dial Peer Features and Configuration section of the Dial Peer Configuration on Voice Gateway Routers Guide <a href="http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgr/vfax_c/int_c/dpeer_c/dp_config.htm">http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgr/vfax_c/int_c/dpeer_c/dp_config.htm</a></li> </ul>

Related Topic	Document Title
Cisco Unified Border Element Configuration Examples	<ul style="list-style-type: none"> <li>• Local-to-remote network using the IPIPGW <a href="http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a00801b0803.shtml">http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a00801b0803.shtml</a></li> <li>• Remote-to-local network using the IPIPGW: <a href="http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a0080203edc.shtml">http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a0080203edc.shtml</a></li> <li>• Remote-to-remote network using the IPIPGW: <a href="http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a0080203edd.shtml">http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a0080203edd.shtml</a></li> <li>• Remote-to-remote network using two IPIPGWs: <a href="http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a0080203edb.shtml">http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a0080203edb.shtml</a></li> <li>• <i>Cisco Unified Border Element SIP TLS Configuration Example</i></li> <li>• <i>Cisco Unified Border Element Transcoding Configuration Example</i></li> </ul>
Related Application Guides	<ul style="list-style-type: none"> <li>• <a href="#">Cisco Unified Communications Manager and Cisco IOS Interoperability Guide</a></li> <li>• <a href="#">Cisco IOS Fax, Modem, and Text Support over IP Configuration Guide</a></li> <li>• “Configuring T.38 Fax Relay” chapter</li> <li>• <a href="#">Cisco IOS SIP Configuration Guide</a></li> <li>• Cisco Unified Communications Manager (CallManager) Programming Guides at: <a href="http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_programming_reference_guides_list.html">http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_programming_reference_guides_list.html</a></li> <li>• <i>Quality of Service for Voice over IP</i> at <a href="http://www.cisco.com/en/US/docs/ios/solutions_docs/qos_solutions/QoSVoIP/QoSVoIP.html">http://www.cisco.com/en/US/docs/ios/solutions_docs/qos_solutions/QoSVoIP/QoSVoIP.html</a></li> </ul>
Related Platform Documents	<ul style="list-style-type: none"> <li>• <a href="#">Cisco 2600 Series Multiservice Platforms</a></li> <li>• <a href="#">Cisco 2800 Series Integrated Services Routers</a></li> <li>• <a href="#">Cisco 3600 Series Multiservice Platforms</a></li> <li>• <a href="#">Cisco 3700 Series Multiservice Access Routers</a></li> <li>• <a href="#">Cisco 3800 Series Integrated Services Routers</a></li> <li>• <a href="#">Cisco 7200 Series Routers</a></li> <li>• <a href="#">Cisco 7301</a></li> </ul>
Related gateway configuration documentation	<p>Media and Signaling Authentication and Encryption Feature for Cisco IOS H.323 Gateways.</p> <p><a href="http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/htsecure.htm">http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/htsecure.htm</a></p>
Cisco IOS NAT Configuration Guide, Release 12.4T	<ul style="list-style-type: none"> <li>• <i>Configuring Cisco IOS Hosted NAT Traversal for Session Border Controller</i> <a href="http://www.cisco.com/en/US/docs/ios/12_4t/ip_addr/configuration/guide/htnatsbc.html">http://www.cisco.com/en/US/docs/ios/12_4t/ip_addr/configuration/guide/htnatsbc.html</a></li> </ul>

Related Topic	Document Title
Troubleshooting and Debugging guides	<ul style="list-style-type: none"> <li>• Cisco IOS Debug Command Reference, Release 12.4 at <a href="http://www.cisco.com/en/US/docs/ios/debug/command/reference/db_book.html">http://www.cisco.com/en/US/docs/ios/debug/command/reference/db_book.html</a></li> <li>• <i>Troubleshooting and Debugging VoIP Call Basics</i> at <a href="http://www.cisco.com/en/US/tech/tk1077/technologies_tech_note09186a0080094045.shtml">http://www.cisco.com/en/US/tech/tk1077/technologies_tech_note09186a0080094045.shtml</a></li> <li>• <i>VoIP Debug Commands</i> at <a href="http://www.cisco.com/en/US/docs/routers/access/1700/1750/software/configuration/guide/debug.html">http://www.cisco.com/en/US/docs/routers/access/1700/1750/software/configuration/guide/debug.html</a></li> </ul>

## Standards

Standards	Title
H.323 Version 4 and earlier	<i>H.323 (ITU-T VOIP protocols)</i>

## MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

RFCs	Title
RFC 1889	<i>RTP: A Transport Protocol for Real-Time Applications</i>
RFC 2131	<i>Dynamic Host Configuration Protocol</i>
RFC 2132	<i>DHCP Options and BOOTP Vendor Extensions</i>
RFC 2833	<i>RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals</i>
RFC 3203	<i>DHCP reconfigure extension</i>
RFC 3261	<i>SIP: Session Initiation Protocol</i>
RFC 3262	<i>Reliability of Provisional Responses in Session Initiation Protocol (SIP)</i>
RFC 3323	<i>A Privacy Mechanism for the Session Initiation Protocol (SIP)</i>
RFC 3325	<i>Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks</i>

RFCs	Title
RFC 3361	<i>Dynamic Host Configuration Protocol (DHCP-for-IPv4) Option for Session Initiation Protocol (SIP) Servers</i>
RFC 3455	<i>Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)</i>
RFC 3608	<i>Session Initiation Protocol (SIP) Extension Header Field for Service Route Discovery During Registration</i>
RFC 3711	<i>The Secure Real-time Transport Protocol (SRTP)</i>
RFC 3925	<i>Vendor-Identifying Vendor Options for Dynamic Host Configuration Protocol version 4 (DHCPv4)</i>

## 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>	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>

## Feature Information for SIP-to-SIP Connections on a Cisco Unified Border Element

Table 6 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.3(1) or a later release appear in the table.

For information on a feature in this technology that is not documented here, see the “[Cisco Unified Border Element Features Roadmap](#).”

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS, Catalyst OS, and Cisco IOS XE software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



### Note

Table 6 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 6** Feature Information for SIP-to-SIP Connections in a Cisco Unified Border Element

Feature Name	Releases	Feature Information
Address Hiding	12.4(9)T	Address hiding in all SIP messages.
Adjustable Timers for Registration Refresh and Retries	12.4(22)YB	<p>This feature provides the ability for IOS software to:</p> <ul style="list-style-type: none"> <li>Refresh the REGISTER at a configurable fraction of the expiry timer .</li> <li>Retransmit REGISTER upon failure responses per the min-expires value in a “423 interval too brief” response, or retry-after if present and terminal re-registration interval if retry-after value is absent in 4xx/5xx/6xx responses.</li> <li>Retransmit REGISTER per Timer E up to 32 seconds, and at a user defined random interval thereafter.</li> </ul> <p>The following section provides information about this feature:</p> <ul style="list-style-type: none"> <li><a href="#">Configuring Adjustable Timers for Registration Refresh and Retries, page 176</a></li> </ul> <p>The following commands were modified: <b>registrar</b> and <b>retry register</b></p>
Call Admission Control	12.4(6)T	Enables the SIP-to-SIP functionality to conform with RFC 3261 to interoperate with SIP UAs based on CPU, memory, total calls.
Cisco Unified Communications Manager Connections	12.4(6)T	Interoperability with Cisco Unified Communications Manager 5.0 and BroadSoft.
Codec Support	12.4(4)T 12.4(11)T	<p>12.4(4)T—SIP-to-SIP Basic Functionality for SBC for Cisco UBE provides termination and reorigination of both signaling and media between VoIP and video networks using SIP signaling.</p> <p>12.4(11)T—iLBC Codec</p>
Configurable Bandwidth Parameters for SIP Calls	12.4(15)XZ	This features provides the ability to manually configure the bandwidth that is signaled in the outbound SIP invite.
Configurable SIP Parameters via DHCP	12.4(22)YB	<p>The Configurable SIP Parameters via DHCP feature introduces the configuring of SIP parameters via DHCP.</p> <p>The following commands were introduced or modified: <b>credentials (sip-ua)</b>, <b>debug ccsip dhcp</b>, <b>dhcp interface</b>, <b>ip dhcp-client forcerenew</b>, <b>outbound-proxy</b>, <b>registrar</b>, <b>session target</b> (VoIP dial peer), <b>show sip dhcp</b>, <b>voice-class sip outbound-proxy</b>.</p>



**Table 6** Feature Information for SIP-to-SIP Connections in a Cisco Unified Border Element (continued)

Feature Name	Releases	Feature Information
DTMF Relay	12.4(4)T 12.4(11)T 12.4(6)XE	12.4(4)T—DTMF Relay Digit-Drop for SIP Calls Using NTE.  12.4(11)T—This feature passes DTMF tones out-of-band and drops in-band digits to avoid sending both tones to the outgoing leg on an H.323-to-SIP Cisco Unified Border Element.  12.4(6)XE—G.711 Inband DTMF to RFC 2833
ENUM support	12.4(6)T	Enables the SIP-to-SIP functionality to conform with RFC 3261 to interoperate with SIP UAs
Fax/Modem	12.4(6)T	12.4(6)T—Modem passthrough
Forced Update of SIP Parameters via DHCP	12.4(22)YB	The Configurable SIP Parameters via DHCP feature introduces the configuring of SIP parameters via DHCP.  The following sections provide information about this feature: <ul style="list-style-type: none"> <li>• <a href="#">Enabling Forced Update of SIP Parameters via DHCP</a></li> </ul>
Forced Update to SIP Parameters via DHCP updated in FTS.	12.4(22)YB	This feature was introduced.
Hosted NAT Traversal for SIP	12.4(9)T	This feature was introduced.
Interworking of Secure RTP calls for SIP and H.323	12.4(15)XY	This feature was introduced.
Media Modes	12.3(1) 12.4(9)T	12.3(1)—Media flow-through and flow-around improves scalability and performance when network-topology hiding and bearer-level interworking features are not required  12.4(9)T—Media Flow Around
Out-of-dialog OPTIONS Ping to Monitor Dial-peers to Specified SIP Servers and Endpoints	12.4(22)YB	This feature provides a keepalive mechanism at the SIP level between any number of destinations. The generic heartbeat mechanism allows Cisco UBE to monitor the status of SIP servers or endpoints and provide the option of busying-out associated dial-peer upon total heartbeat failure.  The following section provides information about this feature: <ul style="list-style-type: none"> <li>• <a href="#">Configuring Cisco UBE Out-of-dialog OPTIONS Ping for Specified SIP Servers or Endpoints, page 155</a></li> </ul> The following command was introduced: <b>voice-class sip options-keepalive</b>
Preloaded Routes in Outgoing INVITE Messages Based on REGISTER Information	12.4(22)YB	The following commands were modified: <b>voice-class sip url</b> and <b>url (SIP)</b> ,
Preloaded Routes in Outgoing INVITE Messages Based on REGISTER Information	12.4(22)YB	Supports the use of preloaded routes for outgoing INVITE messages. The system routes INVITE messages based on REGISTER message information, such as the path: and Service-Route values

Table 6 Feature Information for SIP-to-SIP Connections in a Cisco Unified Border Element (continued)

Feature Name	Releases	Feature Information
Selective Filtering of Outgoing Provisional Response on the Cisco Unified Border Element	12.4(22)YB	Supports selective filtering of outgoing provisional responses, including 180 - Alerting, and 183-Session In Progress responses. Selective filtering can be further based on the availability of media information in the received provisional response.
Selectively Using sip: URI or tel: URL Formats on Individual SIP Headers	12.4(22)YB	This feature supports the construction of request URIs in tel: format. The system supports this format for both the To: header and the Request-Line and the system supports appending the phone-context parameter to the tel: URL  The following command was introduced: <b>tel-config to-hdr</b> . The following commands were modified: <b>voice-class sip url, url</b>
Session refresh	12.4(11)T 12.4(15)XZ 12.4(20)T	12.4(11)T—This feature was introduced.  12.4(15)XZ—This feature adds support for SIP-to-SIP session refresh call flows using reINVITES.
Session Refresh with Reinvites	12.5(15)XZ	Expands the ability of the Cisco Unified BE to control the session refresh parameters and ensure the session does not time out.
Signal Interworking	12.4(6)T	Delayed Media Call, Media Inactivity. Enables the SIP-to-SIP functionality to conform with RFC 3261 to interoperate with SIP UAs
SIP Error Message Pass Through	12.4(11)XJ2	This feature was introduced.
SIP Listening Port	12.4(15)XZ 12.4(20)T	Allows users the ability to configure the port that SIP messages are listened on.
SIP Registration Message	12.4(24)T	Provides the ability to send a SIP Registration Message from Cisco Unified Border Element using the <b>credentials</b> command.
SIP Parameter Modification	12.4(15)XZ 12.4(20)T	Allows users to change the standard SIP messages sent from the Cisco SIP stack for better interworking with different SIP entities.
SRTP-RTP Internetworking	12.4(22)YB	This feature allows secure enterprise-to-enterprise calls. Support for SRTP-RTP internetworking between one or multiple Cisco Unified Border Elements is enabled for SIP-SIP audio calls.  The following sections provide information about this feature: <ul style="list-style-type: none"> <li><a href="#">Information About Cisco Unified Border Element Support for SRTP-RTP Internetworking, page 179</a></li> <li><a href="#">How to Configure Cisco Unified Border Element Support for SRTP-RTP Internetworking, page 181</a></li> </ul> The following command was introduced: <b>tls</b> .

**Table 6** Feature Information for SIP-to-SIP Connections in a Cisco Unified Border Element (continued)

Feature Name	Releases	Feature Information
Supplementary Services	12.4(9)T	<ul style="list-style-type: none"> <li>• Message Waiting Indication</li> <li>• Call Waiting</li> <li>• Call Transfer</li> <li>• Call Forward</li> <li>• Distinctive Ringing</li> <li>• Call Hold/Resume</li> <li>• Music on Hold.</li> </ul>
Support for Session Refresh with Reinvites	12.4(15)XZ	Expands the ability of the Cisco Unified Border Element to control the session refresh parameters and ensure the session does not time out.
Support for PAID, PPID, Privacy, PCPID, and PAURI Headers on the Cisco UBE	12.4(22)YB	<p>need the release notes blurb for this 9397, 9609</p> <p>The following commands were introduced: <b>call-route p-called-party-id</b>, <b>privacy-policy</b>, <b>random-contact</b>, <b>random-request-uri validate</b>, <b>voice-class sip call-route p-called-party-id</b>, <b>voice-class sip privacy-policy</b>, <b>voice-class sip random-contact</b>, <b>voice-class sip random-request-uri validate</b>.</p>
Tcl IVR	12.4(6)T	Tcl scripts with SIP NOTIFY VoiceXML with SIP-to-SIP
Transport Protocols	12.4(6)T	TCP and UDP interworking
Unsupported Content Pass-through	12.4(22)YB	<p>supports the ability to pass through end to end headers at a global or dial-peer level, that are not processed or understood in a SIP trunk to SIP trunk scenario. The pass through functionality includes all or only a configured list of unsupported or non-mandatory SIP headers, and all unsupported content/MIME types.</p> <p>The following command was introduced:</p>

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, 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. (0903R)

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.

© 2009 Cisco Systems, Inc. All rights reserved.





# Cisco Unified Border Element for H.323 Cisco Unified Communications Manager to H.323 Service Provider Connectivity

---

**Revised:** July 11, 2008, OL-2670-04

**First Published:** June 19, 2006

**Last Updated:** July 11, 2008

This chapter describes how to configure and enable features for H.323 Cisco Unified Communications Manager to H.323 service provider connections in a Cisco Unified Border Element topology. A Cisco Unified Border Element, in this guide also called an IP-to-IP gateway (IPIP GW), border element (BE), or session border controller, facilitates connectivity between independent VoIP networks by enabling VoIP and videoconferencing calls from one IP network to another.

## Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for Cisco Unified Border Element for H.323 Cisco Unified Communications Manager to H.323 Service Provider Connectivity](#)” section on page 254.

## Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS 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.



### Activation

---

**Cisco Product Authorization Key (PAK)**—A Product Authorization Key (PAK) is required to configure some of the features described in this guide. Please register your products and activate your PAK at <http://www.cisco.com/go/license> before starting your configuration process.

---



---

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

© 2009 Cisco Systems, Inc. All rights reserved.

# Contents

- Prerequisites for Cisco Unified Border Element for H.323 Cisco Unified Communications Manager to H.323 Service Provider Connectivity, page 236
- Restrictions for Cisco Unified Border Element for H.323 Cisco Unified Communications Manager to H.323 Service Provider Connectivity, page 237
- Information About Cisco Unified Border Element for H.323 Cisco Unified Communications Manager to H.323 Service Provider Connectivity, page 238
- How to Configure Cisco Unified Border Elements for H.323 Cisco Unified Communications Manager to H.323 Service Provider Connectivity., page 238
- Configuration Examples for Cisco Unified Border Element for H.323 Cisco Unified Communications Manager to H.323 Service Provider Connectivity, page 248
- Additional References, page 251
- Feature Information for Cisco Unified Border Element for H.323 Cisco Unified Communications Manager to H.323 Service Provider Connectivity, page 254

## Prerequisites for Cisco Unified Border Element for H.323 Cisco Unified Communications Manager to H.323 Service Provider Connectivity



### Activation

**Cisco Product Authorization Key (PAK)**—A Product Authorization Key (PAK) is required to configure some of the features described in this guide. Please register your products and activate your PAK at <http://www.cisco.com/go/license> before starting your configuration process.

- Perform the prerequisites listed in the “[Prerequisites for Cisco Unified Border Element Configuration](#)” section on page 15 in this guide.
- Perform basic H.323 gateway configuration.
- Perform basic H.323 gatekeeper configuration.



**Note** For configuration instructions, see the “[Configuring H.323 Gateways](#)” and “[Configuring H.323 Gatekeepers](#)” chapters of the *Cisco IOS Voice, Video, and Fax Configuration Guide*, Release 12.2.

In order to interconnect with an Cisco UBE, configure Cisco Unified Communications Manager with the following:

- Cisco Unified Communications Manager 3.0 or later release.



**Note** The Cisco Unified Communications Manager 4.1 has a SIP trunk towards the Cisco UBE in an H.323-to-SIP or a SIP-to-SIP network.

- Media termination point (MTP)—Enables the Cisco Unified Communications Manager to extend supplementary services, such as hold and transfer, to calls that are routed through an H.323 endpoint or an H.323 gateway.
  - Cisco IOS Release 12.4(4)T and earlier releases: MTP is required.
  - Cisco IOS Release 12.4(6)T and later releases: MTP is optional for H.323-to-H.323 calls.
- Intercluster Trunk (ICT)—An H.323 connection that enables multiple Cisco Unified Communications Manager systems to be connected over an IP cloud.
- Configure Cisco Unified Communications Manager in gateway mode while interoperating with the Cisco Unified Border Element.

**Note**

- During ICT configuration on the Cisco Unified Communications Manager, you are asked to enter the IP address of the remote Cisco Unified Communications Manager to which the ICT connects. Do not use this IP address. Instead, enter the IP address of the Cisco UBE.
- For more information on MTP, ICT, and Cisco Unified Communications Manager configuration, see the Cisco Unified Communications Manager documentation at [http://www.cisco.com/univercd/cc/td/doc/product/voice/c\\_callmg/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm)

## Restrictions for Cisco Unified Border Element for H.323 Cisco Unified Communications Manager to H.323 Service Provider Connectivity

- This functionality is enabled by default in Cisco IOS images that support the Cisco UBE, so you do not need to enter the commands that follow. However, the commands do appear in software and are explained here for informational purposes.
- Cisco Unified Communications Manager compatibility is as follows:
  - Cisco IOS Release 12.3(7)T and later releases: You must enable Cisco Unified Communications Manager compatibility on the Cisco UBE.
- The **call start interwork** command only supports interwork between fast-start and slow-start. It should not be used in situations where fast-start to fast-start or slow-start to slow-start calls are possible.
- When **call start interwork** is configured, both incoming and outgoing dial-peer need to have a specific codec configured.
- Ringback to the transferee is not supported by the Cisco Unified Border Element Software for calls blind call transferred between Cisco Unified Communications Manager and Cisco Unified Communications Express.

# Information About Cisco Unified Border Element for H.323 Cisco Unified Communications Manager to H.323 Service Provider Connectivity

For more information on Cisco Unified Communications Manager configuration, see the Cisco Unified Communications Manager documentation at [http://www.cisco.com/univercd/cc/td/doc/product/voice/c\\_callmg/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm)

## How to Configure Cisco Unified Border Elements for H.323 Cisco Unified Communications Manager to H.323 Service Provider Connectivity.

The section contains the following tasks:

- [Configuring Cisco Unified Border Element to Transport Calls With Cisco Unified Cisco Unified Communications Manager, page 238](#)
- [Configuring DTMF Relay Digit-Drop on an Cisco Unified Border Element with Cisco Unified Communications Manager, page 240](#)
- [Configuring H.323 Calling Name Display, page 242](#)

## Configuring Cisco Unified Border Element to Transport Calls With Cisco Unified Cisco Unified Communications Manager

To configure the Cisco UBE to transport calls to and from Cisco Unified Communications Manager, perform the steps in this section.

### Prerequisites

Configure Cisco Unified Communications Manager with the following:

- Media termination point (MTP)—Enables Cisco Unified Communications Manager to extend supplementary services, such as hold and transfer, to calls that are routed through an H.323 endpoint or an H.323 gateway. Cisco IOS Release 12.4(6)T and later releases: No MTP is optional.
- Intercluster trunk (ICT)—An H.323 connection that enables multiple Cisco Unified Communications Manager systems to be connected over an IP cloud.

**Note**

During ICT configuration, you are asked to enter the IP address of the remote Cisco Unified Communications Manager to which the ICT connects. Do not use this IP address. Instead, enter the IP address of the Cisco UBE.



## Restrictions

Cisco UBE does not support call preservation. If an Cisco UBE is located between a gateway and a Cisco Unified Communications Manager that have call preservation configured and the Cisco UBE is configured with media flow-around, calls will be preserved on the gateway when the Cisco UBE's IP interface becomes inaccessible due to a network issue or a reload. In this case, call preservation behavior on the gateway will be the same as the case where there is no Cisco UBE between the gateway and the Cisco Unified Communications Manager. Calls that are “held” will not be preserved as the Cisco UBE passes the nonstandard “do not preserve” indication sent in the Notify message from Cisco Unified Communications Manager to the gateway.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **h323**
5. **h225 h245-address**
6. **ccm-compatible**
7. **exit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<code>configure terminal</code>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<code>voice service voip</code>  <b>Example:</b> Router(config)# voice service voip	Enters VoIP voice-service configuration mode.
Step 4	<code>h323</code>  <b>Example:</b> Router(conf-voi-serv)# h323	Enters H.323 voice-service configuration mode.

	Command or Action	Purpose
Step 5	<p><code>h225 h245-address {sync   facility   progress}</code></p> <p><b>Example:</b>  <pre>Router(config-serv-h323)# h225 h245-address</pre></p>	<p>Enables H.225 and H.245 signaling. Keywords are as follows:</p> <ul style="list-style-type: none"> <li>• <b>sync</b>—Synchronized H.245 address reporting. Timing of H.245 messages is controlled by endpoints, not by the Cisco UBE.</li> <li>• <b>facility</b>—Cisco UBE sends a message to instruct the originating Cisco Unified Communications Manager to begin H.245 procedures on call start.</li> <li>• <b>progress</b>—Cisco UBE sends a Progress message that includes the H.245 address and a Progress Indicator value of 0x03.</li> </ul>
Step 6	<p><code>ccm-compatible</code></p> <p><b>Example:</b>  <pre>Router(config-serv-h323)# ccm-compatible</pre></p>	<p>Enables Cisco Unified Communications Manager-compatible signaling.</p>
Step 7	<p><code>exit</code></p> <p><b>Example:</b>  <pre>Router(config-serv-h323)# exit</pre></p>	<p>Exits the current mode.</p>

## Troubleshooting Tips

In the event that calls setup from Cisco Unified Communications Manager to Cisco Unified CallManager Express have no audio, verify the following:

- Interwork between Fast Start and Slow Start is not supported by the **call start interwork** command.
- When **call start interwork** is configured, both incoming and outgoing dial-peer need to have a specific codec configured.

## Configuring DTMF Relay Digit-Drop on an Cisco Unified Border Element with Cisco Unified Communications Manager

To avoid sending both in-band and out-of band tones to the outgoing leg when sending Cisco UBE calls in-band (rtp-nte) to out-of band (h245-alphanumeric), configure the **dtmf-relay rtp-nte digit-drop** command on the incoming SIP dial-peer. On the H.323 side configure either **dtmf-relay h245-alphanumeric** or **dtmf-relay h245-signal** command. This feature may also be used for H.323-to-SIP, and H.323-to-H.323 calls.



### Note

For a SIP (rtp-nte) to H.323 (h245-alphanumeric) via Cisco UBE call, if any RTP-NTE packets are sent before the H.323 Endpoint answers the call, the dual-tone multifrequency (DTMF) signal is not audible on a terminating gateway (TGW)

Perform the following task to configure DTMF relay digit drop on an Cisco UBE with Cisco Unified Communications Manager.

## Restrictions

- Configuring the **digit-drop** command is required for interworking between OOB and RTP NTE.
- Digit-drop for in-band rtp-nte DTMF conversion requiring a transcoder is not supported.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice tag voip**
4. **dtmf-relay [cisco-rtp] [h245-alphanumeric] [h245-signal][rtp-nte [digit-drop]]**
5. **exit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<pre>enable</pre> <p><b>Example:</b> Router&gt; enable</p>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<pre>configure terminal</pre> <p><b>Example:</b> Router# configure terminal</p>	Enters global configuration mode.
Step 3	<pre>dial-peer voice tag voip</pre> <p><b>Example:</b> Router(config)# dial-peer voice 2 voip</p>	Enters dial-peer voice configuration mode for the specified VoIP dial peer.
Step 4	<pre>dtmf-relay [cisco-rtp] [h245-alphanumeric][h245-signal] [rtp-nte [digit-drop]]</pre> <p><b>Example:</b> Router (config-dial-peer)# dtmf-relay rtp-nte digit-drop</p>	Forwards DTMF tones. Keywords are as follows: <ul style="list-style-type: none"> <li>• <b>cisco-rtp</b>—Forwards DTMF tones by using RTP with a Cisco-proprietary payload type.</li> <li>• <b>h245-alphanumeric</b>—Forwards DTMF tones by using the H.245 alphanumeric method.</li> <li>• <b>h245-signal</b>—Forwards DTMF tones by using the H.245 signal UII method.</li> <li>• <b>rtp-nte</b>—Forwards DTMF tones by using Real-Time Transport Protocol (RTP) with the Named Telephone Event (NTE) payload type.</li> <li>• <b>digit-drop</b>—Passes digits out-of-band; and drops in-band digits.</li> </ul> <p><b>Note</b> The <b>digit-drop</b> keyword is available only when the <b>rtp-nte</b> keyword is configured.</p>

	Command or Action	Purpose
Step 5	<pre>exit</pre> <p><b>Example:</b> Router(config-dial-peer)# exit</p>	Exits the current mode.

## Examples

The following example shows DTMF-Relay digits configured to avoid sending both in-band and out-of-band tones to the outgoing leg in an Cisco UBE:

```
.
.
.
dial-peer voice 1 voip
 dtmf-relay h245-alphanumeric rtp-nte digit-drop
.
.
.
```

## Troubleshooting tips

- The debug output will show that the H245 out of band messages are sent to the TGW. However, entry of the digits are not audible on the phone.

## Configuring H.323 Calling Name Display

The H.323 Calling Name Display feature provides a configurable option on the Cisco gateway to send the calling name received in Q931 Facility messages in the Display IE of setup message or Display IE of H.225 Notify messages to the Cisco Unified Communications Manager so that it can interpret the calling name and display it on Cisco IP Phones.

## Prerequisites

- This software operation is transparent to Cisco Unified Communications Manager and works with all releases, although Cisco Unified Communications Manager 4.2 or later is recommended
- The **isdn supp-service name calling** command must be configured under isdn D-channel for the H.323 Calling Name Display feature to work.
- It is recommended that you configure the **signaling forward unconditional** command on the outgoing gateway. This ensures that the outgoing H225 message has both the raw message and the Generic Transparency Descriptor (GTD).
- To configure the H.323 Calling Name Display feature under the voice class configuration, complete your dial-peer configuration first. Additional dial peer configuration information is available in the *Dial Peer Configuration on Voice Gateway Routers Guide* at the following url:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgr/vvfax\\_c/int\\_c/dpeer\\_c/dp\\_config.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgr/vvfax_c/int_c/dpeer_c/dp_config.htm)

## Restrictions

- When a Cisco gateway is connected to ISDN switch that sends the name-to-follow in Q931 Setup message, and the calling name in subsequent Q931 Facility message, It is recommended that you configure **h225 timeout ntf** command to buffer the setup message for the necessary interval.
- Calling name handling for various messages under ISDN, while interoperating with different switch types is not supported.

## Information About H.323 Calling Name Display

Calling name display information can be populated in ISDN messages in the Display Information Element (IE) of a Q.931 Setup or Notify message, or in the Facility IE of a Q.931 Setup or Facility message. The Cisco IOS gateway places this information into the same field of the corresponding H.323 message.

Cisco Unified Communications Manager (Cisco Unified CM) interprets calling name information (for purposes of name display on IP phones registered with Unified CM only in the Display IE of the H.323 Setup and Notify messages. Name display information delivered in an H.323 Facility message is not interpreted by Cisco Unified CM. Some ISDN switch types (for example, NI2) send a “name-to-follow” indication in the Q.931 Setup message and deliver the calling name subsequently in the Facility IE of a Q.931 Facility message. When a Cisco IOS gateway is connected to such an ISDN switch and interoperating with Cisco Unified CM by using the H.323 protocol, Cisco Unified CM is unable to display calling names on IP phones.

Beginning with Cisco IOS Release 12.4(11)XW, two new modes of operation are introduced on Cisco IOS gateway:

### H.323 Calling Name Display Without Buffering

When a Q.931 Setup message with a "name-to-follow" indication is received from an ISDN switch, an H.323 Setup message with no name information is sent to Cisco Unified CM. When the subsequent Q.931 Facility message is received with the calling name information, the message is mapped by the gateway to an H.225 Notify message with the Display IE populated with the calling name, so that the Cisco Unified CM can interpret the message correctly and display the calling name on the IP Phone.

### H.323 Calling Name Display With Buffering

When a Q.931 Setup message with a “name-to-follow” indication is received from an ISDN switch, the gateway can buffer the setup message until the subsequent Q.931 Facility message with calling name information is received. The name information from the Q.931 Facility message is now placed into the H.323 Setup message Display IE and sent to Cisco Unified CM. If the buffer timer expires before the Q.931 Facility message is received, a H.323 Setup is sent with no name information and, if it subsequently arrives, the information is sent by using an H.225 Notify message.

## How to Enable H.323 Calling Name Display

H.323 Calling name display is configured with or without buffering. This section contains the following subsections:

- [Configuring H.323 Calling Name Display Without Buffering, page 244](#)
- [Configuring H.323 Calling Name Display With Buffering, page 246](#)

## Configuring H.323 Calling Name Display Without Buffering

To enable the H.323 Calling Name Display feature without buffering for ISDN trunks that use the Facility message to deliver Name Display information, perform the steps in this section. This section contains the following subsections

- [Configuring H.323 Calling Name Display Without Buffering at the Voice Service Level, page 244](#)
- [Configuring H.323 Calling Name Display Without Buffering at the Voice Class Level, page 245](#)

## Configuring H.323 Calling Name Display Without Buffering at the Voice Service Level

To configure H.323 Calling Name Display without buffering at the voice service level, perform the steps in this section:

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **h323**
5. **h225 display-ie ccm-compatible**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<code>configure terminal</code>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<code>voice service voip</code>  <b>Example:</b> Router(config)# voice service voip	Enters VoIP voice-service configuration mode.
Step 4	<code>h323</code>  <b>Example:</b> Router(conf-voi-serv)# h323	Enters H.323 voice-service configuration mode
Step 5	<code>h225 display-ie ccm-compatible</code>  <b>Example:</b> Router(conf-voi-serv)# h225 display-ie ccm-compatible	Interprets the H.323 Notify Display IE so that the IP Phone can display the calling name on the IP Phone.

## Configuring H.323 Calling Name Display Without Buffering at the Voice Class Level

Behavior and configuration will vary based on the configuration mode the command is configured. When this CLI is configured under voice class:

- When the **h225 display-ie ccm-compatible** command is configured at the global level, and **h225 display-ie ccm-compatible system** command is configured at voice class level under dial-peer, both facility and notify messages are sent.
- When the **h225 display-ie ccm-compatible** command is not configured at global level, and the **h225 display-ie ccm-compatible system** command is configured at voice class level under dial-peer, only the facility message is sent.
- The configured command is visible in the **show running-configuration** output under voice class.
- Configuring the **no h225 display-ie ccm-compatible system** command in voice class configuration mode, the command that is configured under voice class takes precedence. Even when the **no h225 display-ie ccm-compatible system** command is configured under voice class and the **h225 display-ie ccm-compatible** command is configured under voice service voip, the gateway will not send the H225 Notify message received, and the calling name does not display on the IP Phone.

Use the **no** version to disable sending H225 Notify message on a particular VoIP dial-peer. The **no** form of the command is shown under voice class in the **show running-configuration**.

### Prerequisites

To configure the H.323 Calling Name Display feature under the voice class configuration, complete your dial-peer configuration first. Additional dial peer configuration information is available in the *Dial Peer Configuration on Voice Gateway Routers Guide* at the following url:

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax\\_c/int\\_c/dpeer\\_c/dp\\_cfg.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/int_c/dpeer_c/dp_cfg.htm)

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **voice class h323 tag**
5. **h225 display-ie ccm-compatible**

### DETAILED STEPS

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

	Command or Action	Purpose
Step 3	<code>voice service voip</code>  <b>Example:</b> Router(config)# <code>voice service voip</code>	Enters VoIP voice-service configuration mode.
Step 4	<code>voice class h323 tag</code>  <b>Example:</b> Router(conf-voi-serv)# <code>voice class h323 1</code>	Enters H.323 voice-service configuration mode
Step 5	<code>h225 display-ie ccm-compatible</code>  <b>Example:</b> Router(conf-voi-serv)# <code>h225 display-ie ccm-compatible</code>	Interprets the H.323 Notify Display IE so that the IP Phone can display the calling name on the IP Phone.

## Configuring H.323 Calling Name Display With Buffering

To enable the H.323 Calling Name Display feature with buffering for ISDN trunks that use the Facility message to deliver Name Display information, perform the steps in this section. This section contains the following subsections

- [Configuring H.323 Calling Name Display with Buffering at the Voice Service Level, page 246](#)
- [Configuring H.323 Calling Name Display with Buffering at the Voice Class Level, page 247](#)

## Configuring H.323 Calling Name Display with Buffering at the Voice Service Level

To configure H.323 calling name display at the voice service level, perform the steps in this section.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `voice service voip`
4. `h323`
5. `h225 timeout ntf milliseconds`
6. `h225 display-ie ccm-compatible`



## DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> Router> <code>enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>
Step 2	<code>configure terminal</code>  <b>Example:</b> Router# <code>configure terminal</code>	Enters global configuration mode.
Step 3	<code>voice service voip</code>  <b>Example:</b> Router(config)# <code>voice service voip</code>	Enters VoIP voice-service configuration mode.
Step 4	<code>h323</code>  <b>Example:</b> Router(conf-voi-serv)# <code>h323</code>	Enters the H.323 voice-service configuration mode.
Step 5	<code>h225 timeout ntf milliseconds</code>  <b>Example:</b> Router#(conf-voi-h323)# <code>h225 timeout ntf 300</code>	Buffers the setup message until the Q.931 Facility message with calling name information is received. Range is 50-5000 milliseconds.
Step 6	<code>h225 display-ie ccm-compatible</code>  <b>Example:</b> Router#(conf-if)# <code>h225 display-ie ccm-compatible</code>	Interprets the H.323 Notify Display IE so that the IP Phone can display the calling name on the IP Phone.

## Configuring H.323 Calling Name Display with Buffering at the Voice Class Level

To configure H.323 Calling Name Display at the voice class level, perform the steps in this section.

## Prerequisites

To configure the H.323 Calling Name Display feature under the voice class configuration, complete your dial-peer configuration first. Additional dial peer configuration information is available in the *Dial Peer Configuration on Voice Gateway Routers Guide* at the following url:

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax\\_c/int\\_c/dpeer\\_c/dp\\_config.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/int_c/dpeer_c/dp_config.htm)

## SUMMARY STEPS

- `enable`
- `configure terminal`
- `voice class h323 tag`
- `h225 display-ie ccm-compatible system`

5. h225 timeout ntf *milliseconds*

## DETAILED STEPS

	Command or Action	Purpose
Step 1	enable  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>
Step 2	configure terminal  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	voice class h323 tag  <b>Example:</b> Router(config)# voice service voip	Creates an H.323 voice class that is independent of a dial peer and can be used on multiple dial peers. Range is from 1 to 10000. There is no default value.
Step 4	h225 display-ie ccm-compatible system  <b>Example:</b> Router#(conf-voi-h323)# h225 display-ie ccm-compatible system	Interprets the H.323 Notify Display IE so that the IP Phone can display the calling name on the IP Phone.
Step 5	h225 timeout ntf <i>milliseconds</i>  <b>Example:</b> Router#(conf-voi-h323)# h225 timeout ntf 300	Buffers the setup message until the Q.931Facility message with calling name information is received. Range is 50-5000 milliseconds.  <b>Note</b> In the event the facility is received before the timer expires, the gateway will stop the buffer timer, extract the relevant information and send it to terminating endpoint.

## Troubleshooting Tips

- Enable debug isdn q931 to see the calling name coming into the GW in ISDN messages.
- Enable debug h225 q931 to see the calling name sent out by GW in H225 messages.

## Configuration Examples for Cisco Unified Border Element for H.323 Cisco Unified Communications Manager to H.323 Service Provider Connectivity

The following section contains configuration examples for the following:

- [Cisco Unified Border Element and Cisco Unified Communications Manager: Example](#)

## Cisco Unified Border Element and Cisco Unified Communications Manager: Example

Cisco UBE interconnects with Cisco Unified Communications Manager, providing a billing and network demarcation point and enabling service providers to transport calls to and from enterprise customers who use Cisco Unified Communications Manager.

H.245 handles end-to-end control messages between H.323 entities. H.245 procedures establish logical channels for transmission of audio and control channel information and are used to negotiate channel usage, flow control, and capabilities exchange messages.

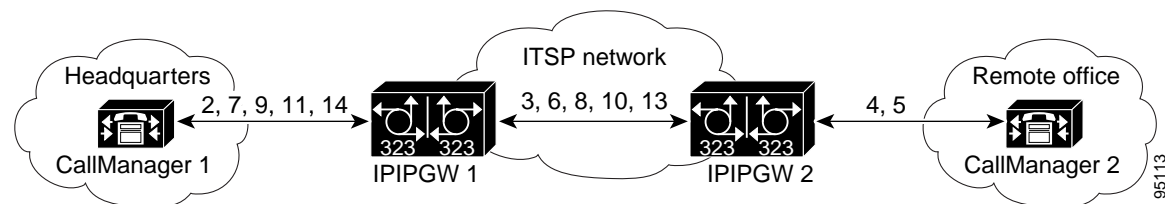
In releases earlier than Cisco IOS Release 12.3(1), the Cisco UBE responded to an incoming slow-start SETUP message with a CALLPROC message containing an H.245 address. This behavior is incompatible with the manner in which Cisco Unified Communications Manager handles H.245 messages. With Cisco IOS Release 12.3(1) and later releases, the Cisco UBE delays the reporting of originating-side H.245 address until a terminating-side H.245 address is received. Thus H.245 procedures are allowed to advance only when the called party is ready to do so.

When a call is set up, the Cisco UBE sends an H.225 message to the originator, instructing it to start H.245 procedures if they have not started by the time the CONNECT message is received from the terminating side. For slow-start calls in this scenario, a FACILITY message is sent containing an H.245 address. Some originating gateways running earlier Cisco IOS releases are unable to process this FACILITY message. To ensure interoperability with these older images, a PROGRESS message is sent containing an H.245 address and a Progress Indicator value of 0x03.

The functionality described above is enabled by default on Cisco UBEs running Cisco IOS Release 12.3(1) and later releases. It can be modified through the use of a new Cisco IOS command (**h225 h245-address facility | on-connect | progress**).

Figure 1 shows a sample topology that connects Cisco Unified Communications Manager systems to an Cisco UBE.

**Figure 1** Cisco UBE and Cisco Unified Communications Manager Topology



The following scenario illustrates a basic call placed from a company's headquarters to its remote office using Cisco Unified Communications Manager and two Cisco UBEs.

1. A caller at headquarters uses an IP phone to call someone at the remote office.
2. Cisco Unified Communications Manager 1 recognizes the called number as an extension at the remote office and sends a SETUP message to Cisco UBE 1.
3. The Cisco UBE, using the ITSP network, sends a SETUP message to Cisco UBE 2. Cisco UBE 1 sends a CALLPROC message to Cisco Unified Communications Manager 1.
4. At the remote office, Cisco UBE 2 sends a SETUP message to Cisco Unified Communications Manager 2 and sends a CALLPROC message to Cisco UBE 1.
5. Cisco Unified Communications Manager 2 rings the extension of the called party and sends an ALERT message with the H.245 address to Cisco UBE 2.

6. Cisco UBE 2 sends an ALERT message with the H.245 address to Cisco UBE 1.
7. Cisco UBE 1 sends an ALERT message with the H.245 address to Cisco Unified Communications Manager 1.
8. Cisco UBE 2 sends a FACILITY message with the H.245 address to Cisco UBE 1.
9. Cisco UBE 1 sends a FACILITY message with the H.245 address to Cisco Unified Communications Manager 1.
10. Cisco UBE 2 sends a PROGRESS message with the H.245 address to Cisco UBE 1.
11. Cisco UBE 1 sends a PROGRESS message with the H.245 address to Cisco Unified Communications Manager 1.
12. The two Cisco Unified Communications Manager systems exchange capabilities and open logical channel messages, and they engage in master/slave determination (not shown in [Figure 1](#)).
13. The called party answers the extension, and Cisco UBE 2 sends a CONNECT message with the H.245 address to Cisco UBE 1.
14. Cisco UBE 1 sends a CONNECT message with the H.245 address to Cisco Unified Communications Manager 1.


## Where to Go Next

- [H.323-to-H.323 Connections on a Cisco Unified Border Element](#)
- [H.323-to-SIP Connections on a Cisco Unified Border Element](#)
- [SIP-to-SIP Connections on a Cisco Unified Border Element](#)
- [Configuring Cisco Unified Border Element Videoconferencing](#)

# Additional References

The following sections provide references related to Cisco Unified Border Element.

## Related Documents

Related Topic	Document Title
Cisco IOS Release 12.4	<ul style="list-style-type: none"> <li>• <a href="#">Cisco IOS Release 12.4 Configuration Guides</a></li> <li>• <a href="#">Cisco IOS Release 12.4T Configuration Guides</a></li> <li>• <a href="#">Cisco IOS Release 12.4 Command References</a></li> <li>• <a href="#">Cisco IOS Voice Configuration Library</a></li> </ul> <p><a href="http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/cisco_ios_voice_configuration_library_glossary/vcl.htm">http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/cisco_ios_voice_configuration_library_glossary/vcl.htm</a></p>  <p><b>Note</b> This website contains the library preface and glossary.</p>
Cisco IOS Release 12.3	<ul style="list-style-type: none"> <li>• <a href="#">Cisco IOS Release 12.3 documentation</a></li> <li>• <a href="#">Cisco IOS voice commands</a></li> <li>• <a href="#">Cisco IOS Voice Troubleshooting and Monitoring Guide</a></li> <li>• <a href="#">Tcl IVR Version 2.0 Programming Guide</a></li> </ul>
Cisco IOS Release 12.2	<ul style="list-style-type: none"> <li>• <i>Cisco IOS Voice, Video, and Fax Configuration Guide</i>, Release 12.2 at <a href="http://www.cisco.com/en/US/docs/ios/12_2/voice/configuration/guide/fvfax_c.html">http://www.cisco.com/en/US/docs/ios/12_2/voice/configuration/guide/fvfax_c.html</a></li> </ul>
DSP documentation	<p>High-Density Packet Voice Feature Card for Cisco AS5350XM and AS5400XM Universal Gateways</p> <p><a href="http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124imit/124x/124xc4/vfc_dsp.htm">http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124imit/124x/124xc4/vfc_dsp.htm</a></p>
GKTMP (GK API) Documents	<ul style="list-style-type: none"> <li>• <i>GKTMP Command Reference</i>: <a href="http://www.cisco.com/en/US/docs/ios/12_2/gktmp/gktmpv4_2/gk_cli.htm">http://www.cisco.com/en/US/docs/ios/12_2/gktmp/gktmpv4_2/gk_cli.htm</a></li> <li>• <i>GKTMP Messages</i>: <a href="http://www.cisco.com/en/US/docs/ios/12_2/gktmp/gktmpv4_2/gk_tmp.html">http://www.cisco.com/en/US/docs/ios/12_2/gktmp/gktmpv4_2/gk_tmp.html</a></li> </ul>
internet Low Bitrate Codec (iLBC) Documents	<ul style="list-style-type: none"> <li>• Codecs section of the Dial Peer Configuration on Voice Gateway Routers Guide <a href="http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vfax_c/int_c/dpeer_c/dp_ovrvw.htm#1035124">http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vfax_c/int_c/dpeer_c/dp_ovrvw.htm#1035124</a></li> <li>• Dial Peer Features and Configuration section of the Dial Peer Configuration on Voice Gateway Routers Guide <a href="http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vfax_c/int_c/dpeer_c/dp_config.htm">http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vfax_c/int_c/dpeer_c/dp_config.htm</a></li> </ul>

Related Topic	Document Title
Cisco Unified Border Element Configuration Examples	<ul style="list-style-type: none"> <li>• Local-to-remote network using the IPIPGW <a href="http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a00801b0803.shtml">http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a00801b0803.shtml</a></li> <li>• Remote-to-local network using the IPIPGW: <a href="http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a0080203edc.shtml">http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a0080203edc.shtml</a></li> <li>• Remote-to-remote network using the IPIPGW: <a href="http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a0080203edd.shtml">http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a0080203edd.shtml</a></li> <li>• Remote-to-remote network using two IPIPGWs: <a href="http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a0080203edb.shtml">http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a0080203edb.shtml</a></li> </ul>
Related Application Guides	<ul style="list-style-type: none"> <li>• <a href="#">Cisco Unified Communications Manager and Cisco IOS Interoperability Guide</a></li> <li>• <a href="#">Cisco IOS Fax, Modem, and Text Support over IP Configuration Guide</a></li> <li>• “Configuring T.38 Fax Relay” chapter</li> <li>• <a href="#">Cisco IOS SIP Configuration Guide</a></li> <li>• Cisco Unified Communications Manager (CallManager) Programming Guides at: <a href="http://www.cisco.com/en/US/products/sw/voicew/ps556/products_programming_reference_guides_list.html">http://www.cisco.com/en/US/products/sw/voicew/ps556/products_programming_reference_guides_list.html</a></li> <li>• <i>Quality of Service for Voice over IP</i> at <a href="http://www.cisco.com/en/US/docs/ios/solutions_docs/qos_solutions/QoSVoIP/QoSVoIP.html">http://www.cisco.com/en/US/docs/ios/solutions_docs/qos_solutions/QoSVoIP/QoSVoIP.html</a></li> </ul>
Related Platform Documents	<ul style="list-style-type: none"> <li>• <a href="#">Cisco 2600 Series Multiservice Platforms</a></li> <li>• <a href="#">Cisco 2800 Series Integrated Services Routers</a></li> <li>• <a href="#">Cisco 3600 Series Multiservice Platforms</a></li> <li>• <a href="#">Cisco 3700 Series Multiservice Access Routers</a></li> <li>• <a href="#">Cisco 3800 Series Integrated Services Routers</a></li> <li>• <a href="#">Cisco 7200 Series Routers</a></li> <li>• <a href="#">Cisco 7301</a></li> </ul>
Related gateway configuration documentation	<p>Media and Signaling Authentication and Encryption Feature for Cisco IOS H.323 Gateways.</p> <p><a href="http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/htsecure.htm">http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/htsecure.htm</a></p>
Cisco IOS NAT Configuration Guide, Release 12.4T	<ul style="list-style-type: none"> <li>• <i>Configuring Cisco IOS Hosted NAT Traversal for Session Border Controller</i> <a href="http://www.cisco.com/en/US/docs/ios/12_4t/ip_addr/configuration/guide/htnatsbc.html">http://www.cisco.com/en/US/docs/ios/12_4t/ip_addr/configuration/guide/htnatsbc.html</a></li> </ul>

Related Topic	Document Title
Troubleshooting and Debugging guides	<ul style="list-style-type: none"> <li>• Cisco IOS Debug Command Reference, Release 12.4 at <a href="http://www.cisco.com/en/US/docs/ios/debug/command/reference/db_book.html">http://www.cisco.com/en/US/docs/ios/debug/command/reference/db_book.html</a></li> <li>• <i>Troubleshooting and Debugging VoIP Call Basics</i> at <a href="http://www.cisco.com/en/US/tech/tk1077/technologies_tech_note09186a0080094045.shtml">http://www.cisco.com/en/US/tech/tk1077/technologies_tech_note09186a0080094045.shtml</a></li> <li>• <i>VoIP Debug Commands</i> at <a href="http://www.cisco.com/en/US/docs/routers/access/1700/1750/software/configuration/guide/debug.html">http://www.cisco.com/en/US/docs/routers/access/1700/1750/software/configuration/guide/debug.html</a></li> </ul>

## Standards

Standards	Title
H.323 Version 4 and earlier	<i>H.323 (ITU-T VOIP protocols)</i>

## MIBs

MIBs	MIBs Link
None.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

RFCs	Title
RFC 2833	<i>RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals</i>
RFC 3261	<i>SIP: Session Initiation Protocol</i>

## Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>

# Feature Information for Cisco Unified Border Element for H.323 Cisco Unified Communications Manager to H.323 Service Provider Connectivity

Table 1 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.3(1) or a later release appear in the table.

For information on a feature in this technology that is not documented here, see the “[Cisco Unified Border Element Features Roadmap](#)”



## Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for Cisco Unified Border Element for H.323 Cisco Unified Communications Manager to H.323 Service Provider Connectivity

Feature Name	Releases	Feature Information
H.323 Calling Name Display	12.4(11)XW 12.4(20)T	Provides a configurable option on the Cisco Gateway so that the display IE received in Q931 Facility message, is sent out to Cisco Unified Communications Manager (Cisco Unified CM), in H.225 Notify message. This way Cisco Unified Cisco Unified CM can interpret it correctly, and display calling name on the IP phones.  The following commands were introduced by this feature: <b>h225 timeout ntf</b> and <b>h225 display-ie ccm-compatible</b>
DTMF Relay Digit-Drop on an Cisco Unified Border Element with Cisco Unified Communications Manager	12.4(11)T	This feature passes DTMF tones out-of-band and drops in-band digits to avoid sending both tones to the outgoing leg on an H.323-to-SIP Cisco Unified Border Element.
Cisco Unified Communications Manager Connections	12.3(1) 12.3(8)T	Cisco Unified Border Element for H.323 Cisco Unified Communications Manager to H.323 Service Provider Connectivity This feature provides interoperability with Cisco Unified Communications Manager for basic calls, caller-ID services, supplementary services, and RSVP synchronization with audio.  12.3(8)T—Restriction for Video Calls made from a Cisco Unified Communications Manager to an Cisco Unified Border Element.

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 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.

© 2009 Cisco Systems, Inc. All rights reserved.





# Configuring Cisco Unified Border Element Videoconferencing

---

**Revised: September 26, 2008,**  
**First Published: June 19, 2006**  
**Last Updated: September 26, 2008**

This chapter describes how to configure the Videoconferencing for the Cisco Unified Border Element (Cisco UBE) feature. The feature provides enhanced quality of service (QoS) through RSVP synchronization with H.323 signaling protocol and differentiated services code point (DSCP) packet marking. A Cisco Unified Border Element, in this guide also called an IP-to-IP gateway (IPIPGW), border element (BE), or session border controller, facilitates connectivity between independent VoIP networks by enabling H.323 VoIP and videoconferencing calls from one IP network to another.

## Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for Configuring Cisco Unified Border Element Videoconferencing”](#) section on page 281.

## Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS 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.

## Contents

- [Prerequisites for Configuring Cisco Unified Border Element Videoconferencing, page 258](#)
- [Restrictions for Configuring Cisco Unified Border Element Videoconferencing, page 258](#)
- [Information About Configuring Cisco Unified Border Element Videoconferencing, page 259](#)
- [How to Configure Cisco Unified Border Element Videoconferencing, page 262](#)
- [Configuration Examples for Cisco Unified Border Element Videoconferencing, page 275](#)



---

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

© 2009 Cisco Systems, Inc. All rights reserved.

- [Additional References](#), page 278
- [Feature Information for Configuring Cisco Unified Border Element Videoconferencing](#), page 281

## Prerequisites for Configuring Cisco Unified Border Element Videoconferencing

- Perform the prerequisites listed in the [“Prerequisites for Cisco Unified Border Element Configuration”](#) section on page 15 in this guide.
- Perform basic H.323 gateway configuration.
- Perform basic H.323 gatekeeper configuration.



**Note** For configuration instructions, see the [“Configuring H.323 Gateways”](#) and [“Configuring H.323 Gatekeepers”](#) chapters of the *Cisco IOS Voice, Video, and Fax Configuration Guide*, Release 12.2.

## Restrictions for Configuring Cisco Unified Border Element Videoconferencing

- H.323-to-SIP video traffic is not supported.
- H.239 for dual video (also known as Picture-in-Picture) is supported in Cisco IOS Release 12.4(20)T and later releases.
- Video is supported with slow-start.
- Dual video is not supported.
- Video with faststart and RSVP is not supported.
- Video and T.120 data are supported only with H.323 slow-start calls.
- T.120 data is supported only in flow-around mode.
- Video endpoints must have the same H.245 version.
- Cisco Unified Border Elements that are configured for videoconferencing cannot coexist with a Multimedia Conference Manager (MCM) proxy in the same zone. See the [“Migrating MCM Proxies”](#) section on page 262 for details.
- Cisco Unified Border Elements are able to process audio and video calls without additional configuration.
- If video calls from Cisco Unified Communications Manager directly to an Cisco UBE fail, go to the Cisco Unified Communications Manager gateway configuration and uncheck the Wait for Far End H.245 Terminal Capability Set check box.
- A Cisco Unified Border Element that is configured for videoconferencing is compatible with MCM proxies. However, the following limitations apply:
  - The videoconferencing gateway cannot coexist with an MCM proxy in the same zone.
  - RSVP status depends on the type of originating and terminating gateway, as shown in the following table.

# Information About Configuring Cisco Unified Border Element Videoconferencing

The Videoconferencing for Cisco Unified Border Element feature improves the quality, reliability, and scalability of IP videoconferencing applications. In addition to the benefits offered by the Cisco UBE feature, the videoconferencing feature provides the following functionality:

- Multiple logical channels per call leg
- Exchange of video and T.120 data between H.323 call legs
- Exchange of H.245 miscellaneous commands and indications and generic capabilities between H.323 call legs
- Far End Camera Control (FECC) support
- Differentiated services code point (DSCP) marking for video streams
- RSVP synchronization of H.323 calls
- New vendor-specific attribute (VSA) for improved accounting of bandwidth usage

Feature benefits include the following:

- FECC enables an endpoint to control the remote camera on a video call connected through the Cisco UBE.
- Cisco gateways can be configured to use the max-bit-rate VSA to report bandwidth usage to accounting servers.

Cisco Unified Border Elements are able to process audio and video calls without additional configuration. However, you will most likely want to set quality-of-service (QoS) levels and control how available bandwidth is divided among the calls passing through the gateway.

This section contains the following information:

- [MCM Proxies, page 259](#)
- [QoS Levels, page 260](#)
- [Bandwidth Usage, page 261](#)

## MCM Proxies

Cisco Multimedia Conference Manager (MCM) is a Cisco IOS software feature set that enables IP networks to support secure, reliable H.323 videoconferencing, with advanced quality of service (QoS) capabilities. MCM functions as a high-performance H.323 gatekeeper and proxy, allowing network managers to control bandwidth and priority setting for H.323 videoconferencing services based on individual network configurations and capacities. These capabilities ensure appropriate allocation of network resources for videoconferencing and other critical applications running simultaneously on the network.

A Cisco Unified Border Element (Cisco UBE) that is configured for videoconferencing is compatible with MCM proxies. However, the following limitations apply:

- The videoconferencing gateway cannot coexist with an MCM proxy in the same zone.
- RSVP status depends on the type of originating and terminating gateway, as shown in the following table.

Gateway Type		RSVP Status
Originating Gateway	Terminating Gateway	
MCM proxy	Cisco UBE	Synchronized
Cisco UBE	MCM proxy	Not synchronized

## QoS Levels

You can configure required and acceptable QoS levels on the gateway by means of the **req-qos** and **acc-qos** commands. The following levels are available:

- Best-effort—Bandwidth reservation is not attempted.
- Controlled-load—Synchronized RSVP is attempted. If it fails, the call is released.
- Guaranteed-delay—Synchronized RSVP is attempted. If it fails, one of the following occurs:
  - If acceptable QoS is best effort, call setup proceeds but without bandwidth reservation.
  - If acceptable QoS on either gateway is anything other than best effort, the call is released.

**Table 1** summarizes the results of nine call-setup scenarios based on the QoS levels configured in the dial peers at the originating and terminating gateways. It does not include cases in which the requested QoS is best-effort and the acceptable QoS is something other than best-effort.

**Table 1** Call Results Based on Configured QoS Levels

Call Scenario	Originating Gateway		Terminating Gateway		
	Requested QoS	Acceptable QoS	Requested QoS	Acceptable QoS	Results
1	controlled-load or guaranteed-delay	controlled-load or guaranteed-delay	controlled-load or guaranteed-delay	controlled-load or guaranteed-delay	Call proceeds only if both RSVP reservations succeed.
2	controlled-load or guaranteed-delay	controlled-load or guaranteed-delay	controlled-load or guaranteed-delay	best-effort	Call proceeds only if both RSVP reservations succeed.
3	controlled-load or guaranteed-delay	controlled-load or guaranteed-delay	best-effort	best-effort	Call is released.
4	controlled-load or guaranteed-delay	best-effort	controlled-load or guaranteed-delay	controlled-load or guaranteed-delay	Call proceeds only if both RSVP reservations succeed.
5	controlled-load or guaranteed-delay	best-effort	controlled-load or guaranteed-delay	best-effort	Call proceeds regardless of RSVP results. If RSVP reservation fails, call receives best-effort service.

**Table 1** Call Results Based on Configured QoS Levels (continued)

Call Scenario	Originating Gateway		Terminating Gateway		Results
	Requested QoS	Acceptable QoS	Requested QoS	Acceptable QoS	
6	controlled-load or guaranteed-delay	best-effort	best-effort	best-effort	Call proceeds with best-effort service.
7	best-effort	best-effort	controlled-load or guaranteed-delay	controlled-load or guaranteed-delay	Call is released.
8	best-effort	best-effort	controlled-load or guaranteed-delay	best-effort	Call proceeds with best-effort service.
9	best-effort	best-effort	best-effort	best-effort	Call proceeds with best-effort service.

## Bandwidth Usage

Cisco Unified Border Elements (Cisco UBE) make bandwidth decisions based on specified or default QoS levels. The **req-qos** command enables you to specify how much bandwidth is used by individual calls passing through the Cisco UBE. You can specify default and maximum amounts of bandwidth to be requested for each call. Bandwidth usage varies depending on the type of gateway, as explained below.

### Originating Cisco Unified Border Element

If you set the required QoS level the default for audio (by means of the **req-qos guaranteed-delay audio bandwidth default** command and keywords), an audio reservation is made for the default value of 64 kbps.

Normally, a video RSVP reservation is made using the value in the SETUP message bearer capability information element (IE). If this value is zero (such as with Microsoft NetMeeting), the value specified with the **video bandwidth default** keyword is used.

When you configure audio streams for either controlled-load or guaranteed-delay and configure maximum values for both audio and video, the setup is rejected if the value from the bearer-capability IE exceeds the sum of the **audio bandwidth max** and **video bandwidth max**. The max values are also checked at the time the audio and video media channels are opened. The Cisco UBE never reserves more bandwidth than the values specified with the **max** keyword.



#### Note

If you do not set a maximum for either audio or video, the bearer-capability IE is not checked against max values during SETUP.

### Terminating Cisco Unified Border Element

The value in the bearer-capability IE is not used. Instead, the audio and video bandwidth values from the SETUP message nonstandard field are used. These values are compared with the maximum values for audio and video max configured on the terminating Cisco UBE. The smaller of the two values is used for RSVP.

[Table 2](#) summarizes the call-setup scenarios based on the configured RSVP behavior in the dial peers at the originating and terminating gateways.

**Table 2** Call Results Based on RSVP Behavior

Sync Mode	RSVP Mode	RSVP Result	Behavior
Sync	Requested, not best effort	Audio and video RSVP failed.	Do nothing.
	Acceptable, not best effort		
	Requested, not best effort	Audio RSVP failed.	Kill the call.
	Acceptable, best effort	Video RSVP failed.	Kill the call.
Nonsync	Requested, not best effort	Audio and video RSVP failed.	Do nothing.
	Acceptable, best effort		
	Requested, not best effort	Audio RSVP failed.	Kill the call.
	Acceptable, not best effort	Video RSVP failed.	Close the video channel.

## How to Configure Cisco Unified Border Element Videoconferencing

This section contains the following information:

- [Migrating MCM Proxies, page 262](#)
- [Configuring Via-Zone Gatekeepers for Video Calls, page 263](#)
- [Configuring Audio and Video QoS Levels and Bandwidth Usage, page 264](#)
- [Configuring RSVP Synchronization for H.323 Slow Start, page 266](#)
- [Configuring Interworking of Polycom Endpoints, page 267](#)
- [Configuring a Voice Class, page 268](#)
- [Configuring Delayed-Offer to Early-Offer for SIP Video Calls, page 269](#)
- [Configuring SIP Video Calls with Flow Around Media, page 272](#)
- [Verifying and Troubleshooting Cisco Unified Border Element Videoconferencing, page 273](#)

### Migrating MCM Proxies

#### Converting MCM Zones

A network that uses MCM usually consists of multiple zones, each of which includes at least one gatekeeper and one MCM proxy.

Migrate a network from MCM proxies to videoconferencing gateways on a zone-by-zone basis. When a zone is converted, replace all of the MCM proxies in that zone with Cisco Unified Border Element videoconferencing gateways.

#### Converting Individual Devices

Frequently the gatekeeper and the MCM proxy are collocated on the same router. The videoconferencing gateway cannot reside on the same device with the gatekeeper, so you need an additional router to perform videoconferencing gateway functions.



You can reuse the router that hosted the collocated gatekeeper and MCM proxy for the via-zone gatekeeper. Upgrade to a Cisco IOS release that supports via-zones. Reuse the original gatekeeper-configuration data during configuration of the new via-zone gatekeeper as appropriate. Remove the portions related to the MCM proxy and replace them with the equivalent via-zone configuration.



**Note** If a local zone is configured for via-zone, the Cisco UBE is used for all calls.

## Configuring Via-Zone Gatekeepers for Video Calls

To configure video calls to use via-zone gatekeepers, perform the steps in this section.



**Note** Video calls can take advantage of the benefits offered by via-zone gatekeeper processing. For more information, see the “Configuring Via-Zones” section of the Gatekeeper guide.

### Restrictions

Although gatekeepers can support multiple local zones, call routing between a local zone and a via zone on the same gatekeeper is not supported in Cisco IOS Release 12.2(4)T and earlier releases. Via-zone gatekeepers must be dedicated to their own via-zones.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **gatekeeper**
4. **zone local**
5. **exit**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> <code>Router&gt; enable</code>	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	<code>configure terminal</code>  <b>Example:</b> <code>Router# configure terminal</code>	Enters global configuration mode.
Step 3	<code>gatekeeper</code>  <b>Example:</b> <code>Router(config)# gatekeeper</code>	Enters gatekeeper configuration mode.

	Command or Action	Purpose
Step 4	<pre>zone local gatekeeper-name domain-name [ras-IP-address] [invia inbound-gatekeeper   outvia outbound gatekeeper [enable-intrazone]]</pre> <p><b>Example:</b> Router(config-gk)# zone local termGK example.com 10.16.193.158 invia hurricane outvia hurricane enable-intrazone</p>	<p>Defines the local gatekeeper zone. Keywords and arguments are as follows:</p> <ul style="list-style-type: none"> <li>• <i>gatekeeper-name</i>—Gatekeeper name or zone name</li> <li>• <i>domain-name</i>—Domain name served by this gatekeeper</li> <li>• <i>ras-IP-address</i>—IP address of one of the interfaces on the gatekeeper</li> <li>• <b>invia</b> <i>inbound-gatekeeper</i>—Name of gatekeeper for calls entering this zone</li> <li>• <b>outvia</b> <i>outbound-gatekeeper</i>—Name of gatekeeper for calls leaving this zone</li> <li>• <b>enable-intrazone</b>—All intrazone calls are forced to use the via-zone gatekeeper</li> </ul> <p><b>Note</b> You can specify <b>invia</b> and <b>outvia</b> gatekeepers to be used for intrazone video calls. You can also specify <b>enable-intrazone</b> to force all intrazone calls to use the via-zone gatekeeper.</p>
Step 5	<pre>exit</pre> <p><b>Example:</b> Router(config-gk)# exit</p>	Exits the current mode.

## Configuring Audio and Video QoS Levels and Bandwidth Usage

To configure QoS and bandwidth usage, perform the steps in this section.



### Note

The following steps include sample settings that may not be appropriate for your network.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice tag voip**
4. **acc-qos guaranteed-delay audio**
5. **acc-qos guaranteed-delay video**
6. **req-qos guaranteed-delay audio bandwidth**
7. **req-qos guaranteed-delay video bandwidth**
8. **ip qos dscp video**
9. **exit**

## DETAILED STEPS

	Command	Purpose
Step 1	<code>enable</code>  <b>Example:</b> Router> enable	Enters privileged EXEC mode. Enter your password when prompted.
Step 2	<code>configure terminal</code>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<code>dial-peer voice tag voip</code>  <b>Example:</b> Router(config)# dial-peer voice tag voip	Enters dial-peer configuration mode for the specified VoIP dial peer.
Step 4	<code>acc-qos guaranteed-delay audio</code>  <b>Example:</b> Router(config-dial-peer)# acc-qos guaranteed-delay audio	Sets acceptable QoS for audio traffic. RSVP reserves bandwidth and guarantees a minimum bit rate and preferential queueing if the bandwidth reserved is not exceeded.  <b>Note</b> You cannot use the <b>acc-qos</b> command by itself. You must also use <b>req-qos</b> to specify a desired QoS for audio traffic. See <a href="#">Step 6</a> .
Step 5	<code>acc-qos guaranteed-delay video</code>  <b>Example:</b> Router(config-dial-peer)# acc-qos guaranteed-delay video	Sets acceptable QoS for video traffic. RSVP reserves bandwidth and guarantees a minimum bit rate and preferential queueing if the bandwidth reserved is not exceeded.  <b>Note</b> You cannot use the <b>acc-qos</b> command by itself. You must also use <b>req-qos</b> to specify a desired QoS for video traffic. See <a href="#">Step 7</a> .
Step 6	<code>req-qos guaranteed-delay audio bandwidth default [value] max [value]</code>  <b>Example:</b> Router(config-dial-peer)# req-qos guaranteed-delay audio bandwidth default 15 max 45	Sets required QoS for audio traffic. RSVP reserves bandwidth and guarantees a minimum bit rate and preferential queueing if the bandwidth reserved is not exceeded. Keywords and arguments are as follows: <ul style="list-style-type: none"> <li>• <b>default [value]</b>—Default audio bandwidth for RSVP, in kbps. Range: 1 to 64. Default: 64.</li> <li>• <b>max [value]</b>—Maximum audio bandwidth for RSVP, in kbps. Range: 1 to 64. Default: no maximum.</li> </ul>
Step 7	<code>req-qos guaranteed-delay video bandwidth default [value] max [value]</code>  <b>Example:</b> Router(config-dial-peer)# req-qos guaranteed-delay video bandwidth default 12 max 65	Sets required QoS for video traffic. RSVP reserves bandwidth and guarantees a minimum bit rate and preferential queueing if the bandwidth reserved is not exceeded. Keywords and arguments are as follows: <ul style="list-style-type: none"> <li>• <b>default [value]</b>—Default video bandwidth for RSVP, in kbps. Range: 1 to 5000. Default: 384.</li> <li>• <b>max [value]</b>—Maximum video bandwidth for RSVP, in kbps. Range: 1 to 5000. Default: no maximum.</li> </ul>

	Command	Purpose
Step 8	<pre>ip qos dscp [value] video [rsvp-none   rsvp-pass   rsvp-fail]</pre> <p><b>Example:</b> Router(config-dial-peer)# ip qos dscp 65 video rsvp-none</p>	<p>Sets the DSCP for QoS. In this case, allows DSCP marking of RTP packets for the video stream. Keywords and arguments are as follows:</p> <ul style="list-style-type: none"> <li>• <i>value</i>—DSCP value. Range: 0 to 63.</li> <li>• <b>video rsvp-none</b>—Applies DSCP to video stream with no RSVP reservations</li> <li>• <b>video rsvp-pass</b>—Applies DSCP to video stream with successful RSVP reservations</li> <li>• <b>video rsvp-fail</b>—Applies DSCP to video stream with failed RSVP reservations</li> </ul>
Step 9	<pre>exit</pre> <p><b>Example:</b> Router(config-dial-peer)# exit</p>	<p>Exits the current mode.</p>

## Configuring RSVP Synchronization for H.323 Slow Start

To configure RSVP synchronization for H.323 slow start for all H.323 calls, perform the steps in this section.



### Note

This task is optional; RSVP synchronization is enabled by default.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **h323**
5. **call start**
6. **exit**

### DETAILED STEPS

	Command	Purpose
Step 1	<pre>enable</pre> <p><b>Example:</b> Router&gt; enable</p>	<p>Enters privileged EXEC mode. Enter your password when prompted.</p>
Step 2	<pre>configure terminal</pre> <p><b>Example:</b> Router# configure terminal</p>	<p>Enters global configuration mode.</p>

	Command	Purpose
Step 3	<code>voice service voip</code>  <b>Example:</b> Router(config)# <code>voice service voip</code>	Enters VoIP voice-service configuration mode.
Step 4	<code>h323</code>  <b>Example:</b> Router(conf-voi-serv)# <code>h323</code>	Enters H.323 configuration mode.
Step 5	<code>call [start {fast   slow   system}]   [sync-rsvp slow-start]</code>  <b>Example:</b> Router(config-class)# <code>call slow sync-rsvp slow-start</code>	Forces an H.323 gateway to use fast-connect or slow-connect procedures for a dial peer. Use the <b>sync-rsvp slow-start</b> keyword to enable RSVP synchronization for slow-start calls. Keywords are as follows: <ul style="list-style-type: none"> <li>• <b>fast</b>—Fast-connect procedures</li> <li>• <b>slow</b>—Slow-connect procedures</li> <li>• <b>system</b>—Voice-service configuration</li> <li>• <b>sync-rsvp slow-start</b>—RSVP synchronization for slow-start calls</li> </ul> Default: <b>system</b>
Step 6	<code>exit</code>  <b>Example:</b> Router(config-class)# <code>exit</code>	Exits the current mode.

## Configuring Interworking of Polycom Endpoints

To configure interworking between Polycom endpoints, perform the steps in this section.

### Restrictions

Interworking between Polycom endpoints are determined by the software version running on each endpoint.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `voice service voip`
4. `h323`
5. `h225 h225 id-passthru`
6. `exit`

**DETAILED STEPS**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<code>enable</code>  <b>Example:</b> <code>Router&gt; enable</code>	Enables privileged EXEC mode. Enter your password if prompted.
<b>Step 2</b>	<code>configure terminal</code>  <b>Example:</b> <code>Router# configure terminal</code>	Enters global configuration mode.
<b>Step 3</b>	<code>voice service voip</code>  <b>Example:</b> <code>Router(config)# voice service voip</code>	Enters VoIP voice-service configuration mode.
<b>Step 4</b>	<code>h323</code>  <b>Example:</b> <code>Router(config-voice-service)# h323</code>	Enters H.323 voice-service configuration mode.
<b>Step 5</b>	<code>h225 h225 id-passthru</code>  <b>Example:</b> <code>Router(config-serv-h323)# h225 h225 id-passthru</code>	Enables signaling between video endpoints with different H.245 versions.
<b>Step 6</b>	<code>exit</code>  <b>Example:</b> <code>Router(config-serv-h323)# exit</code>	Exits the current mode.

**Configuring a Voice Class**

To configure a voice class that is independent of a dial peer and can be used on multiple dial peers, perform the steps in this section.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `voice class`
4. `call start`
5. `exit`

## DETAILED STEPS

	Command	Purpose
Step 1	<code>enable</code>  <b>Example:</b> <code>Router&gt; enable</code>	Enters privileged EXEC mode. Enter your password when prompted.
Step 2	<code>configure terminal</code>  <b>Example:</b> <code>Router# configure terminal</code>	Enters global configuration mode.
Step 3	<code>voice class tag</code>  <b>Example:</b> <code>Router (config)# voice class h323 1234</code>	Creates an H.323 voice class.
Step 4	<code>call [start {fast   slow   system}]   [sync-rsvp slow-start]</code>  <b>Example:</b> <code>Router (config-class)# call sync-rsvp slow-start</code>	Enables RSVP synchronization for slow-start calls. Default: synchronization is enabled.
Step 5	<code>exit</code>  <b>Example:</b> <code>Router(config-class)# exit</code>	Exits the current mode.

## Configuring Delayed-Offer to Early-Offer for SIP Video Calls

This feature alters the default configuration of the Cisco Unified BE from not distinguishing SIP Delayed-Offer to Early-Offer call flows, to forcing the Cisco Unified BE to generate an Early-Offer with the configured codecs for an incoming Delayed-Offer INVITE. To configure a Cisco Unified Border Element to send a SIP invite with Early-Offer (EO) on the Out-Leg (OL) perform the steps in this section.

To Delayed-Offer to Early-Offer for SIP Audio Calls for all VoIP calls, or individual dial peers, perform the steps in this section. This section contains the following subsections:

- [Configuring Delayed-Offer to Early-Offer for SIP Audio Calls at the Global Level, page 270](#)
- [Configuring Delayed-Offer to Early-Offer for SIP Audio Calls for a Dial-Peer, page 271](#)

### Prerequisites

- The **allow-connections sip to sip** command must be configured before you configure media flow-around. For more information and configuration steps see the “[Configuring SIP-to-SIP Connections in a Cisco Unified Border Element](#)” section on page 137 of the “[SIP-to-SIP Connections on a Cisco Unified Border Element](#)” chapter.

## Restrictions

- Cisco Unified Communications Manager 5.x supports Early-Offer over SIP trunk for audio calls with MTP
- Support for Cisco Unified Communications Manager Early-Offer for video calls and audio calls without MTP is not supported

Table 3 shows a list of protocol interworking for SIP.

**Table 3** Supported protocol interworking

Protocol	In Leg	Out Leg	Support
H.323-to-SIP	Fast Start	Early-Offer	Bi-Directional
	Slow Start	Delayed-Offer	Bi-Directional
SIP-to-SIP	Early-Offer	Early-Offer	Bi-Directional
	Delayed-Offer	Delayed-Offer	Bi-Directional
	Delayed-Offer	Early-Offer	Uni-Directional

## Configuring Delayed-Offer to Early-Offer for SIP Audio Calls at the Global Level

To configure Delayed-Offer to Early-Offer for SIP Audio Calls at the global level, perform the steps in this section.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **allow-connections sip**
5. **early-offer forced**
6. **exit**

### DETAILED STEPS

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



	Command or Action	Purpose
Step 3	<code>voice service voip</code>  <b>Example:</b> Router(config)# <code>voice service voip</code>	Enters VoIP voice-service configuration mode.
Step 4	<code>allow-connections from-type to to-type</code>  <b>Example:</b> Router(config-voi-serv)# <code>allow-connections sip to sip</code>	Allows connections between specific types of endpoints in an Cisco UBE. Arguments are as follows: <ul style="list-style-type: none"> <li><i>from-type</i>—Type of connection. Valid values: <b>h323</b>, <b>sip</b>.</li> <li><i>to-type</i>—Type of connection. Valid values: <b>h323</b>, <b>sip</b>.</li> </ul> <b>Note</b> H.323-to-H.323: By default, H.323-to-H.323 connections are disabled and POTS-to-any and any-to-POTS connections are enabled.
Step 5	<code>early-offer forced</code>  <b>Example:</b> Router(config-voi-serv)# <code>early-offer forced</code>	Enables SIP Delayed-Offer to Early-Offer globally.
Step 6	<code>exit</code>  <b>Example:</b> Router(config-voi-serv)# <code>exit</code>	Exits the current mode.

## Configuring Delayed-Offer to Early-Offer for SIP Audio Calls for a Dial-Peer

To configure Delayed-Offer to Early-Offer for SIP Audio Calls for an individual dial-peer, perform the steps in this section.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `dial-peer voice 1 voip`
4. `voice-class sip early-offer forced`
5. `exit`

**DETAILED STEPS**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<code>enable</code>  <b>Example:</b> <code>Router&gt; enable</code>	Enables privileged EXEC mode. Enter your password if prompted.
<b>Step 2</b>	<code>configure terminal</code>  <b>Example:</b> <code>Router# configure terminal</code>	Enters global configuration mode.
<b>Step 3</b>	<code>dial-peer voice <i>number</i> voip</code>  <b>Example:</b> <code>Router(config)# dial-peer voice 2 voip</code>	Enters dial-peer configuration mode for the specified VoIP dial peer.
<b>Step 4</b>	<code>voice-class sip early-offer forced</code>  <b>Example:</b> <code>Router(config-dial-peer)# voice-class sip early-offer forced</code>	Forcefully send Early-Offer
<b>Step 5</b>	<code>exit</code>  <b>Example:</b> <code>Router(config-dial-peer)# exit</code>	Exits the current mode.

## Configuring SIP Video Calls with Flow Around Media

To configure SIP video calls to be placed on the Cisco Unified Border Element (Cisco UBE) where the media flows around the Cisco UBE from endpoint to endpoint.

### Restrictions

- SIP video calls with flow around media is supported in Cisco IOS Release 12.4(20)T and later.
- SIP video calls with flow through media is supported in Cisco IOS Release 12.4(15)XZ and earlier.
- This is normally directly from endpoint to endpoint,

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `voice service voip`
4. `h323`
- 5.
6. `exit`

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> <code>Router&gt; enable</code>	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	<code>configure terminal</code>  <b>Example:</b> <code>Router# configure terminal</code>	Enters global configuration mode.
Step 3	<code>voice service voip</code>  <b>Example:</b> <code>Router(config)# voice service voip</code>	Enters VoIP voice-service configuration mode.
Step 4	<code>h323</code>  <b>Example:</b> <code>Router(conf-voi-serv)# h323</code>	Enters H.323 voice-service configuration mode.
Step 5	  <b>Example:</b> <code>Router(config-serv-h323)#</code>	.
Step 6	<code>exit</code>  <b>Example:</b> <code>Router(config-serv-h323)# exit</code>	Exits the current mode.

## Verifying and Troubleshooting Cisco Unified Border Element Videoconferencing

To troubleshoot or verify Cisco Unified Border Element Videoconferencing, perform the steps in this section. This section contains the following subsections:

- [Troubleshooting Tips, page 273](#)
- [Verifying and Monitoring Cisco Unified Border Element Videoconferencing, page 274](#)

### Troubleshooting Tips

For examples of **show** and **debug** command output and details on interpreting the output, see the following resources:

- [Cisco IOS Debug Command Reference, Release 12.3T](#)
- [Cisco IOS Voice Troubleshooting and Monitoring Guide](#)
- [Troubleshooting and Debugging VoIP Call Basics](#)
- [Voice Gateway Error Decoder for Cisco IOS](#)
- [VoIP Debug Commands](#)

## Verifying and Monitoring Cisco Unified Border Element Videoconferencing

To verify, monitor, and maintain audio and video calls, perform the following steps (listed alphabetically).

### SUMMARY STEPS

1. **show call active video**
2. **show call history video**
3. **show dial-peer voice**
4. **show ip rsvp reservation**
5. **show running-config**

### DETAILED STEPS

---

#### Step 1 **show call active video**

Use this command to display call statistics, including video bytes and packets received, video bytes and packets transmitted, bandwidth used, and UDP ports used, for active calls.

#### Step 2 **show call history video**

Use this command to display the same call statistics for all calls.

#### Step 3 **show dial-peer voice**

Use this command to display dial-peer statistics, including default and maximum bandwidth values for audio and video and DSCP marking for video.

#### Step 4 **show ip rsvp reservation**

Use this command to display RSVP-related receiver information currently in the database.

#### Step 5 **show running-config**

Use this command to verify audio and video QoS.

```
!
interface FastEthernet0/0
 ip address 10.1.1.5 255.255.255.0
 ip route-cache same-interface
 h323-gateway voip interface
 h323-gateway voip id zone1-gk ipaddr 10.1.1.1 1718
 h323-gateway voip tech-prefix 1#
 h323_gateway voip bind srcaddr 10.1.1.5
 ip rsvp bandwidth 7000 1000
!
!
dial-peer voice 100 voip
 voice-class h323 1
 req-qos guaranteed-delay audio bandwidth default 16 max 32
```

```

req-qos guaranteed-delay video bandwidth default 320 max 768
acc-qos guaranteed-delay audio
acc-qos guaranteed-delay video
ip qos dscp af11 media
ip qos dscp af21 signaling
ip qos dscp af33 video rsvp-none
ip qos dscp af31 video rsvp-pass
ip qos dscp af32 video rsvp-fail
codec transparent
!

```

## Configuration Examples for Cisco Unified Border Element Videoconferencing

This section provides the following configuration examples:

- [QoS for Audio and Video on One Gateway: Example, page 275](#)
- [QoS for Audio and Video on Two Gateways: Example, page 276](#)

### QoS for Audio and Video on One Gateway: Example

The following example shows QoS for audio and video configured on a Cisco Unified Border Element. Note that this example uses values and settings that may not be appropriate for your network.

```

!
voice service voip
no allow-connections any to pots
no allow-connections pots to any
allow-connections h323 to h323
h323
no call sync-rsvp slow-start
!
!
voice class h323 1
no call sync-rsvp slow-start
!
!
interface FastEthernet0/0
ip address 10.1.1.2 255.255.255.0
ip route-cache same-interface
h323-gateway voip interface
h323-gateway voip id zonel-gk ipaddr 10.1.1.1 1718
h323-gateway voip tech-prefix 1#
h323_gateway voip bind srcaddr 10.1.1.2
ip rsvp bandwidth 7000 1000
!
!
dial-peer voice 100 voip
voice-class h323 1
req-qos guaranteed-delay audio bandwidth default 16 max 32
req-qos guaranteed-delay video bandwidth default 320 max 768
acc-qos guaranteed-delay audio
acc-qos guaranteed-delay video
ip qos dscp af11 media
ip qos dscp af21 signaling

```

```

ip qos dscp af33 video rsvp-none
ip qos dscp af31 video rsvp-pass
ip qos dscp af32 video rsvp-fail
codec transparent

```

## QoS for Audio and Video on Two Gateways: Example

The following example shows the dial-peers for two Cisco Unified Border Elements that exchange video calls. Each gateway is connected to an endpoint that does not support RSVP; however, RSVP is used between the Cisco UBEs. One endpoint has an E.164 address of 1231000, and the other endpoint has an E.164 address of 4569000. Because the endpoints do not support RSVP, the gateways must have two dial peers for each call leg, one that prevents RSVP reservations to the endpoints and one that allows RSVP between the gateways.

### Cisco Unified Border Element Connected to 1231000

```

dial-peer voice 123 voip
  description dial-peer incoming from ip-ip gateway
  incoming called-number 123....
  session target ras
  req-qos guaranteed-delay audio
  req-qos guaranteed-delay video
  acc-qos guaranteed-delay audio
  acc-qos guaranteed-delay video
  codec transparent
!
dial-peer voice 456 voip
  description dial-peer incoming from video endpoint
  incoming called-number 456....
  session target ras
  codec transparent
!
dial-peer voice 4569 voip
  description dial-peer outgoing to ip-ip gateway
  destination-pattern 456....
  session target ras
  req-qos guaranteed-delay audio
  req-qos guaranteed-delay video
  acc-qos guaranteed-delay audio
  acc-qos guaranteed-delay video
  codec transparent
!
dial-peer voice 1231 voip
  description dial-peer outgoing to video endpoint
  destination-pattern 123....
  session target ras
  codec transparent
!

```

### Cisco Unified Border Element Connected to 4569000

```

dial-peer voice 123 voip
  description dial-peer incoming from video endpoint
  incoming called-number 123....
  session target ras
  codec transparent
!
dial-peer voice 456 voip
  description dial-peer incoming from ip-ip gateway
  incoming called-number 456....
  session target ras

```

```
req-qos guaranteed-delay audio
req-qos guaranteed-delay video
acc-qos guaranteed-delay audio
acc-qos guaranteed-delay video
codec transparent
!
dial-peer voice 1231 voip
description dial-peer outgoing to ip-ip gateway
destination-pattern 123...
session target ras
req-qos guaranteed-delay audio
req-qos guaranteed-delay video
acc-qos guaranteed-delay audio
acc-qos guaranteed-delay video
codec transparent
!
dial-peer voice 4569 voip
description dial-peer outgoing to video endpoint
destination-pattern 456...
session target ras
codec transparent
!
```


## Where to Go Next

- [H.323-to-H.323 Connections on a Cisco Unified Border Element](#)
- [H.323-to-SIP Connections on a Cisco Unified Border Element](#)
- [SIP-to-SIP Connections on a Cisco Unified Border Element](#)
- [Cisco Unified Border Element for H.323 Cisco Unified Communications Manager to H.323 Service Provider Connectivity](#)

# Additional References

The following sections provide references related to Configuring Cisco Unified Border Element Videoconferencing.

## Related Documents

Related Topic	Document Title
Cisco IOS Release 12.4	<ul style="list-style-type: none"> <li>• <a href="#">Cisco IOS Release 12.4 Configuration Guides</a></li> <li>• <a href="#">Cisco IOS Release 12.4T Configuration Guides</a></li> <li>• <a href="#">Cisco IOS Release 12.4 Command References</a></li> <li>• <a href="#">Cisco IOS Voice Configuration Library</a> <a href="http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/cisco_ios_voice_configuration_library_glossary/vcl.htm">http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/cisco_ios_voice_configuration_library_glossary/vcl.htm</a></li> </ul>  <p><b>Note</b> This website contains the library preface and glossary.</p>
Cisco IOS Release 12.3	<ul style="list-style-type: none"> <li>• <a href="#">Cisco IOS Release 12.3 documentation</a></li> <li>• <a href="#">Cisco IOS voice commands</a></li> <li>• <a href="#">Cisco IOS Voice Troubleshooting and Monitoring Guide</a></li> <li>• <a href="#">Tel IVR Version 2.0 Programming Guide</a></li> </ul>
Cisco IOS Release 12.2	<ul style="list-style-type: none"> <li>• <i>Cisco IOS Voice, Video, and Fax Configuration Guide</i>, Release 12.2 at <a href="http://www.cisco.com/en/US/docs/ios/12_2/voice/configuration/guide/fvfax_c.html">http://www.cisco.com/en/US/docs/ios/12_2/voice/configuration/guide/fvfax_c.html</a></li> </ul>
DSP documentation	<p>High-Density Packet Voice Feature Card for Cisco AS5350XM and AS5400XM Universal Gateways</p> <p><a href="http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124imit/124x/124xc4/vfc_dsp.htm">http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124imit/124x/124xc4/vfc_dsp.htm</a></p>
GKTMP (GK API) Documents	<ul style="list-style-type: none"> <li>• <i>GKTMP Command Reference</i>: <a href="http://www.cisco.com/en/US/docs/ios/12_2/gktmp/gktmpv4_2/gk_cli.htm">http://www.cisco.com/en/US/docs/ios/12_2/gktmp/gktmpv4_2/gk_cli.htm</a></li> <li>• <i>GKTMP Messages</i>: <a href="http://www.cisco.com/en/US/docs/ios/12_2/gktmp/gktmpv4_2/gk_tmp.html">http://www.cisco.com/en/US/docs/ios/12_2/gktmp/gktmpv4_2/gk_tmp.html</a></li> </ul>
internet Low Bitrate Codec (iLBC) Documents	<ul style="list-style-type: none"> <li>• Codecs section of the Dial Peer Configuration on Voice Gateway Routers Guide <a href="http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgr/vfax_c/int_c/dpeer_c/dp_ovrvw.htm#1035124">http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgr/vfax_c/int_c/dpeer_c/dp_ovrvw.htm#1035124</a></li> <li>• Dial Peer Features and Configuration section of the Dial Peer Configuration on Voice Gateway Routers Guide <a href="http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgr/vfax_c/int_c/dpeer_c/dp_config.htm">http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgr/vfax_c/int_c/dpeer_c/dp_config.htm</a></li> </ul>



Related Topic	Document Title
Cisco Unified Border Element Configuration Examples	<ul style="list-style-type: none"> <li>• Local-to-remote network using the IPIPGW <a href="http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a00801b0803.shtml">http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a00801b0803.shtml</a></li> <li>• Remote-to-local network using the IPIPGW: <a href="http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a0080203edc.shtml">http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a0080203edc.shtml</a></li> <li>• Remote-to-remote network using the IPIPGW: <a href="http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a0080203edd.shtml">http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a0080203edd.shtml</a></li> <li>• Remote-to-remote network using two IPIPGWs: <a href="http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a0080203edb.shtml">http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a0080203edb.shtml</a></li> </ul>
Related Application Guides	<ul style="list-style-type: none"> <li>• Cisco Unified Communications Manager and Cisco IOS Interoperability Guide</li> <li>• Cisco IOS Fax, Modem, and Text Support over IP Configuration Guide</li> <li>• “Configuring T.38 Fax Relay” chapter</li> <li>• Cisco IOS SIP Configuration Guide</li> <li>• Cisco Unified Communications Manager (CallManager) Programming Guides at: <a href="http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_programming_reference_guides_list.html">http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_programming_reference_guides_list.html</a></li> <li>• <i>Quality of Service for Voice over IP</i> at <a href="http://www.cisco.com/en/US/docs/ios/solutions_docs/qos_solutions/QoSVoIP/QoSVoIP.html">http://www.cisco.com/en/US/docs/ios/solutions_docs/qos_solutions/QoSVoIP/QoSVoIP.html</a></li> </ul>
Related Platform Documents	<ul style="list-style-type: none"> <li>• Cisco 2600 Series Multiservice Platforms</li> <li>• Cisco 2800 Series Integrated Services Routers</li> <li>• Cisco 3600 Series Multiservice Platforms</li> <li>• Cisco 3700 Series Multiservice Access Routers</li> <li>• Cisco 3800 Series Integrated Services Routers</li> <li>• Cisco 7200 Series Routers</li> <li>• Cisco 7301</li> </ul>
Related gateway configuration documentation	<p>Media and Signaling Authentication and Encryption Feature for Cisco IOS H.323 Gateways.</p> <p><a href="http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/htsecure.htm">http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/htsecure.htm</a></p>
Cisco IOS NAT Configuration Guide, Release 12.4T	<ul style="list-style-type: none"> <li>• <i>Configuring Cisco IOS Hosted NAT Traversal for Session Border Controller</i> <a href="http://www.cisco.com/en/US/docs/ios/12_4t/ip_addr/configuration/guide/htnatsbc.html">http://www.cisco.com/en/US/docs/ios/12_4t/ip_addr/configuration/guide/htnatsbc.html</a></li> </ul>

Related Topic	Document Title
Troubleshooting and Debugging guides	<ul style="list-style-type: none"> <li>• Cisco IOS Debug Command Reference, Release 12.4 at <a href="http://www.cisco.com/en/US/docs/ios/debug/command/reference/db_book.html">http://www.cisco.com/en/US/docs/ios/debug/command/reference/db_book.html</a></li> <li>• <i>Troubleshooting and Debugging VoIP Call Basics</i> at <a href="http://www.cisco.com/en/US/tech/tk1077/technologies_tech_note09186a0080094045.shtml">http://www.cisco.com/en/US/tech/tk1077/technologies_tech_note09186a0080094045.shtml</a></li> <li>• <i>VoIP Debug Commands</i> at <a href="http://www.cisco.com/en/US/docs/routers/access/1700/1750/software/configuration/guide/debug.html">http://www.cisco.com/en/US/docs/routers/access/1700/1750/software/configuration/guide/debug.html</a></li> </ul>

## Standards

Standards	Title
H.323 Version 4 and earlier	<i>H.323 (ITU-T VOIP protocols)</i>

## MIBs

MIBs	MIBs Link
None.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

RFCs	Title
RFC 2833	<i>RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals</i>
RFC 3261	<i>SIP: Session Initiation Protocol</i>

## Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>

# Feature Information for Configuring Cisco Unified Border Element Videoconferencing

Table 4 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.3(1) or a later release appear in the table.

For information on a feature in this technology that is not documented here, see the “[Cisco Unified Border Element Features Roadmap](#)” of this guide.



## Note

Table 4 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 4** Feature Information for Configuring Cisco Unified Border Element Videoconferencing

Feature Name	Releases	Feature Information
Delayed offer to Early offer for SIP Video Calls	12.4(20)T1	This feature was introduced.
H.323 Video Calls Support for H.235 Security	12.4(15)XY	This feature was introduced.
H.323 Video Calls Support for H.239 Signaling	12.4(15)XY	This feature was introduced.
Videoconferencing for the Cisco Unified Border Element Feature	12.3(4)T	This feature was introduced.

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 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.

© 2009 Cisco Systems, Inc. All rights reserved.

