Cisco Unified Border Element
Configuration Guide
Software Version 8.5

October 2010

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
Cisco Unified Border Element Configuration Guide Roadmap

This roadmap lists the features documented in the *Cisco Unified Border Element Configuration Guide* and maps them to the chapters in which they appear.

**Activation**

Before you can configure the software features described in this guide, you will need a Product Authorization Key (PAK). Before you start the configuration process, please register your products and activate your PAK at the following URL [http://www.cisco.com/go/license](http://www.cisco.com/go/license).

For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the “Cisco Unified Border Element Configuration Guide Feature support” section on page 4.

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


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>
<thead>
<tr>
<th>Feature Name</th>
<th>Where Documented</th>
<th>Cisco IOS Release</th>
<th>Cisco UBE Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ability to Send a SIP Registration Message on a Border Element</td>
<td>“SIP—Ability to Send a SIP Registration Message on a Border Element”</td>
<td>12.4(24)T</td>
<td>1.3</td>
</tr>
<tr>
<td>Cisco UBE MIB support</td>
<td>Supports CISCO-VOICE-DIAL-CONTROL-MIB objects to obtain call volume and call rate information and CISCO-DSP-MGMT-MIB objects to report transcoding sessions availability information on the Cisco Unified Border Element. See the Additional References section.</td>
<td>15.0(1)XA</td>
<td>1.4</td>
</tr>
<tr>
<td>Clearable SIP-UA Statistics</td>
<td>The Clearable SIP-US Statistics feature adds MIB support. See the Additional References section.</td>
<td>12.3(2)T</td>
<td>1.0</td>
</tr>
<tr>
<td>Configurable Hostname in Locally Generated SIP Header</td>
<td>“SIP—Configurable Hostname in Locally Generated SIP Headers”</td>
<td>12.4(2)T</td>
<td>1.0</td>
</tr>
<tr>
<td>Configurable Pass-through of SIP INVITE Parameters</td>
<td>“Cisco Unified Border Element Support for Configurable Pass-through of SIP INVITE Parameters”</td>
<td>15.0(1)M</td>
<td>1.3</td>
</tr>
<tr>
<td>Core SIP Technology Enhancements</td>
<td>“SIP—Core SIP Technology Enhancements”</td>
<td>12.2(13)T</td>
<td>1.0</td>
</tr>
<tr>
<td>DTMF Events Through SIP Signaling</td>
<td>“DTMF Events through SIP Signaling”</td>
<td>12.2(11)T</td>
<td>1.0</td>
</tr>
<tr>
<td>Dynamic Payload Type Interworking for DTMF and Codec Packets for SIP-to-SIP Calls</td>
<td>“Support for Dynamic Payload Type Interworking for DTMF and Codec Packets for SIP-to-SIP Calls”</td>
<td>15.0(1)XA</td>
<td>1.4</td>
</tr>
<tr>
<td>Error Response Code upon an Out-of-Dialog OPTIONS Ping Failure</td>
<td>“Configuring an Error Response Code upon an Out-of-Dialog OPTIONS Ping Failure”</td>
<td>15.1(1)T</td>
<td>1.4</td>
</tr>
<tr>
<td>Expire Timer Reset on Receiving or Sending SIP 183 Message</td>
<td>“Support for Expires Timer Reset on Receiving or Sending SIP 183 Message”</td>
<td>15.0(1)XA</td>
<td>1.4</td>
</tr>
<tr>
<td>iLBC Support for SIP and H.323</td>
<td>“iLBC Support for SIP and H.323”</td>
<td>12.2(11)T</td>
<td>1.0</td>
</tr>
<tr>
<td>INFO Method for DTMF Tone Generation</td>
<td>“SIP—INFO Method for DTMF Tone Generation”</td>
<td>12.2(11)T</td>
<td>1.0</td>
</tr>
<tr>
<td>Interworking Between RSVP Capable and RSVP Incapable Networks</td>
<td>“Support for Interworking Between RSVP Capable and RSVP Incapable Networks”</td>
<td>15.0(1)XA</td>
<td>1.4</td>
</tr>
<tr>
<td>Interworking of Secure RTP calls for SIP and H.323</td>
<td>“Interworking of Secure RTP calls for SIP and H.323”</td>
<td>12.2(20)T</td>
<td>1.0</td>
</tr>
<tr>
<td>IP-to-IP Gateway: SIP-to-SIP Basic Functionality</td>
<td>IP-to-IP Gateway: SIP-to-SIP Basic Functionality</td>
<td>12.2(13)T3</td>
<td>1.0</td>
</tr>
<tr>
<td>Multiple Registrars on SIP Trunks</td>
<td>“Support for Multiple Registrars on SIP Trunks”</td>
<td>15.0(1)XA</td>
<td>1.4</td>
</tr>
<tr>
<td>Negotiation of an Audio Codec from a List of Codecs on Each Leg of a SIP-to-SIP Call on the Cisco Unified Border Element</td>
<td>“Support for Negotiation of an Audio Codec from a List of Codecs on Each Leg of a SIP-to-SIP Call on the Cisco Unified Border Element”</td>
<td>15.1(2)T</td>
<td>8.5</td>
</tr>
</tbody>
</table>
### Table 1
Cisco Unified Border Element Configuration Guide Feature Support (continued)

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Where Documented</th>
<th>Cisco IOS Release</th>
<th>Cisco UBE Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Out-of-dialog OPTIONS Ping for Specified SIP Servers or Endpoints</td>
<td>“Configuring Cisco UBE Out-of-dialog OPTIONS Ping for Specified SIP Servers or Endpoints”</td>
<td>12.4(22)YB</td>
<td>1.3</td>
</tr>
<tr>
<td>PAID, PPID, Privacy, PCPID, and PAURI Headers on the Cisco Unified Border Element</td>
<td>“Support for PAID, PPID, Privacy, PCPID, and PAURI Headers on the Cisco Unified Border Element”</td>
<td>12.4(22)YB</td>
<td>1.3</td>
</tr>
<tr>
<td>RFC 2782 Compliance with DNS SRV Queries</td>
<td>“SIP—RFC 2782 Compliance with DNS SRV Queries”</td>
<td>12.2(8)T</td>
<td>1.0</td>
</tr>
<tr>
<td>Session Timer Support</td>
<td>“SIP—Session Timer Support”</td>
<td>12.2(8)T</td>
<td>1.0</td>
</tr>
<tr>
<td>SIP - Enhanced 180 Provisional Response Handling</td>
<td>“SIP—Enhanced 180 Provisional Response Handling”</td>
<td>12.2(8)T</td>
<td>1.0</td>
</tr>
<tr>
<td>SIP-to-SIP Basic Feature Functionality for Session Border Controller (SBC)</td>
<td>“SIP-to-SIP Extended Feature Functionality for Session Border Controller (SBC)”</td>
<td>12.4(4)T</td>
<td>1.0</td>
</tr>
<tr>
<td>SIP 181 Call is Being Forwarded Message</td>
<td>“Configuring Support for SIP 181 Call is Being Forwarded Message”</td>
<td>15.0(1)XA</td>
<td>1.4</td>
</tr>
<tr>
<td>SIP Diversion Header Enhancements</td>
<td>“SIP Diversion Header Enhancements”</td>
<td>12.4(22)T</td>
<td>1.3</td>
</tr>
<tr>
<td>SIP Parameter Modification</td>
<td>“SIP Parameter Modification”</td>
<td>12.4(15)XZ</td>
<td>1.2</td>
</tr>
<tr>
<td>SIP SRTP Fallback to Nonsecure RTP</td>
<td>“SIP SRTP Fallback to Nonsecure RTP”</td>
<td>12.4(22)T</td>
<td>1.3</td>
</tr>
<tr>
<td>SIP Video Calls with Flow Around Media</td>
<td>“Support for SIP Video Calls with Flow Around Media”</td>
<td>12.4(15)XZ</td>
<td>1.2</td>
</tr>
<tr>
<td>SIP—Gateway Support for the Bind Command</td>
<td>“SIP—Gateway Support for the bind Command”</td>
<td>12.2(8)T</td>
<td>1.0</td>
</tr>
<tr>
<td>SIP-to-SIP Extended Feature Functionality for Session Border Controllers</td>
<td>“SIP-to-SIP Extended Feature Functionality for Session Border Controllers”</td>
<td>12.4(6)T</td>
<td>1.0</td>
</tr>
<tr>
<td>SIP-to-SIP Supplementary Services for Session Border Controller</td>
<td>“SIP-to-SIP Supplementary Services for Session Border Controller”</td>
<td>12.4(9)T</td>
<td>1.0</td>
</tr>
<tr>
<td>The official marketing name of Cisco Multiservice IP-to-IP Gateway was changed to Cisco Unified Border Element (Cisco UBE).</td>
<td>No configuration is required.</td>
<td>12.4(15)XY</td>
<td>1.1</td>
</tr>
<tr>
<td>Transparent Tunneling of QSIG and Q.931 over SIP TDM Gateway and SIP-SIP Cisco Unified Border Element</td>
<td>“Transparent Tunneling of QSIG and Q.931 over SIP TDM Gateway and SIP-SIP Cisco Unified Border Element”</td>
<td>12.4(15)XZ</td>
<td>1.2</td>
</tr>
<tr>
<td>Cisco Unified Border Element and Cisco Unified Communications Manager Express Support for Universal Packaging</td>
<td>Cisco Unified Border Element and Cisco Unified Communications Manager Express Support for Universal Packaging</td>
<td>15.0(1)M</td>
<td>1.3</td>
</tr>
<tr>
<td>Support inbound dial-peer match based on remote IP address on SIP trunks</td>
<td>Configuring an Inbound Dial-peer to Match the URI on SIP Calls</td>
<td>15.1(2)T</td>
<td>8.5</td>
</tr>
</tbody>
</table>
Cisco Unified Border Element Fundamentals and Basic Setup

This Cisco Unified Border Element is a special Cisco IOS software image that 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.

Activation
Cisco Product Authorization Key (PAK)—A Product Authorization Key (PAK) is required to configure some of the features described in this guide. Before you start the configuration process, please register your products and activate your PAK at the following URL http://www.cisco.com/go/license.

Finding Feature Information
For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the “Cisco Unified Border Element Features Roadmap” section on page 3.

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

Getting Started with Important Concepts

- Prerequisites for Cisco Unified Border Element, page 9
- Restrictions for Cisco Unified Border Element, page 9
Prerequisites for Cisco Unified Border Element

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:

Cisco Product Authorization Key (PAK)—A Product Authorization Key (PAK) is required to configure some of the features described in this guide. Before you start the configuration process, please register your products and activate your PAK at the following URL http://www.cisco.com/go/license.

- 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.

Restrictions for Cisco Unified Border Element

- Cisco Unified Border Elements that require the Registration, Admission, and Status (RAS) protocol must have a via-zone-enabled gatekeeper or equivalent.
- Cisco fax relay is reported as a voice call on a Cisco Unified Border Element. Fax relay is enabled by default for all systems. No further configuration is needed.
- 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 a Cisco Unified Border Element, the Cisco Unified Border Element does not support ringback tone generation.
- Transcoding is not supported.
Information About Cisco Unified Border Element

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. A Cisco Unified Border Element facilitates connectivity between independent VoIP networks by enabling SIP and 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 the Cisco AS1000 platform. It provides a network-to-network interface point for billing, security, call admission control, quality of service, and signaling interworking.

Cisco UBE 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.

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 any Cisco UBE Feature, you should understand the following concepts:

- **Gateway Functionality, page 10**
- **Cisco Unified Border Element Network Topology, page 11**

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 setup 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 reorginates 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 prefix 919 as a local zone and sends an LCF 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.

**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.
Basic SIP-to-SIP Set-up and Functionality Features

This chapter contains the following configuration topics:

**SIP-to-SIP Set-up**
- SIP-to-SIP Basic Functionality
- Transport Control Protocol (TCP) and User Datagram Protocol (UDP) interworking
- Cisco Unified Border Element and Cisco Unified Communications Manager Express Support for Universal Packaging

**IP Addressing**
- SIP—Gateway Support for the bind Command
- Configuring an Inbound Dial-peer to Match the URI on SIP Calls

**Additional References**

**Glossary**

**Feature Information for Cisco UBE Fundamentals and Basic Setup**
IP-to-IP Gateway: SIP-to-SIP Basic Functionality

SIP-to-SIP Basic Functionality for Cisco Unified Border Element (Cisco UBE) and Cisco Unified Border Element (Enterprise) (Cisco UBE (Enterprise)) 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 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)
- 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-to-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

Prerequisites

**Cisco Unified Border Element**
- Cisco IOS Release 12.2(13)T3 or a later release must be installed and running on your Cisco Unified Border Element.

**Cisco Unified Border Element (Enterprise)**
- Cisco IOS XE Release 2.5 or a later release must be installed and running on your Cisco ASR 1000 Series Router.

Restrictions

- Connections are disabled by default in Cisco IOS images that support the Cisco UBE (Enterprise).

How to Configure SIP-to-SIP Connections in a Cisco Unified Border Element (Enterprise)

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

**SUMMARY STEPS**

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

5. exit

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td>Enter your password if prompted.</td>
</tr>
</tbody>
</table>

| **Step 2** configure terminal | Enters global configuration mode. |
| **Example:** Router# configure terminal | |

| **Step 3** voice service voip | Enters VoIP voice-service configuration mode. |
| **Example:** Router(config)# voice service voip | |

| **Step 4** allow-connections from-type to to-type | Allows connections between specific types of endpoints in an Cisco UBE. Arguments are as follows: |
| **Example:** Router(config-voi-serv)# allow-connections sip to sip | • from-type—Type of connection. Valid values: h323, sip. |
| | • to-type—Type of connection. Valid values: h323, sip. |
| **Note** | 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** exit | Exits the current mode. |
| **Example:** Router(config-voi-serv)# exit | |
SIP-to-SIP Extended Feature Functionality for Session Border Controllers

The SIP-to-SIP Extended Feature Functionality for Session Border Controllers (SBCs) enables the SIP-to-SIP functionality to conform with RFC 3261 to interoperate with SIP User Agents (UAs). The SIP-to-SIP Extended Feature Functionality includes:

- Call Admission Control (based on CPU, memory, and total calls)
- Delayed Media Call
- ENUM support
- Configuring SIP Error Message Pass Through
- 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)

Prerequisites

**Cisco Unified Border Element**

- Cisco IOS Release 12.4(6)T or a later release must be installed and running on your Cisco Unified Border Element.

**Cisco Unified Border Element (Enterprise)**

- Cisco IOS XE Release 3.1S or a later release must be installed and running on your Cisco ASR 1000 Series Router.
SIP—Gateway Support for the bind Command

The Gateway Support for the bind Command feature introduces the `bind` command, which allows you to configure the source IP address of signaling packets or both signaling and media packets. Before this feature was introduced, the source address of a packet going out of a Cisco IOS gateway is not deterministic. The session protocols and VoIP layers depended on the IP layer to give the best local address and then used the address for the source address in signaling or media or both, even if multiple interfaces can support a route to the destination address.

Prerequisites

**Cisco Unified Border Element**
- Cisco IOS Release 12.2(8)T or a later release must be installed and running on your Cisco Unified Border Element.

**Cisco Unified Border Element (Enterprise)**
- Cisco IOS XE Release 2.5 or a later release must be installed and running on your Cisco ASR 1000 Series Router.

Information About SIP—Gateway Support for the bind Command

Prior to the Gateway Support for the bind Command feature, the source address of a packet going out of the gateway was never deterministic. That is, the session protocols and VoIP layers always depended on the IP layer to give the best local address. The best local address was then used as the source address (the address showing where the SIP request came from) for signaling and media packets. Using this nondeterministic address occasionally caused confusion for firewall applications, because a firewall could not be configured with an exact address and would take action on several different source address packets.

The `bind` interface command allows you to configure a specific interface’s IP address as the source IP address of signaling and media packets. The address that goes out on the packet is bound to the IP address of the interface specified with the `bind` command. Packets that are not destined to the bound address are discarded.

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

With the `bind` command, SIP signaling and media paths can advertise the same source IP address on the gateway for certain applications, even if the paths use different addresses to reach the source. This eliminates confusion for firewall applications that, without the binding, may have taken action on several different source address packets.

Table 1 lists the results of the bind command based on the state of the interface.
Table 1  Command functions for the bind command based on the state of the interface

<table>
<thead>
<tr>
<th>Interface State</th>
<th>Result Using Bind Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>A bind interface is shut down, or its IP Address is changed, or the physical cable is pulled while SIP calls are active</td>
<td>The call becomes a one-way call with media flowing in only one direction. It flows from the gateway where the change or shutdown took place to the gateway where no change occurred. Thus, the gateway with the status change no longer receives media. The call is then disconnected, but the disconnected message is not understood by the gateway with the status change, and the call is still assumed to be active.</td>
</tr>
<tr>
<td>No Shutdown—With no active calls.</td>
<td>The TCP and UDP socket listeners are initially closed. (Socket listeners receive datagrams addressed to the socket.) Then the sockets are opened and bound to the IP address set by the bind command. The sockets accept packets destined for the bound address only.</td>
</tr>
<tr>
<td>No Shutdown —With active calls.</td>
<td>The TCP and UDP socket listeners are initially closed. Then the sockets are opened to listen to any IP address.</td>
</tr>
<tr>
<td>Shutdown —With or without active calls.</td>
<td>The TCP and User Datagram Protocol (UDP) socket listeners are initially closed. (Socket listeners receive datagrams addressed to the socket.) Then the sockets are opened to listen to any IP address. If the outgoing gateway has the bind command enabled and has an active call, the call becomes a one-way call with media flowing from the outgoing gateway to the terminating gateway.</td>
</tr>
<tr>
<td>The Bound interface’s IP address is removed</td>
<td>The TCP and UDP socket listeners are initially closed. Then the sockets are opened to listen to any address, because the IP address has been removed. A message stating that the IP address has been deleted from SIP bound interface is displayed. If the outgoing gateway has the bind command enabled and has an active call, the call becomes a one-way call with media flowing from the outgoing gateway to the terminating gateway.</td>
</tr>
<tr>
<td>The physical cable is pulled on the bound port, or the Interface layer goes down</td>
<td>The TCP and UDP socket listeners are initially closed. Then the sockets are opened and bound to listen to any address. When the pulled cable is replaced, the result is as documented for no shutdown interfaces.</td>
</tr>
</tbody>
</table>

**Note**  If there are active calls, the bind command will not take effect if it is issued for the first time or if it is issued while another bind command is in effect. A message is displayed reminding you that there are active calls and that the bind command change cannot take effect.
How to Configure SIP—Gateway Support for the bind Command

To configure the SIP—Gateway Support for the bind Command feature, complete these tasks:

- Setting the Bind Address, page 20 (required)
- Setting a Source IP Address for Signaling and Media Packets, page 21 (required)
- Verifying and Troubleshooting Tips, page 23

Setting the Bind Address

To set the bind address, complete the task in this section.

SUMMARY STEPS

1. enable
2. configure terminal
3. dial-peer voice number voip
4. session target ipv4: destination-address
5. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> dial-peer voice number voip</td>
<td>Enters dial peer configuration mode to configure a VoIP dial-peer.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# dial-peer voice 2 voip</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> session target ipv4: destination-address</td>
<td>Specifies a network-specific address for a dial peer.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-dial-peer)# session target ipv4: 172.16.43.3</td>
<td>• This command must be set to the bind address of the receiving gateway before using the bind command.</td>
</tr>
<tr>
<td><strong>Step 5</strong> exit</td>
<td>Exits dial peer voice configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-dial-peer)# exit</td>
<td></td>
</tr>
</tbody>
</table>
Setting a Source IP Address for Signaling and Media Packets

SIP configuration mode starts from voice-service VoIP configuration mode. When the router is in SIP configuration mode, several options are available, including the `bind` command. To enable this feature, review the prerequisites to make sure your network is compliant, and then complete the task in this section.

**Prerequisites**

- Ensure you have Cisco IOS XE Release 2.5 or a later release installed and running on your Cisco ASR 1000 Series Router.
- Ensure that the gateway has voice functionality that is configurable for SIP.
- Establish a working IP network.
- Configure VoIP.
- Set the bind address prior to using the `bind` command.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. voice service voip
4. sip
5. session transport {udp | tcp}
6. bind {control | all} source-interface interface-id
7. default {command}
8. exit

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3voice service voip</td>
<td>Enters voice-service configuration mode</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# voice service voip</td>
<td></td>
</tr>
<tr>
<td>Step 4sip</td>
<td>Enters the SIP configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-voi-srv)# sip</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

**Step 5**

`session transport (udp | tcp)`  
(Optional) Sets the session transport type for the SIP user agent.

- The default is UDP.
- The transport protocol (udp or tcp) specified with the `session transport` command, and the protocol specified with the `transport` command, must be identical.

**Example:**

Router(conf-serv-sip)# `session transport udp`

**Step 6**

`bind (control | all) source-interface interface-id`

Sets a source address for signaling and media packets.

- control: Binds SIP signaling packets.
- all: Binds SIP signaling packets and media packets.
- source-interface: Specifies an interface as the source address of SIP packets.
- `interface-id` argument specifies the type of interface:
  - Async
  - BVI
  - CTunnel
  - Dialer
  - Ethernet
  - FastEthernet
  - Lex
  - Loopback
  - Multilink
  - Null
  - Serial
  - Tunnel
  - Vif
  - Virtual-Template
  - Virtual-TokenRing

**Example:**

Router(conf-serv-sip)# `bind all source-interface fastethernet`
Verifying and Troubleshooting Tips

Two `show` commands verify the correct settings for the `bind` command. The first enables you to verify a bound IP address. The second indicates the status of bind (enabled or disabled):

- **Verifying a Bound IP Address**
- **Verifying Bind Status**

**Verifying a Bound IP Address**

The following examples show output for the `show ip socket` command, indicating that the bind address of the receiving gateway is set:

```
Router# show ip socket
Proto    Remote      Port    Local      Port    In  Out  Stat  TTY  OutputIF
17       0.0.0.0      0       --any--    2517    0   0    9   0
17       --listen--  172.18.192.204 1698    0   0    1   0
17       0.0.0.0      0       172.18.192.204 67      0   0    489  0
17       0.0.0.0      0       172.18.192.204 5060    0   0    A1   0
```

**Verifying Bind Status**

The following example shows output for the `show sip-ua status` command, indicating that bind is enabled.

```
Router# show sip-ua status
SIP User Agent Status
SIP User Agent for UDP : ENABLED
SIP User Agent for TCP : ENABLED
SIP User Agent bind status(signaling): ENABLED 172.18.192.204
SIP User Agent bind status(media): ENABLED 172.18.192.204
SIP max-forwards : 6
SIP DNS SRV version: 1 (rfc 2052)
```
To troubleshoot this feature, perform the following:

- Use the `debug ccsip all` command to enable all SIP debugging capabilities, or use one of the following SIP debug commands:
  - `debug ccsip calls`
  - `debug ccsip error`
  - `debug ccsip events`
  - `debug ccsip messages`
  - `debug ccsip states`
- Use the `show ip socket` command to display IP socket information.
- Use the `show sip-ua status` command to verify if binding is enabled. See the `show sip-ua status` command for details.

**Configuration Examples for SIP — Gateway Support for the bind Command**

This section contains examples for SIP—Gateway Support for the bind Command feature:

- SIP—Gateway Support for the bind Command: Example, page 24

**SIP—Gateway Support for the bind Command: Example**

This section shows partial output from the `show running-config` command, indicating that bind is functional on receiving router 172.18.192.204.

```
ip subnet-zero
ip ftp source-interface Ethernet0
!
voice service voip
sip
  bind all source-interface FastEthernet0
!
interface FastEthernet0
  ip address 172.18.192.204 255.255.255.0
duplex auto
speed auto
fair-queue 64 256 1000
ip rsvp bandwidth 75000 100
!!
```
Table 1 lists the release history for this chapter.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which 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 1 lists only the Cisco IOS software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
</table>
| SIP—Gateway Support for the bind Command | 12.2(8)T  
12.3(2)T  
12.2(11)T  
12.2(15)T | This feature allows you to configure the source IP address of signaling packets, or configure both signaling and media packets.  
The following commands were introduced or modified: bind and sip. |
| SIP-to-SIP Basic Functionality | 12.2(13)T3  
12.3(7)T | This feature provides termination and reorigination of both signaling and media between VoIP and video networks using SIP signaling in conformance with RFC3261.  
The following commands were introduced or modified: allow-connections |
| SIP-to-SIP Extended Feature Functionality for Session Border Controllers | 12.4(6)T | The SIP-to-SIP Extended Feature Functionality for Session Border Controllers (SBCs) enables the SIP-to-SIP functionality to conform with RFC 3261 to interoperate with SIP User Agents (UAs).  
This feature includes the following:  
• TCP and UDP interworking  
This feature uses no new or modified commands. |
| Cisco Unified Border Element and Cisco Unified Communications Manager Express Support for Universal Packaging | 15.0(1)M | This introduces the mode border-element command to distinguish between Cisco Unified Communications Manager Express and Cisco UBE configuration.  
The following command was introduced: mode border-element. |
| Configuring an Inbound Dial-peer to Match the URI on SIP Calls | — | Expands the inbound dial-peer matching logic to include matching based on the source IP address of inbound signaling on a SIP trunk. |
This Cisco Unified Border Element is a special Cisco IOS software image; 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.

**Activation**

Cisco Product Authorization Key (PAK)—A Product Authorization Key (PAK) is required to configure some of the features described in this guide. Before you start the configuration process, please register your products and activate your PAK at the following URL http://www.cisco.com/go/license.

**Finding Feature Information**

For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the “Cisco Unified Border Element Features Roadmap” section on page 3.

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.
Cisco Unified Border Element Protocol-Independent Features and Setup

This chapter contains the following configuration topics:

Cisco UBE Prerequisites and Restrictions
- Prerequisites for Cisco Unified Border Element
- Restrictions for Cisco Unified Border Element

Dial Plan Management
- ENUM Support
- Configuring Tool Command Language (Tcl)

Configuring Call Admission Control (CAC)
- VoIP Call Admissions Control
- VoIP Call Admission Control Using RSVP

RSVP
- Configuring RSVP Agent
- Interworking Between RSVP Capable and RSVP Incapable Networks

Dual-Tone Multifrequency (DTMF) Support and Interworking
- SIP—INFO Method for DTMF Tone Generation
- DTMF Events through SIP Signaling
- Configuring SIP DTMF Features
- H.323 RFC2833 - SIP NOTIFY

Codec Negotiation
- Support for Negotiation of an Audio Codec from a List of Codecs on Each Leg of a SIP-to-SIP Call on the Cisco Unified Border Element

Payload Type Interoperability
- Dynamic payload type interworking for DTMF and codec packets for SIP-to-SIP calls

Transcoding
- iLBC Support for SIP and H.323
- Universal Transcoding

Fax/modem Support
- Modem Passthrough
- T.38 Fax Relay
- Cisco Fax Relay
SIP Video
- Support for SIP Video Calls with Flow Around Media

Telepresence
- SIP Video Support for Telepresence Calls

Security Features
- Toll Fraud Prevention
- SIP—Ability to Send a SIP Registration Message on a Border Element
- SIP Parameter Modification
- SIP—SIP Stack Portability
- Transport Layer Security (TLS)
- Interworking of Secure RTP calls for SIP and H.323
- SIP SRTP Fallback to Nonsecure RTP
- Cisco Unified Communications Trusted Firewall

IPv4 and IPv6 Interworking
- VoIP for IPv6
  - IPv4 to IPv6 Calls (SIP and SIP)
  - IPv6 to IPv6 Calls (SIP and SIP)
  - Support for Dual Stack ANAT

RSVP Interworking
- Support for Interworking Between RSVP Capable and RSVP Incapable Networks

Collocated Services
- Media Termination Point (MTP)
- Cisco Unified SIP Survivable Remote Site Telephony (SRST)
- Cisco IOS Tcl IVR and VoiceXML Application Guide
- Cisco VoiceXML Programmer’s Guide
- Cisco Unified Communications Trusted Firewall
- Cisco Unified Border Element with Gatekeeper

Additional References

Glossary

Feature Information for Cisco UBE Protocol-Independent Features and Setup
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.
SIP-to-SIP Extended Feature Functionality for Session Border Controllers

The SIP-to-SIP Extended Feature Functionality for Session Border Controllers (SBCs) enables the SIP-to-SIP functionality to conform with RFC 3261 to interoperate with SIP User Agents (UAs). The SIP-to-SIP Extended Feature Functionality includes:

- Call Admission Control (based on CPU, memory, and total calls)
- Delayed Media Call
- ENUM support
- Configuring SIP Error Message Pass Through
- 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)

Prerequisites

**Cisco Unified Border Element**

- Cisco IOS Release 12.4(6)T or a later release must be installed and running on your Cisco Unified Border Element.

**Cisco Unified Border Element (Enterprise)**

- Cisco IOS XE Release 3.1S or a later release must be installed and running on your Cisco ASR 1000 Series Router.
Support for Interworking Between RSVP Capable and RSVP Incapable Networks

The Support for Interworking Between RSVP Capable and RSVP Incapable Networks feature provides precondition-based Resource Reservation Protocol (RSVP) support for basic audio call and supplementary services on Cisco Unified Border Element (UBE). This feature improves the interoperability between RSVP and non-RSVP networks. RSVP functionality added to Cisco UBE helps you to reserve the required bandwidth before making a call.

This feature extends RSVP support to delayed-offer to delayed-offer and delayed-offer to early-offer calls, along with the early-offer to early-offer calls.

Prerequisites

- RSVP policies allow you to configure separate bandwidth pools with varying limits so that any one application, such as video, can consume all the RSVP bandwidth on a specified interface at the expense of other applications, such as voice, which would be dropped.

- To limit bandwidth per application, you must configure a bandwidth limit before configuring Support for the Interworking Between RSVP Capable and RSVP Incapable Networks feature. See the “Configuring RSVP on an Interface” section on page 36.

Cisco Unified Border Element

- Cisco IOS Release 15.0(1)XA or a later release must be installed and running on your Cisco Unified Border Element.

Cisco Unified Border Element (Enterprise)

- Cisco IOS XE Release 3.1S or a later release must be installed and running on your Cisco ASR 1000 Series Router.

Restrictions

The Support for Interworking Between RSVP Capable and RSVP Incapable Networks feature has the following restrictions:

- Segmented RSVP is not supported.

- Interoperability between Cisco UBE and Cisco Unified Communications Manager is not available.

- RSVP-enabled video calls are not supported.

How to configure Interworking Between RSVP Capable and RSVP Incapable Networks

To enable support for Interworking Between RSVP Capable and RSVP Incapable Networks feature perform the steps in this section. This section contains the following subsections:

- Configuring RSVP on an Interface, page 36 (required)

- Configuring Optional RSVP on the Dial Peer, page 36 (optional)

- Configuring Mandatory RSVP on the Dial Peer, page 38 (optional)

- Configuring Midcall RSVP Failure Policies, page 39 (optional)

- Configuring DSCP Values, page 40 (optional)
Configuring an Application ID, page 41 (optional)
Configuring Priority, page 42 (optional)

Configuring RSVP on an Interface

You must allocate some bandwidth for the interface before enabling RSVP. Perform this task to configure RSVP on an interface.

SUMMARY STEPS

1. enable
2. configure terminal
3. interface type slot/port
4. ip rsvp bandwidth [reservable-bw [max-reservable-bw] [sub-pool reservable-bw]]
5. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface type slot/port</td>
<td>Configures an interface type and enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# interface FastEthernet 0/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> ip rsvp bandwidth [reservable-bw [max-reservable-bw] [sub-pool reservable-bw]]</td>
<td>Enables RSVP for IP on an interface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# ip rsvp bandwidth 10000 100000</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>(Optional) Exits interface configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# end</td>
<td></td>
</tr>
</tbody>
</table>

Configuring Optional RSVP on the Dial Peer

Perform this task to configure optional RSVP at the dial peer level. This configuration allows you to have uninterrupted call even if there is a failure in bandwidth reservation.
SUMMARY STEPS

1. enable
2. configure terminal
3. dial-peer voice tag voip
4. no acc-qos {controlled-load | guaranteed-delay} [audio | video]
5. req-qos {controlled-load | guaranteed-delay} [audio | video] [bandwidth [default bandwidth-value] [max bandwidth-value]]
6. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 enable     | Enables privileged EXEC mode.  
| Example:          | • Enter your password if prompted. |
| Step 2 configure terminal | Enters global configuration mode. |
| Example:          | Router# configure terminal |
| Step 3 dial-peer voice tag voip | Enters dial peer voice configuration mode. |
| Example:          | Router(config)# dial-peer 77 voip |
| Step 4 no acc-qos {controlled-load | guaranteed-delay} [audio | video] | Removes any value configured for the acc-qos command.  
| Example:          | • Keywords are as follows:  
|                   | – controlled-load—Indicates that RSVP guarantees a single level of preferential service, presumed to correlate to a delay boundary. The controlled load service uses admission (or capacity) control to ensure that preferential service is received even when the bandwidth is overloaded.  
|                   | – guaranteed-delay—Indicates that RSVP reserves bandwidth and guarantees a minimum bit rate and preferential queueing if the bandwidth reserved is not exceeded. |
Configuring Mandatory RSVP on the Dial Peer

Perform this task to configure Mandatory RSVP on the dial peer. This configuration ensures that the call does not connect if sufficient bandwidth is not allocated.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `dial-peer voice tag voip`
4. `acc-qos {best-effort | controlled-load | guaranteed-delay} [audio | video]`
5. `req-qos {best-effort [audio | video] | {controlled-load | guaranteed-delay} [audio | video] [bandwidth [default bandwidth-value] [max bandwidth-value]]}
6. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> dial-peer voice tag voip</td>
<td>Enters dial peer voice configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# dial-peer 77 voip</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Midcall RSVP Failure Policies

Perform this task to enable call handling policies for a midcall RSVP failure.

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **dial-peer voice tag voip**
4. **voice-class sip rsvp-fail-policy {video | voice} post-alert {optional keep-alive | mandatory keep-alive | disconnect retry retry-attempts} | interval seconds**
5. **end**

---

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 4 **acc-qos {best-effort | controlled-load | guaranteed-delay} [audio | video]** | Configures mandatory RSVP on the dial-peer.  
  - Keywords are as follows:  
    - **best-effort**—Indicates that Resource Reservation Protocol (RSVP) makes no bandwidth reservation. This is the default.  
    - **controlled-load**—Indicates that RSVP guarantees a single level of preferential service, presumed to correlate to a delay boundary. The controlled load service uses admission (or capacity) control to ensure that preferential service is received even when the bandwidth is overloaded.  
    - **guaranteed-delay**—Indicates that RSVP reserves bandwidth and guarantees a minimum bit rate and preferential queueing if the bandwidth reserved is not exceeded. |
| Example:  
  Router(config-dial-peer)# acc-qos best-effort | |
| Step 5 **req-qos {best-effort [audio | video] | {controlled-load | guaranteed-delay} [audio | video] [bandwidth [default bandwidth-value] | [max bandwidth-value]]}** | Configures mandatory RSVP on the dial-peer.  
  - Calls continue even if there is a drop in the bandwidth reservation. |
| Example:  
  Router(config-dial-peer)# req-qos controlled-load | |
| Step 6 **end** |  
  - (Optional) Exits dial peer voice configuration mode and returns to privileged EXEC mode. |
| Example:  
  Router(config-dial-peer)# end | |
DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> dial-peer voice tag voip</td>
<td>Enters dial peer voice configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# dial-peer voice 66 voip</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> voice-class sip rsvp-fail-policy {video</td>
<td>voice} post-alert {optional keep-alive</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-dial-peer)# voice-class sip rsvp-fail-policy voice post-alert mandatory keep-alive interval 50</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>(Optional) Exits dial peer voice configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-dial-peer)# end</td>
<td></td>
</tr>
</tbody>
</table>

Configuring DSCP Values

Perform this task to configure different Differentiated Services Code Point (DSCP) values based on RSVP status.

SUMMARY STEPS

1. enable
2. configure terminal
3. dial-peer voice tag voip
4. ip qos dscp {dscp-value | set-af | set-cs | default | ef} {signaling | media | rsvp-pass | rsvp-fail} {video | rsvp-none | rsvp-pass | rsvp-fail} |
5. end
## Detailed Steps

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
*Enter your password if prompted.* |
| Router> enable    |                     |
| **Step 2** configure terminal | Enters global configuration mode. |
| **Example:**     |                     |
| Router# configure terminal |                     |
| **Step 3** dial-peer voice tag voip | Enters dial peer voice configuration mode. |
| **Example:**     |                     |
| Router(config)# dial-peer voice 66 voip |                     |
| **Step 4** ip qos dscp | Configures DSCP values based on RSVP status.  
*Keywords are as follows:*  
  - media rsvp-pass—Specifies that the DSCP value  
  applies to media packets with successful RSVP  
  reservations.  
  - media rsvp-fail—Specifies that the DSCP value  
  applies to packets (media or video) with failed  
  RSVP reservations.  
  - The default DSCP value for all media (voice and  
  fax) packets is ef.  
*Note* You must configure the DSCP values for all cases:  
media rsvp-pass and media rsvp-fail. |
| **Example:**     |                     |
| Router(config-dial-peer)# ip qos dscp af11 media rsvp-pass |                     |
| **Step 5** end   | (Optional) Exits dial peer voice configuration mode and  
returns to privileged EXEC mode. |
| **Example:**     |                     |
| Router(config-dial-peer)# end |                     |

## Configuring an Application ID

Perform this task to configure a specific application ID for RSVP establishment.

## Summary Steps

1. enable  
2. configure terminal  
3. dial-peer voice tag voip  
4. ip qos policy-locator {video | voice} [app app-string] [guid guid-string] [sapp subapp-string] [ver version-string]  
5. end
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> dial-peer voice tag voip</td>
<td>Enters dial peer voice configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# dial-peer voice 66 voip</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> ip qos policy-locator {voice</td>
<td>voice} [app app-string] [guid guid-string] [sapp subapp-string] [ver version-string]</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-dial-peer)# ip qos policy-locator voice</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>(Optional) Exits dial peer voice configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-dial-peer)# end</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring Priority

Perform this task to configure priorities for call preemption.

### SUMMARY STEPS

1. enable
2. configure terminal
3. dial-peer voice tag voip
4. ip qos defending-priority defending-pri-value
5. ip qos preemption-priority preemption-pri-value
6. end
DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Router&gt; enable</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> dial-peer voice tag voip</td>
<td>Enters dial peer voice configuration mode.</td>
</tr>
<tr>
<td>Example: Router(config)# dial-peer voice 66 voip</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> ip qos defending-priority defending-pri-value</td>
<td>Configures the RSVP defending priority value for determining QoS.</td>
</tr>
<tr>
<td>Example: Router(config-dial-peer)# ip qos defending-priority 66</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> ip qos preemption-priority preemption-pri-value</td>
<td>Configures the RSVP preemption priority value for determining QoS.</td>
</tr>
<tr>
<td>Example: Router(config-dial-peer)# ip qos preemption-priority 75</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> end</td>
<td>(Optional) Exits dial peer configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Router(config-dial-peer)# end</td>
<td></td>
</tr>
</tbody>
</table>

Troubleshooting the Support for Interworking Between RSVP Capable and RSVP Incapable Networks Feature

Use the following commands to debug any errors that you may encounter when you configure the Support for Interworking Between RSVP Capable and RSVP Incapable Networks feature.

- debug call rsvp-sync events
- debug call rsvp-sync func-trace
- debug ccsip all
- debug ccsip messages
- debug ip rsvp messages
- debug sccp all

Verifying Support for Interworking Between RSVP Capable and RSVP Incapable Networks

This task explains how to display information to verify the configuration for the Support for Interworking Between RSVP Capable and RSVP Incapable Networks feature. These commands need not be entered in any specific order.
### SUMMARY STEPS

1. enable
2. show sip-ua calls
3. show ip rsvp installed
4. show ip rsvp reservation
5. show ip rsvp interface detail \[interface-type number\]
6. show sccp connections details
7. show sccp connections rsvp
8. show sccp connections internal
9. show sccp \[all | connections | statistics\]

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  • Enter your password if prompted. |
<p>| Example: Router&gt; enable | |
| <strong>Step 2</strong> show sip-ua calls | (Optional) Displays active user agent client (UAC) and user agent server (UAS) information on SIP calls. |
| Example: Router# show sip-ua calls | |
| <strong>Step 3</strong> show ip rsvp installed | (Optional) Displays RSVP-related installed filters and corresponding bandwidth information. |
| Example: Router# show ip rsvp installed | |
| <strong>Step 4</strong> show ip rsvp reservation | (Optional) Displays RSVP-related receiver information currently in the database. |
| Example: Router# show ip rsvp reservation | |
| <strong>Step 5</strong> show ip rsvp interface detail [interface-type number] | (Optional) Displays the interface configuration for hello. |
| Example: Router# show ip rsvp interface detail GigabitEthernet 0/0 | |
| <strong>Step 6</strong> show sccp connections details | (Optional) Displays SCCP connection details, such as call-leg details. |
| Example: Router# show sccp connections details | |
| <strong>Step 7</strong> show sccp connections rsvp | (Optional) Displays information about active SCCP connections that are using RSVP. |
| Example: Router# show sccp connections rsvp | |</p>
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 8</strong> show sccp connections internal</td>
<td>(Optional) Displays the internal SCCP details, such as time-stamp values.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# show sccp connections internal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> show sccp [all</td>
<td>connections</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# show sccp statistics</td>
<td></td>
</tr>
</tbody>
</table>
SIP—INFO Method for DTMF Tone Generation

The SIP—INFO Method for DTMF Tone Generation feature uses the Session Initiation Protocol (SIP) INFO method to generate dual tone multifrequency (DTMF) tones on the telephony call leg. SIP info methods, or request message types, request a specific action be taken by another user agent (UA) or proxy server. The SIP INFO message is sent along the signaling path of the call. Upon receipt of a SIP INFO message with DTMF relay content, the gateway generates the specified DTMF tone on the telephony end of the call.

Prerequisites for SIP—INFO Method for DTMF Tone Generation

Cisco Unified Border Element

- Cisco IOS Release 12.2(11)T or a later release must be installed and running on your Cisco Unified Border Element.

Cisco Unified Border Element (Enterprise)

- Cisco IOS XE Release 2.5 or a later release must be installed and running on your Cisco ASR 1000 Series Router.

Information About SIP—INFO Method for DTMF Tone Generation

The SIP—INFO Method for DTMF Tone Generation feature is always enabled, and is invoked when a SIP INFO message is received with DTMF relay content. This feature is related to the DTMF Events Through SIP Signaling feature, which allows an application to be notified about DTMF events using SIP NOTIFY messages. Together, the two features provide a mechanism to both send and receive DTMF digits along the signaling path. For more information on sending DTMF event notification using SIP NOTIFY messages, refer to the DTMF Events Through SIP Signaling feature.

How to Review SIP INFO Messages

The SIP INFO method is used by a UA to send call signaling information to another UA with which it has an established media session. The following example shows a SIP INFO message with DTMF content:

```
INFO sip:2143302100@172.17.2.33 SIP/2.0
Via: SIP/2.0/UDP 172.80.2.100:5060
From: <sip:9724401003@172.80.2.100>;tag=43
To: <sip:2143302100@172.17.2.33>;tag=9753.0207
Call-ID: 984072_15401962@172.80.2.100
CSeq: 25634 INFO
Supported: 100rel
Supported: timer
Content-Length: 26
Content-Type: application/dtmf-relay

Signal= 1
Duration= 160
```

This sample message shows a SIP INFO message received by the gateway with specifics about the DTMF tone to be generated. The combination of the “From”, “To”, and “Call-ID” headers identifies the call leg. The signal and duration headers specify the digit, in this case 1, and duration, 160 milliseconds in the example, for DTMF tone play.
Prerequisites

The following are general prerequisites for SIP functionality:

- Ensure that the gateway has voice functionality that is configured for SIP.
- Establish a working IP network.
- Configure VoIP.

Restrictions

The SIP—INFO Method for DTMF Tone Generation feature includes the following signal duration parameters:

- Minimum signal duration is 100 milliseconds (ms). If a request is received with a duration less than 100 ms, the minimum duration of 100 ms is used by default.
- Maximum signal duration is 5000 ms. If a request is received with a duration longer than 5000 ms, the maximum duration of 5000 ms is used by default.
- If no duration parameter is included in a request, the gateway defaults to a signal duration of 250 ms.

Configuring for SIP—INFO Method for DTMF Tone Generation

You cannot configure, enable, or disable this feature. No configuration tasks are required to configure the SIP - INFO Method for DTMF Tone Generation feature. The feature is enabled by default.

Troubleshooting Tips

You can display SIP statistics, including SIP INFO method statistics, by using the `show sip-ua statistics` and `show sip-ua status` commands in privileged EXEC mode. See the following fields for SIP INFO method statistics:

- OkInfo 0/0, under SIP Response Statistics, Success, displays the number of successful responses to an INFO request.
- Info 0/0, under SIP Total Traffic Statistics, displays the number of INFO messages received and sent by the gateway.

The following is sample output from the `show sip-ua statistics` command:

```
Router# show sip-ua statistics

SIP Response Statistics (Inbound/Outbound)
  Informational:
    Trying 1/1, Ringing 0/0,
    Forwarded 0/0, Queued 0/0,
    SessionProgress 0/1
  Success:
    OkInvite 0/1, OkBye 1/0,
    OkCancel 0/0, OkOptions 0/0,
    OkPrack 0/0, OkPreconditionMet 0/0
    OkSubscribe 0/0, OkNotify 0/0,
    OkInfo 0/0, 202Accepted 0/0
  Redirection (Inbound only):
    MultipleChoice 0, MovedPermanently 0,
    MovedTemporarily 0, SeeOther 0,
    UseProxy 0, AlternateService 0
  Client Error:
```
BadRequest 0/0, Unauthorized 0/0,
PaymentRequired 0/0, Forbidden 0/0,
NotFound 0/0, MethodNotAllowed 0/0,
NotAcceptable 0/0, ProxyAuthReqd 0/0,
ReqTimeout 0/0, Conflict 0/0, Gone 0/0,
LengthRequired 0/0, ReqEntityTooLarge 0/0,
ReqURITooLarge 0/0, UnsupportedMediaType 0/0,
BadExtension 0/0, TempNotAvailable 0/0,
CallLegNonExistent 0/0, LoopDetected 0/0,
TooManyHops 0/0, AddrIncomplete 0/0,
Ambiguous 0/0, BusyHere 0/0,
BadEvent 0/0
Server Error:
   InternalError 0/0, NotImplemented 0/0,
   BadGateway 0/0, ServiceUnavail 0/0,
   GatewayTimeout 0/0, BadSipVer 0/0
Global Failure:
   BusyEverywhere 0/0, Decline 0/0,
   NotExistAnywhere 0/0, NotAcceptable 0/0
SIP Total Traffic Statistics (Inbound/Outbound)
   Invite 0/0, Ack 0/0, Bye 0/0,
   Cancel 0/0, Options 0/0,
   Prack 0/0, Comet 0/0,
   Subscribe 0/0, Notify 0/0,
   Refer 0/0, Info 0/0
Retry Statistics
   Invite 0, Bye 0, Cancel 0, Response 0, Notify 0

The following is sample output from the show sip-ua status command:
Router# show sip-ua status

SIP User Agent Status
SIP User Agent for UDP : ENABLED
SIP User Agent for TCP : ENABLED
SIP User Agent bind status(signaling) : DISABLED
SIP User Agent bind status(media) : DISABLED
SIP max-forwards : 6
SIP DNS SRV version: 2 (rfc 2782)
SDP application configuration:
   Version line (v=) required
   Owner line (o=) required
   Session name line (s=) required
   Timespec line (t=) required
   Media supported: audio image
   Network types supported: IN
   Address types supported: IP4
   Transport types supported: RTP/AVP udptl
DTMF Events through SIP Signaling

The DTMF Events through SIP Signaling feature provides the following:

- DTMF event notification for SIP messages.
- Capability of receiving hookflash event notification through the SIP NOTIFY method.
- Third-party call control, or other signaling mechanisms, to provide enhanced services, such as calling card and messaging services.
- Communication with the application outside of the media connection.

The DTMF Events through SIP Signaling feature allows telephone event notifications to be sent through SIP NOTIFY messages, using the SIP SUBSCRIBE/NOTIFY method as defined in the Internet Engineering Task Force (IETF) draft, SIP-Specific Event Notification.

The feature also supports sending DTMF notifications based on the IETF draft: Signaled Telephony Events in the Session Initiation Protocol (SIP) (draft-mahy-sip-signaled-digits-01.txt).

Prerequisites

Cisco Unified Border Element

- Cisco IOS Release 12.2(11)T or a later release must be installed and running on your Cisco Unified Border Element.

Cisco Unified Border Element (Enterprise)

- Cisco IOS XE Release 2.5 or a later release must be installed and running on your Cisco ASR 1000 Series Router.

Restrictions

The DTMF Events through SIP Signaling feature adds support for sending telephone-event notifications via SIP NOTIFY messages from a SIP gateway. The events for which notifications are sent out are DTMF events from the local Plain Old Telephone Service (POTS) interface on the gateway. Notifications are not sent for DTMF events received in the Real-Time Transport Protocol (RTP) stream from the recipient user agent.

Configuring DTMF Events through SIP Signaling

To configure the DTMF Events through SIP Signaling feature, perform the following steps.

SUMMARY STEPS

1. enable
2. configure terminal
3. sip-ua
4. timers notify number
5. retry notify number
6. exit
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enters privileged EXEC mode or any other security level set by a system administrator.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router&gt; enable</code></td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> sip-ua</td>
<td>Enters SIP user-agent configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config)# sip-ua</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> timers notify number</td>
<td>Sets the amount of time that the user agent waits before retransmitting the Notify message. The argument is as follows:</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config-sip-ua)# timers notify 100</code></td>
<td><code>number</code>—Time, in milliseconds, to wait before retransmitting. Range: 100 to 1000. Default: 500.</td>
</tr>
<tr>
<td><strong>Step 5</strong> retry notify number</td>
<td>Sets the number of times that the Notify message is retransmitted to the user agent that initiated the transfer or Refer request. The argument is as follows:</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config-sip-ua)# retry notify 6</code></td>
<td><code>number</code>—Number of retries. Range: 1 to 10. Default: 10.</td>
</tr>
<tr>
<td><strong>Step 6</strong> exit</td>
<td>Exits the current mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config-sip-ua)# exit</code></td>
<td></td>
</tr>
</tbody>
</table>

### Verifying SIP DTMF Support

To verify SIP DTMF support, perform the following steps as appropriate (commands are listed in alphabetical order).

### SUMMARY STEPS

1. show running-config
2. show sip-ua retry
3. show sip-ua statistics
4. show sip-ua status
5. show sip-ua timers
6. show voip rtp connections
7. show sip-ua calls
DETAILED STEPS

Step 1  show running-config

Use this command to show dial-peer configurations.

The following sample output shows that the `dtmf-relay sip-notify` command is configured in dial peer 123:

Router# `show running-config`

```
show running-config

dial-peer voice 123 voip
  destination-pattern [12]...
  monitor probe icmp-ping
  session protocol sipv2
  session target ipv4:10.8.17.42
  dtmf-relay sip-notify
```

The following sample output shows that DTMF relay and NTE are configured on the dial peer.

Router# `show running-config`

```
show running-config

! dial-peer voice 1000 pots
  destination-pattern 4961234
  port 1/0/0
!
! dial-peer voice 2000 voip
  application session
  destination-pattern 4965678
  session protocol sipv2
  session target ipv4:192.0.2.34
  dtmf-relay rtp-nte
  ! RTP payload type value = 101 (default)
!
! dial-peer voice 3000 voip
  application session
  destination-pattern 2021010101
  session protocol sipv2
  session target ipv4:192.0.2.34
  dtmf-relay rtp-nte
  rtp payload-type nte 110
  ! RTP payload type value = 110 (user assigned)
```

Step 2  show sip-ua retry

Use this command to display SIP retry statistics.

Router# `show sip-ua retry`

```
SIP UA Retry Values
  invite retry count = 6  response retry count = 1
  bye retry count = 1  cancel retry count = 1
  prack retry count = 10  comet retry count = 10
  reliable 1xx count = 6  notify retry count = 10
```

Step 3  show sip-ua statistics

Use this command to display response, traffic, and retry SIP statistics.
Tip

To reset counters for the show sip-ua statistics display, use the clear sip-ua statistics command.

Router# show sip-ua statistics

SIP Response Statistics (Inbound/Outbound)
  Informational:
    Trying 4/2, Ringing 2/1,
    Forwarded 0/0, Queued 0/0,
    SessionProgress 0/0
  Success:
    OkInvite 1/2, OkBye 0/1,
    OkCancel 1/0, OkOptions 0/0,
    OkPrack 2/0, OkPreconditionMet 0/0,
  OkNotify 1/0, 202Accepted 0/1
  Redirection (Inbound only):
    MultipleChoice 0, MovedPermanently 0,
    MovedTemporarily 0, SeeOther 0,
    UseProxy 0, AlternateService 0
  Client Error:
    BadRequest 0/0, Unauthorized 0/0,
    PaymentRequired 0/0, Forbidden 0/0,
    NotFound 0/0, MethodNotAllowed 0/0,
    NotAcceptable 0/0, ProxyAuthReqd 0/0,
    ReqTimeOut 0/0, Conflict 0/0, Gone 0/0,
    LengthRequired 0/0, ReqEntityTooLarge 0/0,
    ReqURITooLarge 0/0, UnsupportedMediaType 0/0,
    BadExtension 0/0, TempNotAvailable 0/0,
    CallLegNonExistent 0/0, LoopDetected 0/0,
    TooManyHops 0/0, AddrIncomplete 0/0,
    Ambiguous 0/0, BusyHere 0/0
  RequestCancel 1/0, NotAcceptableMedia 0/0
  Server Error:
    InternalError 0/1, NotImplemented 0/0,
    BadGateway 0/0, ServiceUnavailable 0/0,
    GatewayTimeout 0/0, BadSipVer 0/0,
    PreCondFailure 0/0
  Global Failure:
    BusyEverywhere 0/0, Decline 0/0,
    NotExistentAnywhere 0/0, NotAcceptable 0/0
  SIP Total Traffic Statistics (Inbound/Outbound) /* Traffic Statistics
    Invite 3/2, Ack 3/2, Bye 1/0,
    Cancel 0/1, Options 0/0,
    Prack 0/2, Comet 0/0,

Following is sample output verifying configuration of the SIP INFO Method for DTMF Tone Generation feature:

Router# show sip-ua statistics

SIP Response Statistics (Inbound/Outbound)
  Informational:
    Trying 1/1, Ringing 0/0,
    Forwarded 0/0, Queued 0/0,
    SessionProgress 0/1
  Success:
    OkInvite 0/1, OkBye 1/0,
Step 4  show sip-ua status

Use this command to display status for the SIP user agent.

Router# show sip-ua status

SIP User Agent Status
SIP User Agent for UDP : ENABLED
SIP User Agent for TCP : ENABLED
SIP User Agent bind status(signaling): DISABLED
SIP User Agent bind status(media): DISABLED
SIP max-forwards : 6
SIP DNS SRV version: 2 (rfc 2782)
SDP application configuration:
  Version line (v=) required
  Owner line (o=) required
  Session name line (s=) required
  Timespec line (t=) required
  Media supported: audio image
  Network types supported: IN
  Address types supported: IP4
  Transport types supported: RTP/AVP udpl

The following sample output shows that the time interval between consecutive NOTIFY messages for a telephone event is the default of 2000 ms:

Router# show sip-ua status
SIP User Agent Status
SIP User Agent for UDP : ENABLED
SIP User Agent for TCP : ENABLED
SIP User Agent bind status(signaling): DISABLED
SIP User Agent bind status(media): DISABLED
SIP early-media for 180 responses with SDP: ENABLED
SIP max-forwards : 6
SIP DNS SRV version: 2 (rfc 2782)
NAT Settings for the SIP-UA
Role in SDP: NONE
Check media source packets: DISABLED
Maximum duration for a telephone-event in NOTIFYs: 2000 ms
SIP support for ISDN SUSPEND/RESUME: ENABLED
Redirection (3xx) message handling: ENABLED

SDP application configuration:
Version line (v=) required
Owner line (o=) required
Timespec line (t=) required
Media supported: audio image
Network types supported: IN
Address types supported: IP4
Transport types supported: RTP/AVP udptl

The following sample output shows configuration of the SIP INFO Method for DTMF Tone Generation feature:

Router# show sip-ua status

SIP User Agent Status
SIP User Agent for UDP : ENABLED
SIP User Agent for TCP : ENABLED
SIP User Agent bind status(signaling): DISABLED
SIP User Agent bind status(media): DISABLED
SIP max-forwards : 6
SIP DNS SRV version: 2 (rfc 2782)
SDP application configuration:
Version line (v=) required
Owner line (o=) required
Session name line (s=) required
Timespec line (t=) required
Media supported: audio image
Network types supported: IN
Address types supported: IP4
Transport types supported: RTP/AVP udptl

Step 5 show sip-ua timers

Use this command to display the current settings for SIP user-agent timers.

Router# show sip-ua timers

SIP UA Timer Values (milliseconds)
trying 500, expires 300000, connect 500, disconnect 500
comet 500, prack 500, rel1xx 500, notify 500

Step 6 show voip rtp connections

Use this command to show local and remote Calling ID and IP address and port information.

Step 7 show sip-ua calls

Use this command to ensure the DTMF method is SIP-KPML.

The following sample output shows that the DTMF method is SIP-KPML.
router# show sip-ua calls

SIP UAC CALL INFO

Call 1
SIP Call ID : 57633F68-2BE011D6-B013D46B-B4F9B5F60172.18.193.251
State of the call : STATE_ACTIVE (7)
Substate of the call : SUBSTATE_NONE (0)
Calling Number :
Called Number : 8888
Bit Flags : 0xD44018 0x100 0x0
CC Call ID : 6
Source IP Address (Sig ) : 192.0.2.1
Destn SIP Req Addr:Port : 192.0.2.1:5060
Destn SIP Resp Addr:Port : 192.0.2.3:5060
Destination Name : 192.0.2.4.250
Number of Media Streams : 1
Number of Active Streams: 1
RTP Fork Object : 0x0
Media Mode : flow-through
Media Stream 1
State of the stream : STREAM_ACTIVE
Stream Call ID : 6
Stream Type : voice-only (0)
Negotiated Codec : g711ulaw (160 bytes)
Codec Payload Type : 0
Negotiated Dtmf-relay : sip-kpml
Dtmf-relay Payload Type : 0
Media Source IP Addr:Port : 192.0.2.5:17576
Media Dest IP Addr:Port : 192.0.2.6:17468
Orig Media Dest IP Addr:Port : 0.0.0.0:0

Number of SIP User Agent Client(UAC) calls: 1

SIP UAS CALL INFO

Number of SIP User Agent Server(UAS) calls: 0

Troubleshooting Tips

- To enable debugging for RTP named-event packets, use the `debug voip rtp` command.
- To enable KPML debugs, use the `debug kpml` command.
- To enable SIP debugs, use the `debug ccsip` command.
- Collect debugs while the call is being established and during digit presses.
- If an established call is not sending digits through KPML, use the `show sip-ua calls` command to ensure SIP-KPML is included in the negotiation process.
Support for Negotiation of an Audio Codec from a List of Codecs on Each Leg of a SIP-to-SIP Call on the Cisco Unified Border Element

The Support for Negotiation of an Audio Codec from a List of Codecs on Each Leg of a SIP-to-SIP Call on the Cisco Unified Border Element feature supports negotiation of an audio codec using the Voice Class Codec and Codec Transparent infrastructure on the Cisco Unified Border Element (Cisco UBE).

Benefits

Following are the benefits of the Support for Negotiation of an Audio Codec from a List of Codecs on Each Leg of a SIP-to-SIP Call on the Cisco Unified Border Element feature:

- You can configure dissimilar Voice Class Codec configurations on the incoming and outgoing dial peers.
- Both normal transcoding and high-density transcoding are supported with the Voice Class Codec configuration.
- Mid-call codec changes for supplementary services are supported with the Voice Class Codec configuration. Transcoder resources are dynamically inserted or deleted when required.
- Reinvite-based supplementary services invoked from the Cisco Unified Communications Manager (CUCM), like call hold, call resume, music on hold (MOH), call transfer, and call forward are supported with the Voice Class Codec configuration.
- T.38 fax and fax passthru switchover with Voice Class Codec configuration are supported.
- Reinvite-based call hold and call resume for Secure Real-Time Transfer protocol (SRTP) and Real-Time Protocol (RTP) interworking on Cisco UBE are supported with the Voice Class Codec configuration.

Prerequisites

To configure Support for Negotiation of an Audio Codec from a List of Codecs on Each Leg of a SIP-to-SIP Call on the Cisco Unified Border Element feature you must know the following:

- Transcoding configuration on the Cisco UBE.
- The digital signal processor (DSP) requirements to support the transcoding feature on the Cisco UBE.
- The existing Voice Class Codec configuration on the dial peers.

Cisco Unified Border Element

- Cisco IOS Release 15.1(2)T or a later release must be installed and running on your Cisco Unified Border Element.

Cisco Unified Border Element (Enterprise)

- Cisco IOS XE Release 2.5 or a later release must be installed and running on your Cisco ASR 1000 Series Router.

Restrictions

The Support for Negotiation of an Audio Codec from a List of Codecs on Each Leg of a SIP-to-SIP Call on the Cisco Unified Border Element feature has the following limitations:
- Mid-call insertion or deletion of the transcoder with voice class codec for H323-H323 and H323-SIP is not supported.
- Voice class codec is not supported for video calls.

**Disabling Codec Filtering**

Cisco UBE is configured to filter common codecs for the subsets, by default. The filtered codecs are sent in the outgoing offer. You can configure the Cisco UBE to offer all the codecs configured on an outbound leg instead of offering only the filtered codecs.

**Note**

This configuration is applicable only for early offer calls from the Cisco UBE. For delayed offer calls, by default all codecs are offered irrespective of this configuration.

Perform this task to disable codec filtering and allow all the codecs configured on an outbound leg.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `dial-peer voice tag voip`
4. `voice-class codec tag [offer-all]`
5. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router&gt; enable</code></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>dial-peer voice tag voip</code></td>
<td>Enters dial peer voice configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router(config)# dial-peer voice 10 voip</code></td>
<td></td>
</tr>
</tbody>
</table>
Command or Action | Purpose
--- | ---
**Step 4** | voice-class codec tag [offer-all]
**Example:**
Router(config-dial-peer)# voice-class codec 10 offer-all
| Adds all the configured voice class codec to the outgoing offer from the Cisco UBE.

**Step 5** | end
**Example:**
Router(config-dial-peer)# end
| Exits the dial peer voice configuration mode.

Troubleshooting Support for Negotiation of an Audio Codec from a List of Codecs on Each Leg of a SIP-to-SIP Call on the Cisco Unified Border Element

Use the following commands to debug any errors that you may encounter when you configure the Support for Negotiation of an Audio Codec from a List of Codecs on Each Leg of a SIP-to-SIP Call on the Cisco Unified Border Element feature:

- debug ccsip all
- debug voip ccapi input
- debug sccp messages
- debug voip rtp session

Verifying Support for Negotiation of an Audio Codec from a List of Codecs on Each Leg of a SIP-to-SIP Call on the Cisco Unified Border Element

Perform this task to display information to verify Support for Negotiation of an Audio Codec from a List of Codecs on Each Leg of a SIP-to-SIP Call on the Cisco Unified Border Element configuration. These show commands need not be entered in any specific order.

**SUMMARY STEPS**

1. enable
2. show call active voice brief
3. show voip rtp connections
4. show sccp connections
5. show dspfarm dsp active

**DETAILED STEPS**

**Step 1** | enable
Enables privileged EXEC mode.

**Step 2** | show call active voice brief
Displays a truncated version of call information for voice calls in progress.

Router# show call active voice brief
IP   192.0.2.1:19304   SRTP: off   rtt:0ms   pl:0/0ms   lost:0/0/0   delay:0/0/0ms   g711ulaw   TextRelay: off   media inactive detected:n media cntrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a
1243 : 12 971500ms.1 + -1 pid:2 Originate 3210000 connected
dur 00:00:00 tx:5/10 rx:4/8
IP  9.44.26.4:16512  SRTP: off  rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g729br8 TextRelay: off
media inactive detected:n media cntrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a
0    : 13 971560ms.1 +0 pid:0 Originate  connecting
dur 00:00:08 tx:415/66400 rx:17/2561
IP 192.0.2.2:2000 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off
media inactive detected:n media cntrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a
0    : 15 971570ms.1 +0 pid:0 Originate  connecting
dur 00:00:08 tx:5/10 rx:3/6
IP 192.0.2.3:2000 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g729br8 TextRelay: off
media inactive detected:n media cntrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a

Telephony call-legs: 0
SIP call-legs: 2
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 2
Multicast call-legs: 0
Total call-legs: 4
1243 : 11 971490ms.1 + -1 pid:1 Answer 1230000 connecting
dur 00:00:00 tx:415/66400 rx:17/2561
IP 192.0.2.1:19304 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off
media inactive detected:n media cntrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a
1243 : 12 971500ms.1 + -1 pid:2 Originate 3210000 connected
dur 00:00:00 tx:5/10 rx:4/8
IP  9.44.26.4:16512  SRTP: off  rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g729br8 TextRelay: off
media inactive detected:n media cntrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a
0    : 13 971560ms.1 +0 pid:0 Originate  connecting
dur 00:00:08 tx:415/66400 rx:17/2561
IP 192.0.2.2:2000 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off
media inactive detected:n media cntrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a
0    : 15 971570ms.1 +0 pid:0 Originate  connecting
dur 00:00:08 tx:5/10 rx:3/6
IP 192.0.2.3:2000 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g729br8 TextRelay: off
media inactive detected:n media cntrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a

Telephony call-legs: 0
SIP call-legs: 2
H323 call-legs: 0
Step 3  **show voip rtp connections**

Displays Real-Time Transport Protocol (RTP) connections.

```
Router# show voip rtp connections
VoIP RTP active connections :
No. CallId     dstCallId  LocalRTP RmtRTP     LocalIP       RemoteIP
 1     11         12         16662    19304    192.0.2.1 192.0.2.2
 2     12         11         17404    16512    192.0.2.2 192.0.2.2
 3     13         14         18422    2000     192.0.2.4 9.44.26.3
 4     15         14         16576    2000     192.0.2.6 192.0.2.5
Found 4 active RTP connections
```

Step 4  **show sccp connections**

Displays information about the connections controlled by the Skinny Client Control Protocol (SCCP) transcoding and conferencing applications.

```
Router# show sccp connections
sess_id    conn_id      stype mode     codec   sport rport ripaddr
 5          5            xcode sendrecv g729b   16576 2000  192.0.2.3
 5          6            xcode sendrecv g711u   18422 2000  192.0.2.4
Total number of active session(s) 1, and connection(s) 2
```

Step 5  **show dspfarm dsp active**

Displays active DSP information about the DSP farm service.

```
Router# show dspfarm dsp active
SLOT DSP VERSION  STATUS CHNL USE   TYPE    RSC_ID BRIDGE_ID PKTS_TXED PKTS_RXED
 0    1   27.0.201 UP     1    USED  xcode   1      0x9         5         8
 0    1   27.0.201 UP     1    USED  xcode   1      0x8      2558      17
Total number of DSPFARM DSP channel(s) 1
```
Support for Dynamic Payload Type Interworking for DTMF and Codec Packets for SIP-to-SIP Calls

The Support for Dynamic Payload Type Interworking for DTMF and Codec Packets for SIP-to-SIP Calls feature provides dynamic payload type interworking for dual tone multifrequency (DTMF) and codec packets for Session Initiation Protocol (SIP) to SIP calls.

Based on this feature, the Cisco Unified Border Element (Cisco UBE) interworks between different dynamic payload type values across the call legs for the same codec. Also, Cisco UBE supports any payload type value for audio, video, named signaling events (NSEs), and named telephone events (NTEs) in the dynamic payload type range 96 to 127.

Symmetric and Asymmetric Calls

Cisco UBE supports dynamic payload type negotiation and interworking for all symmetric and asymmetric payload type combinations. A call leg on Cisco UBE is considered as symmetric or asymmetric based on the payload type value exchanged during the offer and answer with the endpoint:

- A symmetric endpoint accepts and sends the same payload type.
- An asymmetric endpoint can accept and send different payload types.

The Support for Dynamic Payload Type Interworking for DTMF and Codec Packets for SIP-to-SIP Calls feature is enabled by default for a symmetric call. An offer is sent with a payload type based on the dial-peer configuration. The answer is sent with the same payload type as was received in the incoming offer. When the payload type values negotiated during the signaling are different, the Cisco UBE changes the Real-Time Transport Protocol (RTP) payload value in the VoIP to RTP media path.

To support asymmetric call legs, you must enable The Support for Dynamic Payload Type Interworking for DTMF and Codec Packets for SIP-to-SIP Calls feature. The dynamic payload type value is passed across the call legs, and the RTP payload type interworking is not required. The RTP payload type handling is dependent on the endpoint receiving them.

Prerequisites

Cisco Unified Border Element

- Cisco IOS Release 15.0(1)XA or a later release must be installed and running on your Cisco Unified Border Element.

Cisco Unified Border Element (Enterprise)

- Cisco IOS XE Release 3.1S or a later release must be installed and running on your Cisco ASR 1000 Series Router.
Restrictions

The Support for Dynamic Payload Type Interworking for DTMF and Codec Packets for SIP-to-SIP Calls feature is not supported for the following:

- H323-to-H323 and H323-to-SIP calls.
- All transcoded calls.
- Secure Real-Time Protocol (SRTP) pass-through calls.
- Flow-around calls.
- Asymmetric payload types are not supported on early-offer (EO) call legs in a delayed-offer to early-offer (DO-EO) scenario.
- Multiple $m$ lines with the same dynamic payload types, where $m$ is:
  
  \[
  m = \text{audio <media-port1> RTP/AVP XXX} \\
  m = \text{video <media-port2> RTP/AVP XXX}
  \]

How to Configure Dynamic Payload Type Interworking for DTMF and Codec Packets for SIP-to-SIP Calls

The configuration tasks for this feature are presented in the following sections:

- Configuring Dynamic Payload Support at the Global Level, page 63
- Configuring Dynamic Payload Support for a Dial Peer, page 64
- Verifying Dynamic Payload Interworking for DTMF and Codec Packets Support, page 65
- Troubleshooting Tips, page 66

Configuring Dynamic Payload Support at the Global Level

Perform this task to configure the Support for Dynamic Payload Type Interworking for DTMF and Codec Packets for SIP-to-SIP Calls feature at the global level.

SUMMARY STEPS

1. enable
2. configure terminal
3. voice service voip
4. sip
5. asymmetric payload {dtmf | dynamic-codecs | full | system}
6. end
### Detailed Steps

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>enable</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>Example: Router&gt; enable</td>
</tr>
<tr>
<td></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>configure terminal</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>Example: Router# configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>voice service voip</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>Example: Router(config)# voice service voip</td>
</tr>
<tr>
<td></td>
<td>Enters voice service configuration mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>sip</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>Example: Router(config-voi-serv)# sip</td>
</tr>
<tr>
<td></td>
<td>Enters voice service SIP configuration mode.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>**asymmetric payload {dtmf</td>
</tr>
<tr>
<td>Example:</td>
<td>Example: Router(conf-serv-sip)# asymmetric payload full</td>
</tr>
<tr>
<td></td>
<td>Configures global SIP asymmetric payload support.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>end</strong></td>
</tr>
<tr>
<td>Example:</td>
<td>Example: Router(conf-serv-sip)# end</td>
</tr>
<tr>
<td></td>
<td>Exits voice service SIP configuration mode and enters privileged EXEC mode.</td>
</tr>
</tbody>
</table>

### Configuring Dynamic Payload Support for a Dial Peer

Perform this task to configure Support for Dynamic Payload Type Interworking for DTMF and Codec Packets for SIP-to-SIP Calls feature for a dial peer.

### Summary Steps

1. **enable**
2. **configure terminal**
3. **dial-peer voice tag voip**
4. **voice-class sip asymmetric payload {dtmf | dynamic-codecs | full | system}**
5. **end**
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  - Enter your password if prompted. |
| Example: Router> enable | |
| **Step 2** configure terminal | Enters global configuration mode. |
| Example: Router# configure terminal | |
| **Step 3** dial-peer voice tag voip | Enters dial peer voice configuration mode. |
| Example: Router(config)# dial-peer voice 77 voip | |
| **Step 4** voice-class sip asymmetric payload {dtmf | dynamic-codecs | full | system} | Configures the dynamic SIP asymmetric payload support.  
  **Note** The dtmf and dynamic-codecs keywords are internally mapped to the full keyword to provide asymmetric payload type support for audio and video codecs, DTMF, and NSEs. |
| Example: Router(config-dial-peer)# voice-class sip asymmetric payload full | |
| **Step 5** end | (Optional) Exits dial peer voice configuration mode and enters privileged EXEC mode. |
| Example: Router(config-dial-peer)# end | |

### Verifying Dynamic Payload Interworking for DTMF and Codec Packets Support

This task shows how to display information to verify Support for Dynamic Payload Type Interworking for DTMF and Codec Packets for SIP-to-SIP Calls configuration feature. These show commands need not be entered in any specific order.

### SUMMARY STEPS

1. enable
2. show call active voice compact
3. show call active voice
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> show call active voice compact</td>
<td>(Optional) Displays a compact version of call information.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# show call active voice compact</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> show call active voice</td>
<td>(Optional) Displays call information for voice calls in progress.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# show call active voice</td>
<td></td>
</tr>
</tbody>
</table>

### Troubleshooting Tips

Use the following commands to debug any errors that you may encounter when you configure the Support for Dynamic Payload Type Interworking for DTMF and Codec Packets for SIP-to-SIP Calls feature:

- `debug ccsip all`
- `debug voip ccapi inout`
- `debug voip rtp`
iLBC Support for SIP and H.323

The internet Low Bitrate Codec (iLBC) is a standard, high-complexity speech codec suitable for robust voice communication over IP. The iLBC has built-in error correction functionality that helps the codec perform in networks with high-packet loss. This codec is supported on both Session Initiation Protocol (SIP) and H.323.

Prerequisites

**Cisco Unified Border Element**
- Cisco IOS Release 12.2(11)T or a later release must be installed and running on your Cisco Unified Border Element.

**Cisco Unified Border Element (Enterprise)**
- Cisco IOS XE Release 2.5 or a later release must be installed and running on your Cisco ASR 1000 Series Router.

Restrictions

The iLBC Support for SIP and H.323 feature is supported on the following:
- IP-to-IP gateways with no transcoding and conferencing
- All c5510 DSP-based platforms

Information About iLBC Support for SIP and H.323

The internet Low Bit Rate Codec (iLBC) is designed for narrow band speech and results in a payload bit rate of 13.33 kbits per second for 30-millisecond (ms) frames and 15.20 kbits per second for 20 ms frames.

When the codec operates at block lengths of 20 ms, it produces 304 bits per block, which is packetized as defined in RFC 3952. Similarly, for block lengths of 30 ms it produces 400 bits per block, which is packetized as defined in RFC 3952.

The iLBC has built-in error correction functionality to provide better performance in networks with higher packet loss.

How to Configure an iLBC Codec

This section includes the following tasks:
- Configuring an iLBC Codec on a Dial Peer, page 68
- Configuring an iLBC Codec in the Voice Class, page 70

Configuring an iLBC Codec on a Dial Peer

The iLBC is intended for packet-based communication. Perform the following steps to configure the iLBC codec on a dial peer.
SUMMARY STEPS

1. enable
2. configure terminal
3. dial-peer voice tag voip
4. rtp payload-type cisco-codec-ilbc [number]
5. codec ilbc [mode frame_size [bytes payload_size]]
6. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> dial-peer voice tag voip</td>
<td>Enters dial-peer configuration mode for the VoIP dial peer designated by tag.</td>
</tr>
<tr>
<td>Example: Router(config)# dial-peer voice 10 voip</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> rtp payload-type cisco-codec-ilbc [number]</td>
<td>Identifies the payload type of a Real-Time Transport Protocol (RTP) packet. Keyword and argument are as follows:</td>
</tr>
<tr>
<td>Example: Router(config-dial-peer)# rtp payload-type cisco-codec-ilbc 100</td>
<td>• cisco-codec-ilbc [number]—Payload type is for internet Low Bit Rate Codec (iLBC). Range: 96 to 127. Default: 116.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Do not use the following numbers because they have preassigned values: 96, 97, 100, 117, 121 to 123, and 125 to 127. If you use these values, the command will fail. You must first reassign the value in use to a different unassigned number, for example:</td>
</tr>
<tr>
<td></td>
<td>rtp payload-type nse 105</td>
</tr>
<tr>
<td></td>
<td>rtp payload-type cisco-codec-ilbc 100</td>
</tr>
</tbody>
</table>
When using multiple codecs, you must create a voice class in which you define a selection order for codecs; then, you can apply the voice class to VoIP dial peers. The voice class codec global configuration command allows you to define the voice class that contains the codec selection order. Then, use the voice-class codec dial-peer configuration command to apply the class to individual dial peers.

To configure an iLBC codec in the voice class, perform the following steps.

You can configure more than one voice class codec list for your network. Configure the codec lists and apply them to one or more dial peers based on which codecs (and the order) you want supported for the dial peers. Define a selection order if you want more than one codec supported for a given dial peer.

### Command or Action

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>enable</td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>voice-class codec tag</td>
<td></td>
</tr>
</tbody>
</table>
| 4.     | codec preference value ilbc [mode frame_size] [bytes payload_size] | Specifies the voice coder rate of speech for a dial peer. Keywords and arguments are as follows:  
- `mode frame_size`—The iLBC operating frame mode that will be encapsulated in each packet. Valid entries are 20 (20ms frames for 15.2kbps bit rate) or 30 (30ms frames for 13.33 kbps bit rate). Default is 20.  
- `bytes payload_size`—Number of bytes in an RTP packet. For mode 20, valid values are 38 (default), 76, 114, 152, 190, and 228. For mode 30, valid values are 50 (default), 100, 150, and 200. |
| 5.     | exit              |         |
| 6.     | dial-peer voice tag voip |         |
| 7.     | voice-class codec tag |         |
| 8.     | exit              |         |

### Example:

Router(config-dial-peer)# codec ilbc mode 30 bytes 200

### Example:

Router(config-dial-peer)# exit

### Configuring an iLBC Codec in the Voice Class

When using multiple codecs, you must create a voice class in which you define a selection order for codecs; then, you can apply the voice class to VoIP dial peers. The voice class codec global configuration command allows you to define the voice class that contains the codec selection order. Then, use the voice-class codec dial-peer configuration command to apply the class to individual dial peers.

To configure an iLBC in the voice class for multiple-codec selection order, perform the following steps.

You can configure more than one voice class codec list for your network. Configure the codec lists and apply them to one or more dial peers based on which codecs (and the order) you want supported for the dial peers. Define a selection order if you want more than one codec supported for a given dial peer.

### SUMMARY STEPS

1. enable
2. configure terminal
3. voice-class codec tag
4. codec preference value ilbc [mode frame_size] [bytes payload_size]
5. exit
6. dial-peer voice tag voip
7. voice-class codec tag
8. exit
### Detailed Steps

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enters privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> voice class codec <strong>tag</strong></td>
<td>Enters voice-class configuration mode and assigns an identification tag number for a codec voice class. The argument is as follows:</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# voice class codec 99</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> codec preference <strong>value</strong> ilbc [mode frame_size] [bytes payload_size]</td>
<td>Specifies a list of preferred codecs to use on a dial peer. Keywords and arguments are as follows:</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-voice-class)# codec preference 1 ilbc 30 200</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> exit</td>
<td>Exits the current mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-voice-class)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> dial-peer voice <strong>tag</strong> voip</td>
<td>Enters dial-peer configuration mode for the specified VoIP dial peer.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# dial-peer voice 16 voip</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action | Purpose
--- | ---
**Step 7** voice-class codec tag | Assigns a previously configured codec selection preference list (the codec voice class that you defined in step 3) to the specified VoIP dial peer.

**Example:**
Router(config-dial-peer)# voice-class codec 99

**Note** The voice-class codec command in dial-peer configuration mode contains a hyphen. The voice class command in global configuration mode does not contain a hyphen.

**Step 8** exit | Exits the current mode.

**Example:**
Router(config-dial-peer)# exit

### Verifying iLBC Support for SIP and H.323

You can use the following commands to check iLBC status:

- show voice call summary
- show voice call status
- show voice dsmp stream
- show call active voice
- show call history voice
- show voice dsp and its extensions
- show dial-peer voice
- show voice dsp channel operational-status
Support for SIP Video Calls with Flow Around Media

This feature provides the ability to have a SIP video call where the media flows around the Cisco Unified Border Element (Cisco UBE) and the Cisco Unified Border Element (Enterprise) platform. Previous support was only for call scenarios where the media flowed through the Cisco UBE.

Prerequisites

**Cisco Unified Border Element**

- Cisco IOS Release 12.4(15)XZ or a later release must be installed and running on your Cisco Unified Border Element.

**Cisco Unified Border Element (Enterprise)**

- Cisco IOS XE Release 3.1S or a later release must be installed and running on your Cisco ASR 1000 Series Router.

Restrictions

- Media flow-around for Delayed-Offer to Early-Offer audio and video calls is not supported.

How to Configure Support for SIP Video Calls with Flow Around Media

To enable this feature so that media packets pass directly between endpoints without the intervention of the Cisco UBE, use the `media` command in dial peer, voice class, or voice service configuration mode. For detailed information on the use of this command, see the *Cisco IOS Voice Command Reference*. 
### SIP—Ability to Send a SIP Registration Message on a Border Element

The SIP—Ability to Send a SIP Registration Message on a Border Element feature allows users to register e164 numbers from the Cisco UBE without POTS dial-peers in the UP state. Registration messages can include numbers, number ranges (such as E.164-numbers), or text information.

### Prerequisites

- Configure a registrar in sip user-agent configuration mode.

**Cisco Unified Border Element**

- Cisco IOS Release 12.4(24)T or a later release must be installed and running on your Cisco Unified Border Element.

**Cisco Unified Border Element (Enterprise)**

- Cisco IOS XE Release 2.5 or a later release must be installed and running on your Cisco ASR 1000 Series Router.

### SUMMARY STEPS

1. enable
2. configure terminal
3. sip-ua
4. credentials username username password password realm domain-name
5. exit
6. end

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> sip-ua</td>
<td>Enters sip user-agent configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# sip-ua</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| **Step 4**

```text
credentials username username password password
realm domain-name
```

Enters SIP digest credentials in sip-ua configuration mode.

**Example:**
```text
Router(config-sip-ua)# credentials username alex password test realm cisco.com
```

| **Step 5**

```text
exit
```

Exits the current mode.

**Example:**
```text
Router(config-sip-ua)# exit
```

| **Step 6**

```text
end
```

Returns to privileged EXEC mode.

**Example:**
```text
Router(config)# end
```
SIP Parameter Modification

The SIP Parameter modification 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.

Prerequisites

Cisco Unified Border Element
- Cisco IOS Release 12.4(15)XZ or a later release must be installed and running on your Cisco Unified Border Element.

Cisco Unified Border Element (Enterprise)
- Cisco IOS XE Release 2.5 or a later release must be installed and running on your Cisco ASR 1000 Series Router.

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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | enable | Enables privileged EXEC mode.  
- Enter your password if prompted.  |
| **Example:** | Router> enable |
| **Step 2** | configure terminal | Enters global configuration mode. |
| **Example:** | Router# configure terminal |
| **Step 3** | voice service number voip | Enters VoIP voice-service configuration mode. |
| **Example:** | Router(config)# voice service 1 voip |
| **Step 4** | voice-class sip-profiles group-number | Establishes individual sip profiles defined by a group-number. Valid group-numbers are from 1 to 1000. |
| **Example:** | Router(config)# voice-class sip profiles 42 |
| **Step 5** | response option sip-header option ADD word CR | Add, change, or delete any SIP or SDP header in voice class or sip-profile submode. |
| **Example:** | Router(config)# request INVITE sip-header supported remove |
| **Step 6** | exit | Exits the current mode. |
| **Example:** | Router(config-dial-peer)# exit |
| **Step 7** | end | Returns to privileged EXEC mode. |
| **Example:** | Router(config-voi-srv)# end |

**Example**

```plaintext
!
!
!
voice service voip
allow-connections sip to sip
redirect ip2ip
sip
early-offer forced
mcdall-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"
!
!
!
SIP—SIP Stack Portability

Implements capabilities to the SIP gateway Cisco IOS stack involving user-agent handling of messages, handling of unsolicited messages, support for outbound delayed media, and SIP headers and content in requests and responses.

Prerequisites

Cisco Unified Border Element
• Cisco IOS Release 12.4(2)T or a later release must be installed and running on your Cisco Unified Border Element.

Cisco Unified Border Element (Enterprise)
• Cisco IOS XE Release 2.5 or a later release must be installed and running on your Cisco ASR 1000 Series Router.

Information About SIP—SIP Stack Portability

The SIP Stack Portability feature implements the following capabilities to the Cisco IOS SIP gateway stack:
• It receives inbound Refer message requests both within a dialog and outside of an existing dialog from the user agents (UAs).
• It sends and receives SUBSCRIBE or NOTIFY message requests via UAs.
• It receives unsolicited NOTIFY message requests without having to subscribe to the event that was generated by the NOTIFY message request.
• It supports outbound delayed media.
  It sends an INVITE message request without Session Description Protocol (SDP) and provides SDP information in either the PRACK or ACK message request for both initial call establishment and mid-call re-INVITE message requests.
• It sets SIP headers and content body in requests and responses.
  The stack applies certain rules and restrictions for a subset of headers and for some content types (such as SDP) to protect the integrity of the stack’s functionality and to maintain backward compatibility. When receiving SIP message requests, it reads the SIP header and any attached body without any restrictions.

To make the best use of SIP call-transfer features, you should understand the following concepts:
• SIP Call-Transfer Basics, page 81
SIP Call-Transfer Basics

This section contains the following information:
- Basic Terminology of SIP Call Transfer, page 81
- Types of SIP Call Transfer Using the Refer Message Request, page 84

Basic Terminology of SIP Call Transfer

Call transfer allows a wide variety of decentralized multiparty call operations. These decentralized call operations form the basis for third-party call control, and thus are important features for VoIP and SIP. Call transfer is also critical for conference calling, where calls can transition smoothly between multiple point-to-point links and IP-level multicasting.

Refer Message Request

The SIP Refer message request provides call-transfer capabilities to supplement the SIP BYE and ALSO message requests already implemented on Cisco IOS SIP gateways. The Refer message request has three main roles:
- Originator—User agent that initiates the transfer or Refer request.
- Recipient—User agent that receives the Refer request and is transferred to the final-recipient.
- Final-Recipient—User agent introduced into a call with the recipient.

Note: A gateway can be a recipient or final recipient, but not an originator.

The Refer message request always begins within the context of an existing call and starts with the originator. The originator sends a Refer request to the recipient (user agent receiving the Refer request) to initiate a triggered INVITE request. The triggered INVITE request uses the SIP URL contained in the Refer-To header as the destination of the INVITE request. The recipient then contacts the resource in the Refer-To header (final recipient), and returns a SIP 202 (Accepted) response to the originator. The recipient also must notify the originator of the outcome of the Refer transaction—whether the final recipient was successfully contacted or not. The notification is accomplished using the SIP NOTIFY message request, SIP’s event notification mechanism. A NOTIFY message with a message body of SIP 200 OK indicates a successful transfer, and a message body of SIP 503 Service Unavailable indicates an unsuccessful transfer. If the call was successful, a call between the recipient and the final recipient results.
Figure 1 represents the call flow of a successful Refer transaction initiated within the context of an existing call.

Refer-To Header
The recipient receives from the originator a Refer request that always contains a single Refer-To header. The Refer-To header includes a SIP URL that indicates the party to be invited and must be in SIP URL format.

Note
The TEL URL format cannot be used in a Refer-To header, because it does not provide a host portion, and without one, the triggered INVITE request cannot be routed.

The Refer-To header may contain three additional overloaded headers to form the triggered INVITE request. If any of these three headers are present, they are included in the triggered INVITE request. The three headers are:

- Accept-Contact—Optional in a Refer request. A SIP Cisco IOS gateway that receives an INVITE request with an Accept-Contact does not act upon this header. This header is defined in draft-ietf-sip-callerprefs-03.txt and may be used by user agents that support caller preferences.
- Proxy-Authorization—Nonstandard header that SIP gateways do not act on. It is echoed in the triggered INVITE request because proxies occasionally require it for billing purposes.
- Replaces—Header used by SIP gateways to indicate whether the originator of the Refer request is requesting a blind or attended transfer. It is required if the originator is performing an attended transfer, and not required for a blind transfer.

All other headers present in the Refer-To are ignored, and are not sent in the triggered INVITE.
The Refer-To and Contact headers are required in the Refer request. The absence of these headers results in a 4xx class response to the Refer request. Also, the Refer request must contain exactly one Refer-To header. Multiple Refer-To headers result in a 4xx class response.

**Note**

The Refer-To and Contact headers are required in the Refer request. The absence of these headers results in a 4xx class response to the Refer request. Also, the Refer request must contain exactly one Refer-To header. Multiple Refer-To headers result in a 4xx class response.

**Referred-By Header**

The Referred-By header is required in a Refer request. It identifies the originator and may also contain a signature (included for security purposes). SIP gateways echo the contents of the Referred-By header in the triggered INVITE request, but on receiving an INVITE request with this header, gateways do not act on it.

The Referred-By header is required in a Refer request. The absence of this header results in a 4xx class response to the Refer request. Also, the Refer request must contain exactly one Referred-By header. Multiple Referred-By headers result in a 4xx class response.

**NOTIFY Message Request**

Once the outcome of the Refer transaction is known, the recipient of the Refer request must notify the originator of the outcome of the Refer transaction—whether the final-recipient was successfully contacted or not. The notification is accomplished using the NOTIFY message request, SIP’s event notification mechanism. The notification contains a message body with a SIP response status line and the response class in the status line indicates the success or failure of the Refer transaction.

The NOTIFY message must do the following:

- Reflect the same To, From, and Call-ID headers that were received in the Refer request.
- Contain an Event header refer.
- Contain a message body with a SIP response line. For example: SIP/2.0 200 OK to report a successful Refer transaction, or SIP/2.0 503 Service Unavailable to report a failure. To report that the recipient disconnected before the transfer finished, it must use SIP/2.0 487 Request Canceled.

Two Cisco IOS commands pertain to the NOTIFY message request:

- The **timers notify** command sets the amount of time that the recipient should wait before retransmitting a NOTIFY message to the originator.
- The **retry notify** command configures the number of times a NOTIFY message is retransmitted to the originator.

**Note**

For information on these commands, see the *Cisco IOS Voice Command Reference*. 
Types of SIP Call Transfer Using the Refer Message Request

This section discusses how the Refer message request facilitates call transfer.

There are two types of call transfer: blind and attended. The primary difference between the two is that the Replaces header is used in attended call transfers. The Replaces header is interpreted by the final recipient and contains a Call-ID header, indicating that the initial call leg is to be replaced with the incoming INVITE request.

As outlined in the Refer message request, there are three main roles:

- **Originator**—User agent that initiates the transfer or Refer request.
- **Recipient**—User agent that receives the Refer request and is transferred to the final recipient.
- **Final-Recipient**—User agent introduced into a call with the recipient.

A gateway can be a recipient or final recipient, but not an originator.

**Blind Call-Transfer Process**

A blind, or unattended, transfer is one in which the transferring phone connects the caller to a destination line before ringback begins. This is different from a consultative, or attended, transfer in which one of the transferring parties either connects the caller to a ringing phone (ringback heard) or speaks with the third party before connecting the caller to the third party. Blind transfers are often preferred by automated devices that do not have the capability to make consultation calls.

Blind transfer works as described in the “Refer Message Request” section on page 81. The process is as follows:

1. **Originator** (user agent that initiates the transfer or Refer request) does the following:
   a. Sets up a call with recipient (user agent that receives the Refer request)
   b. Issues a Refer request to recipient

2. **Recipient** does the following:
   a. Sends an INVITE request to final recipient (user agent introduced into a call with the recipient)
   b. Returns a SIP 202 (Accepted) response to originator
   c. Notifies originator of the outcome of the Refer transaction—whether final recipient was successfully (SIP 200 OK) contacted or not (SIP 503 Service Unavailable)

3. If successful, a call is established between recipient and final recipient.

4. The original signaling relationship between originator and recipient terminates when either of the following occurs:
   - One of the parties sends a Bye request.
   - Recipient sends a Bye request after successful transfer (if originator does not first send a Bye request after receiving an acknowledgment for the NOTIFY message).

*Figure 2* shows a successful blind or unattended call transfer in which the originator initiates a Bye request to terminate signaling with the recipient.
Figure 2  Successful Blind or Unattended Transfer—Originator Initiating a Bye Request

Figure 3  Successful Blind or Unattended Transfer—Recipient Initiating a Bye Request

Figure 3 shows a successful blind or unattended call transfer in which the recipient initiates a Bye request to terminate signaling with the originator. A NOTIFY message is always sent by the recipient to the originator after the final outcome of the call is known.
If a failure occurs with the triggered INVITE to the final recipient, the call between originator and recipient is not disconnected. Rather, with blind transfer the process is as follows:

1. Originator sends a re-INVITE that takes the call off hold and returns to the original call with recipient.
2. Final recipient sends an 18x informational response to recipient.
3. The call fails; the originator cannot recover the call with recipient. Failure can be caused by an error condition or timeout.
4. The call leg between originator and recipient remains active (see Figure 4).
5. If the INVITE to final recipient fails (408 Request Timeout), the following occurs:
   a. Recipient notifies originator of the failure with a NOTIFY message.
   b. Originator sends a re-INVITE and returns to the original call with the recipient.

![Failed Blind Transfer—Originator Returns to Original Call with Recipient](image-url)
Attended Transfer

In attended transfers, the Replaces header is inserted by the initiator of the Refer message request as an overloaded header in the Refer-To and is copied into the triggered INVITE request sent to the final recipient. The header has no effect on the recipient, but is interpreted by the final recipient as a way to distinguish between blind transfer and attended transfer. The attended transfer process is as follows:

1. Originator does the following:
   a. Sets up a call with recipient.
   b. Places recipient on hold.
   c. Establishes a call to final recipient.
   d. Sends recipient a Refer message request with an overloaded Replaces header in the Refer-To header.

2. Recipient does the following:
   a. Sends a triggered INVITE request to final recipient. (Request includes the Replaces header, identifying the call leg between the originator and the final recipient.)
   b. Recipient returns a SIP 202 (Accepted) response to originator. (Response acknowledges that the INVITE has been sent.)

3. Final recipient establishes a direct signaling relationship with recipient. (Replaces header indicates that the initial call leg is to be shut down and replaced by the incoming INVITE request.)

4. Recipient notifies originator of the outcome of the Refer transaction. (Outcome indicates whether or not the final recipient was successfully contacted.)

5. Recipient terminates the session with originator by sending a Bye request.

Replaces Header

The Replaces header is required in attended transfers. It indicates to the final recipient that the initial call leg (identified by the Call-ID header and tags) is to be shut down and replaced by the incoming INVITE request. The final recipient sends a Bye request to the originator to terminate its session.

If the information provided by the Replaces header does not match an existing call leg, or if the information provided by the Replaces header matches a call leg but the call leg is not active (a Connect, 200 OK to the INVITE request has not been sent by the final-recipient), the triggered INVITE does not replace the initial call leg and the triggered INVITE request is processed normally.

Any failure resulting from the triggered INVITE request from the recipient to the final recipient does not drop the call between the originator and the final recipient. In these scenarios, all calls that are active (originator to recipient and originator to final recipient) remain active after the failed attended transfer attempt.
Figure 5 shows a call flow for a successful attended transfer.

**Figure 5 Successful Attended Transfer**

- **INVITE/200/ACK**
  - Call ID:1;from_tag:11;to_tag:22
- **2-Way RTP**
- **Invite (hold)** Call ID:1;from_tag:11 to_tag:22
- **200 OK**
- **Ack Call ID:1;from_tag:11;to_tag:22**
- **Refer:Refer-To:<final-recipient?replaces:**
  - Call ID:2;from_tag:33;to_tag:44>
  - Call ID:1;from_tag:11;to_tag:22
  - **202 Accepted**
  - **Notify (100 Trying body)**
  - **200 OK**
- **Invite Call ID:2;from_tag:33**
  - **200 OK Call ID:2;from_tag:33;to_tag:44**
  - **Ack Call ID:2;from_tag:33;to_tag:44**
  - **Refer:Refer-To:<final-recipient?replaces:**
    - Call ID:2;from_tag:33;to_tag:44>
    - Call ID:1;from_tag:11;to_tag:22
  - **202 Accepted**
  - **Notify (200) Call ID:1;from_tag:11 to_tag:22**
  - **200 OK (Notify)**
  - **Bye:Call ID:1 from_tag:11;to_tag:22**
  - **200 OK (Bye)**
- **Invite Call ID:3;from_tag:55**
  - **200 OK Call ID:3;from_tag:55;to_tag:66**
  - **Ack Call ID:3;from_tag:55;to_tag:66**
  - **2-Way RTP**
  - **Notify (100 Trying body)**
  - **200 OK**
  - **100 Trying**
Attended Transfer with Early Completion

Attended transfers allow the originator to have a call established between both the recipient and the final recipient. With attended transfer with early completion, the call between the originator and the final recipient does not have to be active, or in the talking state, before the originator can transfer it to the recipient. The originator establishes a call with the recipient and only needs to be setting up a call with the final recipient. The final recipient may be ringing, but has not answered the call from the originator when it receives a re-INVITE to replace the call with the originator and the recipient.

The process for attended transfer with early completion is as follows (see Figure 6):

1. Originator does the following:
   a. Sets up a call with recipient.
   b. Places the recipient on hold.
   c. Contacts the final recipient.
   d. After receiving an indication that the final recipient is ringing, sends recipient a Refer message request with an overloaded Replaces header in the Refer-To header. (The Replaces header is required in attended transfers and distinguishes between blind transfer and attended transfers.)

2. Recipient does the following:
   a. Returns a SIP 202 (Accepted) response to the originator. (to acknowledge that the INVITE has been sent.)
   b. Upon receipt of the Refer message request, sends a triggered INVITE request to final recipient. (The request includes the Replaces header, which indicates that the initial call leg, as identified by the Call-ID header and tags, is to be shut down and replaced by the incoming INVITE request.)

3. Final recipient establishes a direct signaling relationship with recipient.

4. Final recipient tries to match the Call-ID header and the To or From tag in the Replaces header of the incoming INVITE with an active call leg in its call control block. If a matching active call leg is found, final recipient replies with the same status as the found call leg. However, it then terminates the found call leg with a 487 Request Cancelled response.

   **Note** If early transfer is attempted and the call involves quality of service (QoS) or Resource Reservation Protocol (RSVP), the triggered INVITE from the recipient with the Replaces header is not processed and the transfer fails. The session between originator and final recipient remains unchanged.

5. Recipient notifies originator of the outcome of the Refer transaction—that is, whether final recipient was successfully contacted or not.

6. Recipient or originator terminates the session by sending a Bye request.
VSA for Call Transfer

You can use a vendor-specific attribute (VSA) for SIP call transfer.

Referred-By Header

For consistency with existing billing models, Referred-By and Requested-By headers are populated in call history tables as a VSA. Cisco VSAs are used for VoIP call authorization. The new VSA tag `supp-svc-xfer-by` helps to associate the call legs for call-detail-record (CDR) generation. The call legs can be originator-to-recipient or recipient-to-final-recipient.
The VSA tag `supp-svc-xfer-by` contains the user@host portion of the SIP URL of the Referred-By header for transfers performed with the Refer message request. For transfers performed with the Bye/Also message request, the tag contains user@host portion of the SIP URL of the Requested-By header. For each call on the gateway, two RADIUS records are generated: start and stop. The `supp-svc-xfer-by` VSA is generated only for stop records and is generated only on the recipient gateway—the gateway receiving the Refer or Bye/Also message.

The VSA is generated when a gateway that acts as a recipient receives a Refer or Bye/Also message with the Referred-By or Requested-By headers. There are usually two pairs of start and stop records. There is a start and stop record between the recipient and the originator and also between the recipient to final recipient. In the latter case, the VSA is generated between the recipient to the final recipient only.

**Business Group Field**

A new business group VSA field has been added that assists service providers with billing. The field allows service providers to add a proprietary header to call records. The VSA tag for business group ID is `cust-biz-grp-id` and is generated only for stop records. It is generated when the gateway receives an initial INVITE with a vendor dial-plan header to be used in call records. In cases when the gateway acts as a recipient, the VSA is populated in the stop records between the recipient and originator and the final recipient.

---

**Note**

For information on VSAs, see the *RADIUS VSA Voice Implementation Guide*. 
Interworking of Secure RTP calls for SIP and H.323

The Session Initiation Protocol (SIP) support for the Secure Real-time Transport Protocol (SRTP) is an extension of the Real-time Transport Protocol (RTP) Audio/Video Profile (AVP) and ensures the integrity of RTP and Real-Time Control Protocol (RTCP) packets that provide authentication, encryption, and the integrity of media packets between SIP endpoints.

SIP support for SRTP was introduced in Cisco IOS Release 12.4(15)T. In this and later releases, you can configure the handling of secure RTP calls on both a global level and on an individual dial peer basis on Cisco IOS voice gateways. You can also configure the gateway (or dial peer) either to fall back to (nonsecure) RTP or to reject (fail) the call for cases where an endpoint does not support SRTP.

The option to allow negotiation between SRTP and RTP endpoints was added for Cisco IOS Release 12.4(20)T and later releases, as was interoperability of SIP support for SRTP on Cisco IOS voice gateways with Cisco Unified Communications Manager. In Cisco IOS Release 12.4(22)T and later releases, you can also configure SIP support for SRTP on Cisco Unified Border Elements (Cisco UBEs).

Prerequisites

The following are prerequisites for the Interworking of Secure RTP calls for SIP and H.323 feature:

- Establish a working IP network and configure VoIP.
- Ensure that the gateway has voice functionality configured for SIP.
- Ensure that your Cisco router has adequate memory.
- As necessary, configure the router to use Greenwich Mean Time (GMT). SIP requires that all times be sent in GMT. SIP INVITE messages are sent in GMT. However, the default for routers is to use Coordinated Universal Time (UTC). To configure the router to use GMT, issue the clock timezone command in global configuration mode and specify GMT.

Cisco Unified Border Element

- Cisco IOS Release 12.2(20)T or a later release must be installed and running on your Cisco Unified Border Element.

Cisco Unified Border Element (Enterprise)

- Cisco IOS XE Release 3.1S or a later release must be installed and running on your Cisco ASR 1000 Series Router.

Restrictions

- The SIP gateway does not support codecs other than those listed in the table titled “SIP Codec Support by Platform and Cisco IOS Release” in the “Enhanced Codec Support for SIP Using Dynamic Payloads” section of the Configuring SIP QoS Features module.
- SIP requires that all times be sent in GMT.
SIP SRTP Fallback to Nonsecure RTP

The SIP SRTP Fallback to Nonsecure RTP feature enables a Cisco IOS Session Initiation Protocol (SIP) gateway to fall back from Secure Real-time Transport Protocol (SRTP) to Real-time Transport Protocol (RTP) by accepting or sending an RTP/Audio-Video Profile (AVP) (RTP) profile in response to an RTP/SAVP (SRTP) profile. This feature also allows inbound and outbound SRTP calls with nonsecure SIP signaling schemes (such as SIP URL) and provides the administrator the flexibility to configure Transport Layer Security (TLS), IPsec, or any other security mechanism used in the lower layers for secure signaling of crypto attributes.

For more information about configuring SRTP fallback and negotiation, see the `srtp`, `srtp negotiate`, and `voice-class sip srtp negotiate` commands in the Cisco IOS Voice Command Reference.

Prerequisites

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

**Cisco Unified Border Element (Enterprise)**
- Cisco IOS XE Release 3.1S or a later release must be installed and running on your Cisco ASR 1000 Series Router.

Configuring SIP SRTP Fallback to Nonsecure RTP

To enable this feature, see the `srtp`, `srtp negotiate`, and `voice-class sip srtp negotiate` commands in the Cisco IOS Voice Command Reference.

Additional configuration information is also available in the “Configuring SIP Support for SRTP” chapter of the “Cisco IOS SIP Configuration Guide, Release 15.1”
Feature Information for Cisco UBE Protocol-Independent Features and Setup

Table 1 lists the release history for this chapter.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which 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 lists only the Cisco IOS software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Fax Relay</td>
<td>12.2(13)T</td>
<td>Fax relay is the default mode for passing faxes through a VoIP network, and Cisco fax relay is the default fax relay type on Cisco voice gateways.</td>
</tr>
<tr>
<td>Cisco IOS Tcl IVR and VoiceXML Application Guide</td>
<td>12.3(4)T</td>
<td>Tcl and VoiceXML applications on the Cisco gateway provide Interactive Voice Response (IVR) features and call control functionality such as call forwarding, conference calling, and voice mail.</td>
</tr>
<tr>
<td>Cisco Unified Border Element with Gatekeeper</td>
<td>12.4(4)T</td>
<td>Cisco Unified Border Element with Gatekeeper 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 with Gatekeeper while making use of the routing, billing, and settlement capabilities offered by OSP-based clearinghouses</td>
</tr>
<tr>
<td>Cisco Unified Communications Trusted Firewall</td>
<td>12.4(22)T</td>
<td>Cisco Unified Communications Trusted Firewall Control pushes intelligent services onto the network through a Trusted Relay Point (TRP) firewall. Firewall traversal is accomplished using Session Traversal Utilities for NAT (STUN) on a TRP colocated with a Cisco Unified Communications Manager Express (Cisco Unified CME) or a Cisco Unified Border Element.</td>
</tr>
<tr>
<td>Cisco Unified SIP Survivable Remote Site Telephony (SRST)</td>
<td>12.3(4)T</td>
<td>Cisco Unified SIP SRST provides backup to an external SIP proxy server by providing basic registrar and redirect server or back-to-back user agent (B2BUA) services.</td>
</tr>
<tr>
<td>Cisco VoiceXML Programmer’s Guide</td>
<td>12.4(15)T</td>
<td>Voice Extensible Markup Language (VoiceXML) applications provide access to content and services over the telephone, just as Hypertext Markup Language (HTML) web pages provide access over a web browser residing on a PC.</td>
</tr>
</tbody>
</table>
### Table 1 Feature Information for CUBE Protocol-Independent Features and Setup Features (continued)

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring Tool Command Language (Tcl)</td>
<td>12.2(11)T</td>
<td>The Tool Command Language (TCL) Interactive Voice Response (IVR) application programming interface (API) provides commands that you can use to write TCL scripts to interact with the Cisco IVR feature.</td>
</tr>
<tr>
<td></td>
<td>12.2(11)YV</td>
<td></td>
</tr>
<tr>
<td></td>
<td>12.2(11)T</td>
<td></td>
</tr>
<tr>
<td>DTMF Events through SIP Signaling</td>
<td>12.2(11)T</td>
<td>The DTMF Events through SIP Signaling feature provides the following:</td>
</tr>
<tr>
<td></td>
<td>12.2(8)YN</td>
<td>• DTMF event notification for SIP messages.</td>
</tr>
<tr>
<td></td>
<td>12.2(15)T</td>
<td>• Capability of receiving hookflash event notification through the SIP NOTIFY method.</td>
</tr>
<tr>
<td></td>
<td>12.2(11)YV</td>
<td>• Third-party call control, or other signaling mechanisms, to provide enhanced services, such as calling card and messaging services.</td>
</tr>
<tr>
<td></td>
<td>12.2(11)T,</td>
<td>• Communication with the application outside of the media connection.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The following commands were introduced or modified: timers notify and retry notify.</td>
</tr>
<tr>
<td>Dynamic payload type interworking for DTMF and codec packets for SIP-to-SIP calls</td>
<td>15.0(1)XA</td>
<td>The Support for Dynamic Payload Type Interworking for DTMF and Codec Packets for SIP-to-SIP Calls feature provides dynamic payload type interworking for DTMF and codec packets for SIP-to-SIP calls.</td>
</tr>
<tr>
<td></td>
<td>15.1(1)T</td>
<td>The following commands were introduced or modified: asymmetric payload and voice-class sip asymmetric payload.</td>
</tr>
<tr>
<td>ENUM Support</td>
<td>12.4(6)T</td>
<td>The SIP-to-SIP Extended Feature Functionality Feature includes:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ENUM Support</td>
</tr>
<tr>
<td>H.323 RFC2833 - SIP NOTIFY</td>
<td>12.2(11)T</td>
<td>The SIP event notification mechanism uses NOTIFY messages to signal when certain telephony events take place. In order to send DTMF signals through NOTIFY messages, the gateway notifies the subscriber when DTMF digits are signaled by the originator. The notification contains a message body with a SIP response status line. This feature is introduced as part of the DTMF Events Through SIP Signaling feature set.</td>
</tr>
<tr>
<td>iLBC Support for SIP and H.323</td>
<td>12.2(11)T</td>
<td>The iLBC is a standard, high-complexity speech codec suitable for robust voice communication over IP. The iLBC has built-in error correction functionality that helps the codec perform in networks with high-packet loss. This codec is supported on both Session Initiation Protocol (SIP) and H.323. The following commands were introduced or modified: codec ilbc, codec preference, and rtp payload-type.</td>
</tr>
<tr>
<td></td>
<td>12.2(15)T</td>
<td></td>
</tr>
</tbody>
</table>
### Feature Information for CUBE Protocol-Independent Features and Setup

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
</table>
| Interconnect RSVP capable and RSVP incapable networks | 15.0(1)XA, 15.1(1)T | Support for interworking between RSVP and non-RSVP call legs for SIP calls. This support includes:  
  - Early Offer to Early Offer calls  
  - Delayed Offer to Delayed Offer calls  
  - Delayed Offer to Early Offer calls  
Support for interworking between a non-RSVP H.323 call leg and RSVP SIP call leg include:  
  - Fast Start to Early Offer calls  
  - Slow Start to Delayed Offer calls |
| Interworking of Secure RTP calls for SIP and H.323 | 12.4(20)T | This feature provides an option for a Secure RTP (SRTP) call to be connected from H.323 to SIP and from SIP to SIP. Additionally, this feature extends SRTP fallback support from the Cisco IOS voice gateway to the Cisco Unified Border Element. This feature uses no new or modified commands. |
| Media Termination Point (MTP) | 12.4(15)XY, 15.0(1)M | Software Media Termination Point (MTP) provides the capability for Cisco Unified Communications Manager (Cisco UCM) to interact with a voice gateway via Skinny Client Control Protocol (SCCP) commands. These commands allow the Cisco UCM to establish an MTP for call signaling. |
| Negotiation of an Audio Codec from a List of Codecs on Each Leg of a SIP-to-SIP Call on the Cisco Unified Border Element | 15.1(2)T | The Support for Negotiation of an Audio Codec from a List of Codecs on Each Leg of a SIP-to-SIP Call on the Cisco Unified Border Element feature supports negotiation of an audio codec using the Voice Class Codec and Codec Transparent infrastructure on the Cisco UBE. The following command was introduced or modified:  
  `voice-class codec (dial peer)`. |
| RSVP Agent | 12.4(6)T | The RSVP Agent feature implements a Resource Reservation Protocol enables Cisco Unified Communications Manager to provide resource reservation for voice and video media to ensure QoS and call admission control (CAC). |
### Feature Information for CUBE Protocol-Independent Features and Setup Features (continued)

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
</table>
| SIP DTMF Features                                          | 12.2(8)T, 12.2(11)T | Provides support for dual-tone multifrequency (DTMF) signaling features:  
  - RFC 2833 Dual-Tone Multifrequency (DTMF) Media Termination Point (MTP) Passthrough  
  - DTMF Events Through SIP Signaling  
  - DTMF Relay for SIP Calls Using Named Telephone Events  
  - SIP INFO Method for DTMF Tone Generation  
  - SIP NOTIFY-Based Out-of-Band DTMF Relay Support  
  - SIP KPML-Based Out-of-Band DTMF Relay Support  
  - SIP Support for Asymmetric SDP |
| 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.  
This feature introduces or modifies the following commands:  
* voice class sip-profiles, voice-class sip profiles |
| SIP SRTP Fallback to Nonsecure RTP                         | 12.4(22)T       | The SIP SRTP Fallback to Nonsecure RTP feature enables a Cisco IOS Session Initiation Protocol (SIP) gateway to fall back from SRTP to RTP by accepting or sending an RTP/AVP(RTP) profile in response to an RTP/SAVP(SRTP) profile. This feature also allows inbound and outbound SRTP calls with nonsecure SIP signaling schemes (such as SIP URL) and provides the administrator the flexibility to configure TLS, IPsec, or any other security mechanism used in the lower layers for secure signaling of crypto attributes.  
The following commands were introduced or modified:  
* srtp (voice), srtp negotiate, and voice-class sip srtp negotiate |
| SIP Video Calls with Flow Around Media                     | 12.4(15)XZ, 12.4(20)T | This feature provides the capability for media packets to pass directly between endpoints without the intervention of the Cisco UBE.  
The following command was modified by this feature:  
* media |
| SIP Video Support for Telepresence Calls                   | —              | This feature allows the Cisco Unified Border Element (Enterprise) to generate SIP INVITES that include SDP lines for both Voice and Voice media paths. |
| SIP—Ability to Send a SIP Registration Message on a Border Element | 12.4(24)T | Provides the ability to send a SIP Registration Message from Cisco Unified Border Element.  
The following command was modified:  
* credentials (SIP UA) |
The SIP—INFO Method for DTMF Tone Generation feature uses the Session Initiation Protocol (SIP) INFO method to generate dual-tone multifrequency (DTMF) tones on the telephony call leg. SIP methods, or request message types, request a specific action be taken by another user agent (UA) or proxy server. The SIP INFO message is sent along the signaling path of the call.

The following command was introduced: `show sip-ua`.

SIP—SIP Stack Portability

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP—SIP Stack Portability</td>
<td>12.4(2)T</td>
<td>Implements capabilities to the SIP gateway Cisco IOS stack involving user-agent handling of messages, handling of unsolicited messages, support for outbound delayed media, and SIP headers and content in requests and responses. The following commands were introduced or modified: <strong>None</strong></td>
</tr>
</tbody>
</table>

SIP-to-SIP Extended Feature Functionality for Session Border Controllers

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
</table>
| SIP-to-SIP Extended Feature Functionality for Session Border Controllers | 12.4(6)T | The SIP-to-SIP Extended Feature Functionality for Session Border Controllers (SBCs) enables the SIP-to-SIP functionality to conform with RFC 3261 to interoperate with SIP User Agents (UAs). The SIP-to-SIP Extended Feature Functionality includes:  
  - Call Admission Control (based on CPU, memory, and total calls)  
  - Delayed Media Call  
  - ENUM Support  
  - Configuring SIP Error Message Pass Through  
  - 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) |

Support for Interworking Between RSVP Capable and RSVP Incapable Networks

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support for Interworking Between RSVP Capable and RSVP Incapable Networks</td>
<td>15.0(1)XA 15.1(1)T</td>
<td>The Support for Interworking Between RSVP Capable and RSVP Incapable Networks feature provides precondition-based RSVP support for basic audio call and supplementary services on the Cisco UBE. The following commands were introduced or modified: <code>acc-qos</code>, <code>ip qos defending-priority</code>, <code>ip qos dscp</code>, <code>ip qos policy-locator</code>, <code>ip qos preemption-priority</code>, <code>req-qos</code>, <code>voice-class sip rsvp-fail-policy</code></td>
</tr>
</tbody>
</table>
This chapter describes how to configure T.38 fax relay on an IP network. It includes the following features:

- Fax Relay Packet Loss Concealment
- MGCP Based Fax (T.38) and DTMF Relay
- SIP T.38 Fax Relay
- T.38 Fax Relay for T.37/T.38 Fax Gateway
- T.38 Fax Relay for VoIP H.323

Universal Transcoding allows transcoding from any supported codec to any other supported codec.

Synchronizes RSVP signaling with H.323 Version 2 signaling to ensure that the bandwidth reservation is established in both directions before a call moves to the alerting phase (ringing). This ensures that the called party phone rings only after the resources for the call have been reserved. Using RSVP-based admission control, VoIP applications can reserve network bandwidth and react appropriately if bandwidth reservation fails.

Call Admission Control (CAC) is a deterministic and informed decision that is made before a voice call is established and is based on whether the required network resources are available to provide suitable QoS for the new call.

VoIP for IPv6

- IPv4 to IPv6 Calls (SIP and SIP)
- IPv6 to IPv6 Calls (SIP and SIP)
- Support for Dual Stack ANAT
Cisco Unified Border Element SIP Support

Revised: October 20, 2010
First Published: November 25, 2009
Last Updated: October 20, 2010

This Cisco Unified Border Element is a special Cisco IOS software image that 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.

**Activation**

Cisco Product Authorization Key (PAK)—A Product Authorization Key (PAK) is required to configure some of the features described in this guide. Before you start the configuration process, please register your products and activate your PAK at the following URL http://www.cisco.com/go/license.

**Finding Feature Information**

For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the “Cisco Unified Border Element Features Roadmap” section on page 3.

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.
Cisco Unified Border Element SIP Support Features

This chapter contains the following configuration topics:

**Cisco UBE Prerequisites and Restrictions**
- Prerequisites for Cisco Unified Border Element
- Restrictions for Cisco Unified Border Element

**Basic SIP Set-up**
- SIP—Core SIP Technology Enhancements

**SIP Parameter Settings**
- SIP—Configurable Hostname in Locally Generated SIP Headers
- SIP Parameter Modification
- SIP—Session Timer Support

**SIP Protocol Handling and Supplementary Services**
- SIP-to-SIP Basic Functionality for Session Border Controller
- SIP-to-SIP Extended Feature Functionality for Session Border Controllers
- SIP-to-SIP Supplementary Services for Session Border Controller
- Cisco UBE Support for generating Out-of-dialog SIP OPTIONS Ping messages to monitor SIP Servers
- SIP—INFO Method for DTMF Tone Generation
- SIP—Enhanced 180 Provisional Response Handling
- Configuring Support for SIP 181 Call is Being Forwarded Message
- Support for Expires Timer Reset on Receiving or Sending SIP 183 Message
- Support for PAID, PPID, Privacy, PCPID, and PAURI Headers on the Cisco UBE
- Configuring Selective Filtering of Outgoing Provisional Response on the Cisco UBE
- Cisco Unified Border Element Support for Configurable Pass-through of SIP INVITE Parameters
- Transparent Tunneling of QSIG and Q.931 over SIP TDM Gateway and SIP-SIP Cisco Unified Border Element
- SIP Diversion Header Enhancements

**SIP Registration & Authentication**
- SIP—Ability to Send a SIP Registration Message on a Border Element
- Support for Multiple Registrars on SIP Trunks

**SIP Normalization**
- SIP Parameter Modification
Additional References

Glossary

Feature Information for Cisco UBE SIP Support,
SIP—Core SIP Technology Enhancements

This feature contains the following sections:

- Information About SIP—Core SIP Technology Enhancements, page 104
- Prerequisites for SIP—Core SIP Technology Enhancements, page 107
- Restrictions, page 107
- How to Configure SIP—Core SIP Technology Enhancements, page 107
- Configuration Examples for SIP—Core SIP Technology Enhancements, page 114

Information About SIP—Core SIP Technology Enhancements

The SIP—Core SIP Technology Enhancements feature updates Cisco SIP VoIP gateways with the latest changes in RFC 2543-bis-04. All changes are compatible with older RFC versions. Compliance to RFC 2543-bis-04 adds enhanced SIP support and ensures smooth interoperability and compatibility with multiple vendors.

The enhanced areas are as follows:

- SIP URL Comparison, page 104
- 487 Sent for BYE Requests, page 105
- 3xx Redirection Responses, page 105
- DNS SRV Query Procedure, page 105
- CANCEL Request Route Header, page 106
- Interpret User Parameters, page 106
- user=phone Parameter, page 106
- 303 and 411 SIP Cause Codes, page 106
- Flexibility of Content-Type Header, page 106
- Optional SDP “s=” Line, page 106
- Allow Header Addition to INVITEs and 2xx Responses, page 106
- Simultaneous Cancel and 2xx Class Response, page 107

SIP URL Comparison

When a URL is received, the URLs are compared for equality. URL comparison can be done between two From SIP URLs, or it can be done between two To SIP URLs. For two URLs to be equal, the user, password, host, and port parameters must match. The order of the parameters does not to match.

The SIP—Core SIP Technology Enhancements feature changes the parameters allowed in SIP URLs. The addr parameter and the transport parameter are not allowed in Cisco SIP gateway implementations. The user-param parameter is now the parameter for comparison.

If a compared parameter is omitted or not present, it is matched on the basis of its default value. Table 1 shows a list of SIP URL compared parameters and their default values.
The following is an example of equivalent URLs:

Original URL:
sip:36602@172.18.193.120

Equivalent URLs:
sip:36602@172.18.193.120:
sip:36602@172.18.193.120;tag=499270-A62;pname=pvalue
sip:36602@172.18.193.120;user=ip
sip:36602@172.18.193.120:5060

487 Sent for BYE Requests
RFC 2543-bis-04 requires that a user agent server (UAS) that receives a BYE request first send a response to any pending requests for that call before disconnecting. The SIP—Core SIP Technology Enhancements feature recommends that after receiving a BYE request the UAS respond with a 487 (Request Cancelled) status message.

3xx Redirection Responses
The processing of 3xx redirection responses was updated in the SIP—Core SIP Technology Enhancements feature as follows:

- The Uniform Resource Identifier (URI) of the redirected INVITE is updated to contain the new contact information provided by the 3xx redirect message.
- The transmitted CSeq number found in the CSeq header is increased by one. The new INVITE includes the updated CSeq.
- The To, From, and Call ID headers that identify the call leg remain the same. The same Call ID gives consistency when capturing billing history.
- The user agent client (UAC) retries the request at the new address given by the 3xx Contact header field.

See the “Examples” section on page 111 for a sample call flow that shows the updated CSeq numbers.

DNS SRV Query Procedure
When a Request URI or the session target in the dial peer contains a fully qualified domain name (FQDN), the UAC needs to determine the protocol, port, and IP address of the endpoint before it forwards the request. SIP on Cisco gateways uses a Domain Name System Server (DNS SRV) query to determine the protocol, port, and IP address of the user endpoint.

Before the SIP—Core SIP Technology Enhancements feature, the DNS query procedure did not take into account the destination port.

---

### Table 1  SIP URL Parameter Comparison

<table>
<thead>
<tr>
<th>SIP URL Compared Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>host</td>
<td>mandatory</td>
</tr>
<tr>
<td>password</td>
<td>—</td>
</tr>
<tr>
<td>port</td>
<td>5060</td>
</tr>
<tr>
<td>user</td>
<td>—</td>
</tr>
<tr>
<td>user-param</td>
<td>ip</td>
</tr>
</tbody>
</table>
CANCEL Request Route Header

The SIP—Core SIP Technology Enhancements feature does not allow a CANCEL message sent by a UAC on an initial INVITE request to have a Route header. Route headers cannot appear in a CANCEL message because they take the same path as INVITE requests, and INVITE requests cannot contain Route headers.

Interpret User Parameters

Telephone-subscriber or user parameters in an incoming INVITE message may contain extra characters to incorporate space, control characters, quotation marks, hash marks, and other characters. The SIP—Core SIP Technology Enhancements feature allows, the telephone-subscriber or user parameter to be interpreted before dial-peer matching is done. For example, the telephone number in an incoming INVITE message may appear as:

-%32%32%32

Although 222 is a valid telephone number, it requires interpretation. If the interpretation is not done, the call attempt fails when the user parameter is matched with the dial-peer destination pattern.

user=phone Parameter

A SIP URL identifies a user’s address, whose appearance is similar to that of an e-mail address. The form of the user’s address is user@host where user is the user identification and host is either a domain name or a numeric network address. For example, the request line of an outgoing INVITE request might appear as:

INVITE sip:5550002@companyb.com

With the SIP—Core SIP Technology Enhancements feature. The user=phone parameter formerly required in a SIP URL is no longer necessary. However, if an incoming SIP message has a SIP URL with user=phone, user=phone is parsed and used in the subsequent messages of the transaction.

303 and 411 SIP Cause Codes

The SIP—Core SIP Technology Enhancements feature obsoletes the SIP cause codes 303 Redirection: See Other and 411 Client Error: Length required.

Flexibility of Content-Type Header

The SIP—Core SIP Technology Enhancements feature allows the Content-Type header, which specifies the media type of the message body, to have an empty Session Description Protocol (SDP) body.

Optional SDP “s=” Line

The SIP—Core SIP Technology Enhancements feature accepts the “s=” line in SDP as optional. The “s=” line describes the reason or subject for SDP information. Cisco SIP gateways can create messages with an “s=” line in SDP bodies and can accept messages that have no “s=” line.

Allow Header Addition to INVITEs and 2xx Responses

The SIP—Core SIP Technology Enhancements feature enables the use of the Allow header in an initial or re-INVITE request or in any 2xx class response to an INVITE. The Allow header lists the set of methods supported by the user agent that is generating the message. Because it advertises what methods should be invoked on the user agent sending the message, it avoids congesting the message traffic unnecessarily. The Allow header can contain any or all of the following: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, COMET, REFER, NOTIFY, INFO, SUBSCRIBE.
Simultaneous Cancel and 2xx Class Response

According to RFC 2543-bis-04, if the UAC desires to end the call before a response is received to an INVITE, the UAC sends a CANCEL. However, if the CANCEL and a 2xx class response to the INVITE "pass on the wire", the UAC also receives a 2xx to the INVITE. The SIP—Core SIP Technology Enhancements feature ensures that when the two messages pass, the UAC terminate the call by sending a BYE request.

Prerequisites for SIP—Core SIP Technology Enhancements

- Ensure that your Cisco router has the minimum memory requirements necessary for voice capabilities.
- Establish a working IP network.
- Configure VoIP.

Cisco Unified Border Element

- Cisco IOS Release 12.2(13)T or a later release must be installed and running on your Cisco Unified Border Element.

Cisco Unified Border Element (Enterprise)

- Cisco IOS XE Release 2.5 or a later release must be installed and running on your Cisco ASR 1000 Series Router.

Restrictions

- Via handling for TCP was not implemented in the Cisco SIP—Core SIP Technology Enhancements feature.

How to Configure SIP—Core SIP Technology Enhancements

The SIP—Core SIP Technology Enhancements features are all enabled by default, and no special configurations is necessary. However, several of these features can be monitored through the use of various commands. See the following sections for monitoring tasks for the SIP—Core SIP Technology Enhancements feature. Each task in the list is optional:

- Monitoring 487 Sent for BYE Requests, page 107 (optional)
- Monitoring 3xx Redirection Responses, page 109 (optional)
- Monitoring the Deletion of 303 and 411 Cause Codes, page 111 (optional)

Monitoring 487 Sent for BYE Requests

When a UAS responds with a 487 after receiving a BYE request, the Client Error: Request Cancelled counter increments in the show sip-ua statistics command.

SUMMARY STEPS

1. enable
2. show sip-ua statistics
DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables such as privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2 show sip-ua statistics</td>
<td>(Optional) Displays response, traffic, and retry statistics for the SIP user agent (UA).</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# show sip-ua statistics</td>
</tr>
</tbody>
</table>

Examples

The following sample output from the show sip-ua statistics command with the Client Error: Request Cancelled counter incremented:

```
Router# show sip-ua statistics

SIP Response Statistics (Inbound/Outbound)
  Informational:
    Trying 0/0, Ringing 0/0,
    Forwarded 0/0, Queued 0/0,
    SessionProgress 0/0
  Success:
    OkInvite 0/0, OkBye 0/0,
    OkCancel 0/0, OkOptions 0/0,
    OkPrack 0/0, OkPreconditionMet 0/0,
    OkSubscribe 0/0, OkNotify 0/0,
    202Accepted 0/0
  Redirection (Inbound only):
    MultipleChoice 0, MovedPermanently 0,
    MovedTemporarily 0, UseProxy 0,
    AlternateService 0
  Client Error:
    BadRequest 0/0, Unauthorized 0/0,
    PaymentRequired 0/0, Forbidden 0/0,
    NotFound 0/0, MethodNotAllowed 0/0,
    NotAcceptable 0/0, ProxyAuthReqd 0/0,
    ReqTimeout 0/0, Conflict 0/0, Gone 0/0,
    ReqEntityTooLarge 0/0, ReqURITooLarge 0/0,
    UnsupportedMediaType 0/0, BadExtension 0/0,
    TempNotAvailable 0/0, CallLegNonExistent 0/0,
    LoopDetected 0/0, TooManyHops 0/0,
    AddrIncomplete 0/0, Ambiguous 0/0,
    BusyHere 0/0, RequestCancel 0/1
  NotAcceptableMedia 0/0, BadEvent 0/0
  Server Error:
    InternalError 0/0, NotImplemented 0/0,
    BadGateway 0/0, ServiceUnavail 0/0,
    GatewayTimeout 0/0, BadSipVer 0/0,
    PreCondFailure 0/0
  Global Failure:
    BusyEverywhere 0/0, Decline 0/0,
    NotExistAnywhere 0/0, NotAcceptable 0/0

SIP Total Traffic Statistics (Inbound/Outbound)
  Invite 0/0, Ack 0/0, Bye 0/0,
  Cancel 0/0, Options 0/0,
```
Prack 0/0, Comet 0/0, Subscribe 0/0, Notify 0/0, Refer 0/0

Retry Statistics
Invite 0, Bye 0, Cancel 0, Response 0, Prack 0, Comet 0, Reliable1xx 0, Notify 0

SDP application statistics:
Parses: 0, Builds 0
Invalid token order: 0, Invalid param: 0
Not SDP desc: 0, No resource: 0

Monitoring 3xx Redirection Responses

The processing for 3xx redirection responses was updated in the SIP—Core SIP Technology Enhancements feature. The new implementation can be monitored with the **debug ccsip messages** command.

**SUMMARY STEPS**

1. **enable**
2. **debug ccsip message**

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> debug ccsip message</td>
<td>Displays all SIP Service Provider Interface (SPI) message tracing.</td>
</tr>
<tr>
<td></td>
<td>• Use this command to enable traces for SIP messages exchanged between the SIP user agent client (UAC) and the access server.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# debug ccsip message</td>
<td></td>
</tr>
</tbody>
</table>

**Examples**

The following is **debug ccsip message** output from an originating gateway. The output shows message transactions including the new INVITE message for the redirected address. The output has been updated as follows:

- The URI of the redirected INVITE is updated to contain new contact information provided by the 3xx redirect message.
- The transmitted CSeq number found in the CSeq header is increased by one. The new INVITE includes the updated CSeq.
- The To, From, and Call ID headers that identify the call leg remain the same.
- The UAC retries the request at the new address given by the 3xx Contact header field.

Sent:
INVITE sip:3111100064.102.17.80:5060; SIP/2.0
Via: SIP/2.0/UDP 172.18.193.98:5060
From: "36601" <sip:36601@172.18.193.98> //This header remains consistent throughout the call.
To: <sip:3111100864.102.17.80> //This header remains consistent throughout the call.
Date: Mon, 01 Mar 2002 00:50:50 GMT
Call-ID: A22F0DC8-14F511CC-80329792-19DC655A@172.18.193.98 // Header remains consistent.
Cisco-Guid: 2682312529-351605196-2150668178-433874266
User-Agent: Cisco-SIPGateway/IOS-12.x
CSeq: 101 INVITE
Max-Forwards: 6
Timestamp: 730947050
Contact: <sip:36601@172.18.193.98:5060>
Expires: 180
Content-Type: application/sdp
Content-Length: 160

v=0
o=CiscoSystemsSIP-GW-UserAgent 2378 4662 IN IP4 172.18.193.98
s=SIP Call
c=IN IP4 172.18.193.98
t=0 0
m=audio 19202 RTP/AVP 18
a=rtpmap:18 G729/8000

Received:
SIP/2.0 302 Moved Temporarily
Via: SIP/2.0/UDP 172.18.193.98:5060
From: "36601" <sip:36601@172.18.193.98> //This header remains consistent throughout the call.
To: <sip:3111100864.102.17.80> //This header remains consistent throughout the call.
Date: Mon, 01 Mar 2002 00:50:50 GMT
Call-ID: A22F0DC8-14F511CC-80329792-19DC655A@172.18.193.98 //Header remains consistent.
Cisco-Guid: 2682312529-351605196-2150668178-433874266
User-Agent: Cisco-SIPGateway/IOS-12.x
CSeq: 101 INVITE
Contact: Anonymous <sip:36602@172.18.193.120 //Provides Request URI with the new contact address.
Contact: Anonymous <sip:36601@172.18.193.98>

Sent:
ACK sip:3111100864.102.17.80:5060; SIP/2.0
Via: SIP/2.0/UDP 172.18.193.98:5060
From: "36601" <sip:36601@172.18.193.98> //This header remains consistent throughout the call.
To: <sip:3111100864.102.17.80> //This header remains consistent throughout the call.
Date: Mon, 01 Mar 2002 00:50:50 GMT
Call-ID: A22F0DC8-14F511CC-80329792-19DC655A@172.18.193.98 //Header remains consistent.
Cisco-Guid: 2682312529-351605196-2150668178-433874266
Max-Forwards: 6
Content-Length: 0
CSeq: 101 ACK

Sent:
INVITE sip:36602@172.18.193.120:5060 SIP/2.0 //URI updated with new contact/redirect address.
Via: SIP/2.0/UDP 172.18.193.98:5060
From: "36601" <sip:36601@172.18.193.98> //This header remains consistent throughout the call.
To: <sip:3111100864.102.17.80> //This header remains consistent throughout the call.
Date: Mon, 01 Mar 2002 00:50:50 GMT
Call-ID: A22F0DC8-14F511CC-80329792-19DC655A@172.18.193.98 // Header remains consistent.
Cisco-Guid: 2682312529-351605196-2150668178-433874266
User-Agent: Cisco-SIPGateway/IOS-12.x
CSeq: 102 INVITE //Transmitted CSeq is increased by one.
Max-Forwards: 6
Timestamp: 730947050
Monitoring the Deletion of 303 and 411 Cause Codes

The processing for Monitoring the Deletion of 303 and 411 Cause Codes was updated in the SIP—Core SIP Technology Enhancements feature. The new implementation can be monitored with the `show sip-ua statistics` and `show sip-ua map` commands.

**SUMMARY STEPS**

1. enable
2. show sip-ua statistics
3. show sip-ua map

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2 show sip-ua statistics</td>
<td>Displays response, traffic, and retry statistics for the SIP UA.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Can be used to verify the deletion of the 303 and 411 cause codes.</td>
</tr>
<tr>
<td>Step 3 show sip-ua map</td>
<td>Displays the mapping table of PSTN cause codes and their corresponding</td>
</tr>
<tr>
<td></td>
<td>SIP error status codes or the mapping table of SIP-to-PSTN codes.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Can be used to verify the deletion of 411 cause codes.</td>
</tr>
</tbody>
</table>

**Examples**

The following examples provide different ways to monitor the deletion of the 303 and 411 cause codes.

- `show sip-ua statistics` command
- `show sip-ua map` command
show sip-ua statistics Command

The following is sample output of the **show sip-ua statistics** command that includes the *SeeOther* (303) and *LengthRequired* (411) fields is from the Cisco IOS version before the SIP—Core SIP Technology Enhancements feature:

```
Router# show sip-ua statistics

SIP Response Statistics (Inbound/Outbound)
   Informational:
      Trying 0/4, Ringing 0/0,
      Forwarded 0/0, Queued 0/0,
      SessionProgress 0/5
   Success:
      OkInvite 0/2, OkBye 1/1,
      OkCancel 0/2, OkOptions 0/0,
      OkPrack 0/0, OkPreconditionMet 0/0,
      OkNotify 0/0, 202Accepted 0/0
   Redirection (Inbound only):
      MultipleChoice 0, MovedPermanently 0,
      MovedTemporarily 0, SeeOther 0,
      UseProxy 0, AlternateService 0
   Client Error:
      BadRequest 0/0, Unauthorized 0/0,
      PaymentRequired 0/0, Forbidden 0/0,
      NotFound 0/0, MethodNotAllowed 0/0,
      NotAcceptable 0/0, ProxyAuthReqd 0/0,
      ReqTimeout 0/0, Conflict 0/0, Gone 0/0,
      LengthRequired 0/0, ReqEntityTooLarge 0/0,
      ReqURITooLarge 0/0, UnsupportedMediaType 0/0,
      BadExtension 0/0, TempNotAvailable 0/0,
      CallLegNonExistent 0/0, LoopDetected 0/0,
      TooManyHops 0/0, AddrIncomplete 0/0,
      Ambiguous 0/0, BusyHere 0/0
      RequestCancel 0/2, NotAcceptableMedia 0/0
   Server Error:
      InternalError 0/0, NotImplemented 0/0,
      BadGateway 0/0, ServiceUnavail 0/0,
      GatewayTimeout 0/0, BadSipVer 0/0,
      PreCondFailure 0/0
   Global Failure:
      BusyEverywhere 0/0, Decline 0/0,
      NotExistAnywhere 0/0, NotAcceptable 0/0

SIP Total Traffic Statistics (Inbound/Outbound)
   Invite 5/0, Ack 4/0, Bye 1/1,
   Cancel 2/0, Options 0/0,
   Prack 0/0, Comet 0/0,
   Notify 0/0, Refer 0/0

Retry Statistics
   Invite 0, Bye 0, Cancel 0, Response 0,
   Prack 0, Comet 0, Reliable1xx 0, Notify 0
```

The following is sample output of the **show sip-ua statistics** command from a Cisco IOS version after implementing the SIP—Core SIP Technology Enhancements feature and shows that the *SeeOther* and *LengthRequired* fields are now omitted is from fields:

```
Router# show sip-ua statistics

SIP Response Statistics (Inbound/Outbound)
   Informational:
      Trying 0/0, Ringing 0/0,
```
Forwarded 0/0, Queued 0/0, SessionProgress 0/0
Success:
OkInvite 0/0, OkBye 0/0, OkCancel 0/0, OkOptions 0/0, OkPrack 0/0, OkPreconditionMet 0/0, OKSubscribe 0/0, OkNotify 0/0, 202Accepted 0/0
Redirection (Inbound only):
MultipleChoice 0, MovedPermanently 0, MovedTemporarily 0, UseProxy 0, AlternateService 0
Client Error:
BadRequest 0/0, Unauthorized 0/0, PaymentRequired 0/0, Forbidden 0/0, NotFound 0/0, MethodNotAllowed 0/0, NotAcceptable 0/0, ProxyAuthReqd 0/0, ReqTimeout 0/0, Conflict 0/0, Gone 0/0, ReqEntityTooLarge 0/0, ReqURITooLarge 0/0, UnsupportedMediaType 0/0, BadExtension 0/0, TempNotAvailable 0/0, CallLegNonExistent 0/0, LoopDetected 0/0, TooManyHops 0/0, AddrIncomplete 0/0, Ambiguous 0/0, BusyHere 0/0, RequestCancel 0/0, NotAcceptableMedia 0/0, BadEvent 0/0, Server Error:
InternalError 0/0, NotImplemented 0/0, BadGateway 0/0, ServiceUnavail 0/0, GatewayTimeout 0/0, BadSipVer 0/0, PreCondFailure 0/0
Global Failure:
BusyEverywhere 0/0, Decline 0/0, NotExistAnywhere 0/0, NotAcceptable 0/0
SIP Total Traffic Statistics (Inbound/Outbound)
Invite 0/0, Ack 0/0, Bye 0/0, Cancel 0/0, Options 0/0, Prack 0/0, Comet 0/0, Subscribe 0/0, Notify 0/0, Refer 0/0
Retry Statistics
Invite 0, Bye 0, Cancel 0, Response 0, Prack 0, Comet 0, Reliable1xx 0, Notify 0
SDP application statistics:
Parses: 0, Builds 0
Invalid token order: 0, Invalid param: 0, Not SDP desc: 0, No resource: 0

**show sip-ua map**

The following example is sample output from the `show sip-ua map` command and shows that SIP cause code 411 is omitted from the group of cause codes.

Router# **show sip-ua map sip-pstn**

<table>
<thead>
<tr>
<th>SIP-Status</th>
<th>Configured</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>PSTN-Cause</td>
<td>PSTN-Cause</td>
</tr>
<tr>
<td>400</td>
<td>127</td>
<td>127</td>
</tr>
<tr>
<td>401</td>
<td>57</td>
<td>57</td>
</tr>
<tr>
<td>402</td>
<td>21</td>
<td>21</td>
</tr>
<tr>
<td>403</td>
<td>57</td>
<td>57</td>
</tr>
<tr>
<td>404</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>405</td>
<td>127</td>
<td>127</td>
</tr>
<tr>
<td>406</td>
<td>127</td>
<td>127</td>
</tr>
</tbody>
</table>
Configuration Examples for SIP—Core SIP Technology Enhancements

This section provides a general SIP configuration example:

- **SIP—Core SIP Technology Enhancements: Example**

**SIP—Core SIP Technology Enhancements: Example**

This example contains output from the `show running-config` command.

Router# `show running-config`

Building configuration...

Current configuration : 2791 bytes
!
version 12.2
service config
no service single-slot-reload-enable
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service internal
service udp-small-servers
!
interface FastEthernet2/0
ip address 172.18.200.24 255.255.255.0
duplex auto
no shut
speed 10
ip rsvp bandwidth 7500 7500
!
voice-port 1/1/1
no supervisory disconnect lcfo
!
dial-peer voice 1 pots
application session
destination-pattern 5550111
port 1/1/1
!
dial-peer voice 3 voip
application session
destination-pattern 5550112
session protocol sipv2
session target ipv4:172.18.200.36
codec g711ulaw
!
dial-peer voice 4 voip
application session
destination-pattern 5550133
session protocol sipv2
session target ipv4:172.18.200.33
codec g711ulaw
!
gateway
!
sip-ua
   retry invite 1
   retry bye 1
!
line con 0
line aux 0
line vty 0 4
login
!
end
SIP—Configurable Hostname in Locally Generated SIP Headers

This feature allows you to configure the hostname for use in locally generated SIP headers in either of two configuration modes.

Prerequisites

Cisco Unified Border Element

- Cisco IOS Release 12.4(2)T or a later release must be installed and running on your Cisco Unified Border Element.

Cisco Unified Border Element (Enterprise)

- Cisco IOS XE Release 2.5 or a later release must be installed and running on your Cisco ASR 1000 Series Router.

Restrictions

- Dial-peer-specific configuration takes precedence over more general gateway-wide configuration.

How to Configure the Hostname in Locally Generated SIP Headers

To configure the Hostname in Locally Generated SIP Headers, perform the following tasks:

- Configuring Hostname in Locally Generated SIP Headers at the Global Level, page 116
- Configuring Hostname in Locally Generated SIP Headers at the Dial-Peer-Specific Level, page 117

Configuring Hostname in Locally Generated SIP Headers at the Global Level

To configure the local hostname in global configuration mode for use in locally generated URLs, complete the task in this section.

Note

- Dial-peer-specific configuration takes precedence over more general gateway-wide configuration.

SUMMARY STEPS

1. enable
2. configure terminal
3. voice service voip
4. sip
5. localhost dns:local-host-name-string
6. exit
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  * Enter your password if prompted. |
| **Example:** Router> enable | |
| **Step 2** configure terminal | Enters global configuration mode. |
| **Example:** Router# configure terminal | |
| **Step 3** voice service voip | (Required) Enters the voice-service VoIP configuration mode |
| **Example:** Router(config)# voice service voip | |
| **Step 4** sip | (Required) Enters the SIP configuration mode. |
| **Example:** Router(config-vol-serv)# sip | |
| **Step 5** localhost dns:local-host-name-string | (Optional) Globally configures the gateway to substitute a DNS hostname or domain as the localhost name in place of the physical IP address in the From, Call-ID, and Remote-Party-ID headers in outgoing messages:  
  * dns:local-host-name-string—Alphanumeric value representing the DNS domain (consisting of the domain name with or without a specific hostname) in place of the physical IP address that is used in the host portion of the From, Call-ID, and Remote-Party-ID headers in outgoing messages.  
  * This value can be the hostname and the domain separated by a period (dns:hostname.domain) or just the domain name (dns:domain). In both case, the dns: delimiter must be included as the first four characters. |
| **Example:** Router(conf-serv-sip)# localhost dns:host_one | |
| **Step 6** exit | Exits the current configuration mode. |
| **Example:** Router(conf-serv-sip)# exit | |

### Configuring Hostname in Locally Generated SIP Headers at the Dial-Peer-Specific Level

To configure the local hostname in dial-peer-specific configuration mode for use in locally generated URLs, complete the task in this section.

**Note**  
This configuration takes precedence over global configuration.
### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *tag* voip
4. **voice-class sip localhost dns:[hostname.]domain [preferred]**
5. **exit**

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
• Enter your password if prompted. |
| **Example:** | |
| Router> enable | |
| **Step 2** configure terminal | Enters global configuration mode. |
| **Example:** | |
| Router# configure terminal | |
| **Step 3** dial-peer voice *tag* voip | (Required) Enters dial-peer configuration mode for the specified dial peer. |
| **Example:** | |
| Router# dial-peer voice 100 voip | |
| **Step 4** voice-class sip localhost dns:[hostname.]domain [preferred] | (Optional) Configures individual dial peers to override global settings on the gateway and substitute a DNS hostname or domain as the localhost name in place of the physical IP address in the From, Call-ID, and Remote-Party-ID headers in outgoing messages:  
• **dns:**local-host-name-string—Alphanumeric value representing the DNS domain (consisting of the domain name with or without a specific hostname) in place of the physical IP address that is used in the host portion of the From, Call-ID, and Remote-Party-ID headers in outgoing messages.  
• This value can be the hostname and the domain separated by a period (dns:hostname.domain) or just the domain name (dns:domain). In both case, the dns: delimiter must be included as the first four characters. |
| **Example:** | |
| Router(config-dial-peer)# voice-class sip localhost dns:example.com | |
| **Step 5** exit | Exits the current configuration mode. |
| **Example:** | |
| Router(config-dial-peer)# exit | |
Verifying the Hostname in Locally Generated SIP Headers

To verify the hostname in locally generated SIP headers for global or dial-peer-specific configuration, use the following `show` commands:

- `show call active voice`
- `show call history voice`

**Step 1**  Use the `show call active voice` command to display output when the local hostname is enabled:

```
Router# show call active voice
Telephony call-legs:1
SIP call-legs:1
H323 call-legs:0
Call agent controlled call-legs:0
Multicast call-legs:0
Total call-legs:2
GENERIC:
SetupTime=126640 ms
Index=1
PeerAddress=9001
PeerSubAddress=
PeerId=100
PeerIfIndex=6
LogicalIfIndex=4
ConnectTime=130300 ms
CallDuration=00:00:47 sec
CallState=4
CallOrigin=2
ChargedUnits=0
InfoType=speech
TransmitPackets=2431
TransmitBytes=48620
ReceivePackets=2431
ReceiveBytes=48620
TELE:
ConnectionId=[0xA0DC41CF 0x115511D9 0x8002EC82 0xAB4FD5BE]
IncomingConnectionId=[0xA0DC41CF 0x115511D9 0x8002EC82 0xAB4FD5BE]
CallID=1
TxDuration=48620 ms
VoiceTxDuration=48620 ms
FaxTxDuration=0 ms
CoderTypeRate=g729r8
NoiseLevel=-61
ACOMLevel=3
OutSignalLevel=-35
InSignalLevels=-30
InfoActivity=2
ERLLevel=3
SessionTarget=
ImgPages=0
CallerName=
CallerIDBlocked=False
OriginalCallingNumber=
OriginalCallingOctet=0x0
OriginalCalledNumber=
OriginalCalledOctet=0x80
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0x0
TranslatedCallingNumber=9001
TranslatedCallingOctet=0x0
```
TranslatedCalledNumber=
TranslatedCalledOctet=0x80
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0x0
GwCollectedCalledNumber=9002

GENERIC:
SetupTime=128980 ms
Index=1
PeerAddress=9002
PeerSubAddress=
PeerId=3301
PeerIfIndex=7
LogicalIfIndex=0
ConnectTime=130300 ms
CallDuration=00:00:50 sec
CallState=4
CallOrigin=1
ChargedUnits=0
InfoType=speech
TransmitPackets=2587
TransmitBytes=51740
ReceivePackets=2587
ReceiveBytes=51740

VOIP:
ConnectionId[0xA0DC41CF 0x115511D9 0x8002EC82 0xAB4FD5BE]
IncomingConnectionId[0xA0DC41CF 0x115511D9 0x8002EC82 0xAB4FD5BE]
CallID=2
RemoteIPAddress=172.18.193.87
RemoteUDPPort=17602
RemoteSignallingIP Address=172.18.193.87
RemoteMediaIP Address=172.18.193.87
RemoteMediaPort=17602
RoundTripDelay=2 ms
SelectedQoS=best-effort
tx_DtmfRelay=inband-voice
FastConnect=FALSE
AnnexE=FALSE
Separate H245 Connection=FALSE
H245 Tunneling=FALSE
SessionProtocol=sipv2
ProtocolCallId=2404B4DC-115511D9-8005EC82-AB4FD5BE@pip.example.com
SessionTarget=172.18.193.87
OnTimeRvPlayout=48620
GapFillWith Silence=0 ms
GapFillWithPrediction=0 ms
GapFillWith Interpolation=0 ms
GapFillWith Redundancy=0 ms
HiWaterPlayoutDelay=70 ms
LoWaterPlayoutDelay=69 ms
TxPakNumber=2434
TxSignalPak=0
TxComfortNoisePak=0
TxDuration=48680
TxVoiceDuration=48680
RxPakNumber=2434
RxSignalPak=0
RxDuration=0
TxVoiceDuration=48670
VoiceRxDuration=48620
RxOutOfSeq=0
RxLatePak=0
RxEarlyPak=0
PlayDelayCurrent=69
Step 2 Use the `show call history voice` to display output when the local hostname is enabled:
Router# show call history voice

Telephony call-legs:1
SIP call-legs:1
H323 call-legs:0
Call agent controlled call-legs:0
Total call-legs:2

Generic:
SetupTime=128980 ms
Index=1
PeerAddress=9002
PeerSubAddress=
PeerId=3301
PeerIfIndex=7
LogicalIfIndex=0
DisconnectCause=10
DisconnectText=normal call clearing (16)
ConnectTime=130300 ms
DisconnectTime=329120 ms
CallDuration=00:03:18 sec
CallOrigin=1
ReleaseSource=4
ChargedUnits=0
InfoType=speech
TransmitPackets=9981
TransmitBytes=199601
ReceivePackets=9987
ReceiveBytes=199692

VoIP:
ConnectionId[0xA0DC41CF 0x115511D9 0x8002EC82 0xAB4FD5BE]
IncomingConnectionId[0xA0DC41CF 0x115511D9 0x8002EC82 0xAB4FD5BE]
CallID=2
RemoteIPAddress=172.18.193.87
RemoteUDPPort=17602
RemoteSignallingIPAddress=172.18.193.87
RemoteSignallingPort=5060
RemoteMediaIPAddress=172.18.193.87
RemoteMediaPort=17602
SRTP = off
RoundTripDelay=1 ms
SelectedQoS=best-effort
tx_DtmfRelay=inband-voice
FastConnect=FALSE
AnnexE=FALSE
Separate H245 Connection=FALSE
H245 Tunneling=FALSE
SessionProtocol=sipv2
SessionTarget=172.18.193.87
OnTimeRvPlayout=195880
GapFillWithSilence=0 ms
GapFillWithPrediction=0 ms
GapFillWithInterpolation=0 ms
GapFillWithRedundancy=0 ms
HiWaterPlayoutDelay=70 ms
LoWaterPlayoutDelay=69 ms
ReceiveDelay=69 ms
LostPackets=0
EarlyPackets=0
LatePackets=0
VAD = enabled
CoderTypeRate=g729r8
CodecBytes=20
cvVoIPCallHistoryIcpif=2
MediaSetting=flow-around
CallerName=
CallerIDBlocked=False
OriginalCallingNumber=9001
OriginalCallingOctet=0x0
OriginalCalledNumber=9002
OriginalCalledOctet=0x80
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0x0
TranslatedCallingNumber=9001
TranslatedCallingOctet=0x0
TranslatedCalledNumber=9002
TranslatedCalledOctet=0x80
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0x0
GwCollectedCalledNumber=9002
GwOutpulsedCalledNumber=9002
GwOutpulsedCalledOctet3=0x80
GwOutpulsedCallingNumber=9001
GwOutpulsedCallingOctet3=0x0
GwOutpulsedCallingOctet3a=0x0
MediaInactiveDetected=no
MediaInactiveTimestamp=
MediaControlReceived=
LocalHostname=pip.example.com ! LocalHostname field
Username=
GENERIC:
SetupTime=126640 ms
Index=2
PeerAddress=9001
PeerSubAddress=
PeerId=100
PeerIfIndex=6
LogicalIfIndex=4
DisconnectCause=10
DisconnectText=normal call clearing (16)
ConnectTime=130300 ms
DisconnectTime=330080 ms
CallDuration=00:03:19 sec
CallOrigin=2
ReleaseSource=4
ChargedUnits=0
InfoType=speech
TransmitPackets=9987
TransmitBytes=199692
ReceivePackets=9981
ReceiveBytes=199601
TEL:
ConnectionId=[0xA0DC41CF 0x115511D9 0x8002EC82 0xAB4FD5BE]
IncomingConnectionId=[0xA0DC41CF 0x115511D9 0x8002EC82 0xAB4FD5BE]
CallID=1
TxDuration=195940 ms
VoiceTxDuration=195940 ms
FaxTxDuration=0 ms
CoderTypeRate=g729r8
NoiseLevel=-73
ACOMLevel=4
SessionTarget=
ImgPages=0
CallerName=
CallerIDBlocked=False
OriginalCallingNumber=
OriginalCallingOctet=0x0
OriginalCalledNumber=
OriginalCalledOctet=0x80
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0x0
TranslatedCallingNumber=9001
TranslatedCallingOctet=0x0
TranslatedCalledNumber=
TranslatedCalledOctet=0x80
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0x0
GwCollectedCalledNumber=9002
SIP Parameter Modification

The SIP Parameter modification feature allows 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.

Prerequisites

**Cisco Unified Border Element**
- Cisco IOS Release 12.4(15)XZ or a later release must be installed and running on your Cisco Unified Border Element.

**Cisco Unified Border Element (Enterprise)**
- Cisco IOS XE Release 2.5 or a later release must be installed and running on your Cisco ASR 1000 Series Router.

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  - Enter your password if prompted. |
| **Example:** Router> enable | |
| **Step 2** configure terminal | Enters global configuration mode. |
| **Example:** Router# configure terminal | |
| **Step 3** voice service number voip | Enters VoIP voice-service configuration mode. |
| **Example:** Router(config)# voice service 1 voip | |
| **Step 4** voice-class sip-profiles group-number | Establishes individual sip profiles defined by a  
  group-number. Valid group-numbers are from 1 to 1000. |
| **Example:** Router(config)# voice-class sip profiles 42 | |
| **Step 5** response option sip-header option ADD word CR | Add, change, or delete any SIP or SDP header in voice  
  class or sip-profile submode. |
| **Example:** Router(config)# request INVITE sip-header  
  supported remove | |
| **Step 6** exit | Exits the current mode. |
| **Example:** Router(config-dial-peer)# exit | |
| **Step 7** end | Returns to privileged EXEC mode. |
| **Example:** Router(config-voi-srv)# end | |

**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"
!
!
!
SIP—Session Timer Support

The SIP Session Timer Support feature adds the capability to periodically refresh Session Initiation Protocol (SIP) sessions by sending repeated INVITE requests. The repeated INVITE requests, or re-INVITEs, are sent during an active call leg to allow user agents (UAs) or proxies to determine the status of a SIP session. Without this keepalive mechanism, proxies that remember incoming and outgoing requests (stateful proxies) may continue to retain the call state needlessly. If a UA fails to send a BYE message at the end of a session or if the BYE message is lost because of network problems, a stateful proxy does not know that the session has ended. The re-INVITES ensure that active sessions stay active and completed sessions are terminated.

Prerequisites for SIP—Session Timer Support

**Cisco Unified Border Element**
- Cisco IOS Release 12.2(8)T or a later release must be installed and running on your Cisco Unified Border Element.

**Cisco Unified Border Element (Enterprise)**
- Cisco IOS XE Release 2.5 or a later release must be installed and running on your Cisco ASR 1000 Series Router.

Information About SIP—Session Timer Support

To configure the Session Timer feature, you should understand the following concepts:

- “Interoperability and Compatibility” section on page 128
- “Role of the User Agents” section on page 128
- “Session-Expires Header” section on page 129
- “Min-SE Header” section on page 129
- “422 Response Message” section on page 130
- “Supported and Require Headers” section on page 130

Interoperability and Compatibility

- Interoperability—This feature provides a periodic refresh of SIP sessions. The periodic refresh allows user agents and proxies to monitor the status of a SIP session, preventing hung network resources from pausing indefinitely when network failures occur.

- Compatibility—Only one of the two user agent or proxy participants in a call needs to implemented the SIP Session Timer Support feature. This feature is easily compatible with older SIP networks. The SIP Session Timer Support feature also adds two new general headers that are used to negotiate the value of the refresh interval.

Role of the User Agents

The initial INVITE request establishes the duration of the session and may include a Session-Expires header and a Min-SE header. These headers indicate the session timer value required by the user agent client (UAC). A receiving user agent server (UAS) or proxy can lower the session timer value, but not lower than the value of the Min-SE header. If the session timer duration is lower than the configured minimum, the proxy or UAS can also send out a 422 response message. If the UAS or proxy finds that the session timer value is acceptable, it copies the Session-Expires header into the 2xx class response.
A UAS or proxy can insert a Session-Expires header in the INVITE if the UAC did not include one. Thus a UAC can receive a Session-Expires header in a response even if none was present in the request.

In the 2xx response, the refresher parameter in the Session-Expires header indicates who performs the re-INVITEs. For example, if the parameter contains the value UAC, the UAC performs the refreshes. For compatibility issues, only one of the two user agents needs to support the session timer feature, and in that case, the UA that supports the feature performs the refreshes. The other UA interprets the refreshes as repetitive INVITEs and ignores them.

Re-INVITEs are processed identically to INVITE requests, but go out in predetermined session intervals. Re-INVITEs carry the new session expiration time. The UA responsible for generating re-INVITE requests sends a re-INVITE out before the session expires. If there is no response, the UA sends a BYE request to terminate the call before session expiration. If a re-INVITE is not sent before the session expiration, either the UAC or the UAS can send a BYE.

If the 2xx response does not contain a Session-Expires header, there is no session expiration and re-INVITEs do not need to be sent.

**Session-Expires Header**

The Session-Expires header conveys the session interval for a SIP call. It is placed in an INVITE request and is allowed in any 2xx class response to an INVITE. Its presence indicates that the UAC wants to use the session timer for this call. Unlike the SIP-Expires header, it can contain only a delta-time, which is the current time, plus the session interval from the response.

For example, if a UAS generates a 200 OK response to a re-INVITE that contained a Session-Expires header with a value of 1800 seconds (30 minutes), the UAS computes the session expiration as 30 minutes after the time when the 200 OK response was sent. For each proxy, the session expiration is 30 minutes after the time when the 2xx was received or sent. For the UAC, the expiration time is 30 minutes after the receipt of the final response.

The recommended value for the Session-Expires header is 1800 seconds.

The syntax of the Session-Expires header is:

```
Session-Expires = ("Session-Expires" | "x") ";" delta-seconds
                [refresher]
refresher      = ";" "refresher" ";=" "UAS"|"UAC"
```

The refresher parameter is optional in the initial INVITE, although the UAC can set it to UAC to indicate that it will do the refreshes. The 200 OK response must have the refresher parameter set.

**Min-SE Header**

Because of the processing load of INVITE requests you can configure a minimum timer value that the proxy, UAC, and UAS can accept. The proxy, UAC, and UAS. The min-se command sets the minimum timer, and it is conveyed in the Min-SE header in the initial INVITE request.

When making a call, the presence of the Min-SE header informs the UAS and any proxies of the minimum value that the UAC accepts for the session timer duration, in seconds. The default value is 1800 seconds (30 minutes). By not reducing the session timer below the value set, the UAS and proxies prevent the UAC from having to reject a call with a 422 error. Once set, the min-se command value affects all calls originated by the router. If the Min-SE header is not present, the UA accepts any value.

The syntax of the Min-SE header is:

```
Min-SE = "Min-SE" ";" delta-seconds
```
422 Response Message
If the value of the Session-Expires header is too small, the UAS or proxy rejects the call with a 422 Session Timer Too Small response message. With the 422 response message, the proxy or UAS includes a Min-SE header indicating the minimum session value it can accept. The UAC may then retry the call with a larger session timer value.

If a 422 response message is received after an INVITE request, the UAC can retry the INVITE.

Supported and Require Headers
The presence of the timer argument in the Supported header indicates that the UA supports the SIP session timer. The presence of the timer argument in the Require header indicates that the opposite UA must support the SIP session timer for the call to be successful.

How to Configure SIP—Session Timer Support
This section provides information about how to configure the SIP - Session Timer Support feature. and contains the following section:

- “Configuring SIP—Session Timer Support” section on page 130

Prerequisites

- Ensure that the gateway has voice functionality that is configurable for SIP.
- Establish a working IP network.

Restrictions

- Cisco SIP gateways cannot initiate the use of SIP session timers, but do fully support session timers if another UA requests it.
- The Min-SE value can be set only by using the min-se command in the configuration gateway. It cannot be set using the CISCO-SIP-UA-MIB.

Configuring SIP—Session Timer Support
To configure the SIP—Session Timer Support feature, complete this task.

SUMMARY STEPS
1. enable
2. configure terminal
3. voice service voip
4. sip
5. min-se seconds
6. exit
7. show sip-ua min-se
DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 voice service voip</td>
<td>Enters voice service VoIP configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# voice service voip</td>
<td></td>
</tr>
<tr>
<td>Step 4 sip</td>
<td>Enters SIP configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(conf-voi-serv)# sip</td>
<td></td>
</tr>
<tr>
<td>Step 5 min-se seconds</td>
<td>Sets the minimum session expires header value, in seconds, for all calls.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(conf-serv-sip)# min-se 600</td>
<td></td>
</tr>
<tr>
<td>Step 6 min-se exit</td>
<td>Exits the current configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(conf-serv-sip)# exit</td>
<td></td>
</tr>
<tr>
<td>Step 7 min-se show sip-ua min-se</td>
<td>Verifies the value of the Min-SE header.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# show sip-ua min-se</td>
<td></td>
</tr>
</tbody>
</table>

Examples

This example contains partial output from the `show running-config` command. It shows that the Min-SE value has been changed from its default value.

```plaintext
! voice service voip
    sip
    min-se 950
!```

Troubleshooting Tips

To troubleshoot this feature, perform the following steps:

1. Make sure that you can make a voice call.
2. Use the `debug ccsip all` command to enable all SIP debugging capabilities, or use one of the following SIP `debug` commands:
   - `debug ccsip calls`
   - `debug ccsip error`
   - `debug ccsip events`
   - `debug ccsip messages`
   - `debug ccsip states`
SIP-to-SIP Basic Functionality for Session Border Controller

The SIP-to-SIP Basic Functionality for Session Border Controller (SBC) for Cisco Unified Border Element (Cisco UBE) feature provides termination and re-origination of both signaling and media between VoIP and video networks using SIP signaling in conformance with RFC 3261. The SIP-to-SIP protocol interworking capabilities of the Cisco UBE support the following:

- Basic voice calls (Supported audio codecs include: G.711, G.729, G.728, G.726, G.723, G.722, AAC_LD, iLBC. Video codecs: H.263, and H.264)
- Codec transcoding
- Calling/called name and number
- Dual-Tone Multifrequency (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
- Resource Reservation Protocol (RSVP) synchronized with call signaling
- SIP-SIP Video calls
- Tool Command Language Interactive Voice Response (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

Prerequisites

Cisco Unified Border Element
- Cisco IOS Release 12.4(4)T or a later release must be installed and running on your Cisco Unified Border Element.

Cisco Unified Border Element (Enterprise)
- Cisco IOS XE Release 3.1S or a later release must be installed and running on your Cisco ASR 1000 Series Router.
SIP-to-SIP Extended Feature Functionality for Session Border Controllers

The SIP-to-SIP Extended Feature Functionality for Session Border Controllers (SBCs) enables the SIP-to-SIP functionality to conform with RFC 3261 to interoperate with SIP User Agents (UAs). The SIP-to-SIP Extended Feature Functionality includes:

- Call Admission Control (based on CPU, memory, and total calls)
- Delayed Media Call
- ENUM support
- Configuring SIP Error Message Pass Through
- 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)

Prerequisites

**Cisco Unified Border Element**

- Cisco IOS Release 12.4(6)T or a later release must be installed and running on your Cisco Unified Border Element.

**Cisco Unified Border Element (Enterprise)**

- Cisco IOS XE Release 3.1S or a later release must be installed and running on your Cisco ASR 1000 Series Router.
SIP-to-SIP Supplementary Services for Session Border Controller

The SIP-to-SIP Supplementary Services for Session Border Controller (SBC) feature enhances terminating and re-originating signaling and media between VoIP and Video networks by supporting the following features:

- IP Address Hiding in all SIP messages including supplementary services
- Media
  - Media Flow Around
- Support on Cisco AS5350XM and Cisco AS5400XM platforms
- 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

Prerequisites

Cisco Unified Border Element
- Cisco IOS Release 12.4(9)T or a later release must be installed and running on your Cisco Unified Border Element.

Cisco Unified Border Element (Enterprise)
- Cisco IOS XE Release 3.1.0S or a later release must be installed and running on your Cisco ASR 1000 Series Router.
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 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 preferred dial peer, or else the on call is rejected with an error cause code.

Table 1 describes error codes option ping responses considered unsuccessful and the dial-peer is busied out for following scenarios:

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>503</td>
<td>service unavailable</td>
</tr>
<tr>
<td>505</td>
<td>sip version not supported</td>
</tr>
<tr>
<td>no response</td>
<td>i.e. request timeout</td>
</tr>
</tbody>
</table>

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 continues the heartbeat mechanism and the dial-peer is set 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 be in active state
  - Session protocol must be configured for SIP
  - Configure Session target or outbound proxy must be configured. If both are configured, outbound proxy has preference over session target.

Cisco Unified Border Element

- Cisco IOS Release 15.0(1)M or a later release must be installed and running on your Cisco Unified Border Element.

Cisco Unified Border Element (Enterprise)

- Cisco IOS XE Release 3.1S or a later release must be installed and running on your Cisco ASR 1000 Series Router
Restrictions

- The Cisco Unified Border Element OOD Options ping feature can only be configured at the VoIP Dial-peer level.
- All dial peers start in an active (not busied out) state on a router boot or reboot.
- If a dial-peer has both an outbound proxy and a session target configured, the OOD options ping is sent to the outbound proxy address first.
- Though multiple dial-peers may 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td>Example: enable</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: configure terminal</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 dial-peer voice tag voip</td>
<td>Enters dial-peer configuration mode for the VoIP peer designated by tag.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# dial-peer voice 200 voip</td>
<td></td>
</tr>
</tbody>
</table>
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.

**Example:**
```
Router(config-dial-peer)# show dial-peer voice | in options
voice class sip options-keepalive up-interval 60 down-interval 30 retry 5
```

- **show dial-peer voice summary**—shows Active or Busyout dial-peer status.

**Example:**
```
Router# show dial-peer voice summary
```
```
AD  TAG  TYPE  MIN  OPER  PREFIX  DEST-PATTERN  KEEPALIVE
111  voip  up  up      0  syst  active
  9  voip  up  down  0  syst  busy-out
```

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong> voice-class sip options-keepalive (up-interval</td>
<td>Monitors connectivity between endpoints.</td>
</tr>
<tr>
<td>seconds</td>
<td>down-interval seconds</td>
</tr>
<tr>
<td>Example:</td>
<td>- <strong>up-interval seconds</strong>—Number of up-interval seconds allowed to pass before marking the UA as unavailable. The range is 5-1200. The default is 60.</td>
</tr>
<tr>
<td>Router(config-dial-peer)# voice-class sip options-keepalive</td>
<td>- <strong>down-interval seconds</strong>—Number of down-interval seconds allowed to pass before marking the UA as unavailable. The range is 5-1200. The default is 30.</td>
</tr>
<tr>
<td>up-interval 12 down-interval 65 retry 3</td>
<td>- <strong>retry retries</strong>—Number of retry attempts before marking the UA as unavailable. The range is 1 to 10. The default is 5 attempts.</td>
</tr>
<tr>
<td><strong>Step 5</strong> exit</td>
<td>Exits the current mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-dial-peer)# exit</td>
<td></td>
</tr>
</tbody>
</table>

**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.

**Example:**
```
Router(config-dial-peer)# 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.

**Example:**
```
Router# show dial-peer voice summary
```
```
AD  TAG  TYPE  MIN  OPER  PREFIX  DEST-PATTERN  KEEPALIVE
111  voip  up  up      0  syst  active
  9  voip  up  down  0  syst  busy-out
```
SIP—INFO Method for DTMF Tone Generation

The SIP—INFO Method for DTMF Tone Generation feature uses the Session Initiation Protocol (SIP) INFO method to generate dual tone multifrequency (DTMF) tones on the telephony call leg. SIP info methods, or request message types, request a specific action be taken by another user agent (UA) or proxy server. The SIP INFO message is sent along the signaling path of the call. Upon receipt of a SIP INFO message with DTMF relay content, the gateway generates the specified DTMF tone on the telephony end of the call.

Prerequisites for SIP—INFO Method for DTMF Tone Generation

Cisco Unified Border Element
- Cisco IOS Release 12.2(11)T or a later release must be installed and running on your Cisco Unified Border Element.

Cisco Unified Border Element (Enterprise)
- Cisco IOS XE Release 2.5 or a later release must be installed and running on your Cisco ASR 1000 Series Router.

Information About SIP—INFO Method for DTMF Tone Generation

The SIP—INFO Method for DTMF Tone Generation feature is always enabled, and is invoked when a SIP INFO message is received with DTMF relay content. This feature is related to the DTMF Events Through SIP Signaling feature, which allows an application to be notified about DTMF events using SIP NOTIFY messages. Together, the two features provide a mechanism to both send and receive DTMF digits along the signaling path. For more information on sending DTMF event notification using SIP NOTIFY messages, refer to the DTMF Events Through SIP Signaling feature.

How to Review SIP INFO Messages

The SIP INFO method is used by a UA to send call signaling information to another UA with which it has an established media session. The following example shows a SIP INFO message with DTMF content:

```
INFO sip:2143302100@172.17.2.33 SIP/2.0
Via: SIP/2.0/UDP 172.80.2.100:5060
From: <sip:9724401003@172.80.2.100>;tag=43
To: <sip:2143302100@172.17.2.33>;tag=9753.0207
Call-ID: 984072_15401962@172.80.2.100
CSeq: 25634 INFO
Supported: 100rel
Supported: timer
Content-Length: 26
Content-Type: application/dtmf-relay

Signal= 1
  Duration= 160
```

This sample message shows a SIP INFO message received by the gateway with specifics about the DTMF tone to be generated. The combination of the “From”, “To”, and “Call-ID” headers identifies the call leg. The signal and duration headers specify the digit, in this case 1, and duration, 160 milliseconds in the example, for DTMF tone play.
Prerequisites

The following are general prerequisites for SIP functionality:

- Ensure that the gateway has voice functionality that is configured for SIP.
- Establish a working IP network.
- Configure VoIP.

Restrictions

The SIP—INFO Method for DTMF Tone Generation feature includes the following signal duration parameters:

- Minimum signal duration is 100 milliseconds (ms). If a request is received with a duration less than 100 ms, the minimum duration of 100 ms is used by default.
- Maximum signal duration is 5000 ms. If a request is received with a duration longer than 5000 ms, the maximum duration of 5000 ms is used by default.
- If no duration parameter is included in a request, the gateway defaults to a signal duration of 250 ms.

Configuring for SIP—INFO Method for DTMF Tone Generation

You cannot configure, enable, or disable this feature. No configuration tasks are required to configure the SIP—INFO Method for DTMF Tone Generation feature. The feature is enabled by default.

Troubleshooting Tips

You can display SIP statistics, including SIP INFO method statistics, by using the `show sip-ua statistics` and `show sip-ua status` commands in privileged EXEC mode. See the following fields for SIP INFO method statistics:

- OkInfo 0/0, under SIP Response Statistics, Success, displays the number of successful responses to an INFO request.
- Info 0/0, under SIP Total Traffic Statistics, displays the number of INFO messages received and sent by the gateway.

The following is sample output from the `show sip-ua statistics` command:

```
Router# show sip-ua statistics

SIP Response Statistics (Inbound/Outbound)
  Informational:
    Trying 1/1, Ringing 0/0,
    Forwarded 0/0, Queued 0/0,
    SessionProgress 0/1
  Success:
    OkInvite 0/1, OkBye 1/0,
    OkCancel 0/0, OkOptions 0/0,
    OkPrack 0/0, OkPreconditionMet 0/0
    OkSubscribe 0/0, OkNotify 0/0,
    OkInfo 0/0, 202Accepted 0/0
  Redirection (Inbound only):
    MultipleChoice 0, MovedPermanently 0,
    MovedTemporarily 0, SeeOther 0,
    UseProxy 0, AlternateService 0
Client Error:
```
BadRequest 0/0, Unauthorized 0/0,
PaymentRequired 0/0, Forbidden 0/0,
NotFound 0/0, MethodNotAllowed 0/0,
NotAcceptable 0/0, ProxyAuthReqd 0/0,
ReqTimeout 0/0, Conflict 0/0, Gone 0/0,
LengthRequired 0/0, ReqEntityTooLarge 0/0,
ReqURITooLarge 0/0, UnsupportedMediaType 0/0,
BadExtension 0/0, TempNotAvailable 0/0,
CallLegNonExistent 0/0, LoopDetected 0/0,
TooManyHops 0/0, AddrIncomplete 0/0,
Ambiguous 0/0, BusyHere 0/0,
BadEvent 0/0
Server Error:
InternalError 0/0, NotImplemented 0/0,
BadGateway 0/0, ServiceUnavail 0/0,
GatewayTimeout 0/0, BadSipVer 0/0
Global Failure:
BusyEverywhere 0/0, Decline 0/0,
NotExistAnywhere 0/0, NotAcceptable 0/0
SIP Total Traffic Statistics (Inbound/Outbound)
Invite 0/0, Ack 0/0, Bye 0/0,
Cancel 0/0, Options 0/0,
Prack 0/0, Comet 0/0,
Subscribe 0/0, Notify 0/0,
Refer 0/0, Info 0/0
Retry Statistics
Invite 0, Bye 0, Cancel 0, Response 0, Notify 0

The following is sample output from the `show sip-ua status` command:

Router# `show sip-ua status`

SIP User Agent Status
SIP User Agent for UDP : ENABLED
SIP User Agent for TCP : ENABLED
SIP User Agent bind status(signaling): DISABLED
SIP User Agent bind status(media): DISABLED
SIP max-forwards : 6
SIP DNS SRV version: 2 (rfc 2782)
SDP application configuration:
Version line (v=) required
Owner line (o=) required
Session name line (s=) required
Timespec line (t=) required
Media supported: audio image
Network types supported: IN
Address types supported: IP4
Transport types supported: RTP/AVP udptl
SIP—Enhanced 180 Provisional Response Handling

The SIP—Enhanced 180 Provisional Response Handling feature enables early media cut-through on Cisco IOS gateways for Session Initiation Protocol (SIP) 180 response messages.

Prerequisites SIP—Enhanced 180 Provisional Response Handling

Cisco Unified Border Element
- Cisco IOS Release 12.2(8)T or a later release must be installed and running on your Cisco Unified Border Element.

Cisco Unified Border Element (Enterprise)
- Cisco IOS XE Release 2.5 or a later release must be installed and running on your Cisco ASR 1000 Series Router.

Information About SIP—Enhanced 180 Provisional Response Handling

The Session Initiation Protocol (SIP) feature allows you to specify whether 180 messages with Session Description Protocol (SDP) are handled in the same way as 183 responses with SDP. The 180 Ringing message is a provisional or informational response used to indicate that the INVITE message has been received by the user agent and that alerting is taking place. The 183 Session Progress response indicates that information about the call state is present in the message body media information. Both 180 and 183 messages may contain SDP, which allows an early media session to be established prior to the call being answered.

Prior to this feature, Cisco gateways handled a 180 Ringing response with SDP in the same manner as a 183 Session Progress response; that is, the SDP was assumed to be an indication that the far end would send early media. Cisco gateways handled a 180 response without SDP by providing local ringback, rather than early media cut-through. This feature provides the capability to ignore the presence or absence of SDP in 180 messages, and as a result, treat all 180 messages in a uniform manner. The SIP—Enhanced 180 Provisional Response Handling feature allows you to specify which call treatment, early media or local ringback, is provided for 180 responses with SDP:

Table 1 shows the call treatments available with this feature:

<table>
<thead>
<tr>
<th>Response Message</th>
<th>SIP Enhanced 180 Provisional Response Handling Status</th>
<th>Treatment</th>
</tr>
</thead>
<tbody>
<tr>
<td>180 response with SDP</td>
<td>Enabled (default)</td>
<td>Early media cut-through</td>
</tr>
<tr>
<td>180 response with SDP</td>
<td>Disabled</td>
<td>Local ringback</td>
</tr>
<tr>
<td>180 response without SDP</td>
<td>Not affected by the SIP—Enhanced 180 Provisional Response Handling feature</td>
<td>Local ringback</td>
</tr>
<tr>
<td>183 response with SDP</td>
<td>Not affected by the SIP—Enhanced 180 Provisional Response Handling feature</td>
<td>Early media cut-through</td>
</tr>
</tbody>
</table>
How to Disable the SIP Enhanced 180 Provisional Response Handling Feature

This section describes the configuration tasks for the SIP Enhanced 180 Provisional Response Handling feature:

- Disabling Early Media Cut-Through, page 147 (optional)

Disabling Early Media Cut-Through

The early media cut-through feature is enabled by default. To disable early media cut-through, perform the following task:

**SUMMARY STEPS**

1. enable
2. configure terminal
3. interface type number
4. sip ua
5. disable-early-media 180

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 enable     | Enables privileged EXEC mode.  
|                   | • Enter your password if prompted. |
| Example:          | Router> enable |
| Step 2 configure terminal | Enters global configuration mode. |
| Example:          | Router# configure terminal |
| Step 3 interface type number | Configures an interface type and enters interface configuration mode. |
| Example:          | Router(config)# ethernet 0/0/0 |
| Step 4 sip ua     | Enables SIP UA configuration commands in order to configure the user agent. |
| Example:          | Router(config-sip-ua)# sip ua |
| Step 5 disable-early-media 180 | Disables the gateway’s ability to process SDP in a 180 response as a request for early media cut-through. |
| Example:          | Router(config-sip-ua)# disable-early-media 180 |
Verifying SIP Enhanced 180 Provisional Response Handling

- To verify the SIP Enhanced 180 Provisional Response Handling feature use the `show running configuration` or `show sip-ua status` or `show logging` command to display the output.
- If early media is enabled, which is the default setting, the `show running-config` output does not show any information related to the new feature.
- To monitor this feature, use the `show sip-ua statistics` and `show sip-ua status` EXEC commands.

Configuration Examples for SIP - Enhanced 180 Provisional Response Handling

This section displays sample outputs from the following show commands:

- `show running-config` Command
- `show sip-ua status` Command
- `show logging` Command

**show running-config Command**

The following is sample output from the `show running-config` command after the `disable-early-media 180` command was used:

```
Router# show running-config
.
.
.
dial-peer voice 223 pots
    application session
    destination-pattern 223
    port 1/0/0

! gateway
! sip-ua
    disable-early-media 180
```

**show sip-ua status Command**

The following is sample output from the `show sip-ua status` command after the `disable-early-media 180` command was used.

```
Router# show sip-ua status

SIP User Agent Status
SIP User Agent for UDP :ENABLED
SIP User Agent for TCP :ENABLED
SIP User Agent bind status(signaling):ENABLED 10.0.0.0
SIP User Agent bind status(media):ENABLED 0.0.0.0
SIP early-media for 180 responses with SDP:DISABLED
SIP max-forwards :6
SIP DNS SRV version:2 (rfc 2782)
NAT Settings for the SIP-UA
Role in SDP:NONE
Check media source packets:DISABLED
Redirection (3xx) message handling:ENABLED

SDP application configuration:
    Version line (v=) required
```
Owner line (o=) required
Timespec line (t=) required
Media supported: audio image
Network types supported: IN
Address types supported: IP4
Transport types supported: RTP/AVP udptl

**show logging Command**

The following is partial sample output from the `show logging` command. The outgoing gateway is receiving a 180 message with SDP and is configured to ignore the SDP.

Router# show logging

Log Buffer (600000 bytes):

00:12:19:%SYS-5-CONFIG_I:Configured from console by console
00:12:19:%SYS-5-CONFIG_I:Configured from console by console
00:12:20:0x639F6EEC :State change from (STATE_NONE, SUBSTATE_NONE) to
(State_IDLE, SUBSTATE_NONE)
00:12:20:** Adding to UAC table

00:12:20:adding call id 2 to table

00:12:20: Queued event from SIP SPI : SIP_SPI_EV_CALL_SETUP
00:12:20: :act_idle_call_setup
00:12:20: act_idle_call_setup:Not using Voice Class Codec
00:12:20:act_idle_call_setup:preferred_codec set[0] type :g711ulaw
bytes:160
00:12:20: sipSPICopyPeerDataToCCB:From CLI:Modem NSE payload = 100,
Passthrough = 0, Modem relay = 0, Gw-Xid = 1
SPRT latency 200, SPRT Retries = 12, Dict Size = 1024
String Len = 32, Compress dir = 3
00:12:20: sipSPICanSetFallbackFlag - Local Fallback is not active
00:12:20: ** Deleting from UAC table

00:12:20:** Adding to UAC table

00:12:20: Queued event from SIP SPI : SIP_SPI_EV_CREATE_CONNECTION
00:12:20:0x639F6EEC :State change from (STATE_IDLE, SUBSTATE_NONE) to
(State_IDLE, SUBSTATE_CONNECTING)
00:12:20:0x639F6EEC :State change from (STATE_IDLE, SUBSTATE_CONNECTING)
00:12:20:0x639F6EEC :State change from (STATE_IDLE, SUBSTATE_CONNECTING)
00:12:20: sipSPISetBillingProfile:sipCallId for billing records =
41585FCE-14F011CC-8005AF80-D4AA31530172.31.1.42
00:12:20: CCSIP-SPI-CONTROL: act_idle_connection_created
00:12:20: CCSIP-SPI-CONTROL: act_idle_connection_created:Connid(1)
created to 172.31.1.15:5060, local_port 57838
00:12:20: CCSIP-SPI-CONTROL: sipSPIOutgoingCallSDP
00:12:20: convert_codec_bytes_to_ptime:Values :Codec:g711ulaw
codecbytes :160, ptime:20
00:12:20: sip_generate_sdp_xcaps_list:Modem Relay disabled. X-cap not
needed
00:12:20: Received Octet3A=0x00 -> Setting ;screen=no ;privacy=off
00:12:20: sipSPIAddLocalContact
00:12:20: Queued event from SIP SPI : SIP_SPI_EV_SEND_MESSAGE
00:12:20: sip_stats_method
00:12:20: sipSPIProcessRtpSessions
00:12:20: sipSPIAddStream: Adding stream 1 (callid 2) to the VOIP RTP library
00:12:20: sipSPISetMediaSrcAddr: media src addr for stream 1 = 10.1.1.42
00:12:20: sipSPIUpdateRtcpSession: for m-line 1
00:12:20: sipSPIUpdateRtcpSession: rtcp_session info
     laddr = 10.1.1.42, lport = 18978, raddr = 0.0.0.0, rport=0, do_rtcp=FALSE
     src_callid = 2, dest_callid = -1

00:12:20: sipSPIUpdateRtcpSession: No RTP session, creating a new one

00:12:20: sipSPIAddStream: In State Idle
00:12:20: act_idle_connection_created: Transaction active. Facilities will be queued.
00:12:20: 0x639F6EEC : State change from (STATE_IDLE, SUBSTATE_CONNECTING) to (STATE_SENT_INVITE, SUBSTATE_NONE)
00:12:20: Sent:
INVITE sip:222@172.31.1.15:5060 SIP/2.0
Via:SIP/2.0/UDP 10.1.1.42:5060
From:"111" <sip:111@172.31.1.42>;tag=B4DC4-9E1
To:<sip:222@172.31.1.15>
Date:Mon, 01 Mar 1993 00:12:20 GMT
Call-ID:41585FCE-14F011CC-8005AF80-D4AA31530172.31.1.42
Supported:timer
Min-SE: 1800
Cisco-Guid:1096070726-351277516-2147659648-3567923539
User-Agent:Cisco-SIPGateway/IOS-12.x
Allow:INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, COMET, REFER, SUBSCRIBE, NOTIFY, INFO
CSeq:101 INVITE
Max-Forwards:6
Remote-Party-ID:<sip:111@172.31.1.42>;party=calling;screen=no;privacy=off
Timestamp:730944740
Contact:<sip:111@172.31.1.42:5060>
Expires:180
Allow-Events:telephone-event
Content-Type:application/sdp
Content-Length:230

v=0
o=CiscoSystemsSIP-GW-UserAgent 4629 354 IN IP4 172.31.1.42
s=SIP Call
c=IN IP4 172.31.1.42
t=0 0
m=audio 18978 RTP/AVP 0 100
a=rtpmap:0 PCMU/8000
a=rtpmap:100 X-NSE/8000
a=fmtp:100 192-194
a=ptime:20

00:12:21: Received:
SIP/2.0 100 Trying
Via:SIP/2.0/UDP 10.1.1.42:5060
From:"111" <sip:111@172.31.1.42>;tag=B4DC4-9E1
To:<sip:222@172.31.1.15>;tag=442AC-22
Date:Wed, 16 Feb 2000 18:19:56 GMT
Call-ID:41585FCE-14F011CC-8005AF80-D4AA31530172.31.1.42
Timestamp:730944740
Server:Cisco-SIPGateway/IOS-12.x
CSeq:101 INVITE
Allow-Events:telephone-event
Content-Length:0
00:12:21:HandleUdpSocketReads :Msg enqueued for SPI with IPaddr: 10.1.1.15:5060
00:12:21:CCSIP-SPI-CONTROL: act_sentinvite_new_message
00:12:21:CCSIP-SPI-CONTROL: sipSPICheckResponse
00:12:21:sip_stats_status_code
00:12:21: Roundtrip delay 420 milliseconds for method INVITE

00:12:21:0x639F6EEC :State change from (STATE_SENT_INVITE, SUBSTATE_NONE) to (STATE_RECD_PROCEEDING, SUBSTATE_PROCEEDING_PROCEEDING)
00:12:21:Received: SIP/2.0 180 Ringing
Via:SIP/2.0/UDP 10.1.1.42:5060
From:"111" <sip:111@10.1.1.42>;tag=B4DC4-9E1
To:<sip:222@172.31.1.15>;tag=442AC-22
Date:Wed, 16 Feb 2000 18:19:56 GMT
Call-ID:41585FCE-14F011CC-8005AP80-D4AA31530172.31.1.42
Timestamp:730944740
Server:Cisco-SIPGateway/IOS-12.x
CSeq:101 INVITE
Allow-Events:telephone-event
Contact:<sip:222@172.31.1.59:5060;maddr=10.1.1.15>
Record-Route:<sip:222@10.1.1.15:5060>maddr=10.1.1.15>
Content-Length:230
Content-Type:application/sdp

v=0
o=CiscoSystemsSIP-GW-UserAgent 4629 354 IN IP4 10.1.1.42
c=IN IP4 10.1.1.42
t=0 0
m=audio 18978 RTP/AVP 0 100
c=IN IP4 10.1.1.42
a=rtpmap:0 PCMU/8000
a=rtpmap:100 X-NSE/8000
a=ptime:20

00:12:21:HandleUdpSocketReads :Msg enqueued for SPI with IPaddr: 10.1.1.15:5060
00:12:21:CCSIP-SPI-CONTROL: act_recproc_new_message
00:12:21:CCSIP-SPI-CONTROL: act_recproc_new_message_response
00:12:21:CCSIP-SPI-CONTROL: sipSPICheckResponse
00:12:21:sip_stats_status_code
00:12:21: Roundtrip delay 496 milliseconds for method INVITE
00:12:21:CCSIP-SPI-CONTROL: act_recproc_new_message_response :Early media disabled for 180:Ignoring SDP if present
00:12:21:HandleSIP1xxRinging:SDP in 180 will be ignored if present: No early media cut through
00:12:21:HandleSIP1xxRinging:SDP Body either absent or ignored in 180 RINGING:-- would wait for 200 OK to do negotiation.
00:12:21:HandleSIP1xxRinging:MediaNegotiation expected in 200 OK
00:12:21:sipSPIGetGtdBody:No valid GTD body found.
00:12:21:sipSPICreateRawMsg:No GTD passed.
00:12:21:0x639F6EEC :State change from (STATE_RECV_PROCEEDING, SUBSTATE_PROCEEDING_PROCEEDING) to (STATE_RECV_PROCEEDING, SUBSTATE_PROCEEDING_ALERTING)
00:12:22:Received:
SIP/2.0 200 OK
Via:SIP/2.0/UDP 10.1.1.42:5060
From:"111" <sip:111010.1.1.42>;tag=B4DC4-9E1
To:<sip:222@10.1.1.15>;tag=442AC-22
Date:Wed, 16 Feb 2000 18:19:56 GMT
Call-ID:41585FCE-14F011CC-8005AF80-D4AA31530172.31.1.42
Timestamp:730944740
Server:Cisco-SIPGateway/IOS-12.x
CSeq:101 INVITE
Allow:INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, COMET, REFER, SUBSCRIBE,
NOTIFY, INFO
Allow-Events:telephone-event
Contact:<sip:222@10.1.1.59:5060>
Record-Route:<sip:222@10.1.1.15:5060;maddr=10.1.1.15>
Content-Type:application/sdp
Content-Length:231

v=0
o=CiscoSystemsSIP-GW-UserAgent 9600 4816 IN IP4 10.1.1.59
s=SIP Call
c=IN IP4 10.1.1.59
t=0 0
m=audio 19174 RTP/AVP 0 100
c=IN IP4 10.1.1.59
a=rtpmap:0 PCMU/8000
a=rtpmap:100 X-NSE/8000
a=fmtp:100 192-194
a=ptime:20
Configuring Support for SIP 181 Call is Being Forwarded Message

You can configure support for SIP 181 Call is Being Forwarded messages either globally or on a specific dial-peer. Use the block command in voice service SIP configuration mode to globally configure Cisco IOS voice gateways and Cisco UBEs to drop specified SIP provisional response messages. To configure settings for an individual dial peer, use the voice-class sip block command in dial peer voice configuration mode. Both globally and at the dial peer level, you can also use the sdp keyword to further control when the specified SIP message is dropped based on either the absence or presence of SDP information.

Additionally, you can use commands introduced for this feature to configure a Cisco UBE, either globally or at the dial peer level, to map specific received SIP provisional response messages to a different SIP provisional response message on the outgoing SIP dial peer. To do so, use the map resp-code command in voice service SIP configuration mode for global configuration or, to configure a specific dial peer, use the voice-class sip map resp-code in dial peer voice configuration mode.

This section contains the following tasks:

- Configuring Support for SIP 181 “Call is Being Forwarded” Message Globally, page 153
- Configuring Support for SIP 181 “Call is Being Forwarded” Message at the Dial-Peer Level, page 154
- Configuring Mapping of SIP Provisional Response Messages Globally, page 155
- Configuring Mapping of SIP Provisional Response Messages at the Dial-Peer Level, page 156

Prerequisites

Cisco Unified Border Element
Cisco IOS Release 15.0(1)XA or a later release must be installed and running on your Cisco Unified Border Element.

Cisco Unified Border Element (Enterprise)
- Cisco IOS XE Release 3.1S or a later release must be installed and running on your Cisco ASR 1000 Series Router.

Configuring Support for SIP 181 “Call is Being Forwarded” Message Globally

Perform this task to configure support for SIP 181 messages at a global level in SIP configuration (conf-serv-sip) mode.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. voice service voip
4. sip
5. block {180 | 181 | 183} [sdp {absent | present}]
6. exit
DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enters privileged EXEC mode, or other security level set by a system administrator.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td>Enters privileged EXEC mode, or other security level set by a system administrator.</td>
</tr>
<tr>
<td>• Enter your password if prompted.</td>
<td></td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 3 voice service voip</td>
<td>Enters voice service VoIP configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# voice service voip</td>
<td>Enters voice service VoIP configuration mode.</td>
</tr>
<tr>
<td>Step 4 sip</td>
<td>Enters SIP configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-vol-serv)# sip</td>
<td>Enters SIP configuration mode.</td>
</tr>
<tr>
<td>Step 5 block (180</td>
<td>181</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(conf-serv-sip)# block 181 sdp present</td>
<td>Configures support of SIP 181 messages globally so that messages are passed as is. The sdp keyword is optional and allows for dropping or passing of SIP 181 messages based on the presence or absence of SDP.</td>
</tr>
<tr>
<td>Step 6 exit</td>
<td>Exits the current mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(conf-serv-sip)# exit</td>
<td>Exits the current mode.</td>
</tr>
</tbody>
</table>

Configuring Support for SIP 181 “Call is Being Forwarded” Message at the Dial-Peer Level

Perform this task to configure support for SIP 181 messages at the dial-peer level, in dial peer voice configuration (config-dial-peer) mode.

SUMMARY STEPS

1. enable
2. configure terminal
3. dial-peer voice tag voip
4. voice-class sip block {180 | 181 | 183} [sdp {absent | present}]
5. exit
DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enters privileged EXEC mode, or other security level set by a system administrator.</td>
</tr>
<tr>
<td>Example: Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 dial-peer voice tag voip</td>
<td>Enters dial peer VoIP configuration mode.</td>
</tr>
<tr>
<td>Example: Router(config)# dial-peer voice 2 voip</td>
<td></td>
</tr>
<tr>
<td>Step 4 voice-class sip block (180</td>
<td>181</td>
</tr>
<tr>
<td>Example: Router(config-dial-peer)# voice-class sip block 181 sdp present</td>
<td></td>
</tr>
<tr>
<td>Step 5 exit</td>
<td>Exits the current mode.</td>
</tr>
<tr>
<td>Example: Router(config-dial-peer)# exit</td>
<td></td>
</tr>
</tbody>
</table>

Configuring Mapping of SIP Provisional Response Messages Globally

Perform this task to configure mapping of specific received SIP provisional response messages at a global level in SIP configuration (conf-serv-sip) mode.

SUMMARY STEPS

1. enable
2. configure terminal
3. voice service voip
4. sip
5. map resp-code 181 to 183
6. exit
**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enters privileged EXEC mode, or other security level set by a system administrator.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> voice service voip</td>
<td>Enters voice service VoIP configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# voice service voip</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> sip</td>
<td>Enters SIP configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(conf-voi-serv)# sip</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> map resp-code 181 to 183</td>
<td>Enables mapping globally of received SIP messages of a specified message type to a different SIP message type.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(conf-serv-sip)# map resp-code 181 to 183</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> exit</td>
<td>Exits the current mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(conf-serv-sip)# exit</td>
<td></td>
</tr>
</tbody>
</table>

**Configuring Mapping of SIP Provisional Response Messages at the Dial-Peer Level**

Perform this task to configure mapping of received SIP provisional response messages at the dial-peer level, in dial peer voice configuration (config-dial-peer) mode.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. dial-peer voice tag voip
4. voice-class sip map resp-code 181 to 183
5. exit
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1  enable</strong></td>
<td>Enters privileged EXEC mode, or other security level set by a system administrator.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><em>Enter your password if prompted.</em></td>
</tr>
<tr>
<td><strong>Step 2  configure terminal</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3  dial-peer voice tag voip</strong></td>
<td>Enters dial peer VoIP configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4  voice-class sip map resp-code 181 to 183</strong></td>
<td>Enables mapping of received SIP messages of a specified SIP message type on a specific dial peer to a different SIP message type.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5  exit</strong></td>
<td>Exits the current mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
</tbody>
</table>
Support for Expires Timer Reset on Receiving or Sending SIP 183 Message

This feature enables support for resetting the Expires timer when receiving or sending SIP 183 messages on Cisco Unified Communications Manager Express (Cisco Unified CME), a Cisco IOS voice gateway, or a Cisco Unified Border Element (Cisco UBE). When the terminating device lacks answer supervision or does not send the required SIP 200 OK message within the timer expiry, you can enable this feature to send periodic SIP 183 messages to reset the Expires timer and preserve the call until final response. This feature can be enabled globally or on a specific dial peer. Additionally, you can configure this feature based on the presence or absence of Session Description Protocol (SDP).

For details about enabling this feature, see the `reset timer expires` and `voice-class sip reset timer expires` commands in the *Cisco IOS Voice Command Reference*.

Prerequisites

Before configuring support for Expires timer reset for SIP 183 on Cisco IOS SIP time-division multiplexing (TDM) gateways, Cisco UBEs, or Cisco Unified CME, verify the SIP configuration within the VoIP network for the appropriate originating and terminating gateways as described in the *Cisco IOS SIP Configuration Guide*.

**Cisco Unified Border Element**

- Cisco IOS Release 15.0(1)XA or a later release must be installed and running on your Cisco Unified Border Element.

**Cisco Unified Border Element (Enterprise)**

- Cisco IOS XE Release 3.1S or a later release must be installed and running on your Cisco ASR 1000 Series Router.

How to Configure Support for Expires Timer Reset on Receiving or Sending SIP 183 Message

To configure the Support for Expires Timer Reset on Receiving or Sending SIP 183 Message feature, complete the tasks in this section. You can enable this feature globally, using the `reset timer expires` command in voice service SIP configuration mode, or on a specific dial-peer using the `voice-class sip reset timer expires` command in dial peer voice configuration mode:

1. Configuring Reset of Expires Timer Globally
2. Configuring Reset of Expires Timer at the Dial-Peer Level

Configuring Reset of Expires Timer Globally

Perform this task to enable resetting of the Expires timer at the global level in SIP configuration (conf-serv-sip) mode.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `voice service voip`
4. `sip`
5. `reset timer expires 183`
6. exit

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> voice service voip</td>
<td>Enters voice service VoIP configuration mode.</td>
</tr>
<tr>
<td>Example: Router(config)# voice service voip</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> sip</td>
<td>Enters SIP configuration mode.</td>
</tr>
<tr>
<td>Example: Router(conf-voi-serv)# sip</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> reset timer expires 183</td>
<td>Enables resetting of the Expires timer upon receipt of SIP 183 messages globally.</td>
</tr>
<tr>
<td>Example: Router(conf-serv-sip)# reset timer expires 183</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> exit</td>
<td>Exits the current mode.</td>
</tr>
<tr>
<td>Example: Router(conf-serv-sip)# exit</td>
<td></td>
</tr>
</tbody>
</table>

**Configuring Reset of Expires Timer at the Dial-Peer Level**

Perform this task to enable resetting of the Expires timer at the dial-peer level in dial peer voice configuration (config-dial-peer) mode.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. dial-peer voice tag voip
4. voice-class sip reset timer expires 183
5. exit
## Detailed Steps

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  - Enter your password if prompted. |
| **Example:**  
  Router> enable |
| **Step 2** configure terminal | Enters global configuration mode. |
| **Example:**  
  Router# configure terminal |
| **Step 3** dial-peer voice tag voip | Enters dial peer VoIP configuration mode. |
| **Example:**  
  Router(config)# dial-peer voice 2 voip |
| **Step 4** voice-class sip reset timer expires 183 | Enables resetting of the Expires timer upon receipt of SIP 183 messages on a specific dial peer. |
| **Example:**  
  Router(config-dial-peer)# voice-class sip reset timer expires 183 |
| **Step 5** exit | Exits the current mode. |
| **Example:**  
  Router(config-dial-peer)# exit |
Support for PAID, PPID, Privacy, PCPID, and PAURI Headers on the Cisco Unified Border Element

Figure 1 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).

Figure 1 Cisco Unified Border Element and Next Generation Topology

Devices that connect to an NGN must comply with the User-Network Interface (UNI) specification. The Cisco Unified Border Element supports the NGN UNI specification and can be configured to interconnect NGN with other call manager systems, such as the Cisco Unified Call Manager.

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), 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 and/or pass through of privacy header values
- 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, generates a PAID based on the preferred number, and inserts it into the outgoing INVITE message towards the called party.

However, some call manager systems, such as Cisco Unified Call Manager 5.0, use the Remote-Party Identity (RPID) value to send calling party 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. Similarly, CUBE supports building the RPID and/or From: header values for an outgoing INVITE message to the call manager, using the PAID value received in the incoming INVITE message 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/PPID 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.
If the NGN sets the From: value to anonymous, the PAID is the only value that identifies the caller.

Table 1 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.

Table 1 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 1  
<table>
<thead>
<tr>
<th>P-header Configuration Settings</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Incoming Header</th>
<th>Outgoing Header</th>
<th>Configuration Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>From:</td>
<td>PPID</td>
<td></td>
</tr>
<tr>
<td></td>
<td>To enable the translation to PPID headers in the outgoing header at a global level, use the <code>asserted-id ppi</code> command in voice service VoIP SIP configuration mode. For example: <code>Router(conf-serv-sip)# asserted-id ppi</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>To enable the translation to PPID headers in the outgoing header on a specific dial peer, use the <code>voice-class sip asserted-id ppi</code> command in dial peer voice configuration mode. For example: <code>Router(config-dial-peer)# voice-class sip asserted-id ppi</code></td>
<td></td>
</tr>
<tr>
<td>From:</td>
<td>PAID</td>
<td></td>
</tr>
<tr>
<td></td>
<td>To enable the translation to PAID headers in the outgoing header at a global level, use the <code>asserted-id pai</code> command in voice service VoIP SIP configuration mode. For example: <code>Router(conf-serv-sip)# asserted-id pai</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>To enable the translation to PAID headers in the outgoing header on a specific dial peer, use the <code>voice-class sip asserted-id pai</code> command in dial peer voice configuration mode. For example: <code>Router(config-dial-peer)# voice-class sip asserted-id pai</code></td>
<td></td>
</tr>
<tr>
<td>From:</td>
<td>RPID</td>
<td></td>
</tr>
<tr>
<td></td>
<td>To enable the translation to RPID headers in the outgoing header, use the <code>remote-party-id</code> command in SIP user-agent configuration mode. For example: <code>Router(config-sip-ua)# remote-party-id</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>This is the default system behavior.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Note If both, <code>remote-party-id</code> and <code>asserted-id</code> commands are configured, then the <code>asserted-id</code> command takes precedence over the <code>remote-part-id</code> command.</td>
<td></td>
</tr>
<tr>
<td>PPID</td>
<td>PAID</td>
<td></td>
</tr>
<tr>
<td></td>
<td>To enable the translation to PAID privacy headers in the outgoing header at a global level, use the <code>asserted-id pai</code> command in voice service VoIP SIP configuration mode. For example: <code>Router(conf-serv-sip)# asserted-id pai</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>To enable the translation to PAID privacy headers in the outgoing header on a specific dial peer, use the <code>voice-class sip asserted-id pai</code> command in dial peer voice configuration mode. For example: <code>Router(config-dial-peer)# voice-class sip asserted-id pai</code></td>
<td></td>
</tr>
<tr>
<td>PPID</td>
<td>From:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>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 <code>no remote-party-id</code> command in SIP user-agent configuration mode. For example: <code>Router(config-sip-ua)# no remote-party-id</code></td>
<td></td>
</tr>
</tbody>
</table>
Privacy

If the user is subscribed to a privacy service, the Cisco Unified Border Element can support privacy using one of the following methods:

<table>
<thead>
<tr>
<th>Incoming Header</th>
<th>Outgoing Header</th>
<th>Configuration Notes</th>
</tr>
</thead>
</table>
| PPID            | RPID            | To enable the translation to RPID headers in the outgoing header, use the `remote-party-id` command in SIP user-agent configuration mode. For example: `Router(config-sip-ua)# remote-party-id`  
This is the default system behavior. |
| PAID            | PPID            | To enable the translation to PPID privacy headers in the outgoing header at a global level, use the `asserted-id ppi` command in voice service VoIP SIP configuration mode. For example: `Router(conf-serv-sip)# asserted-id ppi`  
To enable the translation to PPID privacy headers in the outgoing header on a specific dial peer, use the `voice-class sip asserted-id ppi` command in dial peer voice configuration mode. For example: `Router(config-dial-peer)# voice-class sip asserted-id ppi` |
| PAID            | From            | 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 `no remote-party-id` command in SIP user-agent configuration mode. For example: `Router(config-sip-ua)# no remote-party-id` |
| PAID            | RPID            | To enable the translation to RPID headers in the outgoing header, use the `remote-party-id` command in SIP user-agent configuration mode. For example: `Router(config-sip-ua)# remote-party-id`  
This is the default system behavior. |
| RPID            | PPID            | To enable the translation to PPID privacy headers in the outgoing header at a global level, use the `asserted-id ppi` command in voice service VoIP SIP configuration mode. For example: `Router(conf-serv-sip)# asserted-id ppi`  
To enable the translation to PPID privacy headers in the outgoing header on a specific dial peer, use the `voice-class sip asserted-id ppi` command in dial peer voice configuration mode. For example: `Router(config-dial-peer)# voice-class sip asserted-id ppi` |
| RPID            | PAID            | To enable the translation to PAID privacy headers in the outgoing header at a global level, use the `asserted-id pai` command in voice service VoIP SIP configuration mode. For example: `Router(conf-serv-sip)# asserted-id pai`  
To enable the translation to PAID privacy headers in the outgoing header on a specific dial peer, use the `voice-class sip asserted-id pai` command in dial peer voice configuration mode. For example: `Router(config-dial-peer)# voice-class sip asserted-id pai` |
| RPID            | From            | 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 `no remote-party-id` command in SIP user-agent configuration mode. For example: `Router(config-sip-ua)# no remote-party-id` |
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. Here, 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.

Using Privacy values from the peer call leg

If the incoming INVITE has a Privacy header or a RPID with privacy on, the outgoing INVITE can be set to Privacy: id. This behavior is enabled by configuring `privacy pstn` command globally or `voice-class sip privacy pstn` command on the selected dial-per.

Incoming INVITE can have multiple privacy header values, id, user, session, and so on. Configure the `privacy-policy passthru` command globally or `voice-class sip privacy-policy passthru` command to transparently pass across these multiple privacy header values.

Some NGN servers require a Privacy header to be sent even though privacy is not required. In this case the Privacy header must be set to None. The Cisco Unified Border Element can add a privacy header with the value None while forwarding the outgoing INVITE to NGN. Configure the `privacy-policy send-always` globally or `voice-class sip privacy-policy send-always` command in dial-peer to enable this behavior.

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 value in the Request-URI of the incoming INVITE. The Cisco Unified Border Element routes calls based on the PCPID, instead of the Request-URI which contains the random value used in contact header of the REGISTER message.

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. For example: INVITE sip:FefhH3zIHe9i8ImcGjDD1PEc5XfFy51G@10.12.1.46:5060.

The Cisco Unified Border Element will not 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.

**Prerequisites**

**Cisco Unified Border Element**

- Cisco IOS Release 12.4(22)YB or a later release must be installed and running on your Cisco Unified Border Element.

**Cisco Unified Border Element (Enterprise)**

- Cisco IOS XE Release 3.1S or a later release must be installed and running on your Cisco ASR 1000 Series Router.
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 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 166
- Configuring P-Header Translation on an Individual Dial Peer, page 167
- Configuring P-Called-Party-Id Support on a Cisco Unified Border Element, page 168
- Configuring P-Called-Party-Id Support on an Individual Dial Peer, page 169
- Configuring Privacy Support on a Cisco Unified Border Element, page 170
- Configuring Privacy Support on an Individual Dial Peer, page 171
- Configuring Random-Contact Support on a Cisco Unified Border Element, page 172
- Configuring Random-Contact Support for an Individual Dial Peer, page 174

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

| Step 1 enable | Enables privileged EXEC mode.  
• Enter your password if prompted. |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Example: Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 voice service voip</td>
<td>Enters VoIP voice-service configuration mode.</td>
</tr>
<tr>
<td>Example: Router(config)# voice service voip</td>
<td></td>
</tr>
<tr>
<td>Step 4 sip</td>
<td>Enters voice service VoIP SIP configuration mode.</td>
</tr>
<tr>
<td>Example: Router(conf-voi-serv)# sip</td>
<td></td>
</tr>
<tr>
<td>Step 5 asserted-id header-type</td>
<td>Specifies the type of privacy header in the outgoing SIP requests and response messages.</td>
</tr>
<tr>
<td>Example: Router(conf-serv-sip)# asserted-id ppi</td>
<td></td>
</tr>
<tr>
<td>Step 6 exit</td>
<td>Exits the current mode.</td>
</tr>
<tr>
<td>Example: Router(conf-serv-sip)# exit</td>
<td></td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: enable</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: configure terminal</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> dial-peer voice tag voip</td>
<td>Defines the dial peer, specifies the method of voice encapsulation, and enters dial peer voice configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# dial-peer voice 2611 voip</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> voice-class sip asserted-id header-type</td>
<td>Specifies the type of privacy header in the outgoing SIP requests and response messages, on this dial peer.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-dial-peer)# voice-class sip asserted-id ppi</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> exit</td>
<td>Exits the current mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-dial-peer)# exit</td>
<td></td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> voice service voip</td>
<td>Enters VoIP voice-service configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# voice service voip</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> sip</td>
<td>Enters voice service VoIP SIP configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(conf-voi-serv)# sip</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> call-route p-called-party-id</td>
<td>Enables the routing of calls based on the PCPID header.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(conf-serv-sip)# call-route p-called-party-id</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> random-request-uri validate</td>
<td>Enables the validation of the random string in the Request URI of the incoming INVITE message.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(conf-serv-sip)# random-request-uri validate</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> exit</td>
<td>Exits the current mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(conf-serv-sip)# exit</td>
<td></td>
</tr>
</tbody>
</table>

**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
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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> dial-peer voice tag voip</td>
<td>Defines the dial peer, specifies the method of voice encapsulation, and enters dial peer voice configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# dial-peer voice 2611 voip</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> voice-class sip call-route p-called-party-id</td>
<td>Enables the routing of calls based on the PCPID header on this dial peer.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-dial-peer)# voice-class sip call-route p-called-party-id</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> voice-class sip random-request-uri validate</td>
<td>Enables the validation of the random string in the Request URI of the incoming INVITE message on this dial peer.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-dial-peer)# voice-class sip random-request-uri validate</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> exit</td>
<td>Exits the current mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-dial-peer)# exit</td>
<td></td>
</tr>
</tbody>
</table>
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> voice service voip</td>
<td>Enters VoIP voice-service configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# voice service voip</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> sip</td>
<td>Enters voice service VoIP SIP configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(conf-voi-serv)# sip</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> privacy privacy-option</td>
<td>Enables the privacy settings for the header.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(conf-serv-sip)# privacy id</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> privacy-policy privacy-policy-option</td>
<td>Specifies the privacy policy to use when passing the privacy header from one SIP leg to the next.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(conf-serv-sip)# privacy-policy passthru</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> exit</td>
<td>Exits the current mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(conf-serv-sip)# exit</td>
<td></td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | **enable** | Enables privileged EXEC mode.  
- Enter your password if prompted. |
| **Example:** | Router> enable |
| **Step 2** | **configure terminal** | Enters global configuration mode. |
| **Example:** | Router# configure terminal |
| **Step 3** | **dial-peer voice tag voip** | Defines the dial peer, specifies the method of voice encapsulation, and enters dial peer voice configuration mode. |
| **Example:** | Router(config)# dial-peer voice 2611 voip |
| **Step 4** | **voice-class sip privacy privacy-option** | Enables the privacy settings for the header on this dial peer. |
| **Example:** | Router(config-dial-peer)# voice-class sip privacy id |
| **Step 5** | **voice-class sip privacy-policy privacy-policy-option** | Specifies the privacy policy to use when passing the privacy header from one SIP leg to the next, on this dial peer. |
| **Example:** | Router(config-dial-peer)# voice-class sip privacy-policy passthru |
| **Step 6** | **exit** | Exits the current mode. |
| **Example:** | Router(config-dial-peer)# exit |

### 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> sip-ua</td>
<td>Enters SIP user-agent configuration mode.</td>
</tr>
<tr>
<td>Example: Router(config)# sip-ua</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> credentials username <strong>username</strong> password <strong>password</strong> realm <strong>domain-name</strong></td>
<td>Sends a SIP registration message from the Cisco Unified Border Element.</td>
</tr>
<tr>
<td>Example: Router(config-sip-ua)# credentials username 123456 password cisco realm cisco</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> registrar ipv4:destination-address random-contact expires expiry</td>
<td>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.</td>
</tr>
<tr>
<td>Example: Router(config-sip-ua)# registrar ipv4:10.1.2.2 random-contact expires 200</td>
<td>• The random-contact keyword configures the Cisco Unified Border Element to send the random string from the REGISTER message to the registrar.</td>
</tr>
<tr>
<td><strong>Step 6</strong> exit</td>
<td>Exits the current mode.</td>
</tr>
<tr>
<td>Example: Router(config-sip-ua)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> voice service voip</td>
<td>Enters VoIP voice-service configuration mode.</td>
</tr>
<tr>
<td>Example: Router(config)# voice service voip</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> sip</td>
<td>Enters voice service VoIP SIP configuration mode.</td>
</tr>
<tr>
<td>Example: Router(conf-voi-serv)# sip</td>
<td></td>
</tr>
</tbody>
</table>
Configuring Random-Contact Support for an Individual Dial Peer

To 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router&gt; enable</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td>Step 3 sip-ua</td>
<td>Enters SIP user-agent configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# sip-ua</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 4</strong> credentials username <strong>username</strong> password <strong>password</strong> realm <strong>domain-name</strong></td>
<td>Sends a SIP registration message from the Cisco Unified Border Element.</td>
</tr>
<tr>
<td>Example: Router(config-sip-ua)# credentials username 123456 password cisco realm cisco</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> registrar ipv4:destination-address random-contact expires expiry</td>
<td>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.</td>
</tr>
<tr>
<td>Example: Router(config-sip-ua)# registrar ipv4:10.1.2.2 random-contact expires 200</td>
<td>- The <strong>random-contact</strong> keyword configures the Cisco Unified Border Element to send the random string from the REGISTER message to the registrar.</td>
</tr>
<tr>
<td><strong>Step 6</strong> exit</td>
<td>Exits the current mode.</td>
</tr>
<tr>
<td>Example: Router(config-sip-ua)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> dial-peer voice <strong>tag</strong> voip</td>
<td>Defines the dial peer, specifies the method of voice encapsulation, and enters dial peer voice configuration mode.</td>
</tr>
<tr>
<td>Example: Router(config)# dial-peer voice 2611 voip</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> voice-class sip random-contact</td>
<td>Enables random-contact support on this dial peer.</td>
</tr>
<tr>
<td>Example: Router(config-dial-peer)# voice-class sip random-contact</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> exit</td>
<td>Exits the current mode.</td>
</tr>
<tr>
<td>Example: Router(config-dial-peer)# exit</td>
<td></td>
</tr>
</tbody>
</table>
Cisco Unified Border Element Support for Configurable Pass-through of SIP INVITE Parameters

This feature enables the Cisco Unified Border Element (Cisco UBE) platform 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.

Prerequisites

- Configuring the media flow-around command is required for Session Description Protocol (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.

Cisco Unified Border Element

- Cisco IOS Release 15.0(1)M or a later release must be installed and running on your Cisco Unified Border Element.

Cisco Unified Border Element (Enterprise)

- Cisco IOS XE Release 3.1S or a later release must be installed and running on your Cisco ASR 1000 Series Router.

Restrictions

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

Information About Cisco Unified Border Element Support for Configurable Pass-through of SIP INVITE Parameters

The Cisco UBE does not support end-to-end media negotiation between the two endpoints that establish a call session through the Cisco UBE. This is a limitation when the endpoints intend to negotiate codec/payload types that the Cisco UBE does not process, because currently, unsupported payload types will never be negotiated by the Cisco UBE. 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 UBE, so that both the remote ends can negotiate media independently of the Cisco UBE.

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

How to Configure the Cisco Unified Border Element Support for Configurable Pass-through of SIP INVITE Parameters

To enable Cisco UBE Unsupported Content Pass-through perform the steps in this section. This section contains the following subsections:
• Configuring Cisco Unified Border Element Support for Configurable Pass-through of SIP INVITE Parameters at the Global Level
• Configuring Cisco Unified Border Element Support for Configurable Pass-through of SIP INVITE Parameters at the Dial Peer Level

Configuring Cisco Unified Border Element Support for Configurable Pass-through of SIP INVITE Parameters at the Global Level

To configure Unsupported Content Pass-through on a Cisco UBE platform 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 | unsupp} | headers {unsupp | list tag}}
6. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 voice service voip</td>
<td>Enters voice service VoIP configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# voice service voip</td>
<td></td>
</tr>
</tbody>
</table>
**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `dial-peer voice tag voip`
4. `voice-class sip pass-thru {content {sdp | unsupp} | headers {unsupp | list tag}} [system]`
5. `exit`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>dial-peer voice tag voip</code></td>
<td>Enters dial peer VoIP configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# dial-peer voice 2 voip</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><strong>Command or Action</strong></td>
</tr>
<tr>
<td>--------</td>
<td>-----------------------</td>
</tr>
<tr>
<td></td>
<td>`voice-class sip pass-thru {content {sdp</td>
</tr>
</tbody>
</table>

**Example:**
```
Router(config-dial-peer)# voice-class sip pass-thru content sdp
```

<table>
<thead>
<tr>
<th>Step 5</th>
<th><strong>Command or Action</strong></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>exit</code></td>
<td>Exits the current mode.</td>
</tr>
</tbody>
</table>

**Example:**
```
Router(config-dial-peer)# exit
```
Transparent Tunneling of QSIG and Q.931 over SIP TDM Gateway and SIP-SIP Cisco Unified Border Element

Transparent Tunneling of QSIG and Q.931 over Session Initiation Protocol (SIP) Time-Division Multiplexing (TDM) Gateway and SIP-to-SIP Cisco Unified Border Element (Enterprise) was first introduced on Cisco IOS SIP gateways in phases. In the first phase, the Transparent Tunneling of QSIG over SIP TDM Gateway feature added the ability to transparently tunnel Q-signaling (QSIG) protocol ISDN messages across the Session Initiation Protocol (SIP) trunk. With this feature, QSIG messages (supplementary services carried within Q.931 FACILITY-based messages) can be passed end to end across a SIP network. However, in Cisco IOS Release 12.4(15)XY, deployment of this feature is limited to QSIG messages over SIP TDM gateways. In later releases, the ISDN Q.931 Tunneling over SIP TDM Gateway feature adds support for transparent tunneling of all Q.931 messages over SIP and for the Transparent Tunneling of QSIG and Q.931 over a SIP-SIP Cisco Unified Border Element.

Transparent tunneling is accomplished by encapsulating QSIG or Q.931 messages within SIP message bodies. These messages are encapsulated using "application/qsig" or "application/x-q931" Multipurpose Internet Mail Extensions (MIME) to tunnel between SIP endpoints. Using MIME to tunnel through Cisco SIP messaging does not include any additional QSIG/Q.931 services to SIP interworking.

Beginning with Cisco IOS XE Release 3.1S, support for this feature is expanded to include the Cisco ASR 1000 Series Router.

Contents

- Prerequisites, page 180
- Restrictions, page 181
- Information About Transparent Tunneling of QSIG or Q.931 over SIP, page 181
- How to Transparently Tunnel QSIG over SIP, page 184
- Configuration Examples for Transparent Tunneling of QSIG over SIP, page 187

Prerequisites

- Before configuring transparent tunneling of QSIG and Q.931 over a SIP trunk, verify the SIP configuration within the VoIP network for the appropriate originating and terminating gateways.

Cisco Unified Border Element

- Cisco IOS Release 12.4(15)XZ or a later release must be installed and running on your Cisco Unified Border Element.
- The Transparent Tunneling of QSIG over SIP TDM Gateway feature is intended for TDM PBX toll bypass and call center applications. In its first release (Cisco IOS Release 12.4(15)XY), only tunneling of QSIG messages is supported and only on TDM gateways. From Cisco IOS release 12.4(15)XZ and 12.4(20)T onward, support is added for the ISDN Q.931 Tunneling over SIP TDM Gateway and Transparent Tunneling of QSIG and Q.931 over SIP-SIP Cisco Unified Border Element.

Cisco Unified Border Element (Enterprise)

- Cisco IOS XE Release 2.5 or a later release must be installed and running on your Cisco ASR 1000 Series Router.
Restrictions

- Transparent tunneling of QSIG or Q.931 does not function unless both the originating gateway (OGW) and the terminating gateway (TGW) are configured using the same ISDN switch type.
- This function is supported only on SIP-to-SIP configurations on Cisco Unified Border Element. Tunneling of QSIG or Q.931 is not supported on SIP-to-H.323 or H.323-to-H.323 configurations on Cisco Unified Border Element.

Information About Transparent Tunneling of QSIG or Q.931 over SIP

To configure transparent tunneling of QSIG or Q.931 over SIP, you should understand the following concepts:

- Use of the QSIG or Q.931 Protocols, page 181
- Purpose of Tunneling QSIG or Q.931 over SIP, page 181
- Encapsulation of QSIG in SIP Messaging, page 182
- Mapping of QSIG Message Elements to SIP Message Elements, page 183

Use of the QSIG or Q.931 Protocols

Q-series documents, controlled by the International Telecommunication Union (ITU), define the network Layer. The Q.931 document defines the Layer 3 protocol that serves as the connection control protocol for ISDN signaling—it is used primarily to manage the initiation, maintenance, and termination of connections over a digital network.

The Q signaling (QSIG) protocol is based on the Q.931 standard and is used for ISDN communications in a Private Integrated Services Network (PISN). The QSIG protocol makes it possible to pass calls from one circuit switched network, such as a PBX or private integrated services network exchange (PINX), to another. QSIG messages are, essentially, a subset of Q.931 messages that ensure the essential Q.931 FACILITY-based functions successfully traverse the network regardless of the various hardware involved.

Q.931 tunneling over Cisco IOS SIP gateways was introduced as the ability to transparently tunnel only QSIG messages—the FACILITY-based Q.931 messages. Beginning with Cisco IOS Release 12.4(15)XZ and Cisco IOS Release 12.4(20)T, tunneling of all Q.931 messages (SETUP, ALERTING, CONNECT, and RELEASE COMPLETE messages in addition to FACILITY-based messages) is supported on Cisco IOS SIP gateways. However, for clarity, the descriptions and examples in this document focus primarily on QSIG messages.

Purpose of Tunneling QSIG or Q.931 over SIP

TDM Gateways

Transparencyally tunneling QSIG or Q.931 messages over SIP through SIP TDM gateways allows calls from one PINX to another to be passed through a SIP-based IP network with the equivalent functionality of passing through an H.323 network—without losing the functionality of the QSIG or Q.931 protocol to establish the call. To do this, QSIG or Q.931 messages are encapsulated within SIP messages (see Figure 1).
Cisco Unified Border Elements

Transparently tunneling QSIG or Q.931 over SIP through a Cisco Unified Border Element allows calls from one network to be passed through a SIP-to-SIP Cisco Unified Border Element connection to a bordering network (see Figure 2).

Encapsulation of QSIG in SIP Messaging

QSIG messages are tunneled by encapsulating them as a MIME body in a SIP INVITE message on the OGW. Then, the MIME body is extracted from the SIP message by the TGW at the other end of the SIP network. To tunnel QSIG messages to a TGW on another network, configure and use a SIP-to-SIP Cisco Unified Border Element connection between each network over which the SIP INVITE must travel to reach the TGW. This tunneling process helps preserve all QSIG capabilities associated with a call or call-independent signal as it travels to its destination.

The following events make it possible to tunnel QSIG messaging across a SIP network:

- The ingress gateway (OGW) receives a QSIG call (or signal) establishment request (a SETUP message) and generates a corresponding SIP INVITE request.
- A corresponding SIP INVITE message is created and will contain the following:
  - A Request-URI—message part containing a destination derived from the called party number information element (IE) in the QSIG SETUP message. The destination can be the egress (TGW or the Cisco Unified Border Element) for exiting the SIP network or it can be the required destination, leaving SIP proxies to determine which gateway will be used.
  - A From header—message header containing a uniform resource identifier (URI) for either the OGW or calling party itself.
  - A Session Description Protocol (SDP) offer—a message part proposing two media streams, one for each direction.
  - A Multipart-MIME body—message part containing the tunneled QSIG data.
In addition to normal user agent (UA) handling of a SIP response, the OGW performs a corresponding action when it receives a SIP response, as follows:

- OGW receives 18\text{x} response with tunneled content—identifies the QSIG message (FACILITY, ALERTING, or PROGRESS) and sends a corresponding ISDN message.
- OGW receives 3\text{xx}, 4\text{xx}, 5\text{xx}, or 6\text{xx} final response—attempts alternative action to route the initial QSIG message or clears the call or signal using an appropriate QSIG cause value (DISCONNECT, RELEASE, or RELEASE COMPLETE). When the OGW receives a valid encapsulated QSIG RELEASE COMPLETE message, the OGW should use the cause value included in that QSIG message to determine the cause value.

\textbf{Note}
You should expect a SIP 415 final response message (Unsupported Media Type) if the user agent server (UAS) is unable to process tunneled QSIG or Q.931 messages.

- OGW receives a SIP 200 OK response—performs normal SIP processing, which includes sending an ACK message. Additionally, the OGW will encapsulate the QSIG message in the response to the PSTN side and will connect the QSIG user information channel to the appropriate media streams as called out in the SDP reply.

\textbf{Note}
A nonzero port number for each media stream must be provided in a SIP 200 OK response to the OGW before the OGW receives the QSIG CONNECT message. Otherwise, the OGW will behave as if the QSIG T301 timer expired.

The TGW sends and the OGW receives a 200 OK response—the OGW sends an ACK message to the TGW and all successive messages during the session are encapsulated into the body of SIP INFO request messages. There are two exceptions:

- When a SIP connection requires an extended handshake process, renegotiation, or an update, the gateway may encapsulate a waiting QSIG message into a SIP re-INVITE or SIP UPDATE message during QSIG call establishment.
- When the session is terminated, gateways send a SIP BYE message. If the session is terminated by notice of a QSIG RELEASE COMPLETE message, that message can be encapsulated into the SIP BYE message.

\textbf{Mapping of QSIG Message Elements to SIP Message Elements}

This section lists QSIG message elements and their associated SIP message elements when QSIG messages are tunneled over a SIP trunk.

- QSIG FACILITY/NOTIFY/INFO \leftrightarrow SIP INFO
- QSIG SETUP \leftrightarrow SIP INVITE
- QSIG ALERTING \leftrightarrow SIP 180 RINGING
- QSIG PROGRESS \leftrightarrow SIP 183 PROGRESS
- QSIG CONNECT \leftrightarrow SIP 200 OK
- QSIG DISCONNECT \leftrightarrow SIP BYE/CANCEL/4\text{xx}–6\text{xx} Response
How to Transparently Tunnel QSIG over SIP

To create a tunnel for QSIG messages across a SIP trunk, you must configure signaling forward settings on both the OGW and the TGW.

In the IP TDM gateway scenario, a gateway receives QSIG messages from PSTN and the ISDN module passes the raw QSIG message and, additionally, creates and includes a Generic Transparency Descriptor (GTD) that is passed with the raw QSIG message across the IP leg of the call.

In the SIP TDM gateway scenario, there are two options—raw message (rawmsg) and unconditional. The rawmsg option specifies tunneling of only raw message (application/qsig or application/x-q931). The unconditional option specifies tunneling of all additional message bodies, such as GTD and raw message (application/qsig or application/x-q931).

Use the **signaling forward** command at the global configuration level to configure the feature for the entire gateway. You can also enable the QSIG tunneling feature for only a specific interface. If you enable this feature at both the global and dial peer configuration level and the option specified for the interface is different than for the gateway, the interface setting will override the global setting. The processes for specifying either option at both levels are included in the following sections:

- Configuring Signaling Forward Settings for a Gateway, page 184
- Configuring Signaling Forward Settings for an Interface, page 185

**Configuring Signaling Forward Settings for a Gateway**

To create a tunnel for QSIG messages across a SIP trunk using the same signaling forward setting for all interfaces on a gateway, configure the signaling forward settings in voice service voip configuration mode.

**Signaling Forward Settings for a Gateway**

The two options—raw messages (rawmsg) and unconditional—are mutually exclusive, which means you can specify only one option at the global configuration level. To enable and specify the signaling forward option, use the **signaling forward** command in voice service voip configuration mode.

---

**Note**

To override the global setting for a specific interface, use the **signaling forward** command at the dial-peer level (see the "Configuring Signaling Forward Settings for an Interface" section on page 185).

**Prerequisites**

To create QSIG tunnels using the signaling forward configuration, configure both gateways. You can configure gateways globally or you can configure one or more interfaces on a gateway. In either case, you must include the recommended configuration for PRACK to avoid message/data loss.

---

**Note**

It is not necessary that both gateways are configured with the same signaling forward option but, if they are not, only raw QSIG messages can be tunneled. However, it is recommended that you tunnel QSIG messages with at least one interface configured on both gateways. If only one gateway is configured, QSIG tunneling might work in one direction but may not work properly in both directions.

You must also specify the central office switch type on the ISDN interface for both the OGW and the TGW. Use the **isdn switch-type** command in global or dial peer configuration mode to enable and specify the switch type for QSIG or Q.931 support.
Furthermore, before the **isdn switch-type** setting can function properly, you must assign network-side functionality for the primary-qsig switch type (either at the global or dial-peer level) using the **isdn protocol-emulate** command.

**SUMMARY STEPS**

1. enable  
2. configure terminal  
3. voice service voip  
4. signaling forward option

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><em>Example:</em></td>
<td><em>Enter your password if prompted.</em></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><em>Example:</em></td>
<td><em>Router# configure terminal</em></td>
</tr>
<tr>
<td><strong>Step 3</strong> voice service voip</td>
<td>Enters voice-service configuration mode and specifies a voice-encapsulation type globally.</td>
</tr>
<tr>
<td><em>Example:</em></td>
<td><em>Router(config)# voice service voip</em></td>
</tr>
<tr>
<td><strong>Step 4</strong> signaling forward message-type</td>
<td>Enables tunneling of QSIG raw messages (application-qsig) only.</td>
</tr>
<tr>
<td><em>Example:</em></td>
<td><em>Router(config)# signaling forward rawmsg</em></td>
</tr>
<tr>
<td>or</td>
<td><em>Router(config)# signaling forward unconditional</em></td>
</tr>
</tbody>
</table>

**Configuring Signaling Forward Settings for an Interface**

To create a tunnel for QSIG messages across a SIP trunk on a specific interface on a gateway, configure the signaling forward settings in dial peer configuration mode.

**Signaling Forward Settings for an Interface**

The two options—raw messages (rawmsg) and unconditional—are mutually exclusive, which means you can specify only one option per interface at the dial-peer level. To enable and specify the signaling forward option for an interface, use the **signaling forward** command in dial peer configuration mode.

**Note**  
To set the signaling forward option for an entire gateway, use the **signaling forward** command at the global level.
Prerequisites

To create QSIG tunnels using the signaling forward configuration, configure at least one interface on both gateways. You can also configure all interfaces at once by configuring the gateway globally. In either case, you must include the recommended configuration for PRACK to avoid data loss.

Note
It is not necessary that both gateways are configured with the same signaling forward option but, if they are not, only raw QSIG messages can be tunneled. However, it is recommended that you tunnel QSIG messages with at least one interface configured on both gateways. If only one gateway is configured, QSIG tunneling might work in one direction but may not work properly in both directions.

You must also specify the central office switch type on the ISDN interface for both the OGW and the TGW. Use the isdn switch-type command in global or dial peer configuration mode to enable and specify the switch type for QSIG or Q.931 support.

Furthermore, before the isdn switch-type setting can function properly, you must assign network-side functionality for the primary-qsig switch type (either at the global or dial-peer level) using the isdn protocol-emulate command.

SUMMARY STEPS

1. enable
2. configure terminal
3. dial-peer voice number voip
4. signaling forward option

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> dial-peer voice number voip</td>
<td>Enters voice-service configuration mode and specifies a</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>voice-encapsulation type for a specific interface.</td>
</tr>
<tr>
<td>Router(config)# dial-peer voice 3 voip</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> signaling forward message-type</td>
<td>Enables tunneling of QSIG raw messages (application-qsig) only.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>or</td>
</tr>
<tr>
<td>Router(config-dial-peer)# signaling forward rawmsg</td>
<td>Enables tunneling of all QSIG message bodies unconditionally.</td>
</tr>
<tr>
<td>or</td>
<td></td>
</tr>
<tr>
<td>Router(config-dial-peer)# signaling forward unconditional</td>
<td></td>
</tr>
</tbody>
</table>

Cisco Unified Border Element Configuration Guide
**Configuration Examples for Transparent Tunneling of QSIG over SIP**

This section provides the following configuration examples:

- Configuration at the global level:
  - Tunneling QSIG Raw Messages over SIP on an OGW or TGW: Example, page 187
  - Tunneling QSIG Messages Unconditionally over SIP on an OGW or TGW: Example, page 187

- Configuration at the dial peer (interface) level:
  - Tunneling QSIG Raw Messages over SIP on an OGW and TGW Interface: Example, page 187
  - Tunneling QSIG Messages Unconditionally over SIP on an OGW or TGW Interface: Example, page 188

**Tunneling QSIG Raw Messages over SIP on an OGW or TGW: Example**

The following example shows how to configure transparent tunneling of only QSIG raw messages (application-qsig) through a SIP TDM gateway on a SIP trunk at either the OGW or TG:

```plaintext
! voice service voip signaling forward rawmsg sip relxx require "100rel"
```

**Tunneling QSIG Messages Unconditionally over SIP on an OGW or TGW: Example**

The following example shows how to configure transparent tunneling of QSIG messages unconditionally through a SIP TDM gateway on a SIP trunk at either the OGW or TG:

```plaintext
! voice service voip signaling forward unconditional sip relxx require "100rel"
```

**Tunneling QSIG Raw Messages over SIP on an OGW and TGW Interface: Example**

The following example shows how to configure transparent tunneling of only QSIG raw messages (application-qsig) on a gateway interface in a SIP network (see Figure 3):

*Figure 3*  **Tunneling of Only QSIG Raw Messages over a SIP Trunk (Interface-Level)**

![Diagram of SIP trunk with QSIG, OGW, and TGW interfaces]

**Configuration for OGW (172.24.2.15) Tunneling only QSIG Raw Messages**

! 
dial-peer voice 7777 voip
description OGW-OUT-TGW
destination-pattern 222
signaling forward rawmsg
session protocol sipv2
session target ipv4:172.24.2.14
!

**Configuration for TGW (172.24.2.14) Tunneling only QSIG Raw Messages**

! dial-peer voice 333 voip
description TGW_RSVP_IN-DP
session protocol sipv2
signaling forward rawmsg
incoming called-number 222
!

**Tunneling QSIG Messages Unconditionally over SIP on an OGW or TGW Interface: Example**

The following example shows how to configure transparent tunneling of QSIG messages unconditionally over a gateway interface in a SIP network (see [Figure 4](#)):

**Figure 4** Tunneling of QSIG Messages Unconditionally over a SIP Trunk (Interface-Level)

![Tunneling QSIG Messages Unconditionally over a SIP Trunk (Interface-Level)](image)

**Configuration for OGW (172.24.2.14) Tunneling QSIG Messages Unconditionally**

dial-peer voice 7777 voip
description OGW-OUT-TGW
destination-pattern 222
signaling forward unconditional
session protocol sipv2
session target ipv4:172.24.2.14

**Configuration for TGW (172.24.2.15) Tunneling QSIG Messages Unconditionally**

dial-peer voice 333 voip
description TGW-RSVP-IN-DP
session protocol sipv2
signaling forward unconditional
incoming called-number 222
SIP Diversion Header Enhancements

The SIP Diversion Header Enhancements feature enables time-division multiplex (TDM) gateways and Cisco Unified Communications Manager Express to populate the SIP Diversion Header with a domain name. Localhost command-line interface commands can be used to configure the domain name globally or at the dial peer level. This feature also provides choice of transparent pass through or application of address hiding to the SIP Diversion Header on Cisco UBE platforms.

Prerequisites

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

**Cisco Unified Border Element (Enterprise)**
- Cisco IOS XE Release 3.1S or a later release must be installed and running on your Cisco ASR 1000 Series Router.

Information about SIP Diversion Header Enhancements

To enable this feature, you must first configure the `sip-ua` command to place the router in SIP user-agent configuration mode before you can use the `host-registrar` command.

By default, the Session Initiation Protocol (SIP) gateway and Cisco Unified Communications Manager Express (Cisco Unified CME) populate the host portion of the diversion header with the domain name or IP address of the gateway that generates the request or response. The SIP gateway and Cisco Unified CME also populate the host portion of the redirect contact header with the session target IP address or hostname of the matching dial peer.

When the `host-registrar` command and the `registrar` command are both configured in SIP user-agent configuration mode, the SIP gateway or Cisco Unified CME populate the host portion of both the diversion and redirect contact headers with the domain name or IP address configured by the `registrar` command.

The `host-registrar` command should be configured along with the `registrar` command in SIP user-agent configuration mode. If the `host-registrar` command is configured without the `registrar` command, the host portion of the diversion header is populated with the domain name or IP address of the gateway and the host portion of the redirect contact header is populated with the session target IP address or hostname of the matching dial peer.

How to Configure SIP Diversion Header Enhancements

To configure the SIP Diversion Header Enhancements feature, complete this task in this section.

**Note**

Some keywords and arguments have been omitted from the command syntax shown here. For complete command syntax information, see the *Cisco IOS Voice Command Reference*.

**SUMMARY STEPS**

1. `enable`
2. configure terminal
3. sip-ua
4. registrar registrar-server-address
5. host-registrar

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router&gt; enable</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td>Step 3 sip-ua</td>
<td>Enters SIP User Agent configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# sip-ua</td>
</tr>
<tr>
<td>Step 4 registrar registrar-server-address</td>
<td>The SIP registrar server address to be used for endpoint registration. This value can be entered in one of three formats:</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-sip-us)# registrar ipv4:10.1.1.1</td>
</tr>
<tr>
<td>Step 5 host-registrar</td>
<td>Populates the SIP User Agent registrar domain name or IP address value in the host portion of the diversion header and redirects the contact header of the 302 response.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-sip-ua)# host-registrar</td>
</tr>
</tbody>
</table>
SIP—Ability to Send a SIP Registration Message on a Border Element

The SIP—Ability to Send a SIP Registration Message on a Border Element feature allows users to register e164 numbers from the Cisco UBE without POTS dial-peers in the UP state. Registration messages can include numbers, number ranges (such as E.164-numbers), or text information.

Prerequisites

- Configure a registrar in sip user-agent configuration mode.

Cisco Unified Border Element

- Cisco IOS Release 12.4(24)T or a later release must be installed and running on your Cisco Unified Border Element.

Cisco Unified Border Element (Enterprise)

- Cisco IOS XE Release 2.5 or a later release must be installed and running on your Cisco ASR 1000 Series Router.

SUMMARY STEPS

1. enable
2. configure terminal
3. sip-ua
4. credentials username password realm domain-name
5. exit
6. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> sip-ua</td>
<td>Enters sip user-agent configuration mode.</td>
</tr>
<tr>
<td>Example: sip-ua</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

**Step 4**

```
credentials username username password password
realm domain-name
```

**Example:**

```
Router(config-sip-ua)# credentials username alex
password test realm cisco.com
```

Enters SIP digest credentials in sip-ua configuration mode.

**Step 5**

```
exit
```

**Example:**

```
Router(config-sip-ua)# exit
```

Exits the current mode.

**Step 6**

```
end
```

**Example:**

```
Router(config)# end
```

Returns to privileged EXEC mode.
Support for Multiple Registrars on SIP Trunks

The Support for Multiple Registrars on SIP Trunks on a Cisco Unified Border Element, on Cisco IOS SIP TDM Gateways, and on a Cisco Unified Communications Manager Express feature allows configuration of multiple registrars on Session Initiation Protocol (SIP) trunks, each simultaneously registered using its respective authentication instance. Beginning with Cisco IOS XE Release 3.1S, support for this feature is expanded to include the Cisco ASR 1000 Series Router. This feature allows a redundant registrar for each of the SIP trunks, which provides SIP trunk redundancy across multiple service providers.

Prerequisites

Cisco Unified Border Element

- Cisco IOS Release 15.0(1)XA or a later release must be installed and running on your Cisco Unified Border Element.

Cisco Unified Border Element (Enterprise)

- Cisco IOS XE Release 3.1S or a later release must be installed and running on your Cisco ASR 1000 Series Router.

Restrictions for Support for Multiple Registrars on SIP Trunks

The Support for Multiple Registrars on SIP trunks feature has the following restrictions:

- Old and new forms of the registrar command are mutually exclusive: the registrar can be configured in either primary/secondary mode or multiple registrar mode—not both.
- Dynamic Host Configuration Protocol (DHCP) support is not available with multiple registrars (available for primary/secondary mode only).
- Only one authentication configuration per username can be configured at any one time.
- A maximum of six registrars can be configured at any given time.
- A maximum of 12 different realms can be configured for each endpoint.
- You cannot restrict the registration of specific endpoints with specific registrars—once a new registrar is configured, all endpoints will begin registering to the new registrar.
- You cannot remove multiple configurations of credentials simultaneously—only one credential can be removed at a time.

Configuring Support for Multiple Registrars on SIP Trunks Feature

For information about the Support for Multiple Registrars on SIP Trunks feature and for detailed procedures for enabling this feature, see the “Configuring Multiple Registrars on SIP Trunks” chapter of the Cisco IOS SIP Configuration Guide.
Feature Information for Cisco UBE SIP Support

Table 1 lists the release history for this chapter.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which 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 1 lists only the Cisco IOS software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP-to-SIP Basic Functionality for Session Border Controller</td>
<td>12.4(4)T</td>
<td>The SIP-to-SIP Basic Functionality for Session Border Controller (SBC) for Cisco Unified Border Element (Cisco UBE) feature provides termination and re-originating of both signaling and media between VoIP and video networks using SIP signaling in conformance with RFC 3261. This feature uses no new or modified commands.</td>
</tr>
<tr>
<td>SIP-to-SIP Extended Feature Functionality for Session Border Controllers</td>
<td>12.4(6)T</td>
<td>The SIP-to-SIP Extended Feature Functionality for Session Border Controllers (SBCs) enables the SIP-to-SIP functionality to conform with RFC 3261 to interoperate with SIP User Agents (UAs). This feature uses no new or modified commands.</td>
</tr>
<tr>
<td>SIP-to-SIP Supplementary Services for Session Border Controller</td>
<td>12.4(9)T,</td>
<td>The SIP-to-SIP Supplementary Services for Session Border Controller feature enhances terminating and re-originating signaling and media between VoIP and Video networks. This feature uses no new or modified commands.</td>
</tr>
<tr>
<td>Transparent Tunneling of QSIG and Q.931 over SIP TDM Gateway and SIP-SIP Cisco Unified Border Element</td>
<td>12.4(15)XZ 12.4(20)T</td>
<td>This feature adds support for transparent tunneling of all Q.931 messages over SIP and for the Transparent Tunneling of QSIG and Q.931 over a SIP-SIP Cisco Unified Border Element. Transparent tunneling is accomplished by encapsulating QSIG or Q.931 messages within SIP message bodies. These messages are encapsulated using &quot;application/qsig&quot; or &quot;application/x-q931&quot; Multipurpose Internet Mail Extensions (MIME) to tunnel between SIP endpoints. Using MIME to tunnel through Cisco SIP messaging does not include any additional QSIG/Q.931 services to SIP interworking. This feature uses no new or modified commands.</td>
</tr>
<tr>
<td>SIP Parameter Modification</td>
<td>12.4(15)XZ 12.4(20)T</td>
<td>Allows users to change the standard SIP messages sent from the Cisco SIP stack for better interworking with different SIP entities. This feature introduces or modifies the following commands: <strong>voice class sip-profiles, voice-class sip-profiles</strong></td>
</tr>
</tbody>
</table>
### Table 1  Feature Information for Cisco UBE SIP Support Features (continued)

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SIP Diversion Header Enhancements</strong></td>
<td>12.4(22)T</td>
<td>The SIP Diversion Header Enhancements feature enables time-division multiplex (TDM) gateways and Cisco Unified Communications Manager Express to populate the SIP Diversion Header with a domain name. This feature also provides choice of transparent pass through or application of address hiding to the SIP Diversion Header on Cisco UBE platforms. This feature modifies the following commands: <code>host-registrar</code>, and <code>registrar</code></td>
</tr>
<tr>
<td><strong>Cisco Unified Border Element Support for Configurable Pass-through of SIP INVITE Parameters</strong></td>
<td>15.0(1)M</td>
<td>This feature enables the Cisco Unified Border Element platform 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. This feature introduces the following commands: <code>pass-thru</code> and <code>voice-class sip pass-thru</code>.</td>
</tr>
<tr>
<td><strong>SIP—Ability to Send a SIP Registration Message on a Border Element</strong></td>
<td>12.4(24)T</td>
<td>Provides the ability to send a SIP Registration Message from Cisco Unified Border Element. The following command was modified: <code>credentials</code> (SIP UA)</td>
</tr>
<tr>
<td><strong>SIP—INFO Method for DTMF Tone Generation</strong></td>
<td>12.2(11)T, 12.3(2)T, 12.2(8)YN, 12.2(11)YV, 12.2(11)T, 12.2(15)T</td>
<td>The SIP—INFO Method for DTMF Tone Generation feature uses the Session Initiation Protocol (SIP) INFO method to generate dual-tone multifrequency (DTMF) tones on the telephony call leg. SIP methods, or request message types, request a specific action be taken by another user agent (UA) or proxy server. The SIP INFO message is sent along the signaling path of the call. The following command was introduced: <code>show sip-ua</code>.</td>
</tr>
</tbody>
</table>
### Table 1  Feature Information for Cisco UBE SIP Support Features (continued)

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
</table>
| Support for PAID, PPID, Privacy, PCPID, and PAURI Headers on the Cisco UBE   | 12.4(22)YB, 15.0(1)M | This feature enables Cisco UBE platforms to support:  
  - P-Preferred Identity (PPID), P-Asserted Identity (PAID), Privacy, P-Called Party Identity (PCPID), in INVITE messages  
  - Translation of PAID headers to PPID headers and vice versa  
  - Translation of From: or RPID headers to PAID or PPID headers and vice versa  
  - Configuration and/or pass through of privacy header values  
  - PCPID header to route INVITE messages  
  - Multiple PAURI headers in the response messages (200 OK) it receives to REGISTER messages  
  - P-Preferred Identity and P-Asserted Identity Headers  
  The following commands were introduced: `call-route p-called-party-id`, `privacy-policy`, `random-contact`, `random-request-uri validate`, `voice-class sip call-route p-called-party-id`, `voice-class sip privacy-policy`, `voice-class sip random-contact`, and `voice-class sip random-request-uri validate`. |
| Configuring Selective Filtering of Outgoing Provisional Response on the Cisco UBE | 12.4(22)YB, 15.0(1)M | 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.  
  The following commands were introduced or modified: `block` and `voice-class sip block`. |
| RFC 4040-Based Clear Channel Codec Negotiation for SIP Calls                 | 15.0(1)XA, 15.1(1)T | This feature adds support for RFC 4040-based clear channel codec Negotiation for SIP calls.  
  The following commands were modified: `encap clear-channel standard` and `voice-class sip encap clear-channel`. |
| Support for Expires Timer Reset on Receiving or Sending SIP 183 Message     | 15.0(1)XA, 15.1(1)T | This feature enables support for resetting the Expires timer upon receipt of SIP 183 messages on Cisco Unified Communications Manager Express (Cisco Unified CME), a Cisco IOS voice gateway, or a Cisco Unified Border Element (Cisco UBE).  
  The following commands were introduced or modified: `reset timer expires` and `voice-class sip reset timer expires`. |
### Feature Information for Cisco UBE SIP Support

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support for Multiple Registrars on SIP Trunks</td>
<td>15.0(1)XA 15.1(1)T</td>
<td>This feature provides support for multiple registrars on SIP trunks on Cisco IOS SIP TDM gateways, Cisco Unified CME, and Cisco UBeS. This feature allows for a redundant registrar for each SIP trunk and enables registrar redundancy across multiple service providers. This feature includes the following new or modified commands: credentials, localhost, registrar, voice-class sip localhost.</td>
</tr>
<tr>
<td>Cisco UBE Support for generating Out-of-dialog SIP OPTIONS Ping messages to monitor SIP Servers</td>
<td>15.1(1)T</td>
<td>This feature provides option to configure the error response code when a dial peer is busied out because of an Out-of-Dial OPTIONS ping failure. The following commands were introduced or modified in this release: error-code-override options-keepalive failure, voice-class sip error-code-override options-keepalive failure.</td>
</tr>
<tr>
<td>Configuring Support for SIP 181 Call is Being Forwarded Message</td>
<td>12.2(13)T</td>
<td>This feature allows users to configure support for SIP 181 Call is Being Forwarded messages either globally or on a specific dial-peer. This feature includes the following new or modified commands: block, map resp-code, voice-class sip block, voice-class sip map resp-code.</td>
</tr>
<tr>
<td>SIP—Configurable Hostname in Locally Generated SIP Headers</td>
<td>12.4(2)T</td>
<td>This feature allows you to configure the hostname in locally generated SIP headers in global and dial-peer-specific configuration modes. The following commands were introduced or modified: localhost dns and voice-class sip localhost dns.</td>
</tr>
<tr>
<td>SIP—Core SIP Technology Enhancements</td>
<td>12.2(13)T 12.2(15)T</td>
<td>Compliance to RFC 2543-bis-04 adds enhanced SIP support and ensures smooth interoperability and compatibility with multiple vendors. The following commands were modified: debug ccsip messages, show sip-ua map, show sip-ua statistics, and.</td>
</tr>
<tr>
<td>SIP—Enhanced 180 Provisional Response Handling</td>
<td>12.2(11)T 12.2(8)YN 12.2(15)T 12.2(11)YV 12.2(11)T</td>
<td>The Session Initiation Protocol (SIP) Enhanced 180 Provisional Response Handling feature provides the ability to enable or disable early media cut-through on Cisco IOS gateways for SIP 180 response messages. The following commands were introduced or modified: disable-early-media 180 and show sip-ua status.</td>
</tr>
<tr>
<td>SIP—Session Timer Support</td>
<td>12.2(8)YN 12.2(15)T 12.2(11)YV 12.2(11)T 12.3(2)T</td>
<td>The SIP Session Timer Support feature adds the capability to periodically refresh Session Initiation Protocol (SIP) sessions by sending repeated INVITE requests. The repeated INVITE requests, or re-INVITEs, are sent during an active call leg to allow user agents (UAs) or proxies to determine the status of a SIP session. The following commands were introduced or modified: min-se (SIP) and show sip-ua min-se.</td>
</tr>
</tbody>
</table>
Cisco Unified Border Element H.323 Support

This Cisco Unified Border Element is a special Cisco IOS software image that 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.

**Activation**

Cisco Product Authorization Key (PAK)—A Product Authorization Key (PAK) is required to configure some of the features described in this guide. Before you start the configuration process, please register your products and activate your PAK at the following URL [http://www.cisco.com/go/license](http://www.cisco.com/go/license).

**Finding Feature Information**

For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the “Cisco Unified Border Element Features Roadmap” section on page 3.

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. To access Cisco Feature Navigator, go to [http://www.cisco.com/go/cfn](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.
Cisco Unified Border Element H.323 Support Features

This chapter contains the following configuration topics:

Cisco UBE (Enterprise) Prerequisites and Restrictions
- Prerequisites for Cisco Unified Border Element
- Restrictions for Cisco Unified Border Element

Additional References

Glossary

Feature Information for Cisco UBE H.323 Support
Feature Information for Cisco UBE H.323 Support

Table 1 lists the release history for this chapter.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which 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 lists only the Cisco IOS software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 1 **Feature Information for Cisco UBE (Enterprise) H.323 Support Features**

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

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.

© 2010 Cisco Systems, Inc. All rights reserved.
This Cisco Unified Border Element is a special Cisco IOS software image that 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.

**Activation**

**Cisco Product Authorization Key (PAK)**—A Product Authorization Key (PAK) is required to configure some of the features described in this guide. Before you start the configuration process, please register your products and activate your PAK at the following URL http://www.cisco.com/go/license.

**Finding Feature Information**

For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the “Cisco Unified Border Element Features Roadmap” section on page 3.

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.
Cisco Unified Border Element H.323-to-SIP Interworking

This chapter contains the following configuration topics:

**Cisco UBE Prerequisites and Restrictions**
- Prerequisites for Cisco Unified Border Element (Enterprise)
- Restrictions for Cisco Unified Border Element (Enterprise)

**H.323-SIP Protocol Handling and Supplementary Services**
- H.323-to-SIP Supplementary Feature Interworking for Session Border Controller
  - H323-to-SIP Back-to-Back Support

**Additional References**

**Glossary**

**Feature Information for Cisco UBE H.323-to-SIP Interworking**
H.323-to-SIP Supplementary Feature Interworking for Session Border Controller

Provides enhanced termination and re-origination of signaling and media between VoIP and Video Networks in conformance with RFC3261. New capabilities offered in this release include:

- iLBC Codec
  
  Codecs section of the Dial Peer Configuration on Voice Gateway Routers Guide
  

- 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

Prerequisites

**Cisco Unified Border Element**

- Cisco IOS Release 12.4(6)XE or a later release must be installed and running on your Cisco Unified Border Element.

**Cisco Unified Border Element (Enterprise)**

- Cisco IOS XE Release 2.5 or a later release must be installed and running on your Cisco ASR 1000 Series Router.
Feature Information for Cisco UBE H.323-to-SIP Interworking

Table 1 lists the release history for this chapter.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which 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 1 lists only the Cisco IOS software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>H.323-to-SIP Supplementary Feature Interworking for Session Border Controller (SBC)</td>
<td>12.4(6)XE</td>
<td>This feature was introduced.</td>
</tr>
<tr>
<td></td>
<td>12.4(11)T</td>
<td></td>
</tr>
</tbody>
</table>

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco’s trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

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.

© 2010 Cisco Systems, Inc. All rights reserved.
Configuration of SIP Trunking for PSTN Access (SIP-to-SIP)

This Cisco Unified Border Element is a special Cisco IOS software image that 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.

**Activation**

Cisco Product Authorization Key (PAK)—A Product Authorization Key (PAK) is required to configure some of the features described in this guide. Before you start the configuration process, please register your products and activate your PAK at the following URL http://www.cisco.com/go/license.

**Finding Feature Information**

For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the “Cisco Unified Border Element Features Roadmap” section on page 3.

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.
Configuration of SIP Trunking for PSTN Access (SIP-to-SIP) Features

This chapter contains the following configuration topics:

**Cisco UBE Prerequisites and Restrictions**
- Prerequisites for Cisco Unified Border Element
- Restrictions for Cisco Unified Border Element

**SIP trunk Monitoring**
- Configuring Cisco UBE Out-of-dialog OPTIONS Ping for Specified SIP Servers or Endpoints

**Additional References**

**Glossary**

**Feature Information for Configuration of SIP Trunking for PSTN Access (SIP-to-SIP)**
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 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 preferred dial peer, or else the on call is rejected with an error cause code.

Table 1 describes error codes option ping responses considered unsuccessful and the dial-peer is busied out for following scenarios:

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>503</td>
<td>service unavailable</td>
</tr>
<tr>
<td>505</td>
<td>sip version not supported</td>
</tr>
<tr>
<td>no response</td>
<td>i.e. request timeout</td>
</tr>
</tbody>
</table>

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 continues the heartbeat mechanism and the dial-peer is set 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 be in active state
  - Session protocol must be configured for SIP
  - Configure Session target or outbound proxy must be configured. If both are configured, outbound proxy has preference over session target.

Cisco Unified Border Element

- Cisco IOS Release 15.0(1)M or a later release must be installed and running on your Cisco Unified Border Element.

Cisco Unified Border Element (Enterprise)

- Cisco IOS XE Release 3.1S or a later release must be installed and running on your Cisco ASR 1000 Series Router
Restrictions

- The Cisco Unified Border Element OOD Options ping feature can only be configured at the VoIP Dial-peer level.
- All dial peers start in an active (not busied out) state on a router boot or reboot.
- If a dial-peer has both an outbound proxy and a session target configured, the OOD options ping is sent to the outbound proxy address first.
- Though multiple dial-peers may 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 dial-peer voice tag voip</td>
<td>Enters dial-peer configuration mode for the VoIP peer designated by tag.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# dial-peer voice 200 voip</td>
<td></td>
</tr>
</tbody>
</table>
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**—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
   AD  TAG  TYPE  MIN  OPER  PREFIX  DEST-PATTERN  KEEPALIVE
 111  voip  up  up   0   syst   active
   9  voip  up  down  0  syst   busy-out
```

**Command or Action**

| Step 4 | voice-class sip options-keepalive (up-interval seconds | down-interval seconds | retry retries) |
|--------|--------------------------------------------------------|
| Purpose | Monitors connectivity between endpoints. |
| Example: | Router(config-dial-peer)# voice-class sip options-keepalive up-interval 12 down-interval 65 retry 3 |

<table>
<thead>
<tr>
<th>Step 5</th>
<th>exit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Exits the current mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-dial-peer)# exit</td>
</tr>
</tbody>
</table>

**Troubleshooting Tips**

- **debug ccsip all**—shows all Session Initiation Protocol (SIP)-related debugging.
- **show dial-peer voice**—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
   AD  TAG  TYPE  MIN  OPER  PREFIX  DEST-PATTERN  KEEPALIVE
 111  voip  up  up   0   syst   active
   9  voip  up  down  0  syst   busy-out
```
Feature Information for Configuration of SIP Trunking for PSTN Access (SIP-to-SIP)

Table 1 lists the release history for this chapter.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which 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 1 lists only the Cisco IOS software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Out-of-dialog OPTIONS Ping to Monitor Dial-peers to Specified SIP Servers and Endpoints</td>
<td>15.0(1)M</td>
<td>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 command was introduced: <code>voice-class sip options-keepalive</code></td>
</tr>
</tbody>
</table>
Enterprise Application Interoperability for H.323-to-SIP and SIP-to-SIP

This Cisco Unified Border Element is a special Cisco IOS software image that 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.

Cisco Product Authorization Key (PAK)—A Product Authorization Key (PAK) is required to configure some of the features described in this guide. Before you start the configuration process, please register your products and activate your PAK at the following URL http://www.cisco.com/go/license.

Finding Feature Information

For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the “Cisco Unified Border Element Features Roadmap” section on page 3.

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.
Configuration of Enterprise Application Interoperability for H.323-to-SIP and SIP-to-SIP Features

This chapter contains the following configuration topics:

**Cisco UBE (Enterprise) Prerequisites and Restrictions**
- Prerequisites for Cisco Unified Border Element
- Restrictions for Cisco Unified Border Element

**Application specific interworking notes**
- Support for SIP 181 Call is Being Forwarded Message
- Support for Expires Timer Reset on Receiving or Sending SIP 183 Message

**Additional References**

**Glossary**

**Feature Information for Cisco UBE Protocol-Independent Features and Setup**
Configuring Support for SIP 181 Call is Being Forwarded Message

You can configure support for SIP 181 Call is Being Forwarded messages either globally or on a specific dial-peer. Use the `block` command in voice service SIP configuration mode to globally configure Cisco IOS voice gateways and Cisco UBEs to drop specified SIP provisional response messages. To configure settings for an individual dial peer, use the `voice-class sip block` command in dial peer voice configuration mode. Both globally and at the dial peer level, you can also use the `sdp` keyword to further control when the specified SIP message is dropped based on either the absence or presence of SDP information.

Additionally, you can use commands introduced for this feature to configure a Cisco UBE, either globally or at the dial peer level, to map specific received SIP provisional response messages to a different SIP provisional response message on the outgoing SIP dial peer. To do so, use the `map resp-code` command in voice service SIP configuration mode for global configuration or, to configure a specific dial peer, use the `voice-class sip map resp-code` in dial peer voice configuration mode.

This section contains the following tasks:

- Configuring Support for SIP 181 “Call is Being Forwarded” Message Globally, page 215
- Configuring Support for SIP 181 “Call is Being Forwarded” Message at the Dial-Peer Level, page 216
- Configuring Mapping of SIP Provisional Response Messages Globally, page 217
- Configuring Mapping of SIP Provisional Response Messages at the Dial-Peer Level, page 218

Prerequisites

Cisco Unified Border Element
Cisco IOS Release 15.0(1)XA or a later release must be installed and running on your Cisco Unified Border Element.

Cisco Unified Border Element (Enterprise)
- Cisco IOS XE Release 3.1S or a later release must be installed and running on your Cisco ASR 1000 Series Router.

Configuring Support for SIP 181 “Call is Being Forwarded” Message Globally

Perform this task to configure support for SIP 181 messages at a global level in SIP configuration (conf-serv-sip) mode.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. voice service voip
4. sip
5. block \{180 \| 181 \| 183\} [sdp \{absent \| present\}]
6. exit
DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enters privileged EXEC mode, or other security level set by a system administrator.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router&gt; enable</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong> voice service voip</td>
<td>Enters voice service VoIP configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# voice service voip</td>
</tr>
<tr>
<td><strong>Step 4</strong> sip</td>
<td>Enters SIP configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-vol-serv)# sip</td>
</tr>
<tr>
<td><strong>Step 5</strong> block (180</td>
<td>181</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(conf-serv-sip)# block 181 sdp present</td>
</tr>
<tr>
<td><strong>Step 6</strong> exit</td>
<td>Exits the current mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(conf-serv-sip)# exit</td>
</tr>
</tbody>
</table>

Configuring Support for SIP 181 “Call is Being Forwarded” Message at the Dial-Peer Level

Perform this task to configure support for SIP 181 messages at the dial-peer level, in dial peer voice configuration (config-dial-peer) mode.

SUMMARY STEPS

1. enable
2. configure terminal
3. dial-peer voice tag voip
4. voice-class sip block (180 | 181 | 183) [sdp (absent | present)]
5. exit
### Detailed Steps

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enters privileged EXEC mode, or other security level set by a system administrator.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> dial-peer voice tag voip</td>
<td>Enters dial peer VoIP configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# dial-peer voice 2 voip</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> voice-class sip block {180</td>
<td>181</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-dial-peer)# voice-class sip block 181 sdp present</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> exit</td>
<td>Exits the current mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-dial-peer)# exit</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring Mapping of SIP Provisional Response Messages Globally

Perform this task to configure mapping of specific received SIP provisional response messages at a global level in SIP configuration (conf-serv-sip) mode.

### Summary Steps

1. enable
2. configure terminal
3. voice service voip
4. sip
5. map resp-code 181 to 183
6. exit
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong>.enable</td>
<td>Enters privileged EXEC mode, or other security level set by a system administrator.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong>voice service voip</td>
<td>Enters voice service VoIP configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# voice service voip</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong>sip</td>
<td>Enters SIP configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(conf-voi-serv)# sip</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong>map resp-code 181 to 183</td>
<td>Enables mapping globally of received SIP messages of a specified message type to a different SIP message type.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(conf-serv-sip)# map resp-code 181 to 183</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong>exit</td>
<td>Exits the current mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(conf-serv-sip)# exit</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring Mapping of SIP Provisional Response Messages at the Dial-Peer Level

Perform this task to configure mapping of received SIP provisional response messages at the dial-peer level, in dial peer voice configuration (config-dial-peer) mode.

### SUMMARY STEPS

1. enable
2. configure terminal
3. dial-peer voice tag voip
4. voice-class sip map resp-code 181 to 183
5. exit
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enters privileged EXEC mode, or other security level set by a system administrator.  
- Enter your password if prompted. |
| **Example:**  
Router> enable | |
| **Step 2** configure terminal | Enters global configuration mode. |
| **Example:**  
Router# configure terminal | |
| **Step 3** dial-peer voice tag voip | Enters dial peer VoIP configuration mode. |
| **Example:**  
Router(config)# dial-peer voice 2 voip | |
| **Step 4** voice-class sip map resp-code 181 to 183 | Enables mapping of received SIP messages of a specified SIP message type on a specific dial peer to a different SIP message type. |
| **Example:**  
Router(config-dial-peer)# voice-class sip map resp-code 181 to 183 | |
| **Step 5** exit | Exits the current mode. |
| **Example:**  
Router(config-dial-peer)# exit | |
Support for Expires Timer Reset on Receiving or Sending SIP 183 Message

This feature enables support for resetting the Expires timer when receiving or sending SIP 183 messages on Cisco Unified Communications Manager Express (Cisco Unified CME), a Cisco IOS voice gateway, or a Cisco Unified Border Element (Cisco UBE). When the terminating device lacks answer supervision or does not send the required SIP 200 OK message within the timer expiry, you can enable this feature to send periodic SIP 183 messages to reset the Expires timer and preserve the call until final response. This feature can be enabled globally or on a specific dial peer. Additionally, you can configure this feature based on the presence or absence of Session Description Protocol (SDP).

For details about enabling this feature, see the `reset timer expires` and `voice-class sip reset timer expires` commands in the Cisco IOS Voice Command Reference.

Prerequisites

Before configuring support for Expires timer reset for SIP 183 on Cisco IOS SIP time-division multiplexing (TDM) gateways, Cisco UBEs, or Cisco Unified CME, verify the SIP configuration within the VoIP network for the appropriate originating and terminating gateways as described in the Cisco IOS SIP Configuration Guide.

**Cisco Unified Border Element**

- Cisco IOS Release 15.0(1)XA or a later release must be installed and running on your Cisco Unified Border Element.

**Cisco Unified Border Element (Enterprise)**

- Cisco IOS XE Release 3.1S or a later release must be installed and running on your Cisco ASR 1000 Series Router.

How to Configure Support for Expires Timer Reset on Receiving or Sending SIP 183 Message

To configure the Support for Expires Timer Reset on Receiving or Sending SIP 183 Message feature, complete the tasks in this section. You can enable this feature globally, using the `reset timer expires` command in voice service SIP configuration mode, or on a specific dial-peer using the `voice-class sip reset timer expires` command in dial peer voice configuration mode:

- Configuring Reset of Expires Timer Globally
- Configuring Reset of Expires Timer at the Dial-Peer Level

Configuring Reset of Expires Timer Globally

Perform this task to enable resetting of the Expires timer at the global level in SIP configuration (conf-serv-sip) mode.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `voice service voip`
4. `sip`
5. `reset timer expires 183`
6. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Router&gt; enable</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 voice service voip</td>
<td>Enters voice service VoIP configuration mode.</td>
</tr>
<tr>
<td>Example: Router(config)# voice service voip</td>
<td></td>
</tr>
<tr>
<td>Step 4 sip</td>
<td>Enters SIP configuration mode.</td>
</tr>
<tr>
<td>Example: Router(conf-voi-serv)# sip</td>
<td></td>
</tr>
<tr>
<td>Step 5 reset timer expires 183</td>
<td>Enables resetting of the Expires timer upon receipt of SIP 183 messages globally.</td>
</tr>
<tr>
<td>Example: Router(conf-serv-sip)# reset timer expires 183</td>
<td></td>
</tr>
<tr>
<td>Step 6 exit</td>
<td>Expires the current mode.</td>
</tr>
<tr>
<td>Example: Router(conf-serv-sip)# exit</td>
<td></td>
</tr>
</tbody>
</table>

Configuring Reset of Expires Timer at the Dial-Peer Level

Perform this task to enable resetting of the Expires timer at the dial-peer level in dial peer voice configuration (config-dial-peer) mode.

SUMMARY STEPS

1. enable
2. configure terminal
3. dial-peer voice tag voip
4. voice-class sip reset timer expires 183
5. exit
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> dial-peer voice tag voip</td>
<td>Enters dial peer VoIP configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# dial-peer voice 2 voip</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> voice-class sip reset timer expires 183</td>
<td>Enables resetting of the Expires timer upon receipt of SIP 183 messages on a specific dial peer.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-dial-peer)# voice-class sip reset timer expires 183</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> exit</td>
<td>Exits the current mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-dial-peer)# exit</td>
<td></td>
</tr>
</tbody>
</table>
Feature Information for Enterprise Application Interoperability for H.323-to-SIP and SIP-to-SIP

Table 1 lists the release history for this chapter.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which 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 1 lists only the Cisco IOS software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

### Table 1 Feature Information for Enterprise Application Interoperability for H.323-to-SIP and SIP-to-SIP Features

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
</table>

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

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.

© 2010 Cisco Systems, Inc. All rights reserved.
Cisco Unified Border Element Management

This Cisco Unified Border Element is a special Cisco IOS software image that 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.

---

**Activation**

Cisco Product Authorization Key (PAK)—A Product Authorization Key (PAK) is required to configure some of the features described in this guide. Before you start the configuration process, please register your products and activate your PAK at the following URL: [http://www.cisco.com/go/license](http://www.cisco.com/go/license).

---

**Finding Feature Information**

For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the “Cisco Unified Border Element Features Roadmap” section on page 3.

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. To access Cisco Feature Navigator, go to [http://www.cisco.com/go/cfn](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.
Configuration of Cisco UBE Management Features

This chapter contains the following configuration topics:

Cisco UBE Prerequisites and Restrictions
- Prerequisites for Cisco Unified Border Element
- Restrictions for Cisco Unified Border Element

Monitoring the SIP Trunk
- Out-of-dialog SIP OPTIONS

Protocol Monitoring
- Media Inactivity timer based on RTP
- The Clearable SIP-US Statistics feature adds MIB support.

Additional References,

Glossary

Feature Information for Cisco UBE Management
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 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 preferred dial peer, or else the on call is rejected with an error cause code.

Table 1 describes error codes option ping responses considered unsuccessful and the dial-peer is busied out for following scenarios:

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>503</td>
<td>service unavailable</td>
</tr>
<tr>
<td>505</td>
<td>sip version not supported</td>
</tr>
<tr>
<td>no response</td>
<td>i.e. request timeout</td>
</tr>
</tbody>
</table>

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 continues the heartbeat mechanism and the dial-peer is set 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 be in active state
  - Session protocol must be configured for SIP
  - Configure Session target or outbound proxy must be configured. If both are configured, outbound proxy has preference over session target.

Cisco Unified Border Element

- Cisco IOS Release 15.0(1)M or a later release must be installed and running on your Cisco Unified Border Element.

Cisco Unified Border Element (Enterprise)

- Cisco IOS XE Release 3.1S or a later release must be installed and running on your Cisco ASR 1000 Series Router
Restrictions

- The Cisco Unified Border Element OOD Options ping feature can only be configured at the VoIP Dial-peer level.
- All dial peers start in an active (not busied out) state on a router boot or reboot.
- If a dial-peer has both an outbound proxy and a session target configured, the OOD options ping is sent to the outbound proxy address first.
- Though multiple dial-peers may 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>dial-peer voice tag voip</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# dial-peer voice 200 voip</td>
<td>Enters dial-peer configuration mode for the VoIP peer designated by tag.</td>
</tr>
</tbody>
</table>
Step 4  
voice-class sip options-keepalive {up-interval seconds | down-interval seconds | retry retries}

Example:  
Router(config-dial-peer)# voice-class sip options-keepalive up-interval 12 down-interval 65 retry 3

Step 5  
exit

Example:  
Router(config-dial-peer)# exit

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.

Example:

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.

Example:

Router# show dial-peer voice summary

<table>
<thead>
<tr>
<th>AD</th>
<th>TAG</th>
<th>TYPE</th>
<th>MIN</th>
<th>OPER</th>
<th>PREFIX</th>
<th>DEST-PATTERN</th>
<th>KEEPALIVE</th>
</tr>
</thead>
<tbody>
<tr>
<td>111</td>
<td>voip</td>
<td>up</td>
<td>up</td>
<td>up</td>
<td>0 syst</td>
<td>active</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>voip</td>
<td>up</td>
<td>down</td>
<td></td>
<td>0 syst</td>
<td>busy-out</td>
<td></td>
</tr>
</tbody>
</table>
SIP-to-SIP Extended Feature Functionality for Session Border Controllers

The SIP-to-SIP Extended Feature Functionality for Session Border Controllers (SBCs) enables the SIP-to-SIP functionality to conform with RFC 3261 to interoperate with SIP User Agents (UAs). The SIP-to-SIP Extended Feature Functionality includes:

- Call Admission Control (based on CPU, memory, and total calls)
- Delayed Media Call
- ENUM support
- Configuring SIP Error Message Pass Through
- 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)

Prerequisites

Cisco Unified Border Element

- Cisco IOS Release 12.4(6)T or a later release must be installed and running on your Cisco Unified Border Element.

Cisco Unified Border Element (Enterprise)

- Cisco IOS XE Release 3.1S or a later release must be installed and running on your Cisco ASR 1000 Series Router.
Clearable SIP-UA Statistics

This feature introduces the CISCO-SIP-UA-MIB. The MIB is available by default.
To locate and download MIBs for selected platforms, Cisco IOS software releases, and feature sets, use Cisco MIB Locator found at the following URL:
http://www.cisco.com/go/mibs

Prerequisites

Cisco Unified Border Element
- Cisco IOS Release 12.3(2)T or a later release must be installed and running on your Cisco Unified Border Element.

Cisco Unified Border Element (Enterprise)
- Cisco IOS XE Release 2.5 or a later release must be installed and running on your Cisco ASR 1000 Series Router.
Feature Information for Cisco UBE Management

Table 1 lists the release history for this chapter.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which 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 1 lists only the Cisco IOS software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
</table>
| SIP-to-SIP Extended Feature Functionality for Session Border Controllers | 12.4(6)T | The SIP-to-SIP Extended Feature Functionality for Session Border Controllers (SBCs) enables the SIP-to-SIP functionality to conform with RFC 3261 to interoperate with SIP User Agents (UAs).
  This feature includes the following:
  - Media Inactivity timer based on RTP
  This feature uses no new or modified commands. |
| Clearable SIP-UA Statistics | 12.2(13)T  
12.2(15)T  
12.3(2)T | The Clearable SIP-US Statistics feature adds MIB support.
No commands or configurations were introduced or modified in this release. |
Cisco Unified Border Element Standards Compliance

Revised: October 20, 2010  
First Published: November 25, 2009  
Last Updated: October 20, 2010

This Cisco Unified Border Element is a special Cisco IOS software image that 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.

Activation  
Cisco Product Authorization Key (PAK)—A Product Authorization Key (PAK) is required to configure some of the features described in this guide. Before you start the configuration process, please register your products and activate your PAK at the following URL http://www.cisco.com/go/license.

Finding Feature Information

For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the “Cisco Unified Border Element Features Roadmap” section on page 3.

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.
Cisco Unified Border Element Cisco UBE Standards Compliance Features

This chapter contains the following configuration topics:

**Cisco UBE Prerequisites and Restrictions**
- Prerequisites for Cisco Unified Border Element
- Restrictions for Cisco Unified Border Element

**Cisco UBE Standards Compliance**
- ENUM Support (RFC2916)
- SIP—RFC 2782 Compliance with DNS SRV Queries
- SIP - DNS SRV RFC2782 Compliance

**Additional References**

Glossary

Feature Information for Cisco UBE Standards Compliance
SIP-to-SIP Extended Feature Functionality for Session Border Controllers

The SIP-to-SIP Extended Feature Functionality for Session Border Controllers (SBCs) enables the SIP-to-SIP functionality to conform with RFC 3261 to interoperate with SIP User Agents (UAs). The SIP-to-SIP Extended Feature Functionality includes:

- Call Admission Control (based on CPU, memory, and total calls)
- Delayed Media Call
- ENUM support
- Configuring SIP Error Message Pass Through
- 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)

Prerequisites

**Cisco Unified Border Element**

- Cisco IOS Release 12.4(6)T or a later release must be installed and running on your Cisco Unified Border Element.

**Cisco Unified Border Element (Enterprise)**

- Cisco IOS XE Release 3.1S or a later release must be installed and running on your Cisco ASR 1000 Series Router.
SIP—RFC 2782 Compliance with DNS SRV Queries

Effective with Cisco IOS XE Release 2.5, the Domain Name System Server (DNS SRV) query used to determine the IP address of the user endpoint is modified in compliance with RFC 2782 (which supersedes RFC 2052). The DNS SRV query prepends the protocol label with an underscore “_” character to reduce the risk of duplicate names being used for unrelated purposes. The form compliant with RFC 2782 is the default style.

Prerequisites SIP—RFC 2782 Compliance with DNS SRV Queries

Cisco Unified Border Element

- Cisco IOS Release 12.2(8)T or a later release must be installed and running on your Cisco Unified Border Element.

Cisco Unified Border Element (Enterprise)

- Cisco IOS XE Release 2.5 or a later release must be installed and running on your Cisco ASR 1000 Series Router.

Information SIP—RFC 2782 Compliance with DNS SRV Queries

Session Initiation Protocol (SIP) on Cisco VoIP gateways uses the DNS SRV query to determine the IP address of the user endpoint. The query string has a prefix in the form of “protocol.transport.” and is attached to the fully qualified domain name (FQDN) of the next hop SIP server. This prefix style originated in RFC 2052. Beginning with Cisco IOS XE Release 2.5, a second style, in compliance with RFC 2782, prepends the protocol label with an underscore “_”; for example, “_protocol._transport.” The addition of the underscore reduces the risk of the same name being used for unrelated purposes. The form compliant with RFC 2782 is the default style.

How to Configure SIP-RFC 2782 Compliance with DNS SRV Queries

This section contains the following procedures:

- Configuring DNS Server Query Format RFC 2782 Compliance with DNS SRV Queries, page 241 (optional)

Configuring DNS Server Query Format RFC 2782 Compliance with DNS SRV Queries

Compliance with RFC 2782 changes the DNS SRV protocol label style. RFC 2782 updates RFC 2052 by prepending the protocol label with an underscore character. The prefix format compliant with RFC 2782 is the default format. However, backward compatibility is available, allowing newer versions of Cisco IOS software to work with older networks that support only RFC 2052 DNS SRV prefix style.

To configure the format of DNS SRV queries to comply with RFC 2782, complete this task.

Note

You do not have to perform this task if you want to use the default RFC 2782 format.
SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface type number`
4. `sip-ua`
5. `srv version {1 | 2}`
6. `exit`

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
- Enter your password if prompted. |
| **Example:** | Router> enable |
| **Step 2** configure terminal | Enters global configuration mode. |
| **Example:** | Router# configure terminal |
| **Step 3** interface type number | Configures an interface type and enters interface configuration mode |
| **Example:** | Router(config)# interface gigabitethernet 0/0/0 |
| **Step 4** sip-ua | Enters SIP UA configuration mode. |
| **Example:** | Router(config-if)# sip-ua |
| **Step 5** srv version {1 | 2} | Generates DNS SRV queries in either RFC 2782 or RFC 2052 format.  
- 1—The query is set to the domain name prefix of protocol.transport. (RFC 2052 style).  
- 2—The query is set to the domain name prefix of _protocol._transport. (RFC 2782 style). This is the default. |
| **Example:** | Router(config-sip-ua)# srv version 2 |
| **Step 6** exit | Exits the current configuration mode. |
| **Example:** | Router(config-sip-ua)# exit |

Verifying

The following example shows sample is output from the `show sip-ua status` command used to verify the style of DNS server queries:

Router# `show sip-ua status`
SIP User Agent Status
SIP User Agent for UDP : ENABLED
SIP User Agent for TCP : ENABLED
SIP User Agent bind status(signaling): DISABLED
SIP User Agent bind status(media): DISABLED
SIP max-forwards : 6
SIP DNS SRV version: 1 (rfc 2052)
Feature Information for Cisco UBE Standards Compliance

Table 1 lists the release history for this chapter.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which 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 lists only the Cisco IOS software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
</table>
| SIP-to-SIP Extended Feature Functionality for Session Border Controllers | 12.4(6)T | The SIP-to-SIP Extended Feature Functionality for Session Border Controllers (SBCs) enables the SIP-to-SIP functionality to conform with RFC 3261 to interoperate with SIP User Agents (UAs). The SIP-to-SIP Extended Feature Functionality includes:  
  - Call Admission Control (based on CPU, memory, and total calls)  
  - Delayed Media Call  
  - ENUM Support  
  - Configuring SIP Error Message Pass Through  
  - 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)  
  This feature uses no new or modified commands. |
| SIP—RFC 2782 Compliance of DNS SRV Queries | 12.2(8)T, 12.2(11)T, 12.2(15)T | Effective with Cisco IOS XE Release 2.5, the DNS SRV query used to determine the IP address of the user endpoint is modified in compliance with RFC 2782 (which supersedes RFC 2052). The DNS SRV query prepends the protocol label with an underscore “_” character to reduce the risk of duplicate names being used for unrelated purposes. The form compliant with RFC 2782 is the default style.  
  The following command was introduced or modified: srv version. |
Additional References

The following sections provide references related to the Cisco Unified Border Element Configuration Guide.

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Commands List, All Releases</td>
</tr>
<tr>
<td>Cisco IOS Voice commands</td>
<td>Cisco IOS Voice Command Reference</td>
</tr>
<tr>
<td>Cisco IOS Release 15.0</td>
<td>Cisco IOS Release 15.0 Configuration Guides</td>
</tr>
<tr>
<td>Related Application Guides</td>
<td>• Cisco Unified Communications Manager and Cisco IOS Interoperability Guide</td>
</tr>
<tr>
<td></td>
<td>• Cisco IOS SIP Configuration Guide</td>
</tr>
<tr>
<td></td>
<td>• Cisco Unified Communications Manager (CallManager) Programming Guides</td>
</tr>
</tbody>
</table>
Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>CISCO-PROCESS MIB</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS XE software 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></td>
</tr>
<tr>
<td>CISCO-MEMORY-POOL-MIB</td>
<td></td>
</tr>
<tr>
<td>CISCO-SIP-UA-MIB</td>
<td></td>
</tr>
<tr>
<td>DIAL-CONTROL-MIB</td>
<td></td>
</tr>
<tr>
<td>CISCO-VOICE-DIAL-CONTROL-MIB</td>
<td></td>
</tr>
<tr>
<td>CISCO-DSP-MGMT-MIB</td>
<td></td>
</tr>
<tr>
<td>IF-MIB</td>
<td></td>
</tr>
<tr>
<td>IP-TAP-MIB</td>
<td></td>
</tr>
<tr>
<td>TAP2-MIB</td>
<td></td>
</tr>
<tr>
<td>USER-CONNECTION-TAP-MIB</td>
<td></td>
</tr>
</tbody>
</table>

RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 1889</td>
<td><em>RTP: A Transport Protocol for Real-Time Applications</em></td>
</tr>
<tr>
<td>RFC 2131</td>
<td><em>Dynamic Host Configuration Protocol</em></td>
</tr>
<tr>
<td>RFC 2132</td>
<td><em>DHCP Options and BOOTP Vendor Extensions</em></td>
</tr>
<tr>
<td>RFC 2327</td>
<td><em>SDP: Session Description Protocol</em></td>
</tr>
<tr>
<td>RFC 2543</td>
<td><em>SIP: Session Initiation Protocol</em></td>
</tr>
<tr>
<td>RFC 2543-bis-04</td>
<td><em>SIP: Session Initiation Protocol, draft-ietf-sip-rfc2543bis-04.txt</em></td>
</tr>
<tr>
<td>RFC 2782</td>
<td><em>A DNS RR for Specifying the Location of Services (DNS SRV)</em></td>
</tr>
<tr>
<td>RFC 2833</td>
<td><em>RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals</em></td>
</tr>
<tr>
<td>RFC 3203</td>
<td><em>DHCP reconfigure extension</em></td>
</tr>
<tr>
<td>RFC 3261</td>
<td><em>SIP: Session Initiation Protocol</em></td>
</tr>
<tr>
<td>RFC 3262</td>
<td><em>Reliability of Provisional Responses in Session Initiation Protocol (SIP)</em></td>
</tr>
<tr>
<td>RFC 3323</td>
<td><em>A Privacy Mechanism for the Session Initiation Protocol (SIP)</em></td>
</tr>
<tr>
<td>RFC 3325</td>
<td><em>Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks</em></td>
</tr>
<tr>
<td>RFC 3515</td>
<td><em>The Session Initiation Protocol (SIP) Refer Method</em></td>
</tr>
</tbody>
</table>
### Additional References

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 3361</td>
<td>Dynamic Host Configuration Protocol (DHCP-for-IPv4) Option for Session Initiation Protocol (SIP) Servers</td>
</tr>
<tr>
<td>RFC 3455</td>
<td>Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)</td>
</tr>
<tr>
<td>RFC 3608</td>
<td>Session Initiation Protocol (SIP) Extension Header Field for Service Route Discovery During Registration</td>
</tr>
<tr>
<td>RFC 3711</td>
<td>The Secure Real-time Transport Protocol (SRTP)</td>
</tr>
<tr>
<td>RFC 3925</td>
<td>Vendor-Identifying Vendor Options for Dynamic Host Configuration Protocol version 4 (DHCPv4)</td>
</tr>
</tbody>
</table>

### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>
AMR-NB—Adaptive Multi Rate codec – Narrow Band.

Allow header—Lists the set of methods supported by the UA generating the message.

bind — In SIP, configuring the source address for signaling and media packets to the IP address of a specific interface.

call—In SIP, a call consists of all participants in a conference invited by a common source. A SIP call is identified by a globally unique call identifier. A point-to-point IP telephony conversation maps into a single SIP call.

call leg—A logical connection between the router and another endpoint.

CLI—command-line interface.

Content-Type header—Specifies the media type of the message body.

CSeq header—Serves as a way to identify and order transactions. It consists of a sequence number and a method. It uniquely identifies transactions and differentiates between new requests and request retransmissions.

delta—An incremental value. In this case, the delta is the difference between the current time and the time when the response occurred.

dial peer—An addressable call endpoint.

dial peer—An addressable call endpoint.

DNS—Domain Name System. Used to translate H.323 IDs, URLs, or e-mail IDs to IP addresses. DNS is also used to assist in locating remote gatekeepers and to reverse-map raw IP addresses to host names of administrative domains.

DNS SRV—Domain Name System Server. Used to locate servers for a given service.

DSP—Digital Signal Processor.

DTMF—dual-tone multifrequency. Use of two simultaneous voice-band tones for dialing (such as touch-tone).

EFXS—IP phone virtual voice ports.

FQDN—fully qualified domain name. Complete domain name including the host portion; for example, serverA.companyA.com.

FXS—analog telephone voice ports.

gateway—A gateway allows SIP or H.323 terminals to communicate with terminals configured to other protocols by converting protocols. A gateway is the point where a circuit-switched call is encoded and repackaged into IP packets.

H.323—An International Telecommunication Union (ITU-T) standard that describes packet-based video, audio, and data conferencing. H.323 is an umbrella standard that describes the architecture of the conferencing system and refers to a set of other standards (H.245, H.225.0, and Q.931) to describe its actual protocol.

iLBC—internet Low Bitrate Codec.

INVITE—A SIP message that initiates a SIP session. It indicates that a user is invited to participate, provides a session description, indicates the type of media, and provides insight regarding the capabilities of the called and calling parties.

IP—Internet Protocol. A connectionless protocol that operates at the network layer (Layer 3) of the OSI model. IP provides features for addressing, type-of-service specification, fragmentation and reassemble, and security. Defined in RFC 791. This protocol works with TCP and is usually identified as TCP/IP. See TCP/IP.
ISDN—Integrated Services Digital Network.

**Minimum Timer**—Configured minimum value for session interval accepted by SIP elements (proxy, UAC, UAS). This value helps minimize the processing load from numerous INVITE requests.

**Min-SE**—Minimum Session Expiration. The minimum value for session expiration.

**multicast**—A process of transmitting PDUs from one source to many destinations. The actual mechanism (that is, IP multicast, multi-unicast, and so forth) for this process might be different for LAN technologies.

**originator**—User agent that initiates the transfer or Refer request with the recipient.

**PDU**—protocol data units. Used by bridges to transfer connectivity information.

**PER**—Packed Encoding Rule.

**proxy**—A SIP UAC or UAS that forwards requests and responses on behalf of another SIP UAC or UAS.

**proxy server**—An intermediary program that acts as both a server and a client for the purpose of making requests on behalf of other clients. Requests are serviced internally or by passing them on, possibly after translation, to other servers. A proxy interprets and, if necessary, rewrites a request message before forwarding it.

**recipient**—User agent that receives the Refer request from the originator and is transferred to the final recipient.

**redirect server**—A server that accepts a SIP request, maps the address into zero or more new addresses, and returns these addresses to the client. It does not initiate its own SIP request or accept calls.

**re-INVITE**—An INVITE request sent during an active call leg.

**Request URI**—Request Uniform Resource Identifier. It can be a SIP or general URL and indicates the user or service to which the request is being addressed.

**RFC**—Request For Comments.

**RTP**—Real-Time Transport Protocol (RFC 1889)

**SCCP**—Skinny Client Control Protocol.

**SDP**—Session Description Protocol. Messages containing capabilities information that are exchanged between gateways.

**session**—A SIP session is a set of multimedia senders and receivers and the data streams flowing between the senders and receivers. A SIP multimedia conference is an example of a session. The called party can be invited several times by different calls to the same session.

**session expiration**—The time at which an element considers the call timed out if no successful INVITE transaction occurs first.

**session interval**—The largest amount of time that can occur between INVITE requests in a call before a call is timed out. The session interval is conveyed in the Session-Expires header. The UAS obtains this value from the Session-Expires header of a 2xx INVITE response that it sends. Proxies and UACs determine this value from the Session-Expires header in a 2xx INVITE response they receive.

**SIP**—Session Initiation Protocol. An application-layer protocol originally developed by the Multiparty Multimedia Session Control (MMUSIC) working group of the Internet Engineering Task Force (IETF). Their goal was to equip platforms to signal the setup of voice and multimedia calls over IP networks. SIP features are compliant with IETF RFC 2543, published in March 1999.

**SIP URL**—Session Initiation Protocol Uniform Resource Locator. Used in SIP messages to indicate the originator, recipient, and destination of the SIP request. Takes the basic form of `user@host`, where `user` is a name or telephone number, and `host` is a domain name or network address.

**SPI**—service provider interface.
socket listener—Software provided by a socket client to receives datagrams addressed to the socket.

stateful proxy—A proxy in keepalive mode that remembers incoming and outgoing requests.

TCP—Transmission Control Protocol. Connection-oriented transport layer protocol that provides reliable full-duplex data transmissions. TCP is part of the TCP/IP protocol stack. See also TCP/IP and IP.

TDM—time-division multiplexing.

UA—user agent. A combination of UAS and UAC that initiates and receives calls. See UAS and UAC.

UAC—user agent client. A client application that initiates a SIP request.

UAS—user agent server. A server application that contacts the user when a SIP request is received and then returns a response on behalf of the user. The response accepts, rejects, or redirects the request.

UDP—User Datagram Protocol. Connectionless transport layer protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by other protocols. UDP is defined in RFC-768.

URI—Uniform Resource Identifier. Takes a form similar to an e-mail address. It indicates the user’s SIP identity and is used for redirection of SIP messages.

URL—Universal Resource Locator. Standard address of any resource on the Internet that is part of the World Wide Web (WWW).

User Agent—A combination of UAS and UAC that initiates and receives calls. See UAS and UAC.

VFC—Voice Feature Card.

VoIP—Voice over IP. The ability to carry normal telephone-style voice over an IP-based Internet with POTS-like functionality, reliability, and voice quality. VoIP is a blanket term that generally refers to the Cisco standards-based approach (for example, H.323) to IP voice traffic.