# CONTENTS

## CHAPTER 1

**Cisco Unified Border Element Enterprise SIP Support**  
Finding Feature Information 1  
Cisco Unified Border Element Enterprise SIP Support Features 1

## CHAPTER 2

**Reporting End-of-Call Statistics in SIP BYE Message** 5  
Finding Feature Information 6  
Prerequisites for Reporting End-of-Call Statistics in SIP BYE Message 6  
Restrictions for Reporting End-of-Call Statistics in SIP BYE Message 6  
Disabling Reporting End-of-Call Statistics in SIP BYE Message 7  
Defining SIP Profile Rules to Remove a Header 7  
Disabling Reporting End-of-Call Statistics in SIP BYE Message at the Global Level 8  
Disabling Reporting End-of-Call Statistics in SIP BYE Message at the Dial Peer Level 9  
Feature Information for Reporting End-of-Call Statistics in SIP BYE Message 10

## CHAPTER 3

**Configurable Hostname in Locally Generated SIP Headers** 13  
Finding Feature Information 13  
Prerequisites for Configurable Hostname in Locally Generated SIP Headers 13  
Restrictions for Configurable Hostname in Locally Generated SIP Headers 14  
How to Configure the Hostname in Locally Generated SIP Headers 14  
Configuring Hostname in Locally Generated SIP Headers at the Global Level 14  
Configuring Hostname in Locally Generated SIP Headers at the Dial-Peer-Specific Level 15  
Verifying the Hostname in Locally Generated SIP Headers 16  
Feature Information for Configurable Hostname in Locally Generated SIP Headers 22

## CHAPTER 4

**SIP Session Timer Support** 23  
Finding Feature Information 23
Prerequisites for SIP Session Timer Support 23
Information About SIP Session Timer Support 24
How to Configure SIP Session Timer Support 26
  Prerequisites 26
  Restrictions 26
  Configuring SIP Session Timer Support 26
Troubleshooting Tips 27
Feature Information for SIP Session Timer Support 28

CHAPTER 5
SIP-to-SIP Basic Functionality for Session Border Controller 31
Finding Feature Information 32
Prerequisites for SIP-to-SIP Basic Functionality for Session Border Controller 32
Feature Information for SIP-to-SIP Basic Functionality for Session Border Controller 32

CHAPTER 6
SIP-to-SIP Supplementary Services for Session Border Controller 35
Finding Feature Information 35
Prerequisites for SIP-to-SIP Supplementary Services for Session Border Controller 35
Information About SIP-to-SIP Supplementary Services for Session Border Controller 36
  SIP-to-SIP Supplementary Services for Session Border Controller 36
  Digital Signal Processors (DSPs) and SIP Call Hold/Resume 36
How to Configure SIP-to-SIP Supplementary Services for Session Border Controller 36
Feature Information for SIP-to-SIP Supplementary Services for Session Border Controller 37

CHAPTER 7
Mid-call Signaling Consumption 39
Finding Feature Information for Mid-call Signaling 39
Prerequisites 40
Mid-call Signaling Passthrough - Media Change 41
  Restrictions for Mid-Call Signaling Passthrough - Media Change 41
  Behavior of Mid-call Re-INVITE Consumption 41
Configuring Passthrough of Mid-call Signalling 43
Example Configuring Passthrough SIP Messages at Dial Peer Level 44
Example Configuring Passthrough SIP Messages at the Global Level 44
Mid-call Signaling Block 44
  Restrictions for Mid-Call Signaling Block 45
Prerequisites for SIP UPDATE Message per RFC 3311  
Restrictions for SIP UPDATE Message per RFC 3311  
Information About SIP UPDATE Message per RFC 3311  
Feature Information for the SIP UPDATE Message per RFC 3311

CHAPTER 14
Expires Timer Reset on Receiving or Sending SIP 183 Message  
Finding Feature Information
Prerequisites for Expires Timer Reset on Receiving or Sending SIP 183 Message
How to Configure Expires Timer Reset on Receiving or Sending SIP 183 Message
  Configuring Reset of Expires Timer Globally
  Configuring Reset of Expires Timer at the Dial-Peer Level
Feature Information for Configuring Support for Expires Timer Reset on Receiving or Sending SIP 183 Message

CHAPTER 15
Selective Filtering of Outgoing Provisional Response on the Cisco Unified Border Element  
Finding Feature Information
Prerequisites for Selective Filtering of Outgoing Provisional Response on the Cisco UBE
Restrictions for Selective Filtering of Outgoing Provisional Response on the Cisco UBE
How to Configure Selective Filtering of Outgoing Provisional Response on the Cisco UBE
  Configuring Selective Filtering of Outgoing Provisional Response on the Cisco UBE at the Global Level
  Configuring Selective Filtering of Outgoing Provisional Response on the Cisco UBE at the Dial Peer Level
Feature Information for Selective Filtering of Outgoing Provisional Response on the Cisco Unified Border Element

CHAPTER 16
RFC 4040-Based Clear Channel Codec Negotiation for SIP Calls  
Finding Feature Information
Prerequisites for RFC 4040-Based Clear Channel Codec Negotiation for SIP Calls
Restrictions for RFC 4040-Based Clear Channel Codec Negotiation for SIP Calls
Information about RFC 4040-Based Clear Channel Codec Negotiation for SIP Calls
How to Configure RFC 4040-Based Clear Channel Codec Negotiation for SIP Calls
  Configuring RFC 4040-Based Clear Channel Codec Negotiation for SIP Calls Globally for All Dial Peers
**CHAPTER 19**

**Dynamic Refer Handling**

- Feature Information for Dynamic REFER Handling 143
- Prerequisites 144
- Restrictions 144
- Configuring REFER Passthrough with Unmodified Refer-to 144
- Configuring REFER Consumption 146
- Troubleshooting Tips 148

**CHAPTER 20**

**Transparent Tunneling of QSIG and Q.931**

- Finding Feature Information 149
- Prerequisites for Transparent Tunneling of QSIG and Q.931 150
- Restrictions for Transparent Tunneling of QSIG and Q.931 150
- Information About Transparent Tunneling of QSIG or Q.931 150
  - Use of the QSIG or Q.931 Protocols 150
  - Purpose of Tunneling QSIG or Q.931 over SIP 151
  - Encapsulation of QSIG in SIP Messaging 151
  - Mapping of QSIG Message Elements to SIP Message Elements 153
- How to Transparently Tunnel QSIG over SIP 153
  - Configuring Signaling Forward Settings for a Gateway 153
  - Signaling Forward Settings for a Gateway 153
  - Configuring Signaling Forward Settings for an Interface 155
  - Signaling Forward Settings for an Interface 155
- Configuration Examples for Transparent Tunneling of QSIG 157
  - Tunneling QSIG Raw Messages over SIP Example 157
  - Tunneling QSIG Messages Unconditionally over SIP Example 157
  - Tunneling QSIG Raw Messages over SIP on an Interface Example 157
  - Tunneling QSIG Messages Unconditionally over SIP on an Interface Example 158
- Feature Information for Transparent Tunneling of QSIG and Q.931 158

---

Example: Enabling Configurable Pass-Through of SIP INVITE Parameters (Global Level) 140
Example: Enabling Configurable Pass-Through of SIP INVITE Parameters (Dial Peer Level) 140
Example: Configuring a Route String Header Pass-Through Using Pass-Through List 140
Additional References for Configurable Pass-Through of SIP INVITE Parameters 141
Feature Information for Configurable Pass-Through of SIP INVITE Parameters 141
## CHAPTER 21

**SIP Diversion Header Enhancements** 161
- Finding Feature Information 161
- Prerequisites for SIP Diversion Header Enhancements 161
- Information about SIP Diversion Header Enhancements 162
- How to Configure SIP Diversion Header Enhancements 162
- Feature Information for SIP Diversion Header Enhancements 163

## CHAPTER 22

**SIP History INFO** 165
- Finding Feature Information 165
- Prerequisites 165
- Configuring SIP History INFO 166
- Feature Information for SIP History-info Header 166

## CHAPTER 23

**Hiding the Internal Topology Information Embedded Within the History-info Header at the Cisco UBE** 167
- Finding Feature Information 167
- Restrictions for Hiding the Internal Topology Information 167
- Hiding Internal Toplogy Information in History-info Header at global level 168
- Hiding Internal Toplogy Information in History-info Header at the Dial-Peer Level 169
- Feature Information for Hiding Internal Topology in the History-info Header 170

## CHAPTER 24

**Configuring Call Routing logic on Cisco UBE using the History-info Header** 173
- Finding Feature Information 173
- Configuring Call Routing Logic on Cisco UBE using the History-info Header Globally 173
- Configuring all Routing Logic on Cisco UBE using the History-info Header at the Dial-Peer Level 175
- Feature Information for Call Routing logic on Cisco UBE using the History-info Header 176

## CHAPTER 25

**Configurable SIP Parameters via DHCP** 177
- Finding Feature Information 177
- Prerequisites for Configurable SIP Parameters via DHCP 177
- Restrictions for Configurable SIP Parameters via DHCP 178
- Information About Configurable SIP Parameters via DHCP 178
How to Configure SIP Parameters via DHCP 182
  Configuring the DHCP Client 182
  Configuring the DHCP Client Example 183
  Enabling the SIP Configuration 184
  Enabling the SIP Configuration Example 185
  Troubleshooting Tips 185
  Configuring a SIP Outbound Proxy Server 186
  Configuring a SIP Outbound Proxy Server in Voice Service VoIP Configuration Mode 186
  Configuring a SIP Outbound Proxy Server in Voice Service VoIP Configuration Mode Example 187
  Configuring a SIP Outbound Proxy Server and Session Target in Dial Peer Configuration Mode 187
  Configuring a SIP Outbound Proxy Server in Dial Peer Configuration Mode Example 188

Feature Information for Configurable SIP Parameters via DHCP 189

---

CHAPTER 26

Multiple Registrars on SIP Trunks 191
  Finding Feature Information 191
  Prerequisites for Multiple Registrars on SIP Trunks 191
  Restrictions for Multiple Registrars on SIP Trunks 192
  Configuring Multiple Registrars on SIP Trunks Feature 192
  Feature Information for the Multiple Registrars on SIP Trunks Feature 192

---

CHAPTER 27

Session Refresh with Reinvites 195
  Finding Feature Information 195
  Prerequisites for Session Refresh with Reinvites 195
  Information about Session Refresh with Reinvites 196
  How to Configure Session Refresh with Reinvites 196
  Configuring Session refresh with Reinvites 196
  Feature Information for Session Refresh with Reinvites 197

---

CHAPTER 28

V150.1 MER Support in SDP Passthrough Mode 199
  Finding Feature Information 199
  Information About VER.150.1 MER Support in SDP Passthrough Mode 199
  V.150.1 MER Support in SDP Passthrough Mode 199
Cisco Unified Border Element Enterprise SIP Support

This Cisco Unified Border Element (Enterprise) is a special Cisco IOS XE software image that runs on Cisco ASR1000. 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.

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.

Note

- Finding Feature Information, on page 1
- Cisco Unified Border Element Enterprise SIP Support Features, on page 1

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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

Cisco Unified Border Element Enterprise SIP Support Features

This chapter contains the following configuration topics:

Cisco UBE (Enterprise) Prerequisites and Restrictions

- Prerequisites for Cisco Unified Border Element (Enterprise)
- Restrictions for Cisco Unified Border Element (Enterprise)
Basic SIP Set-up

- SIP—Core SIP Technology Enhancements
- Reporting End–of–Call Statistics in SIP BYE Message

SIP Parameter Settings

- SIP—Configurable Hostname in Locally Generated SIP Headers
- SIP Parameter Modification
- Conditional Header Manipulation of SIP Headers
- SIP—Session Timer Support
- Adjustable Timers for REGISTRATION Refresh and Retries

SIP Protocol Handling and Supplementary Services

- SIP—to–SIP Basic Feature Functionality for Session Border Controller
- SIP—to–SIP Extended Feature Functionality for Session Border Controllers
- SIP—to–SIP Supplementary Services for Session Border Controller
- SIP—DNS SRV RFC2782 Compliance
- Mid-call Re-INVITE/UPDATE consumption
- Out–of–dialog SIP OPTIONS Ping
- Cisco Unified Border Element Support for Configuring an Error Response Code upon an Out–of–Dialog OPTIONS Ping Failure
- 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
- Configuring Selective Filtering of Outgoing Provisional Response on the Cisco Unified Border Element
- RFC 4040-Based Clear Channel Codec Negotiation for SIP Calls
- Support for PAID, PPID, Privacy, PCPID, and PAURI Headers on the Cisco Unified Border Element
- 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–to–SIP Cisco Unified Border Element
- SIP Diversion Header Enhancements
- History INFO to Diversion Header
- Hiding the Internal Topology Information Embedded Within the History–info Header at the Cisco UBE
• Call Routing logic on Cisco UBE using the History–info Header

• Reporting End–of–Call Statistics in SIP BYE Message

**SIP Registration and Authentication**

• Configuring SIP Message, Timer, and Response Features —

• SIP—Ability to Send a SIP Registration Message on a Border Element

• SIP Digest Authentication —

• Configurable SIP Parameters via DHCP

• Support for Multiple Registrars on SIP Trunks

**SIP normalization**

• SIP Parameter Modification

• Session Refresh with Reinvites
CHAPTER 2

Reporting End-of-Call Statistics in SIP BYE Message

The Reporting End-of-Call Statistics in Session Initiation Protocol (SIP) BYE Message feature enables you to send call statistics to a remote end when a call terminates. The call statistics are sent as a new header in the BYE message or in the 200 OK message (response to BYE message). The statistics include Real-time Transport Protocol (RTP) packets sent or received, total bytes sent or received, total number of packets that are lost, delay jitter, round-trip delay, and call duration.

This feature enables Cisco Unified Border Element (Cisco UBE) to use the call statistics to update the call data records in Cisco Unified Communications Manager (Cisco UCM) or Cisco Unified Communications Manager Express (Cisco UCME).

The support for Reporting End-of-Call Statistics in SIP BYE Message feature on Cisco Unified Border Element is enabled by the CLI `media bulk-stats` under `voice service voip`.

A new header P-RTP-Stat is added to the BYE and 200 OK messages. The format of P-RTP-Stat is as follows:

P-RTP-Stat: PS=<Packets Sent>, OS=<Octets Sent>, PR=<Packets Recd>, OR=<Octets Recd>, PL=<Packets Lost>, JI=<Jitter>, LA=<Round Trip Delay in ms>, DU=<Call Duration in seconds>

The table below describes the P-RTP-Stat header.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Range of Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>PS</td>
<td>Packets Sent</td>
<td>0 to 4294967295</td>
</tr>
<tr>
<td>OS</td>
<td>Octets Sent</td>
<td>0 to 4294967295</td>
</tr>
<tr>
<td>PR</td>
<td>Packets Received</td>
<td>0 to 4294967295</td>
</tr>
<tr>
<td>OR</td>
<td>Octets Received</td>
<td>0 to 4294967295</td>
</tr>
<tr>
<td>PL</td>
<td>Packets Lost</td>
<td>0 to 4294967295</td>
</tr>
<tr>
<td>JI</td>
<td>Jitter</td>
<td>0 to 4294967295</td>
</tr>
<tr>
<td>LA</td>
<td>Round Trip Delay, in milliseconds (ms)</td>
<td>-2147483648 to +2147483647</td>
</tr>
<tr>
<td>DU</td>
<td>Call Duration, in seconds</td>
<td>0 to 4294967295</td>
</tr>
</tbody>
</table>
Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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

Prerequisites for Reporting End-of-Call Statistics in SIP BYE Message

Cisco Unified Border Element

- Cisco IOS Release 15.1(3)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 3.3S or a later release must be installed and running on your Cisco ASR 1000 Series Router.

Restrictions for Reporting End-of-Call Statistics in SIP BYE Message

- If the media flow-around command is configured, the call statistics are not sent for a 200 OK message.
- If the media flow-around command is configured, the call statistics are passed through the Cisco UBE for a BYE message.
- The values are not validated when the incoming statistics are passed to the endpoints. Hence, in some cases the values may be invalid.
- The value of round-trip delay is valid only if the remote end supports Real-Time Control Protocol (RTCP).
Disabling Reporting End-of-Call Statistics in SIP BYE Message

The Support for Reporting End-of-Call Statistics in SIP BYE Message feature is enabled by default on the Cisco UBE. That is, the P-RTP-Stat header is added to the list of headers that can be processed through the SIP profiles. You must apply SIP profile rules to remove the header from the mandatory header list.

Defining SIP Profile Rules to Remove a Header

Perform this task to define SIP profile rules to remove a header.

SUMMARY STEPS

1. enable
2. configure terminal
3. voice class sip-profiles  tag
4. request  bye sip-header p-rtp-stat remove
5. response  200 sip-header p-rtp-stat remove
6. 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>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td>Example:</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>voice class sip-profiles  tag</td>
</tr>
<tr>
<td>Example:</td>
<td>Configures SIP profiles for a voice class and enters voice class configuration mode.</td>
</tr>
<tr>
<td>Router(config)# voice class sip-profiles 100</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>request  bye sip-header p-rtp-stat remove</td>
</tr>
<tr>
<td>Example:</td>
<td>Removes the P-RTP-Stat SIP header from the BYE message.</td>
</tr>
<tr>
<td>Router(config-class)# request bye sip-header p-rtp-stat remove</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>response  200 sip-header p-rtp-stat remove</td>
</tr>
<tr>
<td>Example:</td>
<td>Removes the P-RTP-Stat SIP header from the 200 OK message.</td>
</tr>
</tbody>
</table>
## Disabling Reporting End-of-Call Statistics in SIP BYE Message at the Global Level

Perform this task to disable the Support for Reporting End-of-Call Statistics in SIP BYE Message feature at the global level.

The Support for Reporting End-of-Call Statistics in SIP BYE Message feature is enabled by default on Cisco UBE. Hence, to disable the feature, you must modify the SIP profiles to remove the P-RTP-Stat SIP header from the request and the response messages and then configure the modified SIP profile on the Cisco UBE.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `voice service voip`
4. `sip`
5. `sip-profiles tag`
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:</td>
<td></td>
</tr>
<tr>
<td><code>Router&gt; enable</code></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><code>Router# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> voice service voip</td>
<td>Specifies VoIP as the voice encapsulation method and enters voice-service configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router(config)# voice service voip</code></td>
<td></td>
</tr>
</tbody>
</table>
Disabling Reporting End-of-Call Statistics in SIP BYE Message at the Dial Peer Level

Perform this task to disable the Support for Reporting End-of-Call Statistics in SIP BYE Message feature at the dial peer level.

The Support for Reporting End-of-Call Statistics in SIP BYE Message feature is enabled by default. Hence, to disable the feature, you must modify the SIP profiles to remove the P-RTP-Stat SIP header from the request and the response messages and then configure the modified SIP profile on the Cisco UBE.

SUMMARY STEPS

1. enable
2. configure terminal
3. dial-peer voice tag voip
4. voice-class sip profiles tag
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.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</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>
</tbody>
</table>
Purpose

Command or Action | Purpose
--- | ---
**Step 3** | Defines a dial peer to specify the method of voice encapsulation and enters dial peer configuration mode.

**dial-peer voice tag voip** Example:

Router(config)# dial-peer voice 100 voip

**Step 4** | Disables the Support for Reporting End-of-Call Statistics in SIP BYE Message feature at the dial peer level.

**voice-class sip profiles tag** Example:

Router(config-dial-peer)# voice-class sip profiles 100

**Step 5** | Exits dial-peer configuration mode.

**exit** Example:

Router(config-dial-peer)# exit

---

**Feature Information for Reporting End-of-Call Statistics in SIP BYE Message**

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Feature History Table entry for the Cisco Unified Border Element.

**Table 2: Feature Information for Reporting End-of-Call Statistics in SIP BYE Message**

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reporting End-of-Call Statistics in SIP BYE Message</td>
<td>15.1(3)T</td>
<td>Allows users to send call statistics to remote ends when a call terminates. These statistics are sent as a new header in a BYE message or in the 200 OK message. The following commands were introduced or modified: request, response.</td>
</tr>
</tbody>
</table>

Feature History Table entry for the Cisco Unified Border Element (Enterprise).
Table 3: Feature Information for Reporting End-of-Call Statistics in SIP BYE Message

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reporting End-of-Call Statistics in SIP BYE Message</td>
<td>Cisco IOS XE Release 3.3S</td>
<td>Allows users to send call statistics to remote ends when a call terminates. These statistics are sent as a new header in a BYE message or in the 200 OK message. The following commands were introduced or modified: request, response.</td>
</tr>
</tbody>
</table>
CHAPTER 3

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.

- Finding Feature Information, on page 13
- Prerequisites for Configurable Hostname in Locally Generated SIP Headers, on page 13
- Restrictions for Configurable Hostname in Locally Generated SIP Headers, on page 14
- How to Configure the Hostname in Locally Generated SIP Headers, on page 14
- Feature Information for Configurable Hostname in Locally Generated SIP Headers, on page 22

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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

Prerequisites for Configurable Hostname in Locally Generated SIP Headers

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 for Configurable Hostname in Locally Generated SIP Headers

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

How to Configure the Hostname in Locally Generated SIP Headers

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>
<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> voice service voip</td>
<td>(Required) Enters the voice-service VoIP configuration mode</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Router(config)# voice service voip</td>
<td>(Required) Enters the SIP configuration mode.</td>
</tr>
</tbody>
</table>

**Step 4**  
**sip**  
**Example:**  
Router(config-voi-serv)# sip  
(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:**  
  - *hostname.domain* (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 cases, the *dns:* delimiter must be included as the first four characters.  

| Step 5 | localhost dns:  
local-host-name-string  
**Example:**  
Router(conf-serv-sip)# localhost dns:host_one |  
(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:**  
  - *hostname.domain* (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 cases, the *dns:* delimiter must be included as the first four characters. |

| Step 6 | exit  
**Example:**  
Router(conf-serv-sip)# exit | Exits the current configuration mode. |

---

**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>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 1    | enable            | Enables privileged EXEC mode.  
  Example:  
  Router> enable  
  - Enter your password if prompted. |
| 2    | configure terminal| Enters global configuration mode.  
  Example:  
  Router# configure terminal |
| 3    | dial-peer voice   | (Required) Enters dial-peer configuration mode for the specified dial peer.  
  Example:  
  Router# dial-peer voice 100 voip |
| 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 |
| 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`
SUMMARY STEPS

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

2. Use the `show call history voice` to display output when the local hostname is enabled:

DETAILED STEPS

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

Example:

```
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
 ACMLevel=3
 OutSignalLevel=35
 InSignalLevel=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
RemoteSignallingIPAddress=172.18.193.87
RemoteSignallingPort=5060
RemoteMediaIPAddress=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=A240B4DC-115511D9-8005EC82-AB4FD5BE@pip.example.com
SessionTarget=172.18.193.87
OnTimeRvPlayout=48620
GapFillWith Silence=0 ms
GapFillWithPrediction=0 ms
GapFillWithInterpolation=0 ms
GapFillWithRedundancy=0 ms
HiWaterPlayoutDelay=70 ms
LoWaterPlayoutDelay=69 ms
TxPakNumber=2434
TxSignalPak=0
TxVoiceNoisePak=0
TxDuration=48680
TxVoiceDuration=48680
RxPakNumber=2434
RxSignalPak=0
RxDuration=0
TxVoiceDuration=48670
VoiceRxDuration=48620
RxOutOfRange=0
RxLatePak=0
RxEarlyPak=0
PlayDelayCurrent=69
PlayDelayMin=69
PlayDelayMax=70
PlayDelayClockOffset=43547
PlayDelayJitter=0
PlayErrPredictive=0
PlayErrInterpolative=0
PlayErrSilence=0
PlayErrBufferOverFlow=0
PlayErrRetroactive=0
PlayErrTalkspurt=0
OutSignalLevel=-35
InSignalLevel=-30
LevelTxPowerMean=0
LevelRxPowerMean=-302
LevelBgNoise=0
ERLLevel=3
ACOMLevel=3
ErrRxDrop=0
ErrTxDrop=0
ErrTxControl=0
ErrRxControl=0
ReceiveDelay=69 ms
LostPackets=0
EarlyPackets=0
LatePackets=0
SRTP = off
VAD = enabled
CoderTypeRate=g729r8
CodecBytes=20
Media Setting=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
GwOutpulsedCalledOctet=3-0x80
GwOutpulsedCallingNumber=9001
GwOutpulsedCallingOctet3=0x0
MediaInactiveDetected=no
MediaInactiveTimestamp=
Username=
LocalHostname=pip.example.com ! LocalHostname field
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

Step 2 Use the show call history voice to display output when the local hostname is enabled:
Example:

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
ProtocolCallId=A240B4DC-115511D9-8005EC82-AB4FD5BE@pip.example.com
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
TELE:
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
Feature Information for Configurable Hostname in Locally Generated SIP Headers

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

ISR Feature History Information.

Table 4: Feature Information for Configurable Hostname in Locally Generated SIP Headers

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configurable Hostname in Locally Generated SIP Header</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>
</tbody>
</table>

ASR Feature History Information.

Table 5: Feature Information for Configurable Hostname in Locally Generated SIP Headers

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configurable Hostname in Locally Generated SIP Header</td>
<td>Cisco IOS XE</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></td>
<td>Release 2.5</td>
<td></td>
</tr>
</tbody>
</table>
CHAPTER 4

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.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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

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**

- **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:

```plaintext
Session-Expires = ("Session-Expires" | "x") ":" delta-seconds
```

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:

```plaintext
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**

**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. `min-se exit`
7. `min-se show sip-ua min-se`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
  - `enable`
  - **Example:**
    - `Router> enable`
| Enables privileged EXEC mode.
  - Enter your password if prompted. |
| **Step 2**
  - `configure terminal`
  - **Example:**
    - `Router# configure terminal`
| Enters global configuration mode. |
### Command or Action

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td><code>voice service voip</code></td>
<td>Enters voice service VoIP configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config)# voice service voip</code></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td><code>sip</code></td>
<td>Enters SIP configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(conf-voi-serv)# sip</code></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td><code>min-se seconds</code></td>
<td>Sets the minimum session expires header value, in seconds, for all calls.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(conf-serv-sip)# min-se 600</code></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td><code>min-se exit</code></td>
<td>Exits the current configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(conf-serv-sip)# exit</code></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td><code>min-se show sip-ua min-se</code></td>
<td>Verifies the value of the Min-SE header.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config)# show sip-ua min-se</code></td>
<td></td>
</tr>
</tbody>
</table>

### Example

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.

```
! 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:
3. `debug ccsip calls`
4. debug ccsip error
5. debug ccsip events
6. debug ccsip messages
7. debug ccsip states

# Feature Information for SIP Session Timer Support

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

**Table 6: Feature Information for SIP—Session Timer Support**

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<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. In Cisco IOS Release 12.2(8)YN 12.2(15)T 12.2(11)YV 12.2(11)T 12.3(2)T, this feature was implemented on the Cisco Unified Border Element. The following commands were introduced or modified: <strong>min-se (SIP)</strong> and <strong>show sip-ua min-se</strong>.</td>
</tr>
</tbody>
</table>

---

Feature Information for SIP Session Timer Support

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

**Table 6: Feature Information for SIP—Session Timer Support**

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<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. In Cisco IOS Release 12.2(8)YN 12.2(15)T 12.2(11)YV 12.2(11)T 12.3(2)T, this feature was implemented on the Cisco Unified Border Element. The following commands were introduced or modified: <strong>min-se (SIP)</strong> and <strong>show sip-ua min-se</strong>.</td>
</tr>
<tr>
<td>Feature Name</td>
<td>Releases</td>
<td>Feature Information</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SIP - Session Timer Support</td>
<td>Cisco XE Release 2.5</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. In Cisco IOS XE Release 2.5, this feature was implemented on the Cisco Unified Border Element (Enterprise). The following commands were introduced or modified: <code>min-se (SIP)</code> and <code>show sip-ua min-se</code>.</td>
</tr>
</tbody>
</table>
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

- Finding Feature Information, on page 32
- Prerequisites for SIP-to-SIP Basic Functionality for Session Border Controller, on page 32
- Feature Information for SIP-to-SIP Basic Functionality for Session Border Controller, on page 32
Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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

Prerequisites for SIP-to-SIP Basic Functionality for Session Border Controller

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.

Feature Information for SIP-to-SIP Basic Functionality for Session Border Controller

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

ISR Feature History Information

Table 7: Feature Information for Configuring SIP-to-SIP Supplementary Features

<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-origination 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>
</tbody>
</table>
ASR Feature History Information

Table 8: Feature Information for Configuring SIP-to-SIP Supplementary Features

<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>Cisco IOS XE Release 3.1S, Cisco IOS XE Release 3.3S</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-origination 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>
</tbody>
</table>
CHAPTER 6

SIP-to-SIP Supplementary Services for Session Border Controller

The SIP-to-SIP Supplementary Services for Session Border Controller (SBC) feature enhances the terminating and reoriginating of signaling and media between VoIP and video networks.

• Finding Feature Information, on page 35
• Prerequisites for SIP-to-SIP Supplementary Services for Session Border Controller, on page 35
• Information About SIP-to-SIP Supplementary Services for Session Border Controller, on page 36
• How to Configure SIP-to-SIP Supplementary Services for Session Border Controller, on page 36
• Feature Information for SIP-to-SIP Supplementary Services for Session Border Controller, on page 37

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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

Prerequisites for SIP-to-SIP Supplementary Services for Session Border Controller

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.
Information About SIP-to-SIP Supplementary Services for Session Border Controller

SIP-to-SIP Supplementary Services for Session Border Controller

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

- IP Address-Hiding in all Session Initiation Protocol (SIP) messages including supplementary services
- Media Flow Around
- Hosted Network Address Translation (NAT) Traversal for SIP
- Support on Cisco AS5350XM and Cisco AS5400XM platforms
- SIP-to-SIP Supplementary services using REFER/3xx method.

Note: The following features of SIP-to-SIP Supplementary services using REFER/3xx method 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

Digital Signal Processors (DSPs) and SIP Call Hold/Resume

Digital Signal Processors (DSPs) generate and transmit Real-time Transport Protocol (RTP) media packets from a source to a destination address during a SIP call session. However, when a SIP call is put on hold, DSPs stop generating the RTP media packets and resumes generating and transmitting the RTP media packets after the SIP call is resumed. This ensures that the RTP sequence number is continuous from the time of origin until the end of the SIP call.

How to Configure SIP-to-SIP Supplementary Services for Session Border Controller

To configure the SIP-to-SIP Supplementary Services for Session Border Controller feature, see the Supplementary Services Features for FXS Ports on Cisco IOS Voice Gateways Configuration Guide at the
Feature Information for SIP-to-SIP Supplementary Services for Session Border Controller

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 9: Feature Information for Configuring SIP-SIP Supplementary Features

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<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 reoriginating of signaling and media between VoIP and video networks. No new commands were added or modified.</td>
</tr>
<tr>
<td></td>
<td>15.1(1)T5</td>
<td></td>
</tr>
<tr>
<td>SIP-to-SIP Supplementary Services for Session Border Controller</td>
<td>Cisco IOS XE</td>
<td>The SIP-to-SIP Supplementary Services for Session Border Controller feature enhances terminating and reoriginating of signaling and media between VoIP and video networks. No new commands were added or modified.</td>
</tr>
<tr>
<td></td>
<td>Release 3.1S</td>
<td></td>
</tr>
</tbody>
</table>
Mid-call Signaling Consumption

The Cisco Unified Border Element BE Mid-call Signaling support aims to reduce the interoperability issues that arise due to consuming mid-call RE-INVITES/UPDATES.

Mid-call Re-INVITEs/UPDATEs can be consumed in the following ways:

- Mid-call Signaling Passthrough - Media Change
- Mid-call Signaling Block
- Mid-call Signaling Codec Preservation

**Note**

This feature should be used as a last resort only when there is no other option in CUBE. This is because configuring this feature can break video-related features. For Delay-offer Re-INVITE, the configured codec will be passed as an offer in 200 message to change the codec, the transcoder is added in the answer.

**Feature Information for Mid-call Signaling**

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to [www.cisco.com/go/cfn](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.
Table 10: Feature Information for Mid-call Signaling

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mid-call Re-INVITE Consumption</td>
<td>Cisco IOS 15.2(1)T</td>
<td>The Mid-call Re-INVITE consumption feature consumes mid-call Re-INVITEs from CUBE and helps to avoid interoperability issues because of these re-invites. The following commands were introduced or modified: midcall-signaling.</td>
</tr>
<tr>
<td>Mid-call Codec Preservation</td>
<td>Cisco IOS 15.3(2)T</td>
<td>The Mid-call Codec Preservation feature helps to disable codec negotiation in the middle of a call and preserves the codec negotiated before the call. The following commands were introduced or modified: midcall-signaling, preserve-codec, voice-class sip midcall-signaling preserve-codec.</td>
</tr>
<tr>
<td>Mid-call Re-INVITE Consumption Enhancements</td>
<td>Cisco IOS 15.5(3)M</td>
<td>Mid-call signaling Re-INVITE consumption is enhanced to support: Re-INVITE based call transfer, Call transfer with REFER Consume, Normalization of call hold in a call set-up.</td>
</tr>
</tbody>
</table>

**Prerequisites**

- Enable CUBE application on a device
- Cisco IOS Release 15.2(1)T or later, or Cisco IOS-XE Release 15.2(2)S or later must be installed.
- supplementary-service media-renegotiate must be configured in global voice service voip mode.
Mid-call Signaling Passthrough - Media Change

Passthrough media change method optimizes or consumes mid-call, media-related signaling within the call. Mid-call signaling changes will be passed through only when bidirectional media like T.38 or video is added. The command `midcall-signaling passthru media-change` needs to be configured to enable passthrough media change.

Restrictions for Mid-Call Signaling Passthrough - Media Change

- SIP-H.323 calls are not supported.
- TDM Gateways are not supported.
- Session Description Protocol (SDP) -passthrough is not supported.
- When codec T is configured, the offer from CUBE has only audio codecs, and so the video codecs are not consumed.
- Re-invites are not consumed if media flow-around is configured.
- Re-invites are not consumed if media anti-tromboning is configured.
- De-escalation re-invites are consumed. So, one call leg might be de-escalated to audio only while the other call leg continues to support audio and video.
- Re-invites with media direction changes are consumed.
- Video transcoding is not supported.
- Multicast Music On Hold (MMOH) is not supported.
- When the `midcall-signaling passthru media-change` command is configured and high-density transcoder is enabled, there might be some impact on Digital Signal Processing (DSP) resources as the transcoder might be used for all the calls.
- Session timer is handled leg by leg whenever this feature is configured and it includes session timer negotiation for initial INVITE/200 OK transaction as well.
- More than two m-lines in the SDP is not supported.
- Alternative Network Address Types (ANAT) is not supported.
- Video calls and Application streams are not supported when mid-call signaling block is configured.
- In the SRTP-RTP scenario, re-invites are not consumed.

Behavior of Mid-call Re-INVITE Consumption

- If mid-call signaling block is enabled on either of call-legs, video parameters and application streams are not negotiated, and are rejected in the answer.
- When flow around and offer-all is configured, CUBE performs codec renegotiation even if mid-call signaling block is configured globally.
• The following behavior is for refer consume scenario:
  • REFER consume is supported for blind, alert and consult call transfers.
  • Existing codecs or DTMF is used for local bridging of new call legs. No Re-INVITE or UPDATE is sent for media re-negotiation after REFER.
  • Call gets dropped when DSP is required but not available.
  • A call can be escalated to video only if transference and transfer-to dial-peers do not have mid-call signaling block configured.
  • Video calls are de-escalated if mid-call signaling block configuration on transfer-to dial-peer.
  • For Re-INVITE based call-transfer involving Cisco Unified Communications Manager, all Re-INVITE are locally answered and transcoder is invoked if negotiated codecs are different than the codecs before call-transfer.

• The following behavior is for INVITE with REPLACES Header consume scenario:
  • CUBE consumes INVITE with REPLACES Header only when the handle-replaces CLI is configured (under sip-ua or voice-class tenant). In this case, CUBE consumes the INVITE and handles it locally. It triggers an outbound INVITE without replaces header and call gets connected with agent.
  • If the handle-replaces CLI is enabled, the 'transfer-to' party must have the same codec that is used for the original call setup. If there is a different codec offer, CUBE rejects the INVITE with 488 error.
  • If the handle-replaces CLI is not configured, CUBE does not consume the INVITE with REPLACES Header and the outgoing INVITE holds same replace header which CUBE is received.
  • INVITE with REPLACES Header consumption does not support the following configurations:
    • Delayed Offer INVITE
    • Codec, DTMF attribute changes, and RSVP
    • Mid-call Signaling block
    • IPv6

• The following table provides the details of the behavior when the initial call is establish without 'sendrecv' parameter, that means, the initial call is established with 'sendonly', 'recvonly' or 'inactive'.

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>If an Offer is received with 'sendonly' and mid-call block is configured on any or both call legs</td>
<td>Offer is sent with 'sendrecv'.</td>
</tr>
<tr>
<td>If an Answer is received with 'sendonly' and the peer leg supports mid-call signaling</td>
<td>Answer is sent with 'sendonly'. Resume transaction is end-to-end.</td>
</tr>
<tr>
<td>If an Answer is received with 'sendonly' and the peer leg does not supports mid-call signaling</td>
<td>Answer is sent with 'sendrecv'. Resume transaction is consumed.</td>
</tr>
</tbody>
</table>
### Configuring Passthrough of Mid-call Signalling

Perform this task to configure passthrough of mid-call signaling (as Re-invites) only when bidirectional media is added.

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Configure passthrough of mid-call signaling changes only when bidirectional media is added.
   - In Global VoIP SIP configuration mode
     - `midcall-signaling passthru media-change`
   - In dial-peer configuration mode
     - `voice-class sip mid-call signaling passthru media-change`
4. **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>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>enable</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>configure terminal</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Re-Invites are passed through only when bidirectional media is added.</td>
</tr>
<tr>
<td>Configure passthrough of mid-call signaling changes only when bidirectional media is added.</td>
<td></td>
</tr>
<tr>
<td>- In Global VoIP SIP configuration mode</td>
<td></td>
</tr>
<tr>
<td><code>midcall-signaling passthru media-change</code></td>
<td></td>
</tr>
</tbody>
</table>
### Example Configuring Passthrough SIP Messages at Dial Peer Level

The following example shows how to passthrough SIP messages at the dial peer level:

```plaintext
dial-peer voice 600 voip
  destination-pattern 2222222222
  session protocol sipv2
  session target ipv4:9.45.38.39:9001
  voice-class sip mid-call signaling passthru media-change
  incoming called-number 1111111111
  voice-class codec 2 offer-all

dial-peer voice 400 voip
  destination-pattern 1111111111
  session protocol sipv2
  session target ipv4:9.45.38.39:9000
  incoming called-number 2222222222
  voice-class codec 1 offer-all
```

### Example Configuring Passthrough SIP Messages at the Global Level

The following example shows how to passthrough SIP messages at the global level:

```plaintext
Device(config)# voice service voip
Device(conf-voi-serv)# no ip address trusted authenticate
Device(conf-voi-serv)# allow-connections sip to sip
Device(conf-voi-serv)# sip
Device(conf-serv-sip)# midcall-signaling passthru media-change
```

### Mid-call Signaling Block

The Block method blocks all mid-call media-related signaling to the specific SIP trunk. The command `midcall-signaling block` needs to be configured to enable this behavior. Video escalation and T.38 call flow...
are rejected when the midcall-signaling block command is configured. This command should be configured only when basic call is the focus and mid-call can be consumed.

**Restrictions for Mid-Call Signaling Block**

- SIP-H.323 calls are not supported.
- TDM Gateways are not supported.
- Session Description Protocol (SDP) -passthrough is not supported
- Video calls and Application streams are not supported.
- When media flow-around is configured, Mid-call INVITE is rejected with 488 error message.
- Re-invites are not consumed if media anti-tromboning is configured.
- Multicast Music On Hold (MMOH) is not supported.
- When the midcall-signaling passthru media-change command is configured and high-density transcoder is enabled, there might be some impact on Digital Signal Processing (DSP) resources as the transcoder might be used for all the calls.
- Session timer is handled leg by leg whenever this feature is configured.
- More than two m-lines in the SDP is not supported.
- Alternative Network Address Types (ANAT) is not supported.
- When mid-call signaling block is configured, you can either configure REFER consume or enable TCL script. Mid-call signaling block is not supported if both REFER consume and TCL script are enabled. We also recommend not to configure supplementary-service media-renegotiate command.
- In the SRTP-RTP scenario, re-invites are not consumed.

**Blocking Mid-Call Signaling**

Perform this task to block mid-call signaling:

**SUMMARY STEPS**

1. enable
2. configure terminal
3. Configure blocking of mid-call signaling changes:
   - In Global VoIP SIP configuration mode
     
     midcall-signaling block
   - In dial-peer configuration mode
     
     voice-class sip mid-call signaling block
4. 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>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong> Device&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>

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

| **Step 3** | Mid-call signaling is always blocked. |
| Configure blocking of mid-call signaling changes: | |
| • In Global VoIP SIP configuration mode | |
| midcall-signaling block | |
| • In dial-peer configuration mode | |
| voice-class sip mid-call signaling block | |
| **Example:** | |
| In Global VoIP SIP configuration mode: | |
| Device(config)# voice service voip | |
| Device(conf-voi-serv)# sip | |
| Device(conf-serv-sip)# midcall-signaling block | |
| **Example:** | |
| In Dial-peer configuration mode: | |
| Device(config)# dial-peer voice 2 voip | |
| Device(config-dial-peer)# voice-class sip mid-call signaling block | |

| **Step 4** | Exits to privileged EXEC mode. |
| end | |
Example: Blocking SIP Messages at the Global Level

The following example shows how to block SIP messages at the global Level

Device(config)#voice service voip
Device(config-voi-serv)#no ip address trusted authenticate
Device(config-voi-serv)#allow-connections sip to sip
Device(config-voi-serv)#sip
Device(config-serv-sip)#midcall-signaling block

Mid Call Codec Preservation

Mid call codec preservation defines whether a codec can be negotiated after a call has been initiated. You can enable or disable codec negotiation in the middle of a call.

Note

In the SRTP-RTP scenario, re-invites are not consumed.

Configuring Mid Call Codec Preservation

This task disables codec negotiation in the middle of a call and preserves the codec negotiated before the call.

SUMMARY STEPS

1. enable
2. configure terminal
3. Enter one of the following to disable midcall codec renegotiation:
   • In Global VoIP SIP configuration mode
     midcall-signaling preserve-codec
   • In dial-peer configuration mode
     voice-class sip midcall-signaling preserve-codec
4. 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>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device&gt; enable</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Enter one of the following to disable midcall codec renegotiation:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• In Global VoIP SIP configuration mode</td>
</tr>
<tr>
<td></td>
<td>midcall-signaling preserve-codec</td>
</tr>
<tr>
<td></td>
<td>• In dial-peer configuration mode</td>
</tr>
<tr>
<td></td>
<td>voice-class sip midcall-signaling preserve-codec</td>
</tr>
</tbody>
</table>

**Example:**

```
Device(config)# voice service voip
Device(conf-voi-serv)# sip
Device(conf-serv-sip)# midcall-signaling preserve-codec
```

**Example:**

```
Device(config)# dial-peer voice 10 voip
Device(conf-dial-peer)# voice-class sip midcall-signaling preserve-codec
```

<table>
<thead>
<tr>
<th>Step 4</th>
<th>end</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>Device(conf-serv-sip)# end</td>
</tr>
</tbody>
</table>

### Purpose

Disables codec negotiation in the middle of a call and preserves the codec negotiated before the call.

### Exit to privileged EXEC mode.

### Example: Configuring Mid Call Codec Preservation at the Dial Peer Level

```
dial-peer voice 107 voip
  destination-pattern 74000
  session protocol sipv2
  session target ipv4:9.45.36.9
  incoming called-number 84000
  voice-class codec 1 offer-all
!
dial-peer voice 110 voip
  destination-pattern 84000
  session protocol sipv2
  session target ipv4:9.45.35.2
  incoming called-number 74000
  voice-class codec 1 offer-all
  voice-class sip midcall-signaling preserve-codec
```

### Example: Configuring Mid Call Codec Preservation at the Global Level

```
Device(config)# voice service voip
Device(conf-voi-serv)# no ip address trusted authenticate
Device(conf-voi-serv)# allow-connections sip to sip
```
Device(conf-voi-serv)# sip
Device(conf-serv-sip)# midcall-signaling preserve-codec
Example: Configuring Mid Call Codec Preservation at the Global Level
CHAPTER 8

Cisco UBE Out-of-dialog OPTIONS Ping

The Cisco Unified Border Element Out-of-dialog (OOD) Options Ping feature provides a keepalive mechanism at the SIP level between any number of destinations.

- Finding Feature Information, on page 51
- Prerequisites for Out-of-dialog SIP OPTIONS Ping, on page 51
- Restrictions for Cisco Out-of-dialog SIP OPTIONS Ping for Specified SIP Servers or Endpoints, on page 52
- Information about Cisco UBE Out-of-dialog OPTIONS Ping, on page 52
- Configuring Cisco UBE Out-of-dialog OPTIONS Ping for Specified SIP Servers or Endpoints, on page 53
- Troubleshooting Tips, on page 54
- Feature Information for Cisco UBE Out-of-dialog OPTIONS Ping for Specified SIP Servers or Endpoints, on page 54

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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

Prerequisites for Out-of-dialog SIP OPTIONS Ping

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 for Cisco Out-of-dialog SIP OPTIONS Ping for Specified SIP Servers or Endpoints

- 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.

Information about Cisco UBE Out-of-dialog OPTIONS Ping

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.

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

Table 11: Error Codes that busyout the endpoint

<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>
</tbody>
</table>
### Configuring Cisco UBE Out-of-dialog OPTIONS Ping for Specified SIP Servers or Endpoints

#### SUMMARY STEPS

1. enable
2. configure terminal
3. dial-peer voice tag voip
4. voice-class sip options-keepalive \{up-interval seconds | down-interval seconds | retry retries\}
5. exit

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>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>Device(config)# dial-peer voice 200 voip</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>voice-class sip options-keepalive {up-interval seconds</td>
<td>down-interval seconds</td>
</tr>
</tbody>
</table>
### Command or Action

**Example:**

Device(config-dial-peer)# voice-class sip options-keepalive up-interval 12 down-interval 65 retry 3

**Purpose**

- **up-interval seconds** -- Number of up-interval seconds allowed to pass before marking the UA as unavailable. The range is 5-1200. The default is 60.
- **down-interval seconds** -- Number of down-interval seconds allowed to pass before marking the UA as unavailable. The range is 5-1200. The default is 30.
- **retry retries** -- Number of retry attempts before marking the UA as unavailable. The range is 1 to 10. The default is 5 attempts.

---

**Step 5**  
**exit**

**Example:**

Device(config-dial-peer)# exit

Exits the current mode.

---

### Troubleshooting Tips

The following commands can help troubleshoot the OOD Options Ping feature:

- **debug ccsip all** -- shows all Session Initiation Protocol (SIP)-related debugging.
- **show dial-peer voice x** -- shows configuration of keepalive information.

**Device**

```
Device# 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.

**Device**

```
Device# show dial-peer voice summary
AD  PRE PASS
TAG TYPE MIN  OPER PREFIX DEST-PATTERN KEEPALIVE
111 voip up  up     0 syst  active
  9 voip up  up     0 syst  busy-out
```

### Feature Information for Cisco UBE Out-of-dialog OPTIONS Ping for Specified SIP Servers or Endpoints

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to [www.cisco.com/go/cfn](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.
Table 12: Feature Information for Cisco UBE Out-of-dialog OPTIONS Ping for Specified SIP Servers or Endpoints

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
</table>
| Out-of-dialog OPTIONS Ping to Monitor Dial-peers to Specified SIP Servers and Endpoints | 15.0(1)M 12.4(22)YB | This feature provides a keepalive mechanism at the SIP level between any number of destinations. The generic heartbeat mechanism allows Cisco UBE to monitor the status of SIP servers or endpoints and provide the option of busying-out associated dial-peer upon total heartbeat failure.

In Cisco IOS Release 15.0(1)M, this feature was implemented on the Cisco Unified Border Element.

The following command was introduced: `voice-class sip options-keepalive` |
| Out-of-dialog OPTIONS Ping to Monitor Dial-peers to Specified SIP Servers and Endpoints | Cisco IOS XE Release 3.1S | 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.

In Cisco IOS XE Release 3.1S, this feature was implemented on the Cisco Unified Border Element (Enterprise).

The following command was introduced: `voice-class sip options-keepalive` |
Feature Information for Cisco UBE Out-of-dialog OPTIONS Ping for Specified SIP Servers or Endpoints
Configuring an Error Response Code upon an Out-of-Dial Options Ping Failure

Cisco Unified Border Element (Cisco UBE) provides an option to configure the error response code when a dial peer is busied out because of an Out-of-Dial OPTIONS ping failure.

The OPTIONS ping mechanism monitors the status of a remote Session Initiation Protocol (SIP) server, proxy or endpoints. Cisco UBE monitors these endpoints periodically. When there is no response from these monitored endpoints, the configured dial peer is busied out. If the dial-peer endpoint is busied out due to an OPTIONS ping failure, the call is passed on to the next dial-peer endpoint if an alternate dial peer is configured for the same destination. Otherwise the error response 404 is sent. This feature provides the option of configuring the error response code to reroute the call. Therefore when a dial peer is busied out due to the OPTIONS ping failure, the SIP error code configured in the inbound dial-peer is sent as a response.

To configure the SIP error code response, perform the following tasks:

- Finding Feature Information, on page 57
- Prerequisites for Configuring an Error Response Code upon an Out-of-Dial OPTIONS Ping Failure, on page 58
- Restrictions for Configuring an Error Response Code upon an Out-of-Dial OPTIONS Ping Failure, on page 58
- Configuring an Error Response Code upon an Out-of-Dial OPTIONS Ping Failure at the Global Level, on page 58
- Configuring an Error Response Code upon an Out-of-Dial OPTIONS Ping Failure at the Dial Peer Level, on page 60
- Troubleshooting Tips, on page 61
- Feature Information for Configuring an Error Response Code upon an Out-of-Dial OPTIONS Ping Failure, on page 62

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to https://cfnng.cisco.com/. An account on Cisco.com is not required.
Prerequisites for Configuring an Error Response Code upon an Out-of-Dialog OPTIONS Ping Failure

- The Cisco UBE Out-of-Dialog (OOD) OPTIONS Ping for Specified SIP Servers or Endpoints feature should be configured before configuring this error response code for a ping OPTIONS failure.

Cisco Unified Border Element

- Cisco IOS Release 15.1(1)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 for Configuring an Error Response Code upon an Out-of-Dialog OPTIONS Ping Failure

The error code configuration will not have any effect if it is configured on the outbound dial peer.

Configuring an Error Response Code upon an Out-of-Dialog OPTIONS Ping Failure at the Global Level

The table below describes the SIP error codes.

<table>
<thead>
<tr>
<th>Error Code Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>400</td>
<td>Bad Request</td>
</tr>
<tr>
<td>401</td>
<td>Unauthorized</td>
</tr>
<tr>
<td>402</td>
<td>Payment Required</td>
</tr>
<tr>
<td>403</td>
<td>Forbidden</td>
</tr>
<tr>
<td>404</td>
<td>Not Found</td>
</tr>
<tr>
<td>408</td>
<td>Request Timed Out</td>
</tr>
<tr>
<td>416</td>
<td>Unsupported URI</td>
</tr>
<tr>
<td>Error Code Number</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>480</td>
<td>Temporarily Unavailable</td>
</tr>
<tr>
<td>482</td>
<td>Loop Detected</td>
</tr>
<tr>
<td>484</td>
<td>Address Incomplete</td>
</tr>
<tr>
<td>486</td>
<td>Busy Here</td>
</tr>
<tr>
<td>487</td>
<td>Request Terminated</td>
</tr>
<tr>
<td>488</td>
<td>Not Acceptable Here</td>
</tr>
<tr>
<td>500-599</td>
<td>SIP 5xx--Server/Service Failure</td>
</tr>
<tr>
<td>500</td>
<td>Internal Server Error</td>
</tr>
<tr>
<td>502</td>
<td>Bad Gateway</td>
</tr>
<tr>
<td>503</td>
<td>Service Unavailable</td>
</tr>
<tr>
<td>600-699</td>
<td>SIP 6xx--Global Failure</td>
</tr>
</tbody>
</table>

To configure the error response code for the OPTIONS ping failure to support the Cisco Unified Border Element at the global level, perform the steps in this section.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. voice service voip
4. sip
5. error-code-override options-keepalive failure sip-status-code-number
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:</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>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 voice service configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>
Configuring an Error Response Code upon an Out-of-Dialog OPTIONS Ping Failure at the Dial Peer Level

To configure the error response code for the OPTIONS ping failure to support the Cisco Unified Border Element at the dial-peer level, perform the steps in this section.

SUMMARY STEPS

1. enable
2. configure terminal
3. dial-peer voice voice-dial-peer-tag voip
4. voice-class sip error-code-error-override options-keepalive failure {sip-status-code-number | system}
5. end

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>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 4 sip</td>
<td>Enters voice service SIP configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(conf-voi-serv)# sip</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 5 error-code-override options-keepalive failure sip-status-code-number</td>
<td>Configures the specified SIP error code number.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(conf-serv-sip)# error-code-override options-keepalive failure 402</td>
<td>• sip-status-code-number --SIP status code to be sent for an options keepalive failure. Range: 400 to 699. Default: 503.</td>
</tr>
<tr>
<td></td>
<td>• The table above provides more details about these error codes.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 6 end</td>
<td>Exits voice service SIP configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(conf-serv-sip)# end</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>Router# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><code>dial-peer voice voice-dial-peer-tag voip</code></td>
<td>Enters dial peer voice configuration mode.</td>
</tr>
<tr>
<td><code>Router(config)# dial-peer voice 234 voip</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>`voice-class sip error-code-error-override options-keepalive failure {sip-status-code-number</td>
<td>system}`</td>
</tr>
<tr>
<td><code>Router(config-dial-peer)# voice-class sip error-code-override options-keepalive failure 500</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><code>end</code></td>
<td>Exits dial peer voice configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><code>Router(config-dial-peer)# end</code></td>
<td></td>
</tr>
</tbody>
</table>

**Troubleshooting Tips**

The following debug commands display any error that occurs with the error code response:

- `debug ccsip messages`-- shows SIP messages.

```
Router# debug ccsip messages
SIP Call messages tracing is enabled
```

- `debug ccsip all` -- shows all SIP-related debugging.

```
Router# debug ccsip all
This may severely impact system performance. Continue? [confirm]
All SIP Call tracing is enabled
```
Feature Information for Configuring an Error Response Code upon an Out-of-Dialog OPTIONS Ping Failure

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Feature History Table entry for the Cisco Unified Border Element.

Table 14: Feature Information for Configuring an Error Response Code upon an Out-of-Dialog OPTIONS Ping Failure

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Error Response Code upon an Out-of-Dialog OPTIONS Ping Failure</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-Dialog OPTIONS ping failure. The following commands were introduced or modified in this release: <code>error-code-override options-keepalive failure</code>, <code>voice-class sip error-code-override options-keepalive failure</code>.</td>
</tr>
</tbody>
</table>

Feature History Table entry for the Cisco Unified Border Element (Enterprise)

Table 15: Feature Information for Configuring an Error Response Code upon an Out-of-Dialog OPTIONS Ping Failure

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Error Response Code upon an Out-of-Dialog OPTIONS Ping Failure</td>
<td>Cisco IOS XE Release 3.1S</td>
<td>This feature provides option to configure the error response code when a dial peer is busied out because of an Out-of-Dialog OPTIONS ping failure. The following commands were introduced or modified in this release: <code>error-code-override options-keepalive failure</code>, <code>voice-class sip error-code-override options-keepalive failure</code>.</td>
</tr>
</tbody>
</table>
CHAPTER 10

Configurable SIP Error Codes

The Configurable SIP Error Codes feature describes how Cisco Unified Border Element provides support for configurable SIP Error codes to override or modify Session Initiation Protocol (SIP) error response codes. The different methods to modify SIP error codes are listed below:

- Configure user-defined error codes to override SIP Call Admission Control (CAC) response codes for specific failure types.
- Copy SIP status line from an incoming SIP response to an outgoing SIP response.
- Modify the status line for an outgoing SIP response with user defined-values.

Finding Feature Information, on page 63
Information About Configurable SIP Error Codes, on page 63
How to Configure SIP Error Codes, on page 65
Configuration Examples for Configurable SIP Error Codes, on page 67
Additional References for Configurable SIP Error Codes, on page 67
Feature Information for Configurable SIP Error Codes, on page 68

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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

Information About Configurable SIP Error Codes

Prior to the Configurable SIP Error Codes feature, the Cisco Unified Border Element (Cisco UBE) or Session Initiation Protocol (SIP) gateway sent a fixed error response code (503) when an INVITE was rejected due to any of the following Call Admission Control (CAC) thresholds:

- Maximum connections
- Maximum total calls
- CPU
• Memory Used

With the Configurable SIP Error Codes feature, you can configure SIP error codes. This helps the network administrators easily identify the cause of error and troubleshoot the issues. It also helps configure specific alternate routing policies on the calling device based on the error codes that are received. This feature allows:
  • Configuring of error codes for CAC failures
  • Modifying SIP Response Status Line with Conditional SIP Profiles

**Error Codes for CAC Failures**

You can now configure user-defined response codes that can override Session Initiation Protocol (SIP) Call Admission Control (CAC) response codes for the following failure types:
  • Cisco Unified Border Element (Cisco UBE) shutdown—Error generated when the Cisco UBE enters shutdown mode.
  • Total calls exceeded—Error generated when the total system-wide calls exceed their maximum allowed number.
  • Maximum connections exceeded—Error generated when maximum dial peer based connections exceed their maximum allowed number.
  • CPU Failure—Error generated when the CPU processing time exceeds 5 seconds.
  • Memory exceeded—Error generated when thresholds of total memory or input-output (IO) memory exceeds its maximum allowed limit.

You can configure user-defined response codes using the `voice-class sip error-code-override` command in the dial-peer configuration mode. See the call flow below in the following figure:

**Figure 1: Call Flow for Configuring User-Defined Response Codes to Override SIP CAC Response Codes for Maximum Connections Exceeded**

The error codes are applied for the inbound INVITE message only. If the user-defined error codes are not configured, the default SIP response code of 503 is sent.
How to Configure SIP Error Codes

Overriding CAC Failure Codes with User-Defined Values

Configuring SIP Error Code for CAC Failures (Global Level)

SUMMARY STEPS

1. enable
2. configure terminal
3. voice service voip
4. sip
5. error-code-override {options-keepalive | call | cpu | mem | max-conn | total-calls | sip-shutdown} failure sip-status-code-num
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>enable</td>
</tr>
<tr>
<td>Example:</td>
<td>Device&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>configure terminal</td>
</tr>
<tr>
<td>Example:</td>
<td>Device# configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>voice service voip</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config)# voice service voip</td>
</tr>
<tr>
<td></td>
<td>Specifies VoIP encapsulation and enters voice-service configuration mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>sip</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-voi-serv)# sip</td>
</tr>
<tr>
<td></td>
<td>Enters the Session Initiation Protocol (SIP) configuration mode.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>error-code-override {options-keepalive</td>
</tr>
<tr>
<td>Example:</td>
<td>Device(config-serv-sip)# error-code-override mem failure 411</td>
</tr>
<tr>
<td></td>
<td>Configures the SIP error codes.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>end</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ends the current configuration session and returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
### Configuring SIP Error Code for CAC Failures (Dial Peer Level)

#### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `dial-peer voice tag voip`
4. `voice-class sip error-code-override {options-keepalive | call | cpu | mem | max-conn | total-calls | sip-shutdown} failure {sip-status-code-num | system}`
5. `end`

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 1    | `enable`          | Enables privileged EXEC mode.  
  **Example:**  
  Device> enable  
  - Enter your password if prompted. |
| 2    | `configure terminal` | Enters global configuration mode.  
  **Example:**  
  Device# configure terminal |
| 3    | `dial-peer voice tag voip` | Defines a VoIP dial peer and enters dial peer configuration mode.  
  **Example:**  
  Device(config)# dial-peer voice 10 voip |
| 4    | `voice-class sip error-code-override {options-keepalive | call | cpu | mem | max-conn | total-calls | sip-shutdown} failure {sip-status-code-num | system}` | Configures the Session Initiation Protocol (SIP) error code to be used at the dial peer.  
  **Example:**  
  Device(config-dial-peer)# voice-class sip error-code-override max-conn failure 421 |
| 5    | `end`             | Ends the current configuration session and returns to privileged EXEC mode.  
  **Example:**  
  Device(config-dial-peer)# end |
Configuration Examples for Configurable SIP Error Codes

Example: Configuring SIP Error Codes for CAC Failure

The following example shows how to configure SIP error codes for Call Admission Control (CAC) failure at the global level:

```
Device> enable
Device# configure terminal
Device(config)# voice service voip
Device(config-voi-serv)# sip
Device(config-serv-sip)# error-code-override mem failure 411
Device(config-serv-sip)# end
```

The following example shows how to configure SIP error codes for CAC failure at the dial peer level:

```
Device> enable
Device# configure terminal
Device(config)# dial-peer voice 10 voip
Device(config-dial-peer)# voice-class sip error-code-override max-conn failure 421
Device(config-dial-peer)# end
```

Additional References for Configurable SIP Error Codes

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice commands</td>
<td>Cisco IOS Voice Command Reference</td>
</tr>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Command List, All Releases</td>
</tr>
<tr>
<td>SIP configuration tasks</td>
<td>SIP Configuration Guide, Cisco IOS Release 15M&amp;T</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/support">http://www.cisco.com/support</a></td>
</tr>
</tbody>
</table>
Feature Information for Configurable SIP Error Codes

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

### Table 16: Feature Information for Configurable SIP Error Codes

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configurable SIP Error Codes</td>
<td>Cisco IOS XE Release 3.11S</td>
<td>The Configurable SIP Error Codes feature describes how Cisco Unified Border Element provides support for configurable SIP Error codes to override or modify Session Initiation Protocol (SIP) error response codes. The following commands were introduced or modified: sip-header SIP-StatusLine</td>
</tr>
</tbody>
</table>
CHAPTER 11

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.

- Finding Feature Information, on page 69
- Prerequisites SIP Enhanced 180 Provisional Response Handling, on page 69
- Information About SIP Enhanced 180 Provisional Response Handling, on page 70
- How to Disable the SIP Enhanced 180 Provisional Response Handling Feature, on page 70
- Verifying SIP Enhanced 180 Provisional Response Handling, on page 71
- Configuration Examples for SIP - Enhanced 180 Provisional Response Handling, on page 72
- Feature Information for SIP Enhanced 180 Provisional Response Handling, on page 76

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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

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 Ringer 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 Ringer 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:

The table below shows the call treatments available with this feature:

Table 17: Call Treatments with SIP Enhanced 180 Provisional Response Handling

<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</td>
<td>Local ringback</td>
</tr>
<tr>
<td></td>
<td>Response Handling feature</td>
<td></td>
</tr>
<tr>
<td>183 response with SDP</td>
<td>Not affected by the SIP--Enhanced 180 Provisional</td>
<td>Early media cut-through</td>
</tr>
<tr>
<td></td>
<td>Response Handling feature</td>
<td></td>
</tr>
</tbody>
</table>

How to Disable the SIP Enhanced 180 Provisional Response Handling Feature

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

**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

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 :SIPSPI_EV_CC_CALL_SETUP
00:12:20:CCSIP-SPI-CONTROL: 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,
Passsthrough = 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 :SIPSPI_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) to (STATE_IDLE, SUBSTATE_CONNECTING)
00:12:20:sipSPIOutgoingCallSDP
00:12:20:sipSPIAddLocalContact
00:12:20: Queued event from SIP SPI :SIPSPI_EV_SEND_MESSAGE
00:12:20:sip_process_rtp_sessions
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,
disable_rtcp=FALSE
src_callid = 2, dest_callid = -1
00:12:20:sipSPIUpdateRtpSession:
00:12:20:sipSPIUpdateRtpSession:
00:12:20:sipSPIUpdateRtpSession:
00:12:20:sip_SPI_add_stream:
00:12:20:State change from (STATE_IDLE,
SUBSTATE_CONNECTING) to (STATE_SENT_INVITE, SUBSTATE_NONE)
```

Cisco Unified Border Element (Enterprise) SIP Support Configuration Guide, Cisco IOS XE Release 3S
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-D4AA3153@172.31.1.42
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
c=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=ptime:20
00:12:21:Received:
00:12:21:HandleUdpSocketReads :Msg enqueued for SPI with IPaddr:
00:12:21:10.1.1.15:5060
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:
00:12:21:180 Ringing
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)
Cisco Unified Border Element (Enterprise) SIP Support Configuration Guide, Cisco IOS XE Release 3S

Cisco Enhanced 180 Provisional Response Handling

show logging Command

Record-Route:<sip:222@10.1.1.15:5060;maddr=10.1.1.15>
Content-Length:230
Content-Type:application/sdp
v=0
c=CiscoSystemsSIP-GW-UserAgent 4629 354 IN IP4 10.1.1.42
s=SIP Call
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=fmtp:100 192-194
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:CCSIP-SPI-CONTROL: 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:HandleSIP1xxRinging:SDP: No valid GTD body found.
00:12:21:HandleSIP1xxRinging:SDP: No GTD passed.
00:12:21: HandleSIP1xxRinging:SDP: State change from (STATE_RECD_PROCEEDING, SUBSTATE_PROCEEDING_PROCEEDING) to (STATE_RECD_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:111@10.1.1.42>;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-D4AA3153@172.31.1.42
Timestamp:730944740
Server:Cisco-SIPGateway/IOS-12.x
Csseq:101 INVITE
Allow:INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, COMET, REFER, SUBSCRIBE, NOTIFY, INFO
Allow-Events:telephone-event
Contact:<sip:222@10.1.1.15:5060>
Record-Route:<sip:222@10.1.1.15:5060;maddr=10.1.1.15>
Content-Type:application/sdp
Content-Length:231
v=0
c=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
Feature Information for SIP Enhanced 180 Provisional Response Handling

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Feature Information Table for the ISR

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<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: <code>disable-early-media 180</code> and <code>show sip-ua status</code>.</td>
</tr>
</tbody>
</table>

Feature Information Table for the ASR

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP - Enhanced 180 Provisional Response Handling</td>
<td>Cisco IOS XE Release 2.5</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: <code>disable-early-media 180</code> and <code>show sip-ua status</code>.</td>
</tr>
</tbody>
</table>
Configuring 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:

- Finding Feature Information, on page 77
- Prerequisites for SIP 181 Call is Being Forwarded Message, on page 78
- Configuring SIP 181 Call is Being Forwarded Message Globally, on page 78
- Configuring SIP 181 Call is Being Forwarded Message at the Dial-Peer Level, on page 79
- Configuring Mapping of SIP Provisional Response Messages Globally, on page 80
- Configuring Mapping of SIP Provisional Response Messages at the Dial-Peer Level, on page 81
- Feature Information for Configuring SIP 181 Call is Being Forwarded Message, on page 82

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to https://cfnng.cisco.com/. An account on Cisco.com is not required.
Prerequisites for SIP 181 Call is Being Forwarded Message

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 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> 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>
</tbody>
</table>
### Configuring 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></td>
<td>Enters privileged EXEC mode, or other security level set by a system administrator.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Enters dial peer VoIP configuration mode.</td>
</tr>
<tr>
<td><code>dial-peer voice tag voip</code></td>
<td></td>
</tr>
<tr>
<td>Example:</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>
</table>
| enable | Enters privileged EXEC mode, or other security level set by a system administrator.  
  • Enter your password if prompted. |
| configure terminal | Enters global configuration mode. |
| voice service voip | Enters voice service VoIP configuration mode. |

Configures support of SIP 181 messages on a specific dial peer 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.

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>voice-class sip block {180</td>
<td>181</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-dial-peer)# voice-class sip block 181 sdp present</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>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>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Router(config)# voice service voip</td>
<td>Enters SIP configuration mode.</td>
</tr>
</tbody>
</table>

**Step 4**  
Example:  
Router(conf-voi-serv)# sip  
Enters SIP configuration mode.

**Step 5**  
Example:  
Router(conf-voi-serv)# map resp-code 181 to 183  
Enables mapping globally of received SIP messages of a specified message type to a different SIP message type.

**Step 6**  
Example:  
Router(conf-voi-serv)# exit  
Exits the current mode.

---

**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 | Enters privileged EXEC mode, or other security level set by a system administrator.  
Example:  
Router> enable  
• Enter your password if prompted. |
| Step 2 | Enters global configuration mode.  
Example:  
Router# configure terminal |
## Command or Action

<table>
<thead>
<tr>
<th>Step 3</th>
<th>dial-peer voice tag voip</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>voice-class sip map resp-code 181 to 183</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>exit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>

### Purpose

- **Enters dial peer VoIP configuration mode.**
- **Enables mapping of received SIP messages of a specified SIP message type on a specific dial peer to a different SIP message type.**
- **Exits the current mode.**

## Feature Information for Configuring SIP 181 Call is Being Forwarded Message

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Feature History Table entry for the Cisco Unified Border Element.

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

Feature History Table entry for the Cisco Unified Border Element (Enterprise).
### Table 21: Feature Information for SIP 181 Call is Being Forwarded Messages

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP 181 Call is Being Forwarded Message</td>
<td>Cisco IOS XE</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></td>
<td>Release 3.1S</td>
<td></td>
</tr>
</tbody>
</table>
Feature Information for Configuring SIP 181 Call is Being Forwarded Message
CHAPTER 13

SIP UPDATE Message per RFC 3311

The SIP UPDATE Message per RFC 3311 feature provides Session Description Protocol (SDP) support for Session Initiation Protocol (SIP)-to-SIP calls. The SIP Service Provider Interface (SPI) is modified to support the following media changes using the UPDATE message:

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

The Support for SIP UPDATE Message Per RFC 3311 feature is enabled by default on the Cisco Unified Border Element (UBE) and no configuration is required.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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

Prerequisites for SIP UPDATE Message per RFC 3311

- At least one offer or answer negotiation must be completed for Cisco UBE to handle the UPDATE message with SDP.
- An early dialog UPDATE message with SDP is processed only when both endpoints support the UPDATE message.
- For early dialog, both SIP endpoints must support PRACK and UPDATE method. Initial Offer-Answer must be completed with reliable provisional responses.
Cisco Unified Border Element

- Cisco IOS Release 15.1(3)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 3.6S or a later release must be installed and running on your Cisco ASR 1000 Series Router.

Restrictions for SIP UPDATE Message per RFC 3311

- An UPDATE message with SDP is not supported for SIP-to-H323 calls.
- An UPDATE message with SDP with a fully qualified domain name (FQDN) is not supported.
- Contact information in the UPDATE message is not supported.
- A retransmitted UPDATE message with SDP is ignored by the SIP stack. No response is sent for retransmitted UPDATE messages.
- CUBE rejects UPDATE with SDP in early dialog when peer SIP leg does not support UPDATE.

Information About SIP UPDATE Message per RFC 3311

The SIP Update per RFC 3311 feature uses existing mid-call SDP processing logic to negotiate the Offer-Answer with UPDATE, so all media features supported in CUBE with Re-INVITE are supported with UPDATE.

The images below illustrate the call flows when one call-leg supports UPDATE and the other leg does not support UPDATE in early dialog and mid-call dialog.
Feature Information for the SIP UPDATE Message per RFC 3311

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.
Table 22: Feature Information for Support for SIP UPDATE Message per RFC 3311

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
</table>
| Support for SIP UPDATE Message per RFC 3311      | 15.1(3)T          | The Support for SIP UPDATE Message per RFC 3311 feature provides Session Description Protocol (SDP) support for Session Initiation Protocol (SIP)-to-SIP calls. The SIP Service Provider Interface (SPI) is modified to support the following media changes using the UPDATE message:  
  • Early dialog SIP-to-SIP media changes.  
  • Mid dialog SIP-to-SIP media changes.  
  In Cisco IOS Release 12.2(25)S, this feature was implemented on the Cisco Unified Border Element. |
| Support for SIP UPDATE Message per RFC 3311      | Cisco IOS XE Release 3.6S | The Support for SIP UPDATE Message per RFC 3311 feature provides Session Description Protocol (SDP) support for Session Initiation Protocol (SIP)-to-SIP calls. The SIP Service Provider Interface (SPI) is modified to support the following media changes using the UPDATE message:  
  • Early dialog SIP-to-SIP media changes.  
  • Mid dialog SIP-to-SIP media changes.  
  In Cisco IOS XE Release 3.6S, this feature was implemented on the Cisco Unified Border Element (Enterprise). |
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.

- Finding Feature Information, on page 89
- Prerequisites for Expires Timer Reset on Receiving or Sending SIP 183 Message, on page 89
- How to Configure Expires Timer Reset on Receiving or Sending SIP 183 Message, on page 90
- Feature Information for Configuring Support for Expires Timer Reset on Receiving or Sending SIP 183 Message, on page 92

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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

Prerequisites for Expires Timer Reset on Receiving or Sending SIP 183 Message

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 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

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></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Example:</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`
**Example:**
Router> enable | Enables privileged EXEC mode.  
- Enter your password if prompted. |
| **Step 2**
`configure terminal`
**Example:**
Router# configure terminal | Enters global configuration mode. |
### Command or Action

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 3</td>
<td><code>dial-peer voice tag voip</code></td>
<td>Enters dial peer VoIP configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# dial-peer voice 2 voip</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>voice-class sip reset timer expires 183</code></td>
<td>Enables resetting of the Expires timer upon receipt of SIP 183 messages on a specific dial peer.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-dial-peer)# voice-class sip reset timer expires 183</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td><code>exit</code></td>
<td>Exits the current mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-dial-peer)# exit</td>
<td></td>
</tr>
</tbody>
</table>

## Feature Information for Configuring Support for Expires Timer Reset on Receiving or Sending SIP 183 Message

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Feature History Table entry for the Cisco Unified Border Element.

**Table 23: Feature Information for Support for Expires Timer Reset on Receiving or Sending SIP 183 Message**

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support for Expires Timer Reset on Receiving or Sending SIP 183 Message</td>
<td>15.0(1)XA 15.1(1)T</td>
<td>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: <code>reset timer expires</code> and <code>voice-class sip reset timer expires</code>.</td>
</tr>
</tbody>
</table>

Feature History Table entry for the Cisco Unified Border Element (Enterprise) .
## Table 24: Feature Information for Support for Expires Timer Reset on Receiving or Sending SIP 183 Message

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support for Expires Timer Reset on Receiving or Sending SIP 183 Message</td>
<td>Cisco IOS XE Release 3.1S</td>
<td>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: <code>reset timer expires</code> and <code>voice-class sip reset timer expires</code>.</td>
</tr>
</tbody>
</table>
Feature Information for Configuring Support for Expires Timer Reset on Receiving or Sending SIP 183 Message
CHAPTER 15

Selective Filtering of Outgoing Provisional Response on the Cisco Unified Border Element

This feature adds support on the Cisco Unified Border Element (Cisco UBE) platforms for selective filtering of outgoing provisional responses, including "180-Alerting" and "183-Session In Progress" responses. Selective filtering can be further based on the availability of media information in the received provisional response.

Next Generation Network (NGN) restricts the UNI from sending a 183 response with Session Description Protocol (SDP) toward the NGN network. Cisco Unified Communications Manager always sends a 183 response with SDP responses. It is necessary for the Cisco UBE to block these responses to allow Cisco Unified Communications Manager to interwork within the Next Generation network.

• Finding Feature Information, on page 95
• Prerequisites for Selective Filtering of Outgoing Provisional Response on the Cisco UBE, on page 96
• Restrictions for Selective Filtering of Outgoing Provisional Response on the Cisco UBE, on page 96
• How to Configure Selective Filtering of Outgoing Provisional Response on the Cisco UBE, on page 96
• Feature Information for Selective Filtering of Outgoing Provisional Response on the Cisco Unified Border Element, on page 98

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to https://cfnng.cisco.com/. An account on Cisco.com is not required.
Prerequisites for Selective Filtering of Outgoing Provisional Response on the Cisco UBE

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 for Selective Filtering of Outgoing Provisional Response on the Cisco UBE
• Blocking 180 and 183 responses with or without the SDP requirement is to block 183 with SDP only.

How to Configure Selective Filtering of Outgoing Provisional Response on the Cisco UBE

Configuring Selective Filtering of Outgoing Provisional Response on the Cisco UBE at the Global Level

To configure Selective Filtering of Outgoing Provisional Response on the Cisco UBE at the global level, perform the steps in this section:

SUMMARY STEPS

1. enable
2. configure terminal
3. voice service voip
4. sip
5. block 183 sdp absent
6. exit
## DETAILED STEPS

<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>- 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>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 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 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> block 183 sdp absent</td>
<td>Filters outgoing provisional responses, including &quot;180-Alerting&quot; and &quot;183-Session In Progress&quot; responses.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(conf-serv-sip)# block 183 sdp absent</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</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 Selective Filtering of Outgoing Provisional Response on the Cisco UBE at the Dial Peer Level

To configure Selective Filtering of Outgoing Provisional Response on the Cisco UBE at the dial-peer level, configure the outgoing dial peer as follows:

### SUMMARY STEPS

1. enable
2. configure terminal
3. dial-peer voice *number* voip
4. voice-class sip block 183 sdp present
5. exit
### Detailed Steps

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>dial-peer voice number voip</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td><code>voice-class sip block 183 sdp present</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td><code>exit</code></td>
<td></td>
</tr>
</tbody>
</table>

### Feature Information for Selective Filtering of Outgoing Provisional Response on the Cisco Unified Border Element

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Feature History Table entry for the Cisco Unified Border Element.
Table 25: Feature Information for Selective Filtering of Outgoing Provisional Response on the Cisco UBE

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>12.4(22)YB</td>
<td>This feature adds support on Cisco UBE for selective filtering of outgoing provisional responses, including &quot;180-Alerting&quot; and &quot;183-Session In Progress&quot; 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: <code>block</code> and <code>voice-class sip block</code>.</td>
</tr>
<tr>
<td></td>
<td>15.0(1)M</td>
<td></td>
</tr>
</tbody>
</table>

Feature History Table entry for the Cisco Unified Border Element (Enterprise).

Table 26: Feature Information for Selective Filtering of Outgoing Provisional Response on the Cisco UBE

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Cisco IOS XE</td>
<td>This feature adds support on Cisco UBE for selective filtering of outgoing provisional responses, including &quot;180-Alerting&quot; and &quot;183-Session In Progress&quot; 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: <code>block</code> and <code>voice-class sip block</code>.</td>
</tr>
<tr>
<td></td>
<td>Release 3.1S</td>
<td></td>
</tr>
</tbody>
</table>
RFCC 4040-Based Clear Channel Codec Negotiation for SIP Calls

The RFC 4040-Based Clear Channel Codec Negotiation for SIP Calls feature globally enables RFC 4040-based clear-channel codec negotiation [CLEARMODE/8000] for SIP calls on a Cisco IOS voice gateway or Cisco UBE. RFC 4040-based clear-channel codec negotiation allows Cisco IOS voice gateways and Cisco UBEs to successfully interoperate with third-party SIP gateways that do not support legacy Cisco IOS clear-channel codec encapsulation [X-CCD/8000].

• Finding Feature Information, on page 101
• Prerequisites for RFC 4040-Based Clear Channel Codec Negotiation for SIP Calls, on page 101
• Restrictions for RFC 4040-Based Clear Channel Codec Negotiation for SIP Calls, on page 102
• Information about RFC 4040-Based Clear Channel Codec Negotiation for SIP Calls, on page 102
• How to Configure RFC 4040-Based Clear Channel Codec Negotiation for SIP Calls, on page 102
• Feature Information for RFC 4040-Based Clear Channel Codec Negotiation for SIP Calls, on page 104

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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

Prerequisites for RFC 4040-Based Clear Channel Codec Negotiation for SIP Calls

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 RFC 4040-Based Clear Channel Codec Negotiation for SIP Calls

- This feature is supported on Cisco IOS SIP time division multiplexing (TDM) gateways and Cisco Unified Border Elements (Cisco UBEs).

Information about RFC 4040-Based Clear Channel Codec Negotiation for SIP Calls

When the `encap clear-channel standard` command is enabled on a Cisco IOS voice gateway or Cisco UBE, calls using the Cisco IOS clear channel codec are translated into calls that use CLEARMODE/8000 so that the calls do not get rejected when they reach third-party SIP gateways.

To enable RFC 4040-based clear-channel codec negotiation for SIP calls on an individual dial peer, overriding the global configuration for the Cisco IOS voice gateway or Cisco UBE, use the `voice-class sip encap clear-channel standard` command in dial peer voice configuration mode. To globally disable RFC 4040-based clear-channel codec negotiation on a Cisco IOS voice gateway or Cisco UBE, use the `no encap clear-channel standard` command in voice service SIP configuration mode.

How to Configure RFC 4040-Based Clear Channel Codec Negotiation for SIP Calls

This feature can be enabled globally for all dial peers or on an individual dial peer (which overrides the global configuration, if one is in effect). Depending on your requirements, complete one of the following tasks:

Configuring RFC 4040-Based Clear Channel Codec Negotiation for SIP Calls Globally for All Dial Peers

To configure RFC 4040-based clear-channel code negotiation globally for all dial peers on a Cisco IOS voice gateway or Cisco UBE, complete this task:

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `voice service voip`
4. `sip`
### 5. `encap clear-channel standard`

<table>
<thead>
<tr>
<th>DETAILED STEPS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Command or Action</strong></td>
</tr>
<tr>
<td>Step 1</td>
</tr>
<tr>
<td>Step 2</td>
</tr>
<tr>
<td>Step 3</td>
</tr>
<tr>
<td>Step 4</td>
</tr>
<tr>
<td>Step 5</td>
</tr>
</tbody>
</table>

### Configuring RFC 4040-Based Clear Channel Codec Negotiation for SIP Calls for a Single Dial Peer

To configure RFC 4040-based clear-channel code negotiation for one dial peer on a Cisco IOS voice gateway or Cisco UBE, complete this task:

<table>
<thead>
<tr>
<th>SUMMARY STEPS</th>
</tr>
</thead>
</table>
| 1. `enable`  
  2. `configure terminal`  
  3. `dial-peer voice 1 voip`  
  4. `voice-class sip encap clear-channel standard` |

<table>
<thead>
<tr>
<th>DETAILED STEPS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Command or Action</strong></td>
</tr>
<tr>
<td>Step 1</td>
</tr>
</tbody>
</table>
Feature Information for RFC 4040-Based Clear Channel Codec Negotiation for SIP Calls

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Feature History Table entry for the Cisco Unified Border Element.

### Table 27: Feature Information for RFC 4040-Based Clear Channel Codec Negotiation for SIP Calls

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 4040-Based Clear Channel Codec Negotiation for SIP Calls</td>
<td>15.0(1)XA 15.1(1)T</td>
<td>This feature adds support for RFC 4040-based clear channel codec Negotiation for SIP calls. The following commands were modified: <code>encap clear-channel standard</code> and <code>voice-class sip encap clear-channel</code></td>
</tr>
</tbody>
</table>
Feature History Table entry for the Cisco Unified Border Element (Enterprise)

Table 28: Feature Information for RFC 4040-Based Clear Channel Codec Negotiation for SIP Calls

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 4040-Based Clear Channel Codec Negotiation for SIP Calls</td>
<td>Cisco IOS XE</td>
<td>This feature adds support for RFC 4040-based clear channel codec Negotiation for SIP calls. The following commands were modified: <code>encap clear-channel standard</code> and <code>voice-class sip encap clear-channel</code></td>
</tr>
</tbody>
</table>
Support for PAID PPID Privacy PCPID and PAURI Headers on the Cisco Unified Border Element

The figure below 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 4: 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 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.

**Note**
If the NGN sets the From: value to anonymous, the PAID is the only value that identifies the caller.

The table below 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.

The table below 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 29: P-header Configuration Settings**

<table>
<thead>
<tr>
<th>Incoming Header</th>
<th>Outgoing Header</th>
<th>Configuration Notes</th>
</tr>
</thead>
</table>
| From:           | 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. |
| **Note**        |                 | If both, `remote-party-id` and `asserted-id` commands are configured, then the `asserted-id` command takes precedence over the `remote-part-id` command. |

| PPID | 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` |

| 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`

<p>|                  |                  | This is the default system behavior. |</p>
<table>
<thead>
<tr>
<th>Incoming Header</th>
<th>Outgoing Header</th>
<th>Configuration Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>PAID</td>
<td>PPID</td>
<td>To enable the translation to PPIID privacy 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: Router(conf-serv-sip)# <code>asserted-id ppi</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>To enable the translation to PPIID privacy 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: Router(config-dial-peer)# <code>voice-class sip asserted-id ppi</code></td>
</tr>
<tr>
<td>PAID</td>
<td>RPID</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: Router(config-sip-ua)# <code>remote-party-id</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>This is the default system behavior.</td>
</tr>
<tr>
<td>RPID</td>
<td>PPID</td>
<td>To enable the translation to PPIID privacy 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: Router(conf-serv-sip)# <code>asserted-id ppi</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>To enable the translation to PPIID privacy 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: Router(config-dial-peer)# <code>voice-class sip asserted-id ppi</code></td>
</tr>
<tr>
<td>RPID</td>
<td>PAID</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: Router(conf-serv-sip)# <code>asserted-id pai</code></td>
</tr>
<tr>
<td></td>
<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: Router(config-dial-peer)# <code>voice-class sip asserted-id pai</code></td>
</tr>
<tr>
<td>RPID</td>
<td>From:</td>
<td>By default, the translation to RPID headers is enabled and the system translates PPIID headers in incoming messages to RPID headers in the outgoing messages. To disable the default behavior and enable the translation from PPIID to From: headers, use the <code>no remote-party-id</code> command in SIP user-agent configuration mode. For example: Router(config-sip-ua)# <code>no remote-party-id</code></td>
</tr>
</tbody>
</table>

---

**Note:** Privacy functions are not initialized on Unified Border Element without configuring `asserted-id pai` or `asserted-id ppi`. Ensure that you configure `asserted-id pai` or `asserted-id ppi` to support privacy functions on Unified Border Element.

The CUBE can be configured to transparently pass the PAID and PPIID headers in the incoming and outgoing Session Initiation Protocol (SIP) requests or response messages from end-to-end.

- Requests include: INVITEs and UPDATEs
- Responses include: 18x and 200OK

---

**Cisco Unified Border Element (Enterprise) SIP Support Configuration Guide, Cisco IOS XE Release 3S**
The priority of P-headers are in the following order: PAID, PPID, and RPID.

### Table 30: PAID and PPID header configuration settings for mid-call requests and responses

<table>
<thead>
<tr>
<th>Incoming Header</th>
<th>Outgoing Header</th>
<th>Configuration Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>PAID</td>
<td>PPID</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>
</tr>
<tr>
<td></td>
<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>
</tr>
<tr>
<td>RPID</td>
<td>PPID</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>
</tr>
<tr>
<td></td>
<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>
</tr>
<tr>
<td>Incoming Header</td>
<td>Outgoing Header</td>
<td>Configuration Notes</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>PPID</td>
<td>PPID</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. 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: Router(config-dial-peer)# voice-class sip asserted-id ppi</td>
</tr>
<tr>
<td>PAID</td>
<td>PAID</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. 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: Router(config-dial-peer)# voice-class sip asserted-id pai</td>
</tr>
<tr>
<td>RPID</td>
<td>PAID</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. 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.</td>
</tr>
<tr>
<td>Incoming Header</td>
<td>Outgoing Header</td>
<td>Configuration Notes</td>
</tr>
<tr>
<td>----------------</td>
<td>----------------</td>
<td>---------------------</td>
</tr>
</tbody>
</table>
| PPID           | PAID           | To enable the translation to PAID headers in the outgoing header at a global level, use the `asserted-id pai` command in voice service VoIP SIP configuration mode.  
To enable the translation to PAID 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. |
| 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`.  
**Note** PAID and PPID headers are not configured in this case. |
| RPID           | 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`.  
**Note** PAID and PPID headers are not configured in this case. |
| 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` |
<p>| FROM           | FROM           | No configuration required except for the <code>remote-party-id</code> header. |</p>
<table>
<thead>
<tr>
<th>Incoming Header</th>
<th>Outgoing Header</th>
<th>Configuration Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>FROM</td>
<td>RPID</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>
</tr>
<tr>
<td>PAID</td>
<td>PAID</td>
<td>Enables PPID headers on the incoming dial-peer and PAID headers on the outgoing dial-peer.</td>
</tr>
<tr>
<td>RPID</td>
<td>PAID</td>
<td>Enables PPID headers on incoming dial-peer and PAID headers on outgoing dial-peer.</td>
</tr>
<tr>
<td>PPID</td>
<td>PAID</td>
<td>Enables PPID headers on incoming dial-peer and PAID headers on outgoing dial-peer.</td>
</tr>
<tr>
<td>PAID</td>
<td>PAID</td>
<td>Enables RPID headers on incoming dial-peer and PAID headers on outgoing dial-peer.</td>
</tr>
<tr>
<td>RPID</td>
<td>PAID</td>
<td>Enables RPID headers on incoming dial-peer and PAID headers on outgoing dial-peer.</td>
</tr>
<tr>
<td>PPID</td>
<td>PAID</td>
<td>Enables RPID headers on incoming dial-peer and PAID headers on outgoing dial-peer.</td>
</tr>
<tr>
<td>PAID</td>
<td>PPID</td>
<td>Enables PAID headers on incoming dial-peer and PPID headers on outgoing dial-peer.</td>
</tr>
<tr>
<td>RPID</td>
<td>PPID</td>
<td>Enables PAID headers on incoming dial-peer and PPID headers on outgoing dial-peer.</td>
</tr>
<tr>
<td>PPID</td>
<td>PPID</td>
<td>Enables PAID headers on incoming dial-peer and PPID on outgoing dial-peer.</td>
</tr>
<tr>
<td>PAID</td>
<td>PPID</td>
<td>Enables RPID headers on incoming dial-peer and PPID headers on outgoing dial-peer.</td>
</tr>
<tr>
<td>RPID</td>
<td>PPID</td>
<td>Enables RPID headers on incoming dial-peer and PPID headers on outgoing dial-peer.</td>
</tr>
<tr>
<td>Incoming Header</td>
<td>Outgoing Header</td>
<td>Configuration Notes</td>
</tr>
<tr>
<td>-----------------</td>
<td>----------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>PPID</td>
<td>PPID</td>
<td>Enables RPID headers on incoming dial-peer and PPID headers on outgoing dial-peer.</td>
</tr>
</tbody>
</table>
| PAID            | RPID           | Enables PPID headers on incoming dial-peer and RPID headers on outgoing dial-peer.  
                   |                | Note: PAID headers will be given priority and RPID headers will be created using the PAID header information. |
| RPID            | RPID           | Enables PPID headers on incoming dial-peer and RPID headers on outgoing dial-peer. |
| PPID            | RPID           | Enables PPID headers on incoming dial-peer and RPID headers on outgoing dial-peer.  
                   |                | Note: PPID headers will be given priority and RPID headers will be created using the PPID header information. |
| PAID            | RPID           | Enables PAID headers on incoming dial-peer and RPID headers on outgoing dial-peer.  
                   |                | Note: PAID headers will be given priority and RPID headers will be created using the PAID header information. |
| RPID            | RPID           | Enables PAID headers on incoming dial-peer and RPID headers on outgoing dial-peer.  
                   |                | Note: PAID headers will be given priority and RPID headers will be created using the PAID header information. |
| PPID            | RPID           | Enables PAID headers on incoming dial-peer and RPID headers on outgoing dial-peer.  
                   |                | Note: PPID headers will be given priority and RPID headers will be created using the PPID header information. |
Privacy

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

- Using prefixes

The NGN dial plan can specify prefixes to enable privacy settings. For example, the dial plan may specify that if the caller dials a prefix of 184, the calling number is not sent to the called party.

The dial plan may also specify that the caller can choose to send the calling number to the called party by dialing a prefix of 186. 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.

Note

For the Privacy functions to work as intended, the command `asserted-id {pai|ppi}` must be configured.

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.

- Feature Information for PAID PPID Privacy PCPID and PAURI Headers on the Cisco Unified Border Element, on page 117
Feature Information for PAID PPID Privacy PCPID and PAURI Headers on the Cisco Unified Border Element

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 31: Feature Information for PAID and PPID Headers on Cisco Unified Border Element (CUBE)

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
</table>
| PAID and PPID Headers in mid-call re-INVITE and UPDATE request and responses on Cisco Unified Border Element | Cisco IOS 15.5(3)M Cisco IOS XE 3.16S | This feature enables CUBE platforms to support:  
  • P-Preferred Identity (PPID) and P-Asserted Identity (PAID) in mid-call re-INVITE messages and responses from end-to-end.  
  • P-Preferred Identity (PPID) and P-Asserted Identity (PAID) in mid-call UPDATE messages and responses from end-to-end.  
  • Configuration and/or pass through of PAID and PPID header values. |

Feature History Table entry for the Cisco Unified Border Element and Cisco Unified Border Element (Enterprise).
Table 32: Feature Information for PAID, PPID, Privacy, PCPID, and PAURI Headers on CUBE

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
</table>
| PAID, PPID, Privacy, PCPID, and PAURI Headers on the Cisco Unified Border Element | 12.4(22)YB 15.0(1)M Cisco IOS XE Release 3.1S | This feature enables CUBE 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.

Prerequisites for Support for PAID PPID Privacy PCPID and PAURI Headers on the Cisco Unified Border Element

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 for Support for PAID PPID Privacy PCPID and PAURI Headers on the Cisco Unified Border Element

- 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.

- Passing of “+” is not supported with PAID PPID Privacy PCPID and PAURI Headers.

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.

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**

<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>• Enter your password if prompted.</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:</td>
<td>Enter your password if prompted.</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>Example:</td>
<td>* Enter your password if prompted.</td>
</tr>
<tr>
<td>Router&gt; enable</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

### Command or Action | Purpose
--- | ---
**Step 2** configure terminal
*Example:*
Router# configure terminal | Enters global configuration mode.

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

**Step 4** sip
*Example:*
Router(conf-vol-serv)# sip | Enters voice service VoIP SIP configuration mode.

**Step 5** call-route p-called-party-id
*Example:*
Router(conf-serv-sip)# call-route p-called-party-id | Enables the routing of calls based on the PCPID header.

**Step 6** random-request-uri validate
*Example:*
Router(conf-serv-sip)# random-request-uri validate | Enables the validation of the random string in the Request URI of the incoming INVITE message.

**Step 7** exit
*Example:*
Router(conf-serv-sip)# exit | Exits the current mode.
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable&lt;br&gt;Example: <code>Router&gt; enable</code></td>
<td>Enables privileged EXEC mode. &lt;br&gt;• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal&lt;br&gt;Example: <code>Router# configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td>dial-peer voice tag voip&lt;br&gt;Example: <code>Router(config)# dial-peer voice 2611 voip</code></td>
<td>Defines the dial peer, specifies the method of voice encapsulation, and enters dial peer voice configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>voice-class sip call-route p-called-party-id&lt;br&gt;Example: <code>Router(config-dial-peer)# voice-class sip call-route p-called-party-id</code></td>
<td>Enables the routing of calls based on the PCPID header on this dial peer.</td>
</tr>
<tr>
<td>Step 5</td>
<td>voice-class sip random-request-uri validate&lt;br&gt;Example: <code>Router(config-dial-peer)# voice-class sip random-request-uri validate</code></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>Step 6</td>
<td>exit&lt;br&gt;Example: <code>Router(config-dial-peer)# exit</code></td>
<td>Exits the current mode.</td>
</tr>
</tbody>
</table>

## 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></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> 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> privacy privacy-option</td>
<td>Enables the privacy settings for the header.</td>
</tr>
<tr>
<td><strong>Example:</strong></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><strong>Example:</strong></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><strong>Example:</strong></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>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: <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>Example: <code>Router# configure terminal</code></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: <code>Router(config)# dial-peer voice 2611 voip</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> voice-class sip privacy  privacy-option</td>
<td>Enables the privacy settings for the header on this dial peer.</td>
</tr>
<tr>
<td>Example: <code>Router(config-dial-peer)# voice-class sip privacy id</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> voice-class sip 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, on this dial peer.</td>
</tr>
<tr>
<td>Example: <code>Router(config-dial-peer)# voice-class sip privacy-policy passthru</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> exit</td>
<td>Exits the current mode.</td>
</tr>
<tr>
<td>Example: <code>Router(config-dial-peer)# exit</code></td>
<td></td>
</tr>
</tbody>
</table>

### 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`
### 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><strong>Step 4</strong> credentials username username password password realm domain-name</td>
<td>Sends a SIP registration message from the Cisco Unified Border Element.</td>
</tr>
<tr>
<td><strong>Example:</strong> 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><strong>Example:</strong> 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><strong>Example:</strong> 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><strong>Example:</strong></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><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><code>Example:</code></td>
<td></td>
</tr>
<tr>
<td><code>Router&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><code>Example:</code></td>
<td></td>
</tr>
<tr>
<td><code>Router# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>Command or Action</td>
</tr>
<tr>
<td>--------</td>
<td>-------------------</td>
</tr>
<tr>
<td></td>
<td>sip-ua</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Step 4 | credentials username  username password
rearl domain-name | Sends a SIP registration message from the Cisco Unified Border Element. |
|        | Example:          | Router(config-sip-ua)# credentials username 123456 password cisco realm cisco |
|        |                   |         |
| Step 5 | registrar ipv4: destination-address random-contact
expires expiry | 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. |
|        | Example:          | Router(config-sip-ua)# registrar ipv4:10.1.2.2 random-contact expires 200 |
|        |                   |         |
| Step 6 | exit              | Exits the current mode. |
|        | Example:          | Router(config-sip-ua)# exit |
|        |                   |         |
| Step 7 | 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 8 | voice-class sip random-contact | Enables random-contact support on this dial peer. |
|        | Example:          | Router(config-dial-peer)# voice-class sip random-contact |
|        |                   |         |
| Step 9 | exit              | Exits the current mode. |
|        | Example:          | Router(config-dial-peer)# exit |
Configurable Pass-Through of SIP INVITE Parameters

The Configurable Pass-Through of SIP INVITE Parameters 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 Session Initiation Protocol (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 or Multipurpose Internet Mail Extensions (MIME) types.

- Finding Feature Information, on page 129
- Prerequisites for Configurable Pass-Through of SIP INVITE Parameters, on page 130
- Restrictions for Configurable Pass-Through of SIP INVITE Parameters, on page 130
- Information About Configurable Pass-Through of SIP INVITE Parameters, on page 131
- Support for Content-Types, on page 134
- How to Configure Configurable Pass-Through of SIP INVITE Parameters, on page 136
- Configuration Examples for Configurable Pass-Through of SIP INVITE Parameters, on page 140
- Additional References for Configurable Pass-Through of SIP INVITE Parameters, on page 141
- Feature Information for Configurable Pass-Through of SIP INVITE Parameters, on page 141

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to https://cfnng.cisco.com/. An account on Cisco.com is not required.
Prerequisites for Configurable Pass-Through of SIP INVITE Parameters

- 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 fall back 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 for Configurable Pass-Through of SIP INVITE Parameters

When Session Description Protocol (SDP) pass-through is enabled, some of the 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
- Flow-around calls will not work with SDP pass through
- DTMF Interworking Scenarios
- Fax Interworking/QoS Negotiation
- Transcoding

For configurable pass-through of SIP INVITE parameters, the following features for Session Initiation Protocol (SIP)-SIP dial-peer rotary calls are not supported:

- Unsupported header pass-through functionality for SIP-SIP dial-peer rotary calls
- Unsupported content pass-through functionality for SIP-SIP dial-peer rotary calls
With CSCtx41575, the unsupported header and content pass-through functionalities mentioned above are addressed.

Information About Configurable Pass-Through of SIP INVITE Parameters

Cisco Unified Border Element (Unified Border Element) does not support end-to-end media negotiation between the two endpoints that establish a call session. This is a limitation when the endpoints intend to negotiate codec or payload types that Unified Border Element does not process because, currently, unsupported payload types are not negotiated by Unified Border Element. Unsupported content types include text or plain, image or jpeg and application or resource-lists and XML. To address this problem, Session Description Protocol (SDP) is configured to pass transparently through Unified Border Element so that both the remote ends can negotiate media independent of Unified Border Element.

Session Description Protocol (SDP) pass-through is addressed in two modes:

- Flow-through—Unified Border Element plays no role in the media negotiation. It terminates and reoriginates the Real-time Transport Protocol (RTP) packets irrespective of the content type negotiated by both endpoints. Flow-through supports address hiding and Network Address Translation (NAT) traversal.

- Flow-around—Unified Border Element neither plays a part in media negotiation nor does it terminate and reoriginate media. Media negotiation and media exchange is completely end-to-end.

Header passthrough is only applicable to SIP messages and responses that have end-to-end significance. For information on header passthrough support across different SIP methods and SIP Responses, see Table 1: Header Passthrough Support for SIP Method and Table 2: Header Passthrough Support for SIP Response.

<table>
<thead>
<tr>
<th>SIP Method</th>
<th>Passthrough Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACK/PRACK¹</td>
<td>Yes</td>
</tr>
<tr>
<td>BYE</td>
<td>Yes</td>
</tr>
<tr>
<td>CANCEL</td>
<td>No</td>
</tr>
<tr>
<td>INFO</td>
<td>Yes</td>
</tr>
<tr>
<td>INVITE</td>
<td>Yes</td>
</tr>
<tr>
<td>NOTIFY, OPTIONS, PUBLISH</td>
<td>No</td>
</tr>
<tr>
<td>REFER²</td>
<td>Yes</td>
</tr>
<tr>
<td>REGISTER, SUBSCRIBE, UPDATE</td>
<td>No</td>
</tr>
</tbody>
</table>

¹ Only for Delayed Offer to Delayed Offer
2 Only when **supplementary service sip refer** is configured.

### Table 34: Header Passthrough Support for SIP Response

<table>
<thead>
<tr>
<th>SIP Response</th>
<th>Passthrough Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>No</td>
</tr>
<tr>
<td>180</td>
<td>Yes</td>
</tr>
<tr>
<td>183</td>
<td>Yes</td>
</tr>
<tr>
<td>Other 1XX</td>
<td>No</td>
</tr>
<tr>
<td>2XX, 3XX</td>
<td>Yes</td>
</tr>
<tr>
<td>4XX, 5XX, 6XX</td>
<td>Yes</td>
</tr>
</tbody>
</table>

3 Depends on the configuration for handling redirection.

### Supported SIP Headers

You can configure Unified Border Element to pass through SIP headers that are both mandatory and not mandatory (headers that Unified Border Element does not pass through by default). You can configure a list of headers to be passed across for both mandatory and non-mandatory SIP headers.

#### Mandatory Headers

The following table provides a list of mandatory headers that are supported for pass through by Unified Border Element:

<table>
<thead>
<tr>
<th>List of Mandatory Headers Supported on Unified Border Element</th>
</tr>
</thead>
<tbody>
<tr>
<td>Also Authorization Call_ID</td>
</tr>
<tr>
<td>CC-Diversion CC-Redirect Cisco_Gcid</td>
</tr>
<tr>
<td>Cisco_Ccid Contact Content-Disposition</td>
</tr>
<tr>
<td>Content-Encoding Content-Length Content-Type</td>
</tr>
<tr>
<td>Cseq Date From</td>
</tr>
<tr>
<td>Max-Forwards MIME-Version P-Asserted-Identity</td>
</tr>
<tr>
<td>P-Preferred-Identity Privacy Proxy-Authenticate</td>
</tr>
<tr>
<td>Proxy-Authorization Record-Route Route</td>
</tr>
<tr>
<td>Session-Expires Timestamp To</td>
</tr>
<tr>
<td>User-Agent Via WWW-Authenticate</td>
</tr>
</tbody>
</table>
Non-Mandatory Headers

The list of non-mandatory headers can contain any header except the mandatory headers that are configured for pass through. The following table provides a list of non-mandatory headers that are supported for pass through by Unified Border Element:

Table 36: List of Non-Mandatory Headers

<table>
<thead>
<tr>
<th>List of Non-Mandatory Headers Supported on Unified Border Element</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept-Contact</td>
</tr>
<tr>
<td>Accept-Encoding</td>
</tr>
<tr>
<td>Allow</td>
</tr>
<tr>
<td>Content-ID</td>
</tr>
<tr>
<td>Expires</td>
</tr>
<tr>
<td>Min-Expires</td>
</tr>
<tr>
<td>Proxy-Require</td>
</tr>
<tr>
<td>Remote-Party-ID</td>
</tr>
<tr>
<td>RAcc</td>
</tr>
<tr>
<td>Resource-Priority</td>
</tr>
<tr>
<td>Referred-By</td>
</tr>
<tr>
<td>Retry-After</td>
</tr>
<tr>
<td>Sip-etag</td>
</tr>
<tr>
<td>Server</td>
</tr>
<tr>
<td>Unsupported</td>
</tr>
</tbody>
</table>

Unsupported Headers

You can configure Cisco Unified Border Element (Cisco UBE) to pass through unsupported headers (headers Cisco UBE cannot understand). The following are some of the examples for SIP headers that are unsupported on Unified Border Elements:

- P-Early-Media
- SIP-Req-URI
Support for Content-Types

Cisco Unified Border Element consumes, interprets and re-originate the supported Content-Type values as required. The following are the Content-Type values supported by Unified Border Element:

- application/sdp
- application/qsig
- application/media-control+xml
- application/x-q931
- application/gtd
- application/simple-message-summary
- application/kpml-response+xml
- application/dtmf-relay
- application/broadsoft
- message/sipfrag
- audio/telephone-event
- multipart/mixed

Unsupported Content-Type Values

The following are some of the Content-Type values that are not supported (unknown) by Unified Border Element.

- Content-Type: application
  - application/isup (SIP-T)
  - application/xml
  - application/xml-dtd
  - application/xhtml+xml
  - application/isup
  - application/dialog-info+xml
  - application/mpeg4-iod
  - application/conference-info+xml
  - application/kpml-request+xml
  - application/resource-lists+xml
  - application/policy-caps+xml
  - application/session-policy+xml
• application/sip

• Content-Type: text
  • text/plain
  • text/html
  • text/xml
  • text/xml-external-parsed-entity

• Content-Type: multipart (with required parameter “boundary”)
  • multipart/signed
  • multipart/encrypted
  • multipart/mixed/SDP + q931 + text
  • multipart/alternative
  • multipart/parallel
  • multipart/related

• Content-Type: image
  • image/jpeg
  • image/jpeg
  • image/gif
  • image/jp2
  • image/jpm
  • image/jpx

• Content-Type: video
  • video/mpeg
  • video/DV
  • video/h264
  • video/mp4

• Content-Type: audio
  • audio/basic
  • audio/mpeg
  • audio/DV
  • audio/3gpp
  • audio/AMR
How to Configure Configurable Pass-Through of SIP INVITE Parameters

Enabling Configurable Pass-Through of SIP INVITE Parameters (Global Level)

Perform this task to configure unsupported content pass-through on a Cisco UBE platform at the global level.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `voice service voip`
4. `sip`
5. `pass-thru {content {sdp | unsupp} | headers {unsupp | list-tag}}`
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> Device&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> Device# 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> Device(config)# voice service voip</td>
<td></td>
</tr>
</tbody>
</table>
Enabling Configurable Pass-Through of SIP INVITE Parameters (Dial Peer Level)

Perform this task to configure unsupported content pass-through on a Cisco UBE platform at the dial-peer level.

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. end

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: Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# 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:</td>
<td></td>
</tr>
</tbody>
</table>
# Configuring a Route String Header Pass-Through Using Pass-Through List

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice class sip-hdr-passthru list-tag**
4. **passthru-hdr header-name**
5. **passthru-hdr-un supp**
6. **exit**
7. **dial-peer voice tag voip**
8. **description string**
9. **session protocol sipv2**
10. **voice-class sip pass-thru headers list-tag**
11. **end**

## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**
  - enable
  - **Example:**
    - Device> enable
| Enables privileged EXEC mode.  
  * Enter your password if prompted. |
| **Step 2**
  - configure terminal
  - **Example:**
    - Device# configure terminal |
<p>| Enters global configuration mode. |</p>
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td><code>voice class sip-hdr-passthru-list list-tag</code> <strong>Example:</strong>&lt;br&gt;Device(config)# voice class sip-hdr-passthru-list 101</td>
<td>Configures list of headers to be passed through and enters voice class configuration mode.</td>
</tr>
<tr>
<td>4</td>
<td><code>passthru-hdr header-name</code> <strong>Example:</strong>&lt;br&gt;Device(config-class)# passthru-hdr Resource-Priority</td>
<td>Adds header name to the list of headers to be passed through. Repeat this step for every non-mandatory header.</td>
</tr>
<tr>
<td>5</td>
<td><code>passthru-hdr-unsupp</code> <strong>Example:</strong>&lt;br&gt;Device(config-class)# passthru-hdr-unsupp</td>
<td>Adds the unsupported headers to the list of headers to be passed through.</td>
</tr>
<tr>
<td>6</td>
<td><code>exit</code> <strong>Example:</strong>&lt;br&gt;Device(config-class)# exit</td>
<td>Exits the current configuration session and returns to global configuration mode.</td>
</tr>
<tr>
<td>7</td>
<td><code>dial-peer voice tag voip</code> <strong>Example:</strong>&lt;br&gt;Device(config)# dial-peer voice 1 voip</td>
<td>Enters dial peer voice configuration mode.</td>
</tr>
<tr>
<td>8</td>
<td><code>description string</code> <strong>Example:</strong>&lt;br&gt;Device(config-dial-peer)# description inbound-dialpeer</td>
<td>Adds descriptive information about the dial peer.</td>
</tr>
<tr>
<td>9</td>
<td><code>session protocol sipv2</code> <strong>Example:</strong>&lt;br&gt;Device(config-dial-peer)# session protocol sipv2</td>
<td>Configures the IETF Session Initiation Protocol (SIP) for the dial peer.</td>
</tr>
<tr>
<td>10</td>
<td><code>voice-class sip pass-thru headers list-tag</code> <strong>Example:</strong>&lt;br&gt;Device(config-dial-peer)# voice-class sip pass-thru headers 101</td>
<td>Enables call routing based on the destination route string for a dial peer.</td>
</tr>
<tr>
<td>11</td>
<td><code>end</code> <strong>Example:</strong>&lt;br&gt;Device(config-dial-peer)# end</td>
<td>Exits the current configuration mode and returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
Configuration Examples for Configurable Pass-Through of SIP INVITE Parameters

Example: Enabling Configurable Pass-Through of SIP INVITE Parameters (Global Level)

```
Device> enable
Device# configure terminal
Device(config)# voice service voip
Device(conf-voi-serv)# sip
Device(conf-serv-sip)# pass-thru content unsupp
Device(conf-serv-sip)# end
```

Example: Enabling Configurable Pass-Through of SIP INVITE Parameters (Dial Peer Level)

```
Device> enable
Device# configure terminal
Device(config)# dial-peer voice 2 voip
Device(config-dial-peer)# voice-class sip pass-thru content sdp
Device(config-dial-peer)# end
```

Example: Configuring a Route String Header Pass-Through Using Pass-Through List

```
Device> enable
Device# configure terminal
Device(config)# voice class sip-hdr-passthru list 101
Device(config-class)# passthru-hdr X-hdr-1
Device(config-class)# passthru-hdr Resource-Priority
Device(config-class)# passthru-hdr unsupp
Device(config-class)# exit
Device(config)# dial-peer voice 1 voip
Device(config-dial-peer)# description inbound-dialpeer
Device(config-dial-peer)# session protocol sipv2
Device(config-dial-peer)# voice-class sip pass-thru headers 101
Device(config-dial-peer)# end
```
Additional References for Configurable Pass-Through of SIP INVITE Parameters

### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice commands</td>
<td>Cisco IOS Voice Command Reference</td>
</tr>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Command List, All Releases</td>
</tr>
<tr>
<td>SIP configuration tasks</td>
<td>SIP Configuration Guide, Cisco IOS Release 15M&amp;T</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</td>
<td><a href="http://www.cisco.com/support">http://www.cisco.com/support</a></td>
</tr>
<tr>
<td>documentation and tools for troubleshooting and resolving technical issues</td>
<td></td>
</tr>
<tr>
<td>with Cisco products and technologies.</td>
<td></td>
</tr>
<tr>
<td>To receive security and technical information about your products, you can</td>
<td></td>
</tr>
<tr>
<td>subscribe to various services, such as the Product Alert Tool (accessed from</td>
<td></td>
</tr>
<tr>
<td>Field Notices), the Cisco Technical Services Newsletter, and Really Simple</td>
<td></td>
</tr>
<tr>
<td>Syndication (RSS) Feeds.</td>
<td></td>
</tr>
<tr>
<td>Access to most tools on the Cisco Support website requires a Cisco.com user</td>
<td></td>
</tr>
<tr>
<td>ID and password.</td>
<td></td>
</tr>
</tbody>
</table>

### Feature Information for Configurable Pass-Through of SIP INVITE Parameters

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
</table>
| Configurable Unsupported Header using Pass-Through List | Cisco IOS XE Release 3.11S | This feature extends the Pass-Through List functionality to specify the pass-through of unsupported headers as well. The following command was introduced: `passthru-hdr-un supp`.
### Feature Information for Configurable Pass-Through of SIP INVITE Parameters

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configurable Route-String Header Pass-Through using a Pass Through List</td>
<td>Cisco IOS XE Release 3.10S</td>
<td>This feature enables the Cisco UBE to pass through end-to-end headers that are not processed or understood in a SIP trunk to SIP trunk scenario by specifying the headers to be passed through in a pass through list. The pass through functionality will includes only the configured list of non-mandatory SIP headers. The following commands were introduced or modified: <code>passthru-hdr</code>, <code>voice class sip-hdr-passthrulist</code>.</td>
</tr>
<tr>
<td>Configurable Pass-Through of SIP INVITE Parameters</td>
<td>Cisco IOS XE Release 3.1S</td>
<td>This feature enables the Cisco UBE to pass through end-to-end headers that are not processed or understood in a SIP trunk to SIP trunk scenario. The pass through functionality includes all or only a configured list of unsupported or non-mandatory SIP headers, and all unsupported content/MIME types. The following commands were introduced or modified: <code>pass-thru</code> and <code>voice-class sip pass-thru</code>.</td>
</tr>
</tbody>
</table>
Dynamic Refer Handling

When a dial-peer match occurs, CUBE passes the REFER message from an in leg to an out leg. Also, the host part of the Refer-to header is modified with the IP address.

The Dynamic REFER handling feature provides configurations to pass across or consume the REFER message. When an endpoint invokes a supplementary service such as a call transfer, the endpoint generates and sends an in-dialog REFER request towards the Cisco UBE. If the REFER message is consumed, an INVITE is sent towards refer-to dial-peer

- Feature Information for Dynamic REFER Handling, on page 143
- Prerequisites, on page 144
- Restrictions, on page 144
- Configuring REFER Passthrough with Unmodified Refer-to, on page 144
- Configuring REFER Consumption, on page 146
- Troubleshooting Tips, on page 148

Feature Information for Dynamic REFER Handling

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 38: Feature Information for Dynamic REFER Handling

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>REFER Consume (Enhancements)</td>
<td>IOS 15.5(1)T</td>
<td>REFER Consume (Enhancements) provides additional configurations to conditionally forward the REFER message.</td>
</tr>
<tr>
<td></td>
<td>IOS XE 3.14.0 S</td>
<td>The following commands were introduced: refer consume.</td>
</tr>
</tbody>
</table>
Feature Information

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamic REFER Handling</td>
<td>IOS 15.2(1)T</td>
<td>The Dynamic REFER handling feature provides configurations to pass across or consume the REFER message. The following commands were introduced: refer-to-passing, voice-class sip refer-to-passing.</td>
</tr>
<tr>
<td></td>
<td>IOS XE Release 3.7S</td>
<td></td>
</tr>
</tbody>
</table>

Prerequisites

- Transcoding configuration is required on the CUBE for midcall transcoder insertion, deletion, or modification during call transfers.

Restrictions

- Only Session Initiation Protocol (SIP)-to-SIP call transfers are supported.
- Call escalation and de-escalation are not supported.
- Video transcoding is not supported.
- Session Description Protocol (SDP) pass-through is not supported.
- In REFER consume scenario, if TCL script is enabled, then supplementary-service media-renegotiate command should not be configured.

Configuring REFER Passthrough with Unmodified Refer-to

This task configures the passthrough of REFER message from the in leg to the out leg on a dial-peer match. A REFER is sent towards inbound dial peer. This task also ensures that the host part of the Refer-to header is unmodified and not changed to the IP address during passthrough.

<table>
<thead>
<tr>
<th>supplementary service refer</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>yes</td>
<td>REFER is passed through from the in leg to the out leg</td>
</tr>
<tr>
<td>no</td>
<td>INVITE is sent towards refer-to dial-peer</td>
</tr>
</tbody>
</table>

Note

This configurations in this task can be overridden by the refer consume command. Refer to the Configuring REFER Consumption task for more information.
SUMMARY STEPS

1. enable
2. configure terminal
3. Configure REFER passthrough:
   - supplementary-service sip refer in global VoIP configuration mode.
   - supplementary-service sip refer in dial-peer configuration mode.
4. (Optional) Configure unmodified Refer-to:
   - refer-to-passing in Global VoIP SIP configuration mode.
   - voice-class sip refer-to-passing [system] in dial-peer configuration mode.
5. 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></td>
</tr>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>Configure REFER passthrough:</td>
<td>Configures REFER passthrough. A REFER is sent towards the inbound dial peer</td>
</tr>
<tr>
<td>• supplementary-service sip refer</td>
<td>in global VoIP configuration mode.</td>
</tr>
<tr>
<td>• supplementary-service sip refer</td>
<td>in dial-peer configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>In Global VoIP configuration mode:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# voice service voip</td>
<td></td>
</tr>
<tr>
<td>Device(config-voi-serv)# supplementary-service sip refer</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>In dial-peer configuration mode:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# dial-peer voice 22 voip</td>
<td></td>
</tr>
<tr>
<td>Device(config-dial-peer)# supplementary-service sip refer</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>(Optional) Configure unmodified Refer-to:</td>
<td>Ensures that the refer-to header is unmodified and not changed to the IP address during passthrough</td>
</tr>
<tr>
<td>• refer-to-passing</td>
<td>in Global VoIP SIP configuration mode.</td>
</tr>
</tbody>
</table>
### Configuring REFER Consumption

This task configures the consumption of REFER message on a dial-peer match. An INVITE is sent towards the Refer-to dial peer.

#### Table 39: Configurations for REFER Consumption

<table>
<thead>
<tr>
<th>supplementary service refer</th>
<th>refer consume</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>yes</td>
<td>no</td>
<td>REFER is sent towards inbound dial-peer</td>
</tr>
<tr>
<td>yes</td>
<td>yes</td>
<td>INVITE is sent towards refer-to dial-peer</td>
</tr>
<tr>
<td>no</td>
<td>no</td>
<td>INVITE is sent towards refer-to dial-peer</td>
</tr>
<tr>
<td>no</td>
<td>yes</td>
<td>INVITE is sent towards refer-to dial-peer</td>
</tr>
</tbody>
</table>

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Enter one of the following:
   - no supplementary-service sip refer in global VoIP configuration mode.
   - no supplementary-service sip refer in dial-peer configuration mode.
4. **refer consume** in global VoIP configuration mode.
5. (Optional) **supplementary-service media-renegotiate** in global VoIP configuration mode.
6. (Optional) Enter one of the following:
   - xfer target in global VoIP configuration mode.
   - xfer target in voice class tenant configuration mode.
### 7. Dynamic Refer Handling

#### Configuring REFER Consumption

<table>
<thead>
<tr>
<th>DETAILED STEPS</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><em>enable</em></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><em>enable</em></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td><em>Device</em> &gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><em>configure terminal</em></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><em>Device</em> # configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Enter one of the following:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <em>no supplementary-service sip refer</em> in global VoIP configuration mode.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <em>no supplementary-service sip refer</em> in dial-peer configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>In global VoIP configuration mode:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>Device</em>{config)# voice service voip</td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>Device</em>{conf-voi-serv)# no supplementary-service sip refer</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>In dial-peer configuration mode:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>Device</em>{config)# dial-peer voice 22 voip</td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>Device</em>{config-dial-peer)# no supplementary-service sip refer</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><em>refer consume</em> in global VoIP configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>In dial-peer configuration mode:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>Device</em>{config)# dial-peer voice 22 voip</td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>Device</em>{config-dial-peer)# refer consume</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><em>(Optional) supplementary-service media-renegotiate</em> in global VoIP configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>In global VoIP configuration mode:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>Device</em>{config)# voice service voip</td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>Device</em>{conf-voi-serv)# supplementary-service media-renegotiate</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>(Optional) Enter one of the following:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <code>xfer target</code> in global VoIP configuration mode.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <code>xfer target</code> in voice class tenant configuration mode.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>To route the INVITE to refer-to host address.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>In global VoIP configuration mode:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>router(config)#sip-ua</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>router(config-sip-ua)#xfer target refer-to</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>In voice class tenant configuration mode:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config)#voice class tenant 1</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config-class)#xfer target refer-to</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><code>end</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Exits to privileged EXEC mode.</td>
<td></td>
</tr>
</tbody>
</table>

**Troubleshooting Tips**

Use any of the following debug commands:

• `debug ccsip all`
• `debug voip ccapi inout`
• `debug sccp messages`
• `debug voip application supplementary-service`
• `debug voip application state`
• `debug voip application media negotiation`
Transparent Tunneling of QSIG and Q.931

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.

- Finding Feature Information, on page 149
- Prerequisites for Transparent Tunneling of QSIG and Q.931, on page 150
- Restrictions for Transparent Tunneling of QSIG and Q.931, on page 150
- Information About Transparent Tunneling of QSIG or Q.931, on page 150
- How to Transparently Tunnel QSIG over SIP, on page 153
- Configuration Examples for Transparent Tunneling of QSIG, on page 157
- Feature Information for Transparent Tunneling of QSIG and Q.931, on page 158

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to https://cfnng.cisco.com/. An account on Cisco.com is not required.
Prerequisites for Transparent Tunneling of QSIG and Q.931

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 for Transparent Tunneling of QSIG and Q.931

- 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

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

Transparently 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 the figure below).

Figure 5: Tunneling QSIG (or Q.931) Messages Across a SIP Trunk

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 the figure below).

Figure 6: Tunneling QSIG (or Q.931) Messages Through a SIP-SIP Cisco Unified Border Element

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 18x response with tunneled content--identifies the QSIG message (FACILITY, ALERTING, or PROGRESS) and sends a corresponding ISDN message.
- OGW receives 3xx, 4xx, 5xx, or 6xx 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.

Note

You should expect a SIP 415 final response message (Unsupported MediaType) 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.

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.
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.

<table>
<thead>
<tr>
<th>QSIG Message Element</th>
<th>Corresponding SIP Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>FACILITY/NOTIFY/INFO</td>
<td>SIP INFO</td>
</tr>
<tr>
<td>SETUP</td>
<td>SIP INVITE</td>
</tr>
<tr>
<td>ALERTING</td>
<td>SIP 180 RINGING</td>
</tr>
<tr>
<td>PROGRESS</td>
<td>SIP 183 PROGRESS</td>
</tr>
<tr>
<td>CONNECT</td>
<td>SIP 200 OK</td>
</tr>
<tr>
<td>DISCONNECT</td>
<td>SIP BYE/CANCEL/4xx --6xx Response</td>
</tr>
</tbody>
</table>

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.

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.
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, on page 155).

**Before you begin**

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. Do one of the following:
   - **signaling forward** *message-type*

**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> voice service voip</td>
<td>Enters voice-service configuration mode and specifies a voice-encapsulation type globally.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Router(config)# voice service voip</td>
<td>Enables tunneling of QSIG raw messages (application-qsig) only.</td>
</tr>
</tbody>
</table>

**Step 4**

Do one of the following:

- `signaling forward message-type`

**Example:**

Router(conf-voi-serv)# signaling forward rawmsg

**Example:**

Router(conf-voi-serv)# signaling forward unconditional

---

**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 (see the Feature Information for Transparent Tunneling of QSIG and Q.931, on page 158).

---

**Before you begin**

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. Do one of the following:
   - `signaling forward message-type`

**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><strong>Example:</strong></td>
<td>Enters privileged EXEC mode.</td>
</tr>
<tr>
<td>Router&gt; enable</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><strong>Example:</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>dial-peer voice number voip</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Enters voice-service configuration mode and specifies a 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></td>
<td>Do one of the following:</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Enables tunneling of QSIG raw messages (application-qsig) only.</td>
</tr>
<tr>
<td>Router(config-dial-peer)# signaling forward rawmsg</td>
<td>or</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Enables tunneling of all QSIG message bodies unconditionally.</td>
</tr>
<tr>
<td>Router(config-dial-peer)# signaling forward unconditional</td>
<td></td>
</tr>
</tbody>
</table>
Configuration Examples for Transparent Tunneling of QSIG

Tunneling QSIG Raw Messages over SIP 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
    rel1xx require "100rel"
```

Tunneling QSIG Messages Unconditionally over SIP 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
    rel1xx require "100rel"
```

Tunneling QSIG Raw Messages over SIP on an 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 the figure below):

*Figure 7: Tunneling of Only QSIG Raw Messages over a SIP Trunk (Interface-Level)*

![Diagram showing QSIG raw messages tunneling over a SIP trunk]

Configuration for OGW (172.24.2.15) Tunneling only QSIG Raw Messages

```plaintext
dial-peer voice 7777 voip
description OGW-OUT-TGW
  destination-pattern 222
  signaling forward rawmsg
  session protocol sipv2
```
Tunneling QSIG Messages Unconditionally over SIP on an Interface Example

The following example shows how to configure transparent tunneling of QSIG messages unconditionally over a gateway interface in a SIP network (see the figure below):

*Figure 8: Tunneling of QSIG Messages Unconditionally over a SIP Trunk (Interface-Level)*

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

Feature Information for Transparent Tunneling of QSIG and Q.931

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.
Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

History Table for the Cisco Unifired Border Element

Table 40: Feature Information for Transparent Tunneling of QSIG and Q.931 over SIP TDM Gateway and SIP-SIP Cisco Unified Border Element

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transparent Tunneling of QSIG and Q.931 over SIP TDM Gateway and SIP-SIP</td>
<td>12.4(15)XZ</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.</td>
</tr>
<tr>
<td>Cisco Unified Border Element</td>
<td>12.4(20)T</td>
<td>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>
</tbody>
</table>

History Table for the Cisco Unifired Border Element (Enterprise)

Table 41: Feature Information for Transparent Tunneling of QSIG and Q.931 over SIP TDM Gateway and SIP-SIP Cisco Unified Border Element

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transparent Tunneling of QSIG and Q.931 over SIP TDM Gateway and SIP-SIP</td>
<td>Cisco IOS XE</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.</td>
</tr>
<tr>
<td>Cisco Unified Border Element</td>
<td>Release 3.1S</td>
<td>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>
</tbody>
</table>
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.

- Finding Feature Information, on page 161
- Prerequisites for SIP Diversion Header Enhancements, on page 161
- Information about SIP Diversion Header Enhancements, on page 162
- How to Configure SIP Diversion Header Enhancements, on page 162
- Feature Information for SIP Diversion Header Enhancements, on page 163

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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

Prerequisites for SIP Diversion Header Enhancements

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 at the following URL: http://www.cisco.com/en/US/docs/ios/voice/command/reference/vr_book.html

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><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router&gt; enable</code></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
</tr>
</tbody>
</table>
| Step 2 | configure terminal  
**Example:**  
Router# configure terminal | Enters global configuration mode. |
| Step 3 | sip-ua  
**Example:**  
Router(config)# sip-ua | Enters SIP User Agent configuration mode. |
| Step 4 | registrar registrar-server-address  
**Example:**  
Router(config-sip-us)# registrar ipv4:10.1.1.1 | The SIP registrar server address to be used for endpoint registration. This value can be entered in one of three formats:  
- **dns**: *address* --the Domain Name System (DNS) address of the primary SIP registrar server (the **dns**: delimiter must be included as the first four characters).  
- **ipv4**: *address* --the IP address of the SIP registrar server (the **ipv4**: delimiter must be included as the first five characters).  
- **ipv6:** *address* --the IPv6 address of the SIP registrar server (the **ipv6**: delimiter must be included as the first five characters and the address itself must include opening and closing square brackets). |
| Step 5 | host-registrar  
**Example:**  
Router(config-sip-ua)# host-registrar | 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. |

### Feature Information for SIP Diversion Header Enhancements

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Feature History Table entry for the Cisco Unified Border Element.
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: `host-registrar`, and `registrar`.

Table 43: Feature Information for SIP Diversion Header Enhancements

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP Diversion Header</td>
<td>Cisco IOS XE</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>Enhancements</td>
<td>Release 3.1S</td>
<td></td>
</tr>
</tbody>
</table>
CHAPTER 22

SIP History INFO

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

- Finding Feature Information, on page 165
- Prerequisites, on page 165
- Configuring SIP History INFO, on page 166
- Feature Information for SIP History-info Header, on page 166

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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

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 3.1 or a later release must be installed and running on your Cisco ASR 1000 Series Router.
**Configuring SIP History INFO**

To configure the SIP History INFO feature, see the Configuring SIP History-info Header Support section of the "Cisco IOS SIP Configuration Guide, Release 15.1" at the following URL:

**Feature Information for SIP History-info Header**

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Feature History Table entry for the Cisco Unified Border Element.

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP History-info Header</td>
<td>12.4(22)T</td>
<td>The SIP History-info feature provides the capability for the SIP TDM gateway to generate History-info messages in the INVITE dialog for calls that are forwarded or transferred. Cisco Unified Border Element platforms transparently pass the History-info across SIP legs. The receiving application uses the history-info header information to determine how and why the call has reached it. The following commands were introduced or modified: <strong>history-info</strong> and <strong>voice-class sip history-info</strong></td>
</tr>
</tbody>
</table>

Feature History Table entry for the Cisco Unified Border Element (Enterprise).

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP History-info Header</td>
<td>Cisco IOS XE Release 3.1S</td>
<td>The SIP History-info feature provides the capability for the SIP TDM gateway to generate History-info messages in the INVITE dialog for calls that are forwarded or transferred. Cisco Unified Border Element platforms transparently pass the History-info across SIP legs. The receiving application uses the history-info header information to determine how and why the call has reached it. The following commands were introduced or modified: <strong>history-info</strong> and <strong>voice-class sip history-info</strong>.</td>
</tr>
</tbody>
</table>
CHAPTER 23

Hiding the Internal Topology Information Embedded Within the History-info Header at the Cisco UBE

SIP History-info stores information on address, topology and so on. Cisco UBE has the address hiding security feature where only the host section of a History-Info header is masked with the CUBE address. However, it does not hide the topology information like the details of the targets where a request was tried upon. It is important to strip the topology information from Cisco UBE before it is passed on to an external device. When the topology hiding for history-info is enabled, the diversion headers are also stripped from the history-info header. Topology information hiding has to be enabled on both inbound and outbound call legs. For example, if topology information is enabled only on the outbound dial-peer, this results in stripping all the History-info headers it received from the inbound leg and it sends just the single History-info header. However, on the inbound leg, all the History-info headers received from the outbound leg will be passed on to the external devices. If this feature is enabled on both inbound and outbound dialpeers, then the History-info headers will be stripped for both inbound and outbound legs of Cisco UBE.

- Finding Feature Information, on page 167
- Restrictions for Hiding the Internal Topology Information, on page 167
- Hiding Internal Toplogy Information in History-info Header at global level, on page 168
- Hiding Internal Toplogy Information in History-info Header at the Dial-Peer Level, on page 169
- Feature Information for Hiding Internal Topology in the History-info Header, on page 170

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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

Restrictions for Hiding the Internal Topology Information

- The user needs to be in the same network as the network in which the call is received.
Topology hiding will result in the History-Info headers received on one call leg to be stripped on the other leg and this could result in the call-routing functionality to disfunction. Hence, topology hiding and call-routing are mutually exclusive and cannot function together.

Hiding Internal Topology Information in History-info Header at global level

Perform this task to hide topology information in history-info header 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. privacy policy strip diversion
6. privacy policy strip history-info
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>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></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> privacy policy strip diversion</td>
<td>Strips the diversion headers received from the next call leg</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
</tbody>
</table>
Hiding Internal Topology Information in History-info Header at the Dial-Peer Level

Perform this task to hide topology information in history-info header support 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 privacy policy strip diversion
5. voice class sip privacy policy strip history-info
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: 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:</td>
<td></td>
</tr>
</tbody>
</table>
**Command or Action**

Router(config)# dial-peer voice 2 voip

**Purpose**

Sripsthediversionheadersreceivedfromthenextcallleg.

**Step 4**

voice class sip privacy policy strip diversion

Example:

Router(config-dial-peer)# voice-class sip
call-route history-info

**Step 5**

voice class sip privacy policy strip history-info

Example:

Router(conf-serv-sip)# privacy policy strip
history-info

**Step 6**

exit

Example:

Router(config-dial-peer)# exit

---

**Feature Information for Hiding Internal Topology in the History-info Header**

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Feature History table for the ISR

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hiding the Internal Topology Information Embedded Within the History-info Header at the Cisco UBE</td>
<td>15.1(2)T</td>
<td>This feature enables privacy across the enterprise domain by hiding internal topology information by stripping topology information from the history-info header. The following command was introduced or modified: <code>privacy policy, voice class sip privacy policy</code>.</td>
</tr>
</tbody>
</table>

Feature History table for the ASR
Table 47: Feature Information for Hiding Internal Topology in the History-info Header

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hiding the Internal Topology Information Embedded Within the History-info Header at the Cisco UBE</td>
<td>Cisco IOS XE Release 3.3S</td>
<td>This feature enables privacy across the enterprise domain by hiding internal topology information by stripping topology information from the history-info header. The following command was introduced or modified: privacy policy, voice class sip privacy policy.</td>
</tr>
</tbody>
</table>
Feature Information for Hiding Internal Topology in the History-info Header
Configuring Call Routing logic on Cisco UBE using the History-info Header

The history-info header has the call or dialog history information. The receiving application uses the history-info header information to determine how and why the call has reached it. SIP IOS GW does not utilize this information in History-Info header. The information stored in the History-Info headers can be used to bypass the dial-peers that were already tried during the course of a call, ensuring that the call is not being redirected again to the same target. The called-numbers and host portion of request URI in History-Info headers will be compared with the matching dial-peers, if incase the comparison succeeds, then those dial-peers will be bypassed.

This section contains the following procedures:

- Finding Feature Information, on page 173
- Configuring Call Routing Logic on Cisco UBE using the History-info Header Globally, on page 173
- Configuring all Routing Logic on Cisco UBE using the History-info Header at the Dial-Peer Level, on page 175
- Feature Information for Call Routing logic on Cisco UBE using the History-info Header, on page 176

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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

Configuring Call Routing Logic on Cisco UBE using the History-info Header Globally

Perform this task to configure call routing on history-info header 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. call-route history-info
6. 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>Enters privileged EXEC mode, or other security level set by a system administrator.</td>
</tr>
<tr>
<td>enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router&gt; enable</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td>Example: Router# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Enters voice service VoIP configuration mode.</td>
</tr>
<tr>
<td>voice service voip</td>
<td>Example: Router(config)# voice service voip</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Enters SIP configuration mode.</td>
</tr>
<tr>
<td>sip</td>
<td>Example: Router(conf-voi-serv)# sip</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Configures call-route history-info header support globally.</td>
</tr>
<tr>
<td>call-route history-info</td>
<td>Example: Router(conf-serv-sip)# call-route history-info</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Exits the current mode.</td>
</tr>
<tr>
<td>exit</td>
<td>Example: Router(conf-serv-sip)# exit</td>
</tr>
</tbody>
</table>
Configuring Call Routing logic on Cisco UBE using the History-info Header

Perform this task to configure call routing on history-info header support 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 call-route history-info
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>Example:</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>Example:</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>Example:</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 call-route history-info</td>
<td>Configures call-route history-info header support for a dial peer.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-dial-peer)# voice-class sip call-route history-info</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>
Feature Information for Call Routing logic on Cisco UBE using the History-info Header

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

**Feature History table for the ISR**

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call routing logic on the Cisco Unified Border Element based on the information embedded in the history-info header.</td>
<td>15.1(2)T</td>
<td>The call-routing logic on the Cisco UBE is enhanced by utilizing the information embedded in the history-info header of SIP requests that are retargeted or routed across domains. This is done by utilizing the information in the history-info header to bypass retargeting dial-peer entries that are indicated in the history-info header. The following command was introduced or modified: call-route history-info, voice clas sip call-route history-info.</td>
</tr>
</tbody>
</table>

**Feature History table for the ASR**

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call routing logic on the Cisco Unified Border Element based on the information embedded in the history-info header.</td>
<td>Cisco IOS XE Release 3.3S</td>
<td>The call-routing logic on the Cisco UBE is enhanced by utilizing the information embedded in the history-info header of SIP requests that are retargeted or routed across domains. This is done by utilizing the information in the history-info header to bypass retargeting dial-peer entries that are indicated in the history-info header. The following command was introduced or modified: call-route history-info, voice clas sip call-route history-info.</td>
</tr>
</tbody>
</table>
Configurable SIP Parameters via DHCP

The Configurable SIP Parameters via DHCP feature allows a Dynamic Host Configuration Protocol (DHCP) server to provide Session Initiation Protocol (SIP) parameters via a DHCP client. These parameters are used for user registration and call routing.

The DHCP server returns the SIP Parameters via DHCP options 120 and 125. These options are used to specify the SIP user registration and call routing information. The SIP parameters returned are the SIP server address via Option 120, and vendor-specific information such as the pilot, contract or primary number, an additional range of secondary numbers, and the SIP domain name via Option 125.

In the event of changes to the SIP parameter values, this feature also allows a DHCP message called DHCPFORCERENEW to reset or apply a new set of values.

The SIP parameters provisioned by DHCP are stored, so that on reboot they can be reused.

- Finding Feature Information, on page 177
- Prerequisites for Configurable SIP Parameters via DHCP, on page 177
- Restrictions for Configurable SIP Parameters via DHCP, on page 178
- Information About Configurable SIP Parameters via DHCP, on page 178
- How to Configure SIP Parameters via DHCP, on page 182
- Feature Information for Configurable SIP Parameters via DHCP, on page 189

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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

Prerequisites for Configurable SIP Parameters via DHCP

- A DHCP interface has to be associated with SIP before configurable SIP parameters via DHCP can be enabled.
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 3.17S or a later release must be installed and running on your Cisco ASR 1000 Series Router.

Restrictions for Configurable SIP Parameters via DHCP

- DHCP Option 120 is the standard DHCP option (RFC 3361) to get a SIP server address, and this can be used by any vendor DHCP server. Only one address is supported, which is in the IPv4 address format. Multiple IPv4 address entries are not supported. Also, there is no support for a DNS name in this or for any port number given behind the IPv4 address.

- DHCP Option 125 (RFC 3925) provides vendor-specific information and its interpretation is associated with the enterprise identity. The primary and secondary phone numbers and domain are obtained using Option 125, which is vendor-specific. As long as other customers use the same format as in the Next Generation Network (NGN) DHCP specification, they can use this feature.

- A primary or contract number is required in suboption 202 of DHCP Option 125. There can be only one instance of the primary number and not multiple instances.

- Multiple secondary or numbers in suboption 203 of DHCP Option 125 are supported. Up to five numbers are accepted and the rest ignored. Also, they have to follow the contract number in the DHCP packet data.

- Authentication is not supported for REGISTER and INVITE messages sent from a Cisco Unified Border Element that uses DHCP provisioning.

- The DHCP provisioning of SIP Parameters is supported only over one DHCP interface.

- The DHCP option is available only to be configured for the primary registrar. It will not be available for a secondary registrar.

Information About Configurable SIP Parameters via DHCP

To perform basic Configurable SIP Parameters via DHCP configuration tasks, you should understand the following concepts:

Cisco Unified Border Element Support for Configurable SIP Parameters via DHCP

The Cisco Unified Border Element provides the support for the DHCP provisioning of the SIP parameters. The NGN is modeled using SIP as a VoIP protocol. In order to connect to NGN, the User to Network Interface (UNI) specification is used. Cisco TelePresence Systems (CTS), consisting of an IP Phone, a codec, and Cisco Unified Communications Manager, are required to internetwork over the NGN for point-to-point and point-to-multipoint video calls. Because Cisco Unified Communications Manager does not provide a UNI
interface, there has to be an entity to provide the UNI interface. The Cisco Unified Border Element provides the UNI interface and has several advantages such as demarcation, delayed offer to early offer, and registration. The figure below shows the Cisco Unified Border Element providing the UNI interface for the NGN.

Figure 9: Cisco NGN with Cisco Unified Border Element providing UNI interface

DHCP to Provision SIP Server, Domain Name, and Phone Number

NGN requires Cisco Unified Border Element to support DHCP (RFC 2131 and RFC 2132) to provision the following:

- IP address for Cisco Unified Border Element’s UNI interface facing NGN
- SIP server address using option 120
- Option 125 vendor specific information to get:
  - Pilot number (also called primary or contract number), there is only one pilot number in DHCPACK, and REGISTER is done only for the pilot number
  - Additional numbers, or secondary numbers, are in DHCPACK; there is no REGISTER for additional numbers
  - SIP domain name
- DHCPFORSRERENEW to reset or apply a new set of SIP parameters (RFC 3203)

DHCP-SIP Call Flow

The following scenario shows the DHCP messages involved in provisioning information such as the IP address for UNI interface, and SIP parameters including the SIP server address, phone number, and domain name, along with how SIP messages use the provisioned information.

The figure below shows the DHCP and SIP messages involved in obtaining the SIP parameters and using them for REGISTER and INVITE.
Figure 10: DHCP-SIP Call Flow

DHCP Message Details
The DHCP call flow involved in obtaining Cisco Unified Border Element provision information, including the IP address for UNI interface and SIP information such as phone number, domain, and SIP server, is shown in the figure below.
The DHCP messages involved in provisioning the SIP parameters are described in Steps 1 to 6.

1. **F1**: The Cisco Unified Border Element DHCP client sends a DHCPDISCOVER message to find the available NGN DHCP servers on the network and obtain a valid IPv4 address. The Cisco Unified Border Element DHCP client identity (computer name) and MAC address are included in this message.

2. **F2**: The Cisco Unified Border Element DHCP client receives a DHCPOFFER message from each available NGN DHCP server. The DHCPOFFER message includes the offered DHCP server’s IPv4 address, the DHCP client’s MAC address, and other configuration parameters.

3. **F3**: The Cisco Unified Border Element DHCP client selects an NGN DHCP server and its IPv4 address configuration from the DHCPOFFER messages it receives, and sends a DHCPREQUEST message requesting its usage. Note that this is where Cisco Unified Border Element requests SIP server information via DHCP Option 120 and vendor-identifying information via DHCP Option 125.

4. **F4**: The chosen NGN DHCP server assigns its IPv4 address configuration to the Cisco Unified Border Element DHCP client by sending a DHCPACK message to it. The Cisco Unified Border Element DHCP client receives the DHCPACK message. This is where the SIP server address, phone number and domain name information are received via DHCP options 120 and 125. The Cisco Unified Border Element will use the information for registering the phone number and routing INVITE messages to the given SIP server.
5. F5: When NGN has a change of information or additional information (such as changing SIP server address from 1.1.1.1 to 2.2.2.2) for assigning to Cisco Unified Border Element, the DHCP server initiates DHCPFORCERENEW to the Cisco Unified Border Element. If the authentication is successful, the Cisco Unified Border Element DHCP client accepts the DHCPFORCERENEW and moves to the next stage of sending DHCPREQUEST. Otherwise DHCPFORCERENEW is ignored and the current information is retained and used.

6. F6 and F7: In response to DHCPFORCERENEW, similar to steps F3 and F4, the Cisco Unified Border Element requests DHCP Options 120 and 125. Upon getting the response, SIP will apply these parameters if they are different by sending an UN-REGISTER message for the previous phone number and a REGISTER message for the new number. Similarly, a new domain and SIP server address will be used. If the returned information is the same as the current set, it is ignored and hence registration and call routing remains the same.

# How to Configure SIP Parameters via DHCP

## Configuring the DHCP Client

To receive the SIP configuration parameters the Cisco Unified Border Element has to act as a DHCP client. This is because in the NGN network, a DHCP server pushes the configuration to a DHCP client. Thus the Cisco Unified Border Element must be configured as a DHCP client.

Perform this task to configure the DHCP client.

**Before you begin**

You must configure the `ip dhcp client` commands before entering the `ip address dhcp` command on an interface to ensure that the DHCPDISCOVER messages that are generated contain the correct option values. The `ip dhcp client` commands are checked only when an IP address is acquired from DHCP. If any of the `ip dhcp client` commands are entered after an IP address has been acquired from DHCP, the DHCPDISCOVER messages’ correct options will not be present or take effect until the next time the router acquires an IP address from DHCP. This means that the new configuration will only take effect after either the `ip address dhcp` command or the `release dhcp` and `renew dhcp` EXEC commands have been configured.

### SUMMARY STEPS

1. enable
2. configure terminal
3. interface type number
4. ip dhcp client request sip-server-address
5. ip dhcp client request vendor-identifying-specific
6. ip address dhcp
7. 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>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Example:</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>Configures an interface type and enters interface configuration mode.</td>
</tr>
<tr>
<td>Step 3 interface type number</td>
<td>Configures the DHCP client to request a SIP server address from a DHCP server.</td>
</tr>
<tr>
<td>Example:</td>
<td>Configures the DHCP client to request vendor-specific information from a DHCP server.</td>
</tr>
<tr>
<td>Step 4 ip dhcp client request sip-server-address</td>
<td>Acquires an IP address on the interface from the DHCP.</td>
</tr>
<tr>
<td>Example:</td>
<td>Exit the current mode.</td>
</tr>
</tbody>
</table>

### Configuring the DHCP Client Example

The following is an example of how to enable the DHCP client:

```
Router> enable
Router# configure terminal
Router(config)# interface gigabitethernet 1/1
Router(config-if)# ip dhcp client request sip-server-address
Router(config-if)# ip dhcp client request vendor-identifying-specific
Router(config-if)# ip address dhcp
Router(config-if)# exit
```
Enabling the SIP Configuration

Enabling the SIP configuration allows the Cisco Unified Border Element to use the SIP parameters received via DHCP for user registration and call routing. Perform this task to enable the SIP configuration.

Before you begin

The `dhcp interface` command has to be entered to declare the interface before the `registrar` and `credential` commands are entered.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface type number`
4. `sip-ua`
5. `dhcp interface type number`
6. `registrar dhcp expires seconds random-contact refresh-ratio seconds`
7. `credentials dhcp password [0|7] password realm domain-name`
8. `exit`

### DETAILED STEPS

<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 number</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 gigabitethernet 0/0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> sip-ua</td>
<td>Enters SIP user-agent configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# sip-ua</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> dhcp interface type number</td>
<td>Assigns a specific interface for DHCP provisioning of SIP parameters.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><code>Router(sip-ua)# dhcp interface gigabitethernet 0/0</code></td>
<td>• Multiple interfaces on the CUBE can be configured with DHCP--this command specifies the DHCP interface used with SIP.</td>
</tr>
</tbody>
</table>

**Step 6**

`registrar dhcp expires seconds random-contact refresh-ratio seconds`

**Example:**

```
Router(sip-ua)# registrar dhcp expires 100 random-contact refresh-ratio 90
```

Registers E.164 numbers on behalf of analog telephone voice ports (FXS) and IP phone virtual voice ports (EFXS) with an external SIP proxy or SIP registrar server.

- **expires seconds** --Specifies the default registration time, in seconds. Range is 60 to 65535. Default is 3600.
- **refresh-ratio seconds** --Specifies the refresh-ratio, in seconds. Range is 1 to 100 seconds. Default is 80.

**Step 7**

`credentials dhcp password [0-7] password realm domain-name`

**Example:**

```
Router(sip-ua)# credentials dhcp password cisco realm cisco.com
```

Sends a SIP registration message from a Cisco Unified Border Element in the UP state.

**Step 8**

`exit`

**Example:**

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

Exits the current mode.

### Enabling the SIP Configuration Example

The following is an example of how to enable the SIP configuration:

```
Router> enable
Router# configure terminal
Router(config)# interface gigabitethernet 1/0
Router(config-if)# sip-ua
Router(sip-ua)# dhcp interface gigabitethernet 1/0
Router(sip-ua)# registrar dhcp expires 90 random-contact refresh-ratio 90
Router(sip-ua)# credentials dhcp password cisco realm cisco.com
Router(sip-ua)# exit
```

### Troubleshooting Tips

To display information on DHCP and SIP interaction when SIP parameters are provisioned by DHCP, use the `debug ccsip dhcp` command in privileged EXEC mode.
Configuring a SIP Outbound Proxy Server

An outbound-proxy configuration sets the Layer 3 address (IP address) for any outbound REGISTER and INVITE SIP messages. The SIP server can be configured as an outbound proxy server in voice service SIP configuration mode or dial peer configuration mode. When enabled in voice service SIP configuration mode, all the REGISTER and INVITE messages are forwarded to the configured outbound proxy server. When enabled in dial-peer configuration mode, only the messages hitting the defined dial-peer will be forwarded to the configured outbound proxy server.

The configuration tasks in each mode are presented in the following sections:

Perform either of these tasks to configure the SIP server as a SIP outbound proxy server.

Configuring a SIP Outbound Proxy Server in Voice Service VoIP Configuration Mode

Perform this task to configure the SIP server as a SIP outbound proxy server in voice service SIP configuration mode.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. voice service voip
4. sip
5. outbound-proxy dhcp
6. exit

**DETAILED STEPS**

<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>• Enter your password if prompted.</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 and specifies VoIP as the</td>
</tr>
<tr>
<td>Example:</td>
<td>voice-encapsulation type.</td>
</tr>
<tr>
<td>Router(config)# voice service voip</td>
<td></td>
</tr>
<tr>
<td>Step 4 sip</td>
<td>Enters voice service SIP configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Router(config-voi-srv)# sip</td>
<td>Configures the DHCP client to request a SIP server address from a DHCP server.</td>
</tr>
</tbody>
</table>

**Step 5**

outbound-proxy dhcp

Example:

Router(config-serv-sip)# outbound-proxy dhcp

**Step 6**

exit

Example:

Router(config-serv-sip)# exit

---

### Configuring a SIP Outbound Proxy Server in Voice Service VoIP Configuration Mode Example

The following is an example of how to configure a SIP outbound proxy in voice service SIP configuration mode:

```
Router> enable
Router# configure terminal

Router(config)# voice service voip
Router(config-voi-srv)# sip
Router(config-serv-sip)# outbound-proxy dhcp
Router(config-serv-if)# exit
```

### Configuring a SIP Outbound Proxy Server and Session Target in Dial Peer Configuration Mode

Perform this task to configure the SIP server as a SIP outbound proxy server in dial peer configuration mode.

> SIP must be configured on the dial pier before DHCP is configured. Therefore the `session protocol sipv2` command must be executed before the `session target dhcp` command. DHCP is supported only with SIP configured on the dial peer.

#### SUMMARY STEPS

1. enable
2. configure terminal
3. dial-peer voice number voip
4. session protocol sipv2
5. voice-class sip outbound-proxy dhcp
6. session target dhcp
7. exit

DETAILED STEPS

<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 dial-peer voice number voip</td>
<td>Defines a dial peer, specifies VoIP as the</td>
</tr>
<tr>
<td>Example:</td>
<td>method of voice encapsulation, and enters</td>
</tr>
<tr>
<td>Router(config)# dial-peer voice 10</td>
<td>dial peer configuration mode.</td>
</tr>
<tr>
<td>Step 4 session protocol sipv2</td>
<td>Enters the session protocol type as SIP.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-dial-peer)# session</td>
<td></td>
</tr>
<tr>
<td>Step 5 voice-class sip outbound-proxy dhcp</td>
<td>Configures the SIP server received from the DHCP server as a SIP outbound proxy server.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-dial-peer)# voice-class sip outbound-proxy dhcp</td>
<td></td>
</tr>
<tr>
<td>Step 6 session target dhcp</td>
<td>Specifies that the DHCP protocol is used to</td>
</tr>
<tr>
<td>Example:</td>
<td>determine the IP address of the session</td>
</tr>
<tr>
<td>Router(config-dial-peer)# session</td>
<td>target.</td>
</tr>
<tr>
<td>Step 7 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 a SIP Outbound Proxy Server in Dial Peer Configuration Mode Example

The following is an example of how to configure a SIP outbound proxy in dial peer configuration mode:
The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

### Feature History Table for the ISR.

**Table 50: Feature Information for Configurable SIP Parameters via DHCP**

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configurable SIP Parameters via DHCP</td>
<td>12.4(22)YB 15.0(1)M</td>
<td>The Configurable SIP Parameters via DHCP feature introduces the configuring of SIP parameters via DHCP. The following commands were introduced or modified: credentials (sip-ua), debug ccsip dhcp, dhcp interface, ip dhcp-client forcerenew, outbound-proxy, registrar, session target (VoIP dial peer), show sip dhcp, voice-class sip outbound-proxy.</td>
</tr>
</tbody>
</table>

### Feature History Table for the ASR.

**Table 51: Feature Information for Configurable SIP Parameters via DHCP**

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configurable SIP Parameters via DHCP</td>
<td>IOS XE Release 3.17S</td>
<td>The Configurable SIP Parameters via DHCP feature introduces the configuring of SIP parameters via DHCP. The following commands were introduced or modified: credentials (sip-ua), debug ccsip dhcp, dhcp interface, ip dhcp-client forcerenew, outbound-proxy, registrar, session target (VoIP dial peer), show sip dhcp, voice-class sip outbound-proxy.</td>
</tr>
</tbody>
</table>
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.

- Finding Feature Information, on page 191
- Prerequisites for Multiple Registrars on SIP Trunks, on page 191
- Restrictions for Multiple Registrars on SIP Trunks, on page 192
- Configuring Multiple Registrars on SIP Trunks Feature, on page 192
- Feature Information for the Multiple Registrars on SIP Trunks Feature, on page 192

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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

Prerequisites for Multiple Registrars on SIP Trunks

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 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 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 the Multiple Registrars on SIP Trunks Feature

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Feature History Table entry for the Cisco Unified Border Element.
Table 52: Feature Information for the Multiple Registrars on SIP Trunks Feature

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

Feature History Table entry for the Cisco Unified Border Element (Enterprise).

Table 53: Feature Information for the Multiple Registrars on SIP Trunks Feature

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multiple Registrars on SIP Trunks</td>
<td>Cisco IOS XE Release 3.1S</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>
</tbody>
</table>
CHAPTER 27

Session Refresh with Reinvites

- Finding Feature Information, on page 195
- Prerequisites for Session Refresh with Reinvites, on page 195
- Information about Session Refresh with Reinvites, on page 196
- How to Configure Session Refresh with Reinvites, on page 196
- Feature Information for Session Refresh with Reinvites, on page 197

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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

Prerequisites for Session Refresh with Reinvites

The allow-connections sip to sip command must be configured before you configure the Session refresh with Reinvites feature. For more information and configuration steps see the "Configuring SIP-to-SIP Connections in a Cisco Unified Border Element" section.

Cisco Unified Border Element

- Cisco IOS Release 12.4(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 2.5 or a later release must be installed and running on your Cisco ASR 1000 Series Router.
Information about Session Refresh with Reinvites

Configuring support for session refresh with reinvites expands the ability of the Cisco Unified Border Element to receive a REINVITE message that contains either a session refresh parameter or a change in media via a new SDP and ensure the session does not time out. The midcall-signaling command distinguishes between the way a Cisco Unified Communications Express and Cisco Unified Border Element releases signaling messages. Most SIP-to-SIP video and SIP-to-SIP ReInvite-based supplementary services features require the Configuring Session Refresh with Reinvites feature to be configured.

Cisco IOS Release 12.4(15)XZ and Earlier Releases
Session refresh support via OPTIONS method. For configuration information, see the "Enabling In-Dialog OPTIONS to Monitor Active SIP Sessions" section.

Cisco IOS Release 12.4(15)XZ and Later Releases
Cisco Unified BE transparently passes other session refresh messages and parameters so that UAs and proxies can establish keepalives on a call.

How to Configure Session Refresh with Reinvites

Configuring Session refresh with Reinvites

Before you begin

Note
SIP-to-SIP video calls and SIP-to-SIP ReInvite-based supplementary services fail if the midcall-signaling command is not configured.

Note
The following features function if the midcall-signaling command is not configured: session refresh, fax, and refer-based supplementary services.

• Configuring Session Refresh with Reinvites is for SIP-to-SIP calls only. All other calls (H323-to-SIP, and H323-to-H323) do not require the midcall-signaling command be configured
• Configuring the Session Refresh with Reinvites feature on a dial-peer basis is not supported.

SUMMARY STEPS

1. enable
2. configure terminal
3. voice service voip
4. sip
5. midcall-signaling passthru
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>voice service voip</td>
<td>Enters VoIP voice-service configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config)# voice service voip</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>sip</td>
<td>Enters SIP configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(conf-voi-serv)# sip</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>midcall-signaling passthru</td>
<td>Passes SIP messages from one IP leg to another IP leg.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(conf-serv-sip)# midcall-signaling passthru</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>exit</td>
<td>Exits the current mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(conf-serv-sip)# exit</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(conf-serv-sip) end</td>
<td></td>
</tr>
</tbody>
</table>

### Feature Information for Session Refresh with Reinvites

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.
Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to [www.cisco.com/go/cfn](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

### Feature Information for Session Refresh with Reinvites

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session Refresh with Reinvites</td>
<td>12.4(20)T</td>
<td>Expands the ability of the Cisco Unified BE to control the session refresh parameters and ensure the session does not time out.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>In Cisco IOS Release 12.4(20)T, this feature was implemented on the Cisco Unified Border Element.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>midcall-signaling</strong></td>
</tr>
<tr>
<td>Session Refresh with Reinvites</td>
<td>Cisco IOS XE</td>
<td>Expands the ability of the Cisco Unified BE to control the session refresh parameters and ensure the session does not time out.</td>
</tr>
<tr>
<td></td>
<td>Release 2.5</td>
<td>In Cisco IOS XE Release 2.5, this feature was implemented on the Cisco Unified Border Element (Enterprise).</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>midcall-signaling</strong></td>
</tr>
</tbody>
</table>
CHAPTER 28

V150.1 MER Support in SDP Passthrough Mode

The Cisco V.150.1 Minimum Essential Requirements (MER) feature complies with the requirements of the National Security Agency (NSA) SCIP-216 Minimum Essential Requirements for V.150.1 recommendation, which provides for four states: audio, voice-band data (VBD), modem relay, and T.38. This feature is added in CUBE (IP-to-IP gateway) for V.150.1 calls to traverse a CUBE in SDP passthrough flow-through mode.

• Finding Feature Information, on page 199

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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

Information About VER.150.1 MER Support in SDP Passthrough Mode

V.150.1 MER Support in SDP Passthrough Mode

V.150.1 is an ITU standard for relaying modem or fax transmission that uses state signaling event (SSE) packets to trigger the transition from audio to modem-relay mode or fax-relay mode. The SSE headers are carried in the RTP packet. After call setup, in-band signaling through Simple Packet Relay Transport (SPRT) and SSE messages is used to transition from one state to another. SPRT packets (non-RTP packets) carry the data after the digital signal processor (DSP) transitions into modem relay mode. UDPTL packets carry the data after the DSP transitions into fax-relay mode.

This feature is added in CUBE (IP-to-IP gateway) to support the V.150.1 MER modem relay in SDP passthrough mode. This is of importance when CUBE is in the media path between V.150.1 MER supported gateways and needs to handle non-RTP packets (such as SPRT packets).
How to Configure V.150.1 MER Support for SDP Passthrough

Configuring V.150.1 MER Support for SDP Passthrough

SUMMARY STEPS

1. enable
2. configure terminal
3. Set passthrough SDP mode to non-RTP:
   • voice-class sip pass-thru content sdp mode non-rtp in the dial-peer configuration mode.
   • pass-thru content sdp mode non-rtp in the global VoIP SIP configuration mode.
4. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
V150.1 MER Support in SDP Passthrough Mode

### Purpose

Command or Action | Purpose
--- | ---
Step 3 | Set passthrough SDP mode to non-RTP:

- **voice-class sip pass-thru content sdp mode non-rtp** in the dial-peer configuration mode.
- **pass-thru content sdp mode non-rtp** in the global VoIP SIP configuration mode.

**Example:**

In dial-peer configuration mode

```
!Setting passthrough SDP mode for one dial peer only
Device (config)#dial-peer voice 20 voip
Device (config-dial-peer)#voice-class sip pass-thru
   content sdp mode non-rtp
Device (config-dial-peer)#end
```

**Example:**

In global VoIP SIP mode

```
!Setting passthrough SDP mode globally
Device (config)#voice service voip
Device (config-voi-serv)#sip
Device (config-serv-sip)#pass-thru content sdp mode
   non-rtp
Device (config-serv-sip)#end
```

### Step 4

| Command or Action | Purpose |
--- | --- |
| end | Exits to privileged EXEC mode. |

### Verifying V.150.1 MER Support in SDP Passthrough Mode

**SUMMARY STEPS**

1. enable
2. debug ccsip verbose

**DETAILED STEPS**

#### Step 1

**enable**

**Example:**

```
Device> enable
```

Enables privileged EXEC mode.

#### Step 2

**debug ccsip verbose**

**Example:**

```
Device# debug ccsip verbose

010362: *Jan 31 12:34:00.148: //31/14B4F1000000/SIP/Function/sipSPI_ipip_SetSdpPthruCfg:
```
Feature Information for V.150.1 MER Support for SDP Passthrough

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 54: Feature Information for V.150.1 MER Support for SDP Passthrough

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>V.150.1 MER Support for SDP Passthrough</td>
<td>Cisco IOS XE Release 3.12S</td>
<td>The Cisco V.150.1 Minimum Essential Requirements (MER) feature complies with the requirements of the National Security Agency (NSA) SCIP-216 Minimum Essential Requirements for V.150.1 recommendation, which provides for four states: audio, voice-band data (VBD), modem relay, and T.38. This feature is added in CUBE (IP-IP gateway) for V.150.1 calls to traverse a CUBE in SDP passthrough flow-through mode. The following commands were introduced or modified: pass-thru content sdp mode non-rtp and voice-class sip pass-thru content sdp mode non-rtp</td>
</tr>
</tbody>
</table>
Additional References

The following sections provide references related to the CUBE Configuration Guide.

- Related References, on page 203
- Standards, on page 204
- MIBs, on page 204
- RFCs, on page 204
- Technical Assistance, on page 206

## Related References

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feature Navigator</td>
<td>For information about platforms supported, and Cisco IOS software image support, search by Feature Name listed in Feature Information Table in <a href="http://www.cisco.com/go/cfn">www.cisco.com/go/cfn</a></td>
</tr>
<tr>
<td>Bug Search Tool Kit</td>
<td>For information about latest caveats and feature information, see Bug Search Tool</td>
</tr>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Commands List, All Releases</td>
</tr>
<tr>
<td>Cisco IOS Voice commands</td>
<td><em>Cisco IOS Voice Command Reference</em></td>
</tr>
</tbody>
</table>

- **Related Application Guides**
  - *Cisco Unified Communications Manager and Cisco IOS Interoperability Guide*
  - *Cisco IOS SIP Configuration Guide*
  - *Cisco Unified Communications Manager (CallManager) Programming Guides*
### Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITU-T G.711</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>&quot;RTP: A Transport Protocol for Real-Time Applications&quot;</td>
</tr>
<tr>
<td>RFC 2131</td>
<td>&quot;Dynamic Host Configuration Protocol&quot;</td>
</tr>
<tr>
<td>RFC</td>
<td>Title</td>
</tr>
<tr>
<td>-----------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>RFC 2132</td>
<td>DHCP Options and BOOTP Vendor Extensions</td>
</tr>
<tr>
<td>RFC 2198</td>
<td>RTP Payload for Redundant Audio Data</td>
</tr>
<tr>
<td>RFC 2327</td>
<td>SDP: Session Description Protocol</td>
</tr>
<tr>
<td>RFC 2543</td>
<td>SIP: Session Initiation Protocol</td>
</tr>
<tr>
<td>RFC 2543-bis-04</td>
<td>SIP: Session Initiation Protocol, draft-ietf-sip-rfc2543bis-04.txt</td>
</tr>
<tr>
<td>RFC 2782</td>
<td>A DNS RR for Specifying the Location of Services (DNS SRV)</td>
</tr>
<tr>
<td>RFC 2806</td>
<td>URLs for Telephone Calls</td>
</tr>
<tr>
<td>RFC 2833</td>
<td>RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals</td>
</tr>
<tr>
<td>RFC 3203</td>
<td>DHCP reconfigure extension</td>
</tr>
<tr>
<td>RFC 3261</td>
<td>SIP: Session Initiation Protocol</td>
</tr>
<tr>
<td>RFC 3262</td>
<td>Reliability of Provisional Responses in Session Initiation Protocol (SIP)</td>
</tr>
<tr>
<td>RFC 3323</td>
<td>A Privacy Mechanism for the Session Initiation Protocol (SIP)</td>
</tr>
<tr>
<td>RFC 3325</td>
<td>Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks</td>
</tr>
<tr>
<td>RFC 3515</td>
<td>The Session Initiation Protocol (SIP) Refer Method</td>
</tr>
<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</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>
<tr>
<td>documentation and tools for troubleshooting and resolving technical issues</td>
<td></td>
</tr>
<tr>
<td>with Cisco products and technologies.</td>
<td></td>
</tr>
<tr>
<td>To receive security and technical information about your products, you</td>
<td></td>
</tr>
<tr>
<td>can subscribe to various services, such as the Product Alert Tool (accessed</td>
<td></td>
</tr>
<tr>
<td>from Field Notices), the Cisco Technical Services Newsletter, and Really</td>
<td></td>
</tr>
<tr>
<td>Simple Syndication (RSS) Feeds.</td>
<td></td>
</tr>
<tr>
<td>Access to most tools on the Cisco Support website requires a Cisco.com user</td>
<td></td>
</tr>
<tr>
<td>ID and password.</td>
<td></td>
</tr>
</tbody>
</table>
Glossary

- Glossary, on page 207

Glossary

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.

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, re-writes 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.