Cisco Unified Border Element SIP Support Configuration Guide, Cisco IOS Release 15M&T

Last Modified: 2017-04-14

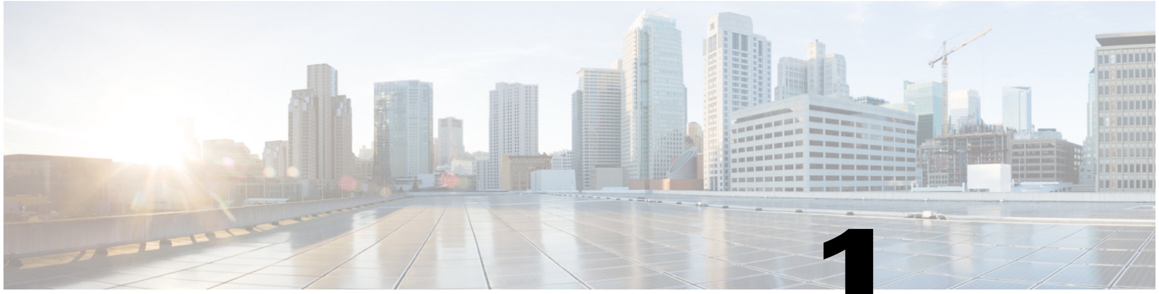
Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

CHAPTER 1

CHAPTER 2

CHAPTER 3



CHAPTER 1

Cisco Unified Border Element SIP Support

This Cisco Unified Border Element is a special Cisco IOS software image that provides a network-to-network interface point for billing, security, call admission control, quality of service, and signaling interworking. This chapter describes basic gateway functionality, software images, topology, and summarizes supported features.

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

Finding Feature Information

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 www.cisco.com/go/cfn. An account on Cisco.com is not required.

Cisco Unified Border Element SIP Support Features

This chapter contains the following configuration topics:

Cisco UBE Prerequisites and Restrictions

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

Basic SIP Set-up

- SIP--Core SIP Technology Enhancements

SIP Parameter Settings

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

SIP Protocol Handling and Supplementary Services

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

SIP Registration and Authentication

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

SIP Normalization

- SIP Parameter Modification

CHAPTER 2

SIP Core SIP Technology Enhancements

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

The enhanced areas are as follows:

SIP URL Comparison

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

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

If a compared parameter is omitted or not present, it is matched on the basis of its default value. The table below shows a list of SIP URL compared parameters and their default values.

Table 1: SIP URL Parameter Comparison

SIP URL Compared Parameter	Default
host	mandatory
password	--
port	5060
user	--
user-param	ip

The following is an example of equivalent URLs:

Original URL:

sip:36602@172.18.193.120

Equivalent URLs:

sip:36602@172.18.193.120:

sip:36602@172.18.193.120;tag=499270-A62;pname=pvalue

sip:36602@172.18.193.120;user=ip

sip:36602@172.18.193.120:5060

487 Sent for BYE Requests

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

3xx Redirection Responses

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

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

See the Examples, on page 11 for a sample call flow that shows the updated CSeq numbers.

DNS SRV Query Procedure

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

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

CANCEL Request Route Header

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

Interpret User Parameters

Telephone-subscriber or user parameters in an incoming INVITE message may contain extra characters to incorporate space, control characters, quotation marks, hash marks, and other characters. The SIP: Core SIP

Technology Enhancements feature allows, the telephone-subscriber or user parameter to be interpreted before dial-peer matching is done. For example, the telephone number in an incoming INVITE message may appear as:

-%32%32%32

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

user=phone Parameter

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

INVITE sip:5550002@companyb.com

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

303 and 411 SIP Cause Codes

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

Flexibility of Content-Type Header

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

Optional SDP s= Line

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

Allow Header Addition to INVITEs and 2xx Responses

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

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 www.cisco.com/go/cfn. An account on Cisco.com is not required.

Simultaneous Cancel and 2xx Class Response

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

Prerequisites for SIP Core SIP Technology Enhancements

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

Cisco Unified Border Element

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

Cisco Unified Border Element (Enterprise)

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

Restrictions for SIP Core SIP Technology Enhancements

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

How to Configure SIP Core SIP Technology Enhancements

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

Monitoring 487 Sent for BYE Requests

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

SUMMARY STEPS

1. **enable**
2. **show sip-ua statistics**

DETAILED STEPS

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

Example

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

```
Router# show sip-ua statistics
SIP Response Statistics (Inbound/Outbound)
    Informational:
      Trying 0/0, Ringing 0/0,
      Forwarded 0/0, Queued 0/0,
      SessionProgress 0/0
    Success:
      OkInvite 0/0, OkBye 0/0,
      OkCancel 0/0, OkOptions 0/0,
      OkPrack 0/0, OkPreconditionMet 0/0,
      OKSubscribe 0/0, OkNotify 0/0,
      202Accepted 0/0
    Redirection (Inbound only):
      MultipleChoice 0, MovedPermanently 0,
      MovedTemporarily 0, UseProxy 0,
      AlternateService 0
    Client Error:
      BadRequest 0/0, Unauthorized 0/0,
      PaymentRequired 0/0, Forbidden 0/0,
      NotFound 0/0, MethodNotAllowed 0/0,
      NotAcceptable 0/0, ProxyAuthReqd 0/0,
      ReqTimeout 0/0, Conflict 0/0, Gone 0/0,
      ReqEntityTooLarge 0/0, ReqURITooLarge 0/0,
      UnsupportedMediaType 0/0, BadExtension 0/0,
      TempNotAvailable 0/0, CallLegNonExistent 0/0,
      LoopDetected 0/0, TooManyHops 0/0,
      AddrIncomplete 0/0, Ambiguous 0/0,
      BusyHere 0/0, RequestCancel 0/1
      NotAcceptableMedia 0/0, BadEvent 0/0
    Server Error:
      InternalError 0/0, NotImplemented 0/0,
      BadGateway 0/0, ServiceUnavail 0/0,
      GatewayTimeout 0/0, BadSipVer 0/0,
      PreCondFailure 0/0
    Global Failure:
      BusyEverywhere 0/0, Decline 0/0,
      NotExistAnywhere 0/0, NotAcceptable 0/0
SIP Total Traffic Statistics (Inbound/Outbound)
    Invite 0/0, Ack 0/0, Bye 0/0,
    Cancel 0/0, Options 0/0,
    Prack 0/0, Comet 0/0,
    Subscribe 0/0, Notify 0/0,
    Refer 0/0
Retry Statistics
    Invite 0, Bye 0, Cancel 0, Response 0,
    Prack 0, Comet 0, Reliable1xx 0, Notify 0
SDP application statistics:
 Parses: 0,  Builds 0
 Invalid token order: 0,  Invalid param: 0
 Not SDP desc: 0,  No resource: 0
```

Monitoring 3xx Redirection Responses

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug ccsip message**	Displays all SIP Service Provider Interface (SPI) message tracing.

	Command or Action	Purpose
	Example: `Router# debug ccsip message`	• Use this command to enable traces for SIP messages exchanged between the SIP user agent client (UAC) and the access server.

Example

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

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

```
Sent:
INVITE sip:3111100@64.102.17.80:5060; SIP/2.0
Via: SIP/2.0/UDP  172.18.193.98:5060
From: "36601" <sip:36601@172.18.193.98> //This header remains consistent throughout the
call.
To: <sip:3111100@64.102.17.80> //This header remains consistent throughout the call.
Date: Mon, 01 Mar 2002 00:50:50 GMT
Call-ID: A22F0DC8-14F511CC-80329792-19DC655A@172.18.193.98 // Header remains consistent.
Cisco-Guid: 2682312529-351605196-2150668178-433874266
User-Agent: Cisco-SIPGateway/IOS-12.x
CSeq: 101 INVITE
Max-Forwards: 6
Timestamp: 730947050
Contact: <sip:36601@172.18.193.98:5060>
Expires: 180
Content-Type: application/sdp
Content-Length: 160
v=0
o=CiscoSystemsSIP-GW-UserAgent 2378 4662 IN IP4 172.18.193.98
s=SIP Call
c=IN IP4 172.18.193.98
t=0 0
m=audio 19202 RTP/AVP 18
a=rtpmap:18 G729/8000
Received:
SIP/2.0 302 Moved Temporarily
Via: SIP/2.0/UDP  172.18.193.98:5060
From: "36601" <sip:36601@172.18.193.98> //This header remains consistent throughout the
call.
To: <sip:3111100@64.102.17.80> //This header remains consistent throughout the call.
Date: Mon, 01 Mar 2002 00:50:50 GMT
Call-ID: A22F0DC8-14F511CC-80329792-19DC655A@172.18.193.98 //Header remains consistent.
Cisco-Guid: 2682312529-351605196-2150668178-433874266
User-Agent: Cisco-SIPGateway/IOS-12.x
CSeq: 101 INVITE
Contact: Anonymous <sip:36602@172.18.193.120 //Provides Request URI with the new contact
address.
Contact: Anonymous <sip:36601@172.18.193.98>
```

```
Sent:
ACK sip:3111100@64.102.17.80:5060; SIP/2.0
Via: SIP/2.0/UDP  172.18.193.98:5060
From: "36601" <sip:36601@172.18.193.98> //This header remains consistent throughout the
call.
To: <sip:3111100@64.102.17.80> //This header remains consistent throughout the call.
Date: Mon, 01 Mar 2002 00:50:50 GMT
Call-ID: A22F0DC8-14F511CC-80329792-19DC655A@172.18.193.98 // Header remains consistent.
Max-Forwards: 6
Content-Length: 0
CSeq: 101 ACK
Sent:
INVITE sip:36602@172.18.193.120:5060 SIP/2.0 //URI updated with new contact/redirect address.
Via: SIP/2.0/UDP  172.18.193.98:5060
From: "36601" <sip:36601@172.18.193.98> //This header remains consistent throughout the
call.
To: <sip:3111100@64.102.17.80> //This header remains consistent throughout the call.
Date: Mon, 01 Mar 2002 00:50:50 GMT
Call-ID: A22F0DC8-14F511CC-80329792-19DC655A@172.18.193.98 // Header remains consistent.
Cisco-Guid: 2682312529-351605196-2150668178-433874266
User-Agent: Cisco-SIPGateway/IOS-12.x
CSeq: 102 INVITE //Transmitted CSeq is increased by one.
Max-Forwards: 6
Timestamp: 730947050
Contact: <sip:36601@172.18.193.98:5060>
Expires: 180
Content-Type: application/sdp
Content-Length: 159
v=0
o=CiscoSystemsSIP-GW-UserAgent 5957 524 IN IP4 172.18.193.98
s=SIP Call
c=IN IP4 172.18.193.98
t=0 0
m=audio 17018 RTP/AVP 18
a=rtpmap:18 G729/8000
```

Monitoring the Deletion of 303 and 411 Cause Codes

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show sip-ua statistics**	Displays response, traffic, and retry statistics for the SIP UA.

	Command or Action	Purpose
	Example: `Router# show sip-ua statistics`	• Can be used to verify the deletion of the 303 and 411 cause codes.
Step 3	**show sip-ua map** **Example:** `Router# show sip-ua map`	Displays the mapping table of PSTN cause codes and their corresponding SIP error status codes or the mapping table of SIP-to-PSTN codes. • Can be used to verify the deletion of 411 cause codes.

Examples

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

- show sip-ua statistics Command, on page 11 command
- show sip-ua map, on page 13 command

show sip-ua statistics Command

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

```
Router# show sip-ua statistics
SIP Response Statistics (Inbound/Outbound)
    Informational:
      Trying 0/4, Ringing 0/0,
      Forwarded 0/0, Queued 0/0,
      SessionProgress 0/5
    Success:
      OkInvite 0/2, OkBye 1/1,
      OkCancel 0/2, OkOptions 0/0,
      OkPrack 0/0, OkPreconditionMet 0/0,
      OkNotify 0/0, 202Accepted 0/0
    Redirection (Inbound only):
      MultipleChoice 0, MovedPermanently 0,
MovedTemporarily 0, SeeOther 0,
      UseProxy 0, AlternateService 0
    Client Error:
      BadRequest 0/0, Unauthorized 0/0,
      PaymentRequired 0/0, Forbidden 0/0,
      NotFound 0/0, MethodNotAllowed 0/0,
      NotAcceptable 0/0, ProxyAuthReqd 0/0,
      ReqTimeout 0/0, Conflict 0/0, Gone 0/0,
      LengthRequired 0/0, ReqEntityTooLarge 0/0,
      ReqURITooLarge 0/0, UnsupportedMediaType 0/0,
      BadExtension 0/0, TempNotAvailable 0/0,
      CallLegNonExistent 0/0, LoopDetected 0/0,
      TooManyHops 0/0, AddrIncomplete 0/0,
      Ambiguous 0/0, BusyHere 0/0
      RequestCancel 0/2, NotAcceptableMedia 0/0
    Server Error:
      InternalError 0/0, NotImplemented 0/0,
      BadGateway 0/0, ServiceUnavail 0/0,
      GatewayTimeout 0/0, BadSipVer 0/0,
      PreCondFailure 0/0
    Global Failure:
      BusyEverywhere 0/0, Decline 0/0,
      NotExistAnywhere 0/0, NotAcceptable 0/0
SIP Total Traffic Statistics (Inbound/Outbound)
    Invite 5/0, Ack 4/0, Bye 1/1,
    Cancel 2/0, Options 0/0,
    Prack 0/0, Comet 0/0,
    Notify 0/0, Refer 0/0
Retry Statistics
    Invite 0, Bye 0, Cancel 0, Response 0,
    Prack 0, Comet 0, Reliable1xx 0, Notify 0
```

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

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

show sip-ua map

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

```
Router# show sip-ua map sip-pstn
SIP-Status   Configured      Default
             PSTN-Cause      PSTN-Cause
400          127             127
401           57             57
402           21             21
403           57             57
404           1              1
405           127            127
406           127            127
407           21             21
408           102            102
409           41             41
410           1              1
413           127            127
414           127            127
415           79             79
420           127            127
480           18             18
481           127            127
482           127            127
483           127            1
```

Configuration Examples for SIP Core SIP Technology Enhancements

This section provides a general SIP configuration example:

- SIP Core SIP Technology Enhancements Example, on page 13

SIP Core SIP Technology Enhancements Example

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

```
Router# show running-config
Building configuration...
Current configuration : 2791 bytes
!
version 12.2
service config
no service single-slot-reload-enable
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service internal
service udp-small-servers
!
interface FastEthernet2/0
ip address 172.18.200.24 255.255.255.0
duplex auto
no shut
speed 10
```

```
ip rsvp bandwidth 7500 7500
!
voice-port 1/1/1
no supervisory disconnect lcfo
!
dial-peer voice 1 pots
application session
destination-pattern 5550111
port 1/1/1
!
dial-peer voice 3 voip
application session
destination-pattern 5550112
session protocol sipv2
session target ipv4:172.18.200.36
codec g711ulaw
!
dial-peer voice 4 voip
application session
destination-pattern 5550133
session protocol sipv2
session target ipv4:172.18.200.33
codec g711ulaw
!
gateway
!
sip-ua
   retry invite 1
   retry bye 1
!
line con 0
line aux 0
line vty 0 4
login
!
end
```

Feature Information for SIP Core SIP Technology 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. An account on Cisco.com is not required. ISR Feature History Information.

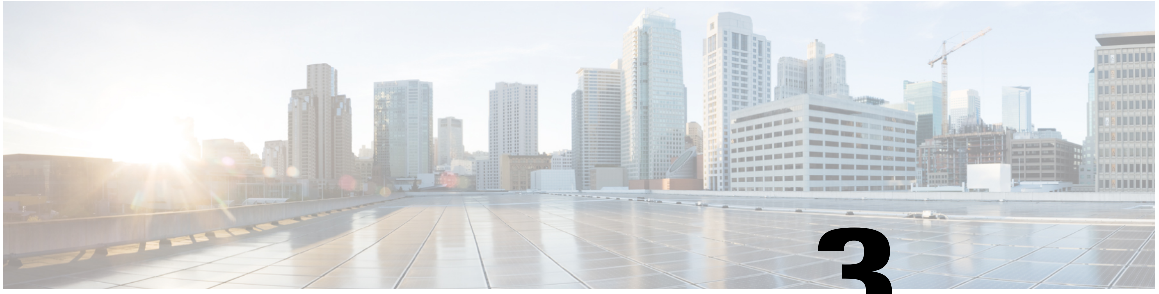
Table 2: Feature Information for SIP: Core SIP Technology Enhancements

Feature Name	Releases	Feature Information
SIP: Core SIP Technology Enhancements	12.2(13)T 12.2(15)T	Compliance to RFC 2543-bis-04 adds enhanced SIP support and ensures smooth interoperability and compatibility with multiple vendors. The following commands were modified: **debug ccsip messages, show sip-ua map**, **show sip-ua statistics**,and.

ASR Feature History Information.

Table 3: Feature Information for SIP: Core SIP Technology Enhancements

Feature Name	Releases	Feature Information
SIP: Core SIP Technology Enhancements	Cisco IOS XE Release 2.5	Compliance to RFC 2543-bis-04 adds enhanced SIP support and ensures smooth interoperability and compatibility with multiple vendors. The following commands were modified: **debug ccsip messages, show sip-ua map**, **show sip-ua statistics**,and.



CHAPTER 3

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 is enabled by default on Cisco UBE.

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 4: P-RTP-Stat Header Fields

Field	Description	Range of Values
PS	Packets Sent	0 to 4294967295
OS	Octets Sent	0 to 4294967295
PR	Packets Received	0 to 4294967295
OR	Octets Received	0 to 4294967295
PL	Packets Lost	0 to 4294967295
JI	Jitter	0 to 4294967295

Field	Description	Range of Values
LA	Round Trip Delay, in milliseconds (ms)	-2147483648 to +2147483647
DU	Call Duration, in seconds	0 to 4294967295

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 www.cisco.com/go/cfn. 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

	Command or Action	Purpose
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.
Step 3	**voice class sip-profiles** *tag* **Example:** `Router(config)# voice class sip-profiles 100`	Configures SIP profiles for a voice class and enters voice class configuration mode.

	Command or Action	Purpose
Step 4	**request bye sip-header p-rtp-stat remove** **Example:** `Router(config-class)# request bye sip-header p-rtp-stat remove`	Removes the P-RTP-Stat SIP header from the BYE message.
Step 5	**response 200 sip-header p-rtp-stat remove** **Example:** `Router(config-class)# response 200 sip-header p-rtp-stat remove`	Removes the P-RTP-Stat SIP header from the 200 OK message.
Step 6	**exit** **Example:** `Router(config-class)# exit`	Exits voice class configuration mode.

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

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice service voip** **Example:** `Router(config)# voice service voip`	Specifies VoIP as the voice encapsulation method and enters voice-service configuration mode.
Step 4	**sip** **Example:** `Router(conf-voi-serv)# sip`	Enters service SIP configuration mode.
Step 5	**sip-profiles** *tag* **Example:** `Router(conf-serv-sip)# sip-profiles 100`	Disables the Support for Reporting End-of-Call Statistics in SIP BYE Message feature at the global level.
Step 6	**exit** **Example:** `Router(config-class)# exit`	Exits service SIP configuration mode.

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

	Command or Action	Purpose
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.
Step 3	**dial-peer voice** *tag* **voip** **Example:** `Router(config)# dial-peer voice 100 voip`	Defines a dial peer to specify the method of voice encapsulation and enters dial peer configuration mode.
Step 4	**voice-class sip profiles** *tag* **Example:** `Router(config-dial-peer)# voice-class sip profiles 100`	Disables the Support for Reporting End-of-Call Statistics in SIP BYE Message feature at the dial peer level.
Step 5	**exit** **Example:** `Router(config-dial-peer)# exit`	Exits dial-peer configuration mode.

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. An account on Cisco.com is not required.
Feature History Table entry for the Cisco Unified Border Element.

Table 5: Feature Information for Reporting End-of-Call Statistics in SIP BYE Message

Feature Name	Releases	Feature Information
Reporting End-of-Call Statistics in SIP BYE Message	15.1(3)T	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**.

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

Table 6: Feature Information for Reporting End-of-Call Statistics in SIP BYE Message

Feature Name	Releases	Feature Information
Reporting End-of-Call Statistics in SIP BYE Message	Cisco IOS XE Release 3.3S	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**.

CHAPTER 4

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

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 www.cisco.com/go/cfn. 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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	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`	(Required) Enters the voice-service VoIP configuration mode
Step 4	**sip** **Example:** `Router(config-voi-serv)# sip`	(Required) Enters the SIP configuration mode.
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:** *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.
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

	Command or Action	Purpose
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.
Step 3	**dial-peer voice** *tag* **voip** **Example:** `Router# dial-peer voice 100 voip`	(Required) Enters dial-peer configuration mode for the specified dial peer.
Step 4	**voice-class sip localhost dns:** [*hostname* **.**]*domain* [**preferred**] **Example:** `Router(config-dial-peer)# voice-class sip localhost dns:example.com`	(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.

	Command or Action	Purpose
Step 5	**exit** **Example:** `Router(config-dial-peer)# exit`	Exits the current configuration mode.

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
ACOMLevel=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
GapFillWithSilence=0 ms
```

```
GapFillWithPrediction=0 ms
GapFillWithInterpolation=0 ms
GapFillWithRedundancy=0 ms
HiWaterPlayoutDelay=70 ms
LoWaterPlayoutDelay=69 ms
TxPakNumber=2434
TxSignalPak=0
TxComfortNoisePak=0
TxDuration=48680
TxVoiceDuration=48680
RxPakNumber=2434
RxSignalPak=0
RxDuration=0
TxVoiceDuration=48670
VoiceRxDuration=48620
RxOutOfSeq=0
RxLatePak=0
RxEarlyPak=0
PlayDelayCurrent=69
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
GwOutpulsedCalledOctet3=0x80
GwOutpulsedCallingNumber=9001
GwOutpulsedCallingOctet3=0x0
GwOutpulsedCallingOctet3a=0x0
MediaInactiveDetected=no
MediaInactiveTimestamp=
MediaControlReceived=
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
OriginalCalledNumber=
OriginalCalledOctet=0x80
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0x0
TranslatedCallingNumber=9001
TranslatedCallingOctet=0x0
TranslatedCalledNumber=
TranslatedCalledOctet=0x80
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0x0
GwCollectedCalledNumber=9002
```

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 7: Feature Information for Configurable Hostname in Locally Generated SIP Headers

Feature Name	Releases	Feature Information
Configurable Hostname in Locally Generated SIP Header	12.4(2)T	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**

ASR Feature History Information.

Table 8: Feature Information for Configurable Hostname in Locally Generated SIP Headers

Feature Name	Releases	Feature Information
Configurable Hostname in Locally Generated SIP Header	Cisco IOS XE Release 2.5	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**

CHAPTER 5

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

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 www.cisco.com/go/cfn. 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

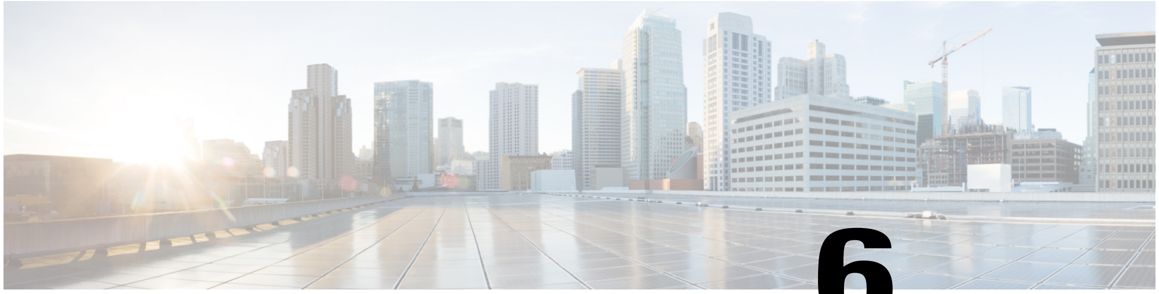
Table 9: Feature Information for Configuring SIP-to-SIP Supplementary Features

Feature Name	Releases	Feature Information
SIP-to-SIP Basic Functionality for Session Border Controller	12.4(4)T	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.

ASR Feature History Information

Table 10: Feature Information for Configuring SIP-to-SIP Supplementary Features

Feature Name	Releases	Feature Information
SIP-to-SIP Basic Functionality for Session Border Controller	Cisco IOS XE Release 3.1S, Cisco IOS XE Release 3.3S	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.



CHAPTER 6

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 www.cisco.com/go/cfn. 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 2*xx* 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 2*xx* 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 2*xx* 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 2*xx* 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 2*xx* was received or sent. For the UAC, the expiration time is 30 minutes after the receipt of the final response.

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

The syntax of the Session-Expires header is:

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

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

Min-SE Header

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

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

The syntax of the Min-SE header is:

```
Min-SE  =  "Min-SE" ":" delta-seconds
```

422 Response Message

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

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

Supported and Require Headers

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

How to Configure SIP Session Timer Support

Prerequisites

- Ensure that the gateway has voice functionality that is configurable for SIP.
- Establish a working IP network.
- Configure VoIP--Information about configuring VoIP in a SIP environment can be found here: http://www.cisco.com/en/US/tech/tk652/tk701/tech_configuration_guides_list.html .

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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	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 voice service VoIP configuration mode.
Step 4	**sip** **Example:** `Router(conf-voi-serv)# sip`	Enters SIP configuration mode.
Step 5	**min-se** *seconds* **Example:** `Router(conf-serv-sip)# min-se 600`	Sets the minimum session expires header value, in seconds, for all calls. - Range is 90 to 86,400 (one day). The default value is 1800 (30 minutes).
Step 6	**min-se** *exit* **Example:** `Router(conf-serv-sip)# exit`	Exits the current configuration mode.
Step 7	**min-se show sip-ua min-se** **Example:** `Router(config)# show sip-ua min-se`	Verifies the value of the Min-SE header.

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. An account on Cisco.com is not required.

Table 11: Feature Information for SIP—Session Timer Support

Feature Name	Releases	Feature Information
SIP - Session Timer Support	12.2(8)YN 12.2(15)T 12.2(11)YV 12.2(11)T 12.3(2)T	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: **min-se (SIP)** and **show sip-ua min-se**.

Feature Name	Releases	Feature Information
SIP - Session Timer Support	Cisco XE Release 2.5	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: **min-se (SIP)** and **show sip-ua min-se**.

CHAPTER 7

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

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 www.cisco.com/go/cfn. An account on Cisco.com is not required.

PrerequisitesforSIP-to-SIPSupplementaryServicesforSession 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 following URL: http://www.cisco.com/en/US/docs/ios/voice/fxs/configuration/guide/15_0/fxs_15_0_cg.html .

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 12: Feature Information for Configuring SIP-SIP Supplementary Features

Feature Name	Releases	Feature Information
SIP-to-SIP Supplementary Services for Session Border Controller	12.4(9)T 15.1(1)T5	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.
SIP-to-SIP Supplementary Services for Session Border Controller	Cisco IOS XE Release 3.1S	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.

CHAPTER 8

Session Refresh with Reinvites

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 www.cisco.com/go/cfn. 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**
6. **exit**
7. **end**

DETAILED STEPS

	Command or Action	Purpose
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.
Step 3	**voice service voip** **Example:** `Router(config)# voice service voip`	Enters VoIP voice-service configuration mode.
Step 4	**sip** **Example:** `Router(conf-voi-serv)# sip`	Enters SIP configuration mode.
Step 5	**midcall-signaling passthru** **Example:** `Router(conf-serv-sip)# midcall-signaling passthru`	Passes SIP messages from one IP leg to another IP leg.
Step 6	**exit** **Example:** `Router(conf-serv-sip)# exit`	Exits the current mode.

	Command or Action	Purpose

Step 7	**end**
	Example:
	`Router(conf-serv-sip) end`
		Returns to privileged EXEC mode.

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. An account on Cisco.com is not required.

Feature Name	Releases	Feature Information
Session Refresh with Reinvites	12.4(20)T	Expands the ability of the Cisco Unified BE to control the session refresh parameters and ensure the session does not time out. In Cisco IOS Release 12.4(20)T, this feature was implemented on the Cisco Unified Border Element. **midcall-signaling**
Session Refresh with Reinvites	Cisco IOS XE Release 2.5	Expands the ability of the Cisco Unified BE to control the session refresh parameters and ensure the session does not time out. In Cisco IOS XE Release 2.5, this feature was implemented on the Cisco Unified Border Element (Enterprise). **midcall-signaling**

CHAPTER 9

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

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 www.cisco.com/go/cfn. 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 13: Error Codes that busyout the endpoint

Error Code	Description
503	service unavailable
505	sip version not supported
no response	i.e. request timeout

All other error codes, including 400 are considered a valid response and the dial peer is not busied out.

Note The purpose of this feature is to determine if the SIP session protocol on the endpoint is UP and available to handle calls. It may not handle OPTIONS message but as long as the SIP protocol is available, it should be able to handle calls.

When a dial-peer is busied out, Cisco Unified Border Element continues the heartbeat mechanism and the dial-peer is set to active upon receipt of a response.

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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**dial-peer voice** *tag* **voip** **Example:** `Device(config)# dial-peer voice 200 voip`	Enters dial-peer configuration mode for the VoIP peer designated by tag.

Step 4	**voice-class sip options-keepalive** {**up-interval** *seconds* | **down-interval** *seconds* | **retry** *retries*}
	Example:
	`Device(config-dial-peer)# voice-class sip options-keepalive up-interval 12 down-interval 65 retry 3`
		Monitors connectivity between endpoints.
		• **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# 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# 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    down              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. An account on Cisco.com is not required.

Table 14: Feature Information for Cisco UBE Out-of-dialog OPTIONS Ping for Specified SIP Servers or Endpoints

Feature Name	Releases	Feature Information
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**

CHAPTER 10

SIP Out-of-Dialog OPTIONS Ping Group

This feature groups the monitoring of SIP dial-peers endpoints and servers by consolidating dial peers with the same SIP Out-of-Dialog (OOD) OPTIONS ping setup.

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 www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About SIP Out-Of-dialog OPTIONS Ping Group

SIP Out-of-Dialog OPTIONS Ping Group Overview

The SIP Out-Of-Dialog OPTIONS (OODO) Ping Group feature is an existing mechanism used by CUBE to monitor the status of a single SIP dial-peer destination (keepalive). A generic heartbeat mechanism allows you to monitor the status of SIP servers or endpoints and provide the option of marking a dial peer as inactive (busyout) upon total heartbeat failure.

You can now consolidate the sending of SIP OODO ping packets by grouping dial peers with the same SIP OODO ping setup. A keepalive profile is created and referenced by different SIP dial peers. An OODO Options ping heartbeat keepalive connection is set up for each dial-peer destination of a keepalive profile. If a heartbeat failure occurs for any of the dial peers of the profile, the status of the respective dial peer is changed to inactive (busyout) by CUBE.

You can use the **shutdown** command to suspend monitoring of all dial peers associated with a keepalive profile.

The new command **voice-class sip options-keepalive profile tag** is used to monitor a group of SIP servers or endpoints and the existing **voice-class sip options-keepalive** command is used to monitor a single SIP endpoint or server.

You can configure a server group to be a part of a SIP OODO ping group. A SIP dial peer is updated to BUSY state only if all targets of its server group does not response to the OODO ping

How to Configure SIP Out-Of-dialog OPTIONS Ping Group

Configuring SIP Out-of-Dialog OPTIONS Ping Group

Before You Begin

Configure SIP profiles and server groups.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice class sip-options-keepalive** *keepalive-group-profile-id*
4. **description** *text*
5. **transport {tcp [tls] | udp | system}**
6. **sip-profiles** *profile-number*
7. **down-interval** *down-interval*
8. **up-interval** *up-interval*
9. **retry** *retry-interval*
10. **exit**
11. **dial-peer voice** *dial-peer-id* **voip**
12. **session protocol sipv2**
13. **voice-class sip options-keepalive profile** *keepalive-group-profile-id*
14. **session server-group** *server-group-id*
15. **end**
16. **show voice class sip-options-keepalive** *keepalive-group-profile-id*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enters privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**voice class sip-options-keepalive** *keepalive-group-profile-id* **Example:** `Device(config)# voice class sip-options-keepalive 171`	Configures a keepalive profile and enters voice class configuration mode. • You can use the **shutdown** command to suspend keepalive activity for all dial peers associated with the keepalive profile.
Step 4	**description** *text* **Example:** `Device(config-class)# description Target Boston`	Configures a textual description for the keepalive heartbeat connection.

Step 5	**transport {tcp [tls] | udp | system}**
	Example:
	`Device(config-class)# transport tcp`
		Defines the transport protocol used for the keepalive heartbeat connection.
		• The default value is system.

Step 6	**sip-profiles** *profile-number* **Example:** `Device(config-class)# sip-profiles 100`	Specifies the SIP profile that is to be used to send this message. • To configure a SIP profile, refer to “Configuring SIP Parameter Modification”.
Step 7	**down-interval** *down-interval* **Example:** `Device(config-class)# down-interval 35`	Configures the time (in seconds) at which an SIP OODO ping is sent to the dial-peer endpoint when the heartbeat connection to the endpoint is in Down status. • The default value is 30.
Step 8	**up-interval** *up-interval* **Example:** `Device(config-class)# up-interval 65`	Configures the time (in seconds) at which an SIP OODO ping is sent to the dial-peer endpoint when the heartbeat connection to the endpoint is in Up status. • The default value is 60.

	Command or Action	Purpose
Step 9	**retry** *retry-interval* **Example:** `Device(config-class)# retry 30`	Configures the maximum number of OODO ping retrials permitted for a dial-peer destination. After receiving failed responses for the configured number of OODO ping, the heartbeat connection status should be switched from Up to Down. • The default value is 5. • If a successful response is received for an OODO ping, the retry counter is set to zero.
Step 10	**exit** **Example:** `Device(config-class)# exit`	Exits voice class configuration mode and enters global configuration mode.
Step 11	**dial-peer voice** *dial-peer-id* **voip** **Example:** `Device(config)# dial-peer voice 123 voip`	Defines a local dial peer and enters dial peer configuration mode.
Step 12	**session protocol sipv2** **Example:** `Device(config-dial-peer)# session protocol sipv2`	Specifies SIP version 2 as the session protocol for calls between local and remote routers using the packet network.
Step 13	**voice-class sip options-keepalive profile** *keepalive-group-profile-id* **Example:** `Device(config-dial-peer)# voice-class sip options-keepalive profile 171`	Associates the dial peer with the specified keepalive group profile. The dial peer is monitored by CUBE according to the parameters defined by this profile.
Step 14	**session server-group** *server-group-id* **Example:** `Device(config-dial-peer)# session server-group 151`	Associates the dial peer with the specified keepalive group profile. The dial peer is monitored by the device according to the parameters defined by this profile.

Step 15	**end**
	Example:
	`Device(config-dial-peer)# end`
		Exits dial peer configuration mode and enters privileged EXEC mode.

Step 16	**show voice class sip-options-keepalive** *keepalive-group-profile-id*	Displays information about voice class server group.

	Command or Action	Purpose
	Example: `Device# show voice class sip-options-keepalive 171`	

Configuration Examples For SIP Out-of-Dialog OPTIONS Ping Group

Example: SIP Out-of-Dialog OPTIONS Ping for Group of SIP Endpoints

```
!Configuring the SIP profile
Device(config)# voice class sip-profiles 100
Device(config-class)# request INVITE sip-header SIP-Req-URI modify "; SIP/2.0" ";user=phone
 SIP/2.0"

!Configuring the SIP Keepalive Group
Device(config)# voice class sip-options-keepalive 171
Device(config-class)# transport tcp
Device(config-class)# sip-profile 100
Device(config-class)# down-interval 30
Device(config-class)# up-interval 60
Device(config-class)# retry 5
Device(config-class)# description Target New York
Device(config-class)# exit

!Configuring an outbound SIP Dial Peer
Device(config)# dial-peer voice 123 voip
Device(config-dial-peer)# session protocol sipv2
!Associating the Dial Peer with a keepalive profile group
Device(config-dial-peer)# voice-class sip options-keepalive profile 171
Device(config-dial-peer)# end

!Verifying the Keepalive group configurations
Device# show voice class sip-options-keepalive 171

Voice class sip-options-keepalive: 171           AdminStat: Up
 Description: Target New York
 Transport: system              Sip Profiles: 100
 Interval(seconds) Up: 60               Down: 30
 Retry: 5

  Peer Tag      Server Group    OOD SessID      OOD Stat        IfIndex
  --------      ------------    ----------      --------        -------
  123                                                           100
```

Example: SIP Out-of-dialog OPTIONS Ping for Group of SIP Servers

```
!Configuring the Server Group
Device(config)# voice class server-group 151
Device(config-class)# ipv4 10.1.1.1 preference 1
Device(config-class)# ipv4 10.1.1.2 preference 2
Device(config-class)# ipv4 10.1.1.3 preference 3
Device(config-class)# hunt-scheme round-robin
Device(config-class)# description It has 3 entries
Device(config-class)# exit

!Configuring an E164 pattern map class
Device(config)# voice class e164-pattern-map 3000
Device(config-class)# e164 300

!Configuring an outbound SIP dial peer.
Device(config)# dial-peer voice 181 voip
!Associate a destination pattern map
Device(config-dial-peer)# destination e164-pattern-map 3000
Device(config-dial-peer)# session protocol sipv2
!Associate a server group with the dial peer
Device(config-dial-peer)# session server-group 151
!Associate the dial peer with a keepalive profile group
Device(config-dial-peer)# voice-class sip options-keepalive profile 171
Device(config-dial-peer)# end

!Verifying the Keepalive group configurations
Device# show voice class sip-options-keepalive 171

Voice class sip-options-keepalive: 171           AdminStat: Up
 Description: Target New York
 Transport: system               Sip Profiles: 100
 Interval(seconds) Up: 60                Down: 30
 Retry: 5

  Peer Tag      Server Group    OOD SessID      OOD Stat        IfIndex
  --------      ------------    ----------      --------        -------
  123                                                           100
  181           151                             Busy            106

  Server Group: 151              OOD Stat: Busy
   OOD SessID   OOD Stat
   ----------   --------
   1            Busy
   2            Busy
   3            Busy

 OOD SessID: 1                   OOD Stat: Busy
  Target: ipv4:10.1.1.1
  Transport: system              Sip Profiles: 100

 OOD SessID: 2                   OOD Stat: Busy
  Target: ipv4:10.1.1.2
  Transport: system              Sip Profiles: 100

 OOD SessID: 3                   OOD Stat: Busy
  Target: ipv4:10.5.0.1
  Transport: system              Sip Profiles: 100

------------------------------------------------------
```

Additional References

Related Documents

Related Topic	Document Title
Voice commands	Cisco IOS Voice Command Reference
Cisco IOS Commands	Cisco IOS Master Command List, All Releases
SIP Configuration Guide	SIP Configuration Guide
Configuring SIP profiles	SIP Parameter Modificaton.

Related Topic	Document Title
Configuring server groups	Configuring Server Groups.

Technical Assistance

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

Feature Information for SIP Out-of-dialog OPTIONS Ping Group

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 15: Feature Information for SIP Out-of-dialog OPTIONS Ping Group

Feature Name	Releases	Feature Information
SIP Out-of-dialog OPTIONS Ping Group	Cisco IOS XE Release 3.11S 15.4(1)T	This feature groups the monitoring of SIP dial peers endpoints and servers by consolidating SIP Out-Of-Dialog (OOD) Options of dial peers with the similar SIP OOD Options ping setup. The following commands were introduced or modified: **voice class sip-options-keepalive**, **description**, **transport**, **sip-profiles**, **down-interval**, **up-interval**, **voice-class sip options-keepalive profile**, **retry**, **show voice class sip-options-keepalive**.

CHAPTER 11

Configuring an Error Response Code upon an Out-of-Dialog 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-Dialog 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

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 www.cisco.com/go/cfn. 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 16: SIP Error Codes

Error Code Number	Description
400	Bad Request
401	Unauthorized
402	Payment Required
403	Forbidden

Error Code Number	Description
404	Not Found
408	Request Timed Out
416	Unsupported URI
480	Temporarily Unavailable
482	Loop Detected
484	Address Incomplete
486	Busy Here
487	Request Terminated
488	Not Acceptable Here
500-599	SIP 5xx--Server/Service Failure
500	Internal Server Error
502	Bad Gateway
503	Service Unavailable
600-699	SIP 6xx--Global Failure

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

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	- Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice service voip** **Example:** `Router(config)# voice service voip`	Enters voice service configuration mode.
Step 4	**sip** **Example:** `Router(conf-voi-serv)# sip`	Enters voice service SIP configuration mode.
Step 5	**error-code-override options-keepalive failure** *sip-status-code-number* **Example:** `Router(conf-serv-sip)# error-code-override options-keepalive failure 402`	Configures the specified SIP error code number. - *sip-status-code-number* --SIP status code to be sent for an options keepalive failure. Range: 400 to 699. Default: 503. - The table above provides more details about these error codes.

Step 6	**end**
	Example:
	`Router(conf-serv-sip)# end`
		Exits voice service SIP configuration mode and returns to privileged EXEC mode.

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

	Command or Action	Purpose
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.
Step 3	**dial-peer voice** *voice-dial-peer-tag* **voip** **Example:** `Router(config)# dial-peer voice 234 voip`	Enters dial peer voice configuration mode.

Step 4	**voice-class sip error-code-error-override options-keepalive failure** {*sip-status-code-number* | **system**}
	Example:
	`Router(config-dial-peer)# voice-class sip error-code-override options-keepalive failure 500`
		Configures the specified SIP error code number.
		• *sip-status-code-number* --SIP status code to be sent for an options keepalive failure. Range: 400 to 699. Default: 503.
		• Configuring an Error Response Code upon an Out-of-Dialog OPTIONS Ping Failure at the Dial Peer Level, on page 74 provides more details about these error codes.
		Note If the **system** keyword is configured, the global level configuration will override the dial-peer configuration.

Step 5	**end**
	Example:
	`Router(config-dial-peer)# end`
		Exits dial peer voice configuration mode and returns to privileged EXEC mode.

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

Feature Name	Releases	Feature Information
Error Response Code upon an Out-of-Dialog OPTIONS Ping Failure	15.1(1)T	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: **error-code-override options-keepalive failure**, **voice-class sip error-code-override options-keepalive failure**.

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

Table 18: Feature Information for Configuring an Error Response Code upon an Out-of-Dialog OPTIONS Ping Failure

Feature Name	Releases	Feature Information
Error Response Code upon an Out-of-Dialog OPTIONS Ping Failure	Cisco IOS XE Release 3.1S	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: **error-code-override options-keepalive failure**, **voice-class sip error-code-override options-keepalive failure**.

CHAPTER 12

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

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 www.cisco.com/go/cfn. 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

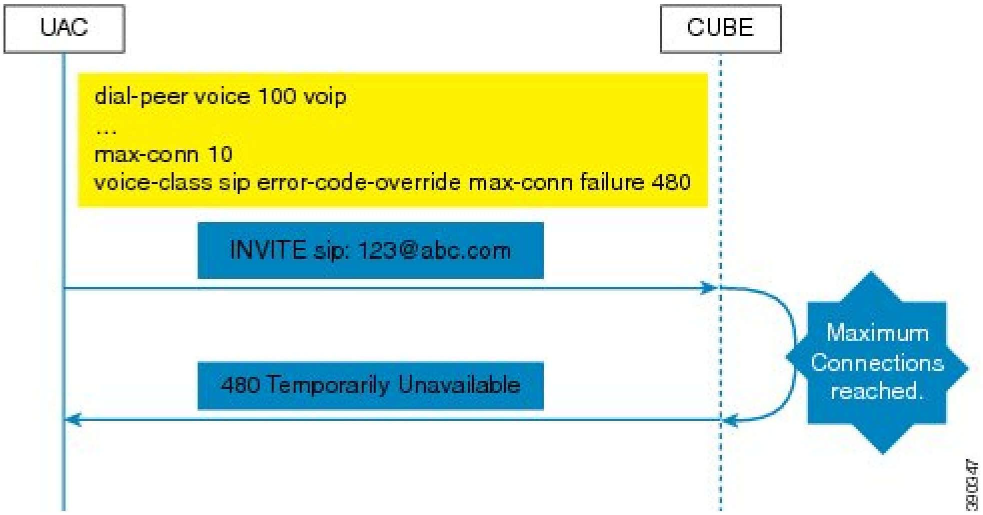
Error Codes for CAC Failures

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


UAC
CUBE
dial-peer voice 100 voip
...
max-conn 10
voice-class sip error-code-override max-conn failure 480
INVITE sip: 123@abc.com
Maximum Connections reached.
480 Temporarily Unavailable
390347

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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**voice service voip** **Example:** `Device(config)# voice service voip`	Specifies VoIP encapsulation and enters voice-service configuration mode.
Step 4	**sip** **Example:** `Device(conf-voi-serv)# sip`	Enters the Session Initiation Protocol (SIP) configuration mode.
Step 5	**error-code-override** {**options-keepalive** | **call** | **cpu** | **mem** | **max-conn** | **total-calls** | **sip-shutdown**} **failure** *sip-status-code-num* **Example:** `Device(conf-serv-sip)# error-code-override mem failure 411`	Configures the SIP error codes.

Step 6	**end**
	Example:
	`Device(config-dial-peer)# end`
		Ends the current configuration session and returns to privileged EXEC mode.

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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**dial-peer voice** *tag* **voip** **Example:** `Device(config)# dial-peer voice 10 voip`	Defines a VoIP dial peer and enters dial peer configuration mode.

Step 4	**voice-class sip error-code-override** {**options-keepalive** | **call** | **cpu** | **mem** | **max-conn** | **total-calls** | **sip-shutdown**} **failure** {*sip-status-code-num* | **system**}
	Example:
	`Device(config-dial-peer)# voice-class sip error-code-override max-conn failure 421`
		Configures the Session Initiation Protocol (SIP) error code to be used at the dial peer.

Step 5	**end**
	Example:
	`Device(config-dial-peer)# end`
		Ends the current configuration session and returns to privileged EXEC mode.

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(conf-voi-serv)# sip
Device(conf-serv-sip)# error-code-override mem failure 411
Device(conf-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

Related Documents

Related Topic	Document Title
Voice commands	Cisco IOS Voice Command Reference
Cisco IOS commands	Cisco IOS Master Command List, All Releases
SIP configuration tasks	SIP Configuration Guide, Cisco IOS Release 15M&T

Technical Assistance

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

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 19: Feature Information for Configurable SIP Error Codes

Feature Name	Releases	Feature Information
Configurable SIP Error Codes	15.4(1)T	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**

CHAPTER 13

Configuring SIP Error Message Pass Through

The Configuring SIP Error Message Pass Through feature allows an error response that is received from one SIP leg to pass transparently over to another SIP leg. This functionality will pass SIP error responses that are not yet supported on the Cisco Unified Border Element (Cisco UBE) or will preserve the Q.850 cause code across two sip call-legs.

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 www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Configuring SIP Error Message Pass Through

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

Information About Configuring SIP Error Message Pass Through

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

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

Error Code Received	Corresponding Error Reported on the Peer Leg
400—Bad request	500—Internal Server Error
401—Unauthorized	503—Service Unavailable
406—Not acceptable	500—Internal Server Error
407—Authentication required	503—Service Unavailable
413—Request message body too large	500—Internal Server Error
414—Request URI too large	500—Internal Server Error
416—Unsupported URI scheme	500—Internal Server Error
423—Interval too brief	500—Internal Server Error
482—Loop detected	500—Internal Server Error
483—Too many hops	500—Internal Server Error
488— Not acceptable media (applicable only when the call is transcoded)	500—Internal Server Error

How to Configure SIP Error Message Pass Through

Configuring SIP Error Message Pass Through

Perform this task to configure the SIP Error Message Pass Through feature.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **sip**
5. **header-passing error pass-thru**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**voice service voip** **Example:** `Device(config)# voice service voip`	Enters VoIP voice service configuration mode.
Step 4	**sip** **Example:** `Device(config-voi-serv)# sip`	Enters SIP configuration mode.
Step 5	**header-passing error pass-thru** **Example:** `Device(conf-serv-sip)# header-passing error pass-thru`	Passes received error responses from one SIP leg to pass transparently to another SIP leg.

Step 6	**end**
	Example:
	`Device(conf-serv-sip)# end`
		Returns to privileged EXEC mode.

Feature Information for Configuring SIP Error Message Pass Through

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 20: Feature Information for Configuring SIP Error Message Pass Through

Feature Name	Releases	Feature Information
Configuring SIP Error Message Pass Through	12.4(11)XJ2 15.2(4)M	This feature allows a received error response from one SIP leg to pass transparently over to another SIP leg.

CHAPTER 14

SIP INFO Method for DTMF Tone Generation

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

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 www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for SIP INFO Method for DTMF Tone Generation

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

Cisco Unified Border Element

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

Cisco Unified Border Element (Enterprise)

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

Restrictions for SIP INFO Methods for DTMF Tone Generation

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

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

Information About SIP INFO Method for DTMF Tone Generation

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

How to Review SIP INFO Messages

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

```
INFO sip:2143302100@172.17.2.33 SIP/2.0
Via: SIP/2.0/UDP 172.80.2.100:5060
From:  <sip:9724401003@172.80.2.100>;tag=43
To:  <sip:2143302100@172.17.2.33>;tag=9753.0207
Call-ID: 984072_15401962@172.80.2.100
CSeq: 25634 INFO
Supported: 100rel
Supported: timer
Content-Length: 26
Content-Type: application/dtmf-relay
Signal= 1
Duration= 160
```

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

Configuring for SIP INFO Method for DTMF Tone Generation

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

Troubleshooting Tips

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

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

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

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

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

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

Feature Information for SIP INFO Method for DTMF Tone Generation

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 21: Feature Information for SIP: INFO Method for DTMF Tone Generation

Feature Name	Releases	Feature Information
SIP: INFO Method for DTMF Tone Generation	12.2(11)T 12.3(2)T 12.2(8)YN 12.2(11)YV 12.2(11)T 12.2(15)T	The SIP: INFO Method for DTMF Tone Generation feature uses the Session Initiation Protocol (SIP) INFO method to generate dual-tone multifrequency (DTMF) tones on the telephony call leg. SIP methods, or request message types, request a specific action be taken by another user agent (UA) or proxy server. The SIP INFO message is sent along the signaling path of the call. The following command was introduced: **show sip-ua**.

Feature Name	Releases	Feature Information
SIP: INFO Method for DTMF Tone Generation	Cisco IOS XE Release 2.5S	The SIP: INFO Method for DTMF Tone Generation feature uses the Session Initiation Protocol (SIP) INFO method to generate dual-tone multifrequency (DTMF) tones on the telephony call leg. SIP methods, or request message types, request a specific action be taken by another user agent (UA) or proxy server. The SIP INFO message is sent along the signaling path of the call. The following command was introduced: **show sip-ua**.

CHAPTER 15

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

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 www.cisco.com/go/cfn. 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 Ringing message is a provisional or informational response used to indicate that the INVITE message has been received by the user agent and that alerting is taking place. The 183 Session Progress response indicates that information about the call state is present in the message body media information. Both 180 and 183 messages may contain SDP, which allows an early media session to be established prior to the call being answered.

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

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

Table 22: Call Treatments with SIP Enhanced 180 Provisional Response Handling

Response Message	SIP Enhanced 180 Provisional Response Handling Status	Treatment
180 response with SDP	Enabled (default)	Early media cut-through
180 response with SDP	Disabled	Local ringback
180 response without SDP	Not affected by the SIP--Enhanced 180 Provisional Response Handlingfeature	Local ringback
183 response with SDP	Not affected by the SIP--Enhanced 180 Provisional Response Handling feature	Early media cut-through

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

	Command or Action	Purpose
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.
Step 3	**interface** *type number* **Example:** `Router(config)# ethernet 0/0/0`	Configures an interface type and enters interface configuration mode.
Step 4	**sip ua** **Example:** `Router(config-sip-ua)# sip ua`	Enables SIP UA configuration commands in order to configure the user agent.

	Command or Action	Purpose
Step 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,
Passthrough = 0,Modem relay = 0, Gw-Xid = 1
SPRT latency 200, SPRT Retries = 12, Dict Size = 1024
String Len = 32, Compress dir = 3
00:12:20:sipSPICanSetFallbackFlag - Local Fallback is not active
00:12:20:****Deleting from UAC table
00:12:20:****Adding to UAC table
00:12:20: Queued event from SIP SPI :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:sipSPIUsetBillingProfile:sipCallId for billing records =
41585FCE-14F011CC-8005AF80-D4AA3153@172.31.1.42
00:12:20:CCSIP-SPI-CONTROL: act_idle_connection_created
00:12:20:CCSIP-SPI-CONTROL: act_idle_connection_created:Connid(1)
created to 172.31.1.15:5060, local_port 57838
00:12:20:CCSIP-SPI-CONTROL: sipSPIOutgoingCallSDP
00:12:20:sipSPISetMediaSrcAddr: media src addr for stream 1 = 10.1.1.42
00:12:20:sipSPIReserveRtpPort:reserved port 18978 for stream 1
```

```
00:12:20: convert_codec_bytes_to_ptime:Values :Codec:g711ulaw
codecbytes :160, ptime:20
00:12:20:sip_generate_sdp_xcaps_list:Modem Relay disabled. X-cap not
needed
00:12:20:Received Octet3A=0x00 -> Setting ;screen=no ;privacy=off
00:12:20:sipSPIAddLocalContact
00:12:20: Queued event from SIP SPI :SIPSPI_EV_SEND_MESSAGE
00:12:20:sip_stats_method
00:12:20:sipSPIProcessRtpSessions
00:12:20:sipSPIAddStream:Adding stream 1 (callid 2) to the VOIP RTP
library
00:12:20:sipSPISetMediaSrcAddr: media src addr for stream 1 = 10.1.1.42
00:12:20:sipSPIUpdateRtcpSession:for m-line 1
00:12:20:sipSPIUpdateRtcpSession:rtcp_session info
laddr = 10.1.1.42, lport = 18978, raddr = 0.0.0.0,
rport=0, do_rtcp=FALSE
src_callid = 2, dest_callid = -1
00:12:20:sipSPIUpdateRtcpSession:No rtp session, creating a new one
00:12:20:sipSPIAddStream:In State Idle
00:12:20:act_idle_connection_created:Transaction active. Facilities will
be queued.
00:12:20:0x639F6EEC :State change from (STATE_IDLE,
SUBSTATE_CONNECTING)  to (STATE_SENT_INVITE, SUBSTATE_NONE)
00:12:20:Sent:
INVITE sip:222@172.31.1.15:5060 SIP/2.0
Via:SIP/2.0/UDP  10.1.1.42:5060
From:"111" <sip:111@172.31.1.42>;tag=B4DC4-9E1
To:<sip:222@172.31.1.15>
Date:Mon, 01 Mar 1993 00:12:20 GMT
Call-ID:41585FCE-14F011CC-8005AF80-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
o=CiscoSystemsSIP-GW-UserAgent 4629 354 IN IP4 172.31.1.42
s=SIP Call
c=IN IP4 172.31.1.42
t=0 0
m=audio 18978 RTP/AVP 0 100
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:Received:
SIP/2.0 100 Trying
Via:SIP/2.0/UDP  10.1.1.42:5060
From:"111" <sip:111@172.31.1.42>;tag=B4DC4-9E1
To:<sip:222@172.31.1.15>;tag=442AC-22
Date:Wed, 16 Feb 2000 18:19:56 GMT
Call-ID:41585FCE-14F011CC-8005AF80-D4AA3153@172.31.1.42
Timestamp:730944740
Server:Cisco-SIPGateway/IOS-12.x
CSeq:101 INVITE
Allow-Events:telephone-event
Content-Length:0
00:12:21:HandleUdpSocketReads :Msg enqueued for SPI with IPaddr:
10.1.1.15:5060
00:12:21:CCSIP-SPI-CONTROL: act_sentinvite_new_message
00:12:21:CCSIP-SPI-CONTROL: sipSPICheckResponse
00:12:21:sip_stats_status_code
```

```
00:12:21: Roundtrip delay 420 milliseconds for method INVITE
00:12:21:0x639F6EEC :State change from (STATE_SENT_INVITE,
SUBSTATE_NONE)  to (STATE_RECD_PROCEEDING, SUBSTATE_PROCEEDING_PROCEEDING)
00:12:21:Received:
SIP/2.0 180 Ringing
Via:SIP/2.0/UDP  10.1.1.42:5060
From:"111" <sip:111@10.1.1.42>;tag=B4DC4-9E1
To:<sip:222@172.31.1.15>;tag=442AC-22
Date:Wed, 16 Feb 2000 18:19:56 GMT
Call-ID:41585FCE-14F011CC-8005AF80-D4AA3153@172.31.1.42
Timestamp:730944740
Server:Cisco-SIPGateway/IOS-12.x
CSeq:101 INVITE
Allow-Events:telephone-event
Contact:<sip:222@172.31.1.59:5060>
Record-Route:<sip:222@10.1.1.15:5060;maddr=10.1.1.15>
Content-Length:230
Content-Type:application/sdp
v=0
o=CiscoSystemsSIP-GW-UserAgent 4629 354 IN IP4 10.1.1.42
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_recdproc_new_message
00:12:21:CCSIP-SPI-CONTROL: act_recdproc_new_message_response
00:12:21:CCSIP-SPI-CONTROL: sipSPICheckResponse
00:12:21:sip_stats_status_code
00:12:21: Roundtrip delay 496 milliseconds for method INVITE
00:12:21:CCSIP-SPI-CONTROL: act_recdproc_new_message_response :Early
media disabled for 180:Ignoring SDP if present
00:12:21:HandleSIP1xxRinging:SDP in 180 will be ignored if present: No
early media cut through
00:12:21:HandleSIP1xxRinging:SDP Body either absent or ignored in 180
RINGING:- would wait for 200 OK to do negotiation.
00:12:21:HandleSIP1xxRinging:MediaNegotiation expected in 200 OK
00:12:21:sipSPIGetGtdBody:No valid GTD body found.
00:12:21:sipSPICreateRawMsg:No GTD passed.
00:12:21:0x639F6EEC :State change from (STATE_RECD_PROCEEDING,
SUBSTATE_PROCEEDING_PROCEEDING)  to (STATE_RECD_PROCEEDING,
SUBSTATE_PROCEEDING_ALERTING)
00:12:21:HandleSIP1xxRinging:Transaction Complete. Lock on Facilities
released.
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
CSeq:101 INVITE
Allow:INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, COMET, REFER, SUBSCRIBE,
NOTIFY, INFO
Allow-Events:telephone-event
Contact:<sip:222@10.1.1.59:5060>
Record-Route:<sip:222@10.1.1.15:5060;maddr=10.1.1.15>
Content-Type:application/sdp
Content-Length:231
v=0
o=CiscoSystemsSIP-GW-UserAgent 9600 4816 IN IP4 10.1.1.59
s=SIP Call
c=IN IP4 10.1.1.59
t=0 0
m=audio 19174 RTP/AVP 0 100
```

```
c=IN IP4 10.1.1.59
a=rtpmap:0 PCMU/8000
a=rtpmap:100 X-NSE/8000
a=fmtp:100 192-194
a=ptime:20
```

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 23: Feature Information for SIP :Enhanced 180 Provisional Response Handling

Feature Name	Releases	Feature Information
SIP - Enhanced 180 Provisional Response Handling	12.2(11)T 12.2(8)YN 12.2(15)T 12.2(11)YV 12.2(11)T	The Session Initiation Protocol (SIP) Enhanced 180 Provisional Response Handling feature provides the ability to enable or disable early media cut-through on Cisco IOS gateways for SIP 180 response messages. The following commands were introduced or modified: **disable-early-media 180** and **show sip-ua status**.

Feature Information Table for the ASR

Table 24: Feature Information for SIP: Enhanced 180 Provisional Response Handling

Feature Name	Releases	Feature Information
SIP - Enhanced 180 Provisional Response Handling	Cisco IOS XE Release 2.5	The Session Initiation Protocol (SIP) Enhanced 180 Provisional Response Handling feature provides the ability to enable or disable early media cut-through on Cisco IOS gateways for SIP 180 response messages. The following commands were introduced or modified: **disable-early-media 180** and **show sip-ua status**.

CHAPTER 16

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

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 www.cisco.com/go/cfn. 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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode, or other security level set by a system administrator. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**voice service voip** **Example:** `Router(config)# voice service voip`	Enters voice service VoIP configuration mode.
Step 4	**sip** **Example:** `Router(conf-voi-serv)# sip`	Enters SIP configuration mode.
Step 5	**block** {**180** | **181** | **183**} [**sdp** {**absent** | **present**}] **Example:** `Router(conf-serv-sip)# block 181 sdp present`	Configures support of SIP 181 messages globally so that messages are passed as is. The sdp keyword is optional and allows for dropping or passing of SIP 181 messages based on the presence or absence of SDP.
Step 6	**exit** **Example:** `Router(conf-serv-sip)# exit`	Exits the current mode.

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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode, or other security level set by a system administrator. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**dial-peer voice** *tag* **voip** **Example:** `Router(config)# dial-peer voice 2 voip`	Enters dial peer VoIP configuration mode.
Step 4	**voice-class sip block** {**180** | **181** | **183**} [**sdp** {**absent** | **present**}] **Example:** `Router(config-dial-peer)# voice-class sip block 181 sdp present`	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.
Step 5	**exit** **Example:** `Router(config-dial-peer)# exit`	Exits the current mode.

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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode, or other security level set by a system administrator. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice service voip** **Example:** `Router(config)# voice service voip`	Enters voice service VoIP configuration mode.
Step 4	**sip** **Example:** `Router(conf-voi-serv)# sip`	Enters SIP configuration mode.
Step 5	**map resp-code 181 to 183** **Example:** `Router(conf-serv-sip)# 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	**exit** **Example:** `Router(conf-serv-sip)# 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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode, or other security level set by a system administrator. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**dial-peer voice** *tag* **voip** **Example:** `Router(config)# dial-peer voice 2 voip`	Enters dial peer VoIP configuration mode.
Step 4	**voice-class sip map resp-code 181 to 183** **Example:** `Router(config-dial-peer)# voice-class sip map resp-code 181 to 183`	Enables mapping of received SIP messages of a specified SIP message type on a specific dial peer to a different SIP message type.
Step 5	**exit** **Example:** `Router(config-dial-peer)# exit`	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. An account on Cisco.com is not required.

Feature History Table entry for the Cisco Unified Border Element.

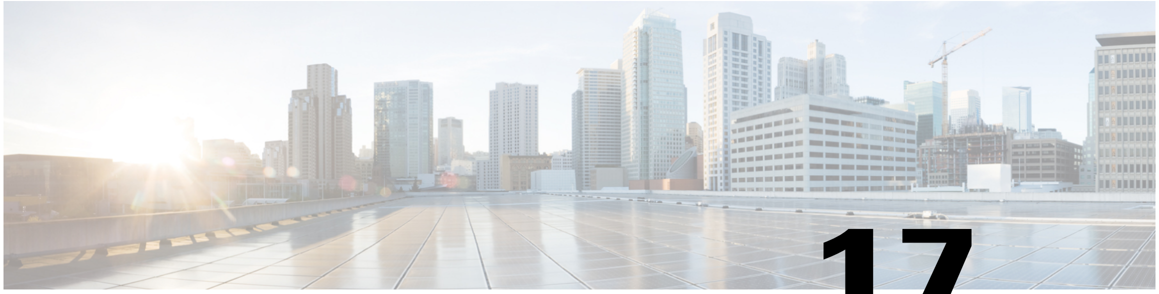
Table 25: Feature Information for SIP 181 Call is Being Forwarded Messages

Feature Name	Releases	Feature Information
SIP 181 Call is Being Forwarded Message	12.2(13)T	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**.

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

Table 26: Feature Information for SIP 181 Call is Being Forwarded Messages

Feature Name	Releases	Feature Information
SIP 181 Call is Being Forwarded Message	Cisco IOS XE Release 3.1S	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**.



CHAPTER 17

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 www.cisco.com/go/cfn. 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.

Figure 2: Early Dialog Update with SDP and Peer Leg does not support UPDATE

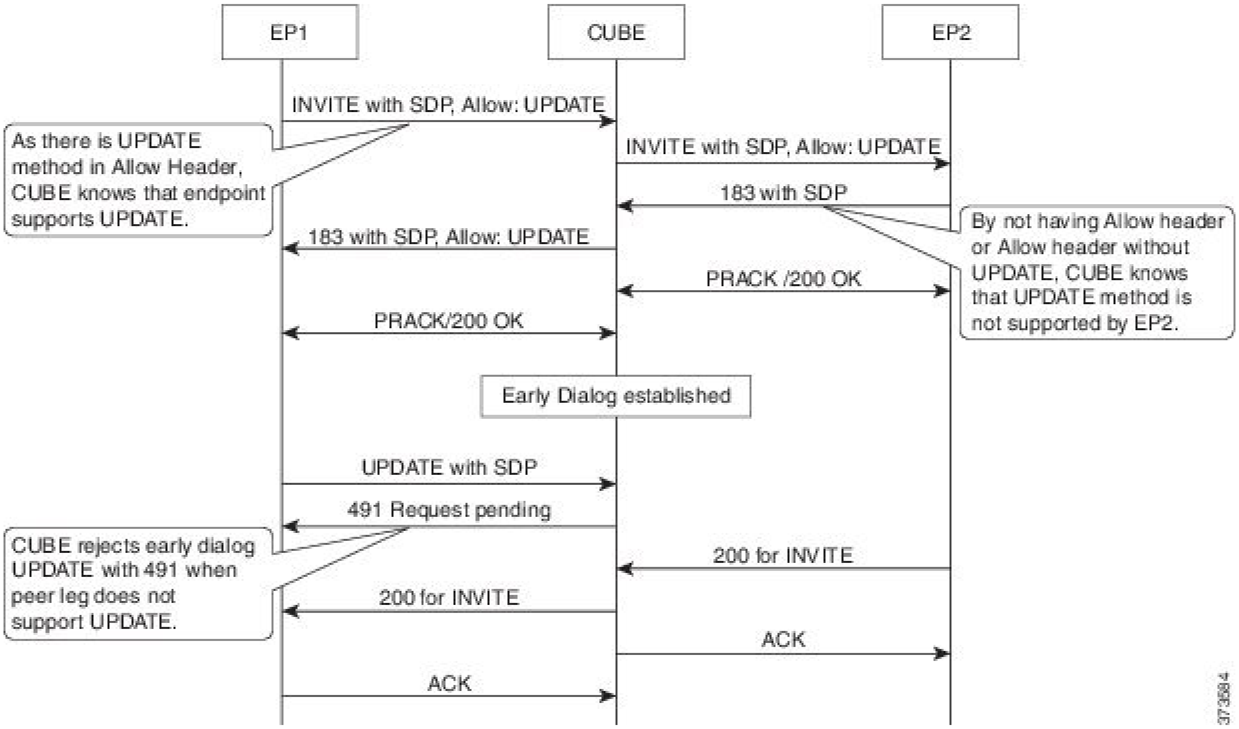
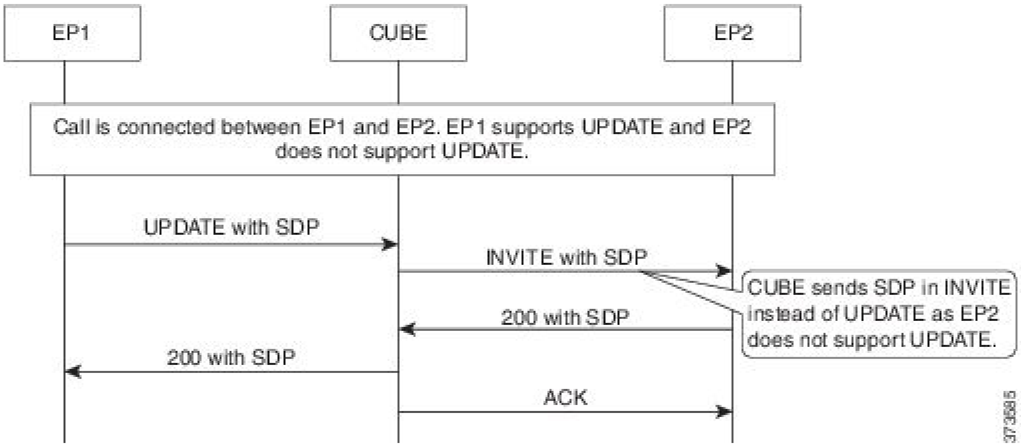

EP1
CUBE
EP2
INVITE with SDP, Allow: UPDATE
As there is UPDATE method in Allow Header, CUBE knows that endpoint supports UPDATE.
INVITE with SDP, Allow: UPDATE
183 with SDP
By not having Allow header or Allow header without UPDATE, CUBE knows that UPDATE method is not supported by EP2.
183 with SDP, Allow: UPDATE
PRACK /200 OK
PRACK/200 OK
Early Dialog established
UPDATE with SDP
491 Request pending
CUBE rejects early dialog UPDATE with 491 when peer leg does not support UPDATE.
200 for INVITE
200 for INVITE
ACK
ACK
373584

Figure 3: Mid-Dialog Update with SDP and Peer Leg does not support UPDATE


EP1
CUBE
EP2
Call is connected between EP1 and EP2. EP1 supports UPDATE and EP2 does not support UPDATE.
UPDATE with SDP
INVITE with SDP
CUBE sends SDP in INVITE instead of UPDATE as EP2 does not support UPDATE.
200 with SDP
200 with SDP
ACK
373585

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 27: Feature Information for Support for SIP UPDATE Message per RFC 3311

Feature Name	Releases	Feature Information
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.

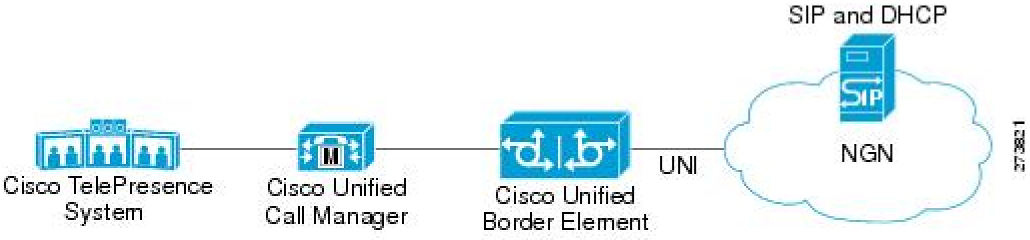
Feature Name	Releases	Feature Information
Support for SIP UPDATE Message per RFC 3311	Cisco IOS XE Release 3.6S	The Support for SIP UPDATE Message per RFC 3311 feature provides Session Description Protocol (SDP) support for Session Initiation Protocol (SIP)-to-SIP calls. The SIP Service Provider Interface (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).

CHAPTER 18

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


SIP and DHCP
SIP
NGN
UNI
Cisco TelePresence System
Cisco Unified Call Manager
Cisco Unified Border Element
373821

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 us 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 28: P-header Configuration Settings

Incoming Header	Outgoing Header	Configuration Notes
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.

Incoming Header	Outgoing Header	Configuration Notes
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** This is the default system behavior.
PAID	PPID	To enable the translation to PPID privacy headers in the outgoing header at a global level, use the **asserted-id ppi** command in voice service VoIP SIP configuration mode. For example: Router(conf-serv-sip)# **asserted-id ppi** To enable the translation to PPID privacy headers in the outgoing header on a specific dial peer, use the **voice-class sip asserted-id ppi** command in dial peer voice configuration mode. For example: Router(config-dial-peer)# **voice-class sip asserted-id ppi**

Incoming Header	Outgoing Header	Configuration Notes
PAID	RPID	To enable the translation to RPID headers in the outgoing header, use the **remote-party-id** command in SIP user-agent configuration mode. For example: Router(config-sip-ua)# **remote-party-id** This is the default system behavior.
RPID	PPID	To enable the translation to PPID privacy headers in the outgoing header at a global level, use the **asserted-id ppi** command in voice service VoIP SIP configuration mode. For example: Router(conf-serv-sip)# **asserted-id ppi** To enable the translation to PPID privacy headers in the outgoing header on a specific dial peer, use the **voice-class sip asserted-id ppi** command in dial peer voice configuration mode. For example: Router(config-dial-peer)# **voice-class sip asserted-id ppi**
RPID	PAID	To enable the translation to PAID privacy headers in the outgoing header at a global level, use the **asserted-id pai** command in voice service VoIP SIP configuration mode. For example: Router(conf-serv-sip)# **asserted-id pai** To enable the translation to PAID privacy headers in the outgoing header on a specific dial peer, use the **voice-class sip asserted-id pai** command in dial peer voice configuration mode. For example: Router(config-dial-peer)# **voice-class sip asserted-id pai**

Incoming Header	Outgoing Header	Configuration Notes
RPID	From:	By default, the translation to RPID headers is enabled and the system translates PPID headers in incoming messages to RPID headers in the outgoing messages. To disable the default behavior and enable the translation from PPID to From: headers, use the **no remote-party-id** command in SIP user-agent configuration mode. For example: Router(config-sip-ua)# **no remote-party-id**

The CUBE can be configured to transparently pass the PAID and PPID 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

Note The priority of P-headers are in the following order: PAID, PPID, and RPID.

Table 29: PAID and PPID header configuration settings for mid-call requests and responses

Incoming Header	Outgoing Header	Configuration Notes
PAID	PPID	To enable the translation to PPID headers in the outgoing header at a global level, use the **asserted-id ppi** command in voice service VoIP SIP configuration mode. For example: Router(conf-serv-sip)# **asserted-id ppi** To enable the translation to PPID headers in the outgoing header on a specific dial peer, use the **voice-class sip asserted-id ppi** command in dial peer voice configuration mode. For example: Router(config-dial-peer)# **voice-class sip asserted-id ppi**

Incoming Header	Outgoing Header	Configuration Notes
RPID	PPID	To enable the translation to PPID headers in the outgoing header at a global level, use the **asserted-id ppi** command in voice service VoIP SIP configuration mode. For example: Router(conf-serv-sip)# **asserted-id ppi** To enable the translation to PPID headers in the outgoing header on a specific dial peer, use the **voice-class sip asserted-id ppi** command in dial peer voice configuration mode. For example: Router(config-dial-peer)# **voice-class sip asserted-id ppi**
PPID	PPID	To enable the translation to PPID headers in the outgoing header at a global level, use the **asserted-id ppi** 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 **voice-class sip asserted-id ppi** command in dial peer voice configuration mode. For example: Router(config-dial-peer)# **voice-class sip asserted-id ppi**
PAID	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. For example: Router(config-dial-peer)# **voice-class sip asserted-id pai**

Incoming Header	Outgoing Header	Configuration Notes
RPID	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.
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.

Incoming Header	Outgoing Header	Configuration Notes
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**
FROM	FROM	No configuration required except for the **remote-party-id** header.
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**
PAID	PAID	Enables PPID headers on the incoming dial-peer and PAID headers on the outgoing dial-peer.
RPID	PAID	Enables PPID headers on incoming dial-peer and PAID headers on outgoing dial-peer.
PPID	PAID	Enables PPID headers on incoming dial-peer and PAID headers on outgoing dial-peer.
PAID	PAID	Enables RPID headers on incoming dial-peer and PAID headers on outgoing dial-peer.
RPID	PAID	Enables RPID headers on incoming dial-peer and PAID headers on outgoing dial-peer.
PPID	PAID	Enables RPID headers on incoming dial-peer and PAID headers on outgoing dial-peer.
PAID	PPID	Enables PAID headers on incoming dial-peer and PPID headers on outgoing dial-peer.

Incoming Header	Outgoing Header	Configuration Notes
RPID	PPID	Enables PAID headers on incoming dial-peer and PPID headers on outgoing dial-peer.
PPID	PPID	Enables PAID headers on incoming dial-peer and PPID on outgoing dial-peer.
PAID	PPID	Enables RPID headers on incoming dial-peer and PPID headers on outgoing dial-peer.
RPID	PPID	Enables RPID headers on incoming dial-peer and PPID headers on outgoing dial-peer.
PPID	PPID	Enables RPID headers on incoming dial-peer and PPID headers on outgoing dial-peer.
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.

Incoming Header	Outgoing Header	Configuration Notes
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.
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.

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, page 132
- Prerequisites for Support for PAID PPID Privacy PCPID and PAURI Headers on the Cisco Unified Border Element, page 135
- Restrictions for Support for PAID PPID Privacy PCPID and PAURI Headers on the Cisco Unified Border Element, page 135
- Configuring P-Header and Random-Contact Support on the Cisco Unified Border Element, page 135

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

Feature Name	Releases	Feature Information
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 31: Feature Information for PAID, PPID, Privacy, PCPID, and PAURI Headers on CUBE

Feature Name	Releases	Feature Information
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

	Command or Action	Purpose
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.
Step 3	**voice service voip** **Example:** `Router(config)# voice service voip`	Enters VoIP voice-service configuration mode.
Step 4	**sip** **Example:** `Router(conf-voi-serv)# sip`	Enters voice service VoIP SIP configuration mode.
Step 5	**asserted-id** *header-type* **Example:** `Router(conf-serv-sip)# asserted-id ppi`	Specifies the type of privacy header in the outgoing SIP requests and response messages.
Step 6	**exit** **Example:** `Router(conf-serv-sip)# exit`	Exits the current mode.

Configuring P-Header Translation on an Individual Dial Peer

To configure P-Header translation on an individual dial peer, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *tag* **voip**
4. **voice-class sip asserted-id** *header-type*
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**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.
Step 3	**dial-peer voice** *tag* **voip** **Example:** `Router(config)# dial-peer voice 2611 voip`	Defines the dial peer, specifies the method of voice encapsulation, and enters dial peer voice configuration mode.
Step 4	**voice-class sip asserted-id** *header-type* **Example:** `Router(config-dial-peer)# voice-class sip asserted-id ppi`	Specifies the type of privacy header in the outgoing SIP requests and response messages, on this dial peer.
Step 5	**exit** **Example:** `Router(config-dial-peer)# exit`	Exits the current mode.

Configuring P-Called-Party-Id Support on a Cisco Unified Border Element

To configure P-Called-Party-Id support on a Cisco Unified Border Element, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **sip**
5. **call-route p-called-party-id**
6. **random-request-uri validate**
7. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**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.
Step 3	**voice service voip** **Example:** `Router(config)# voice service voip`	Enters VoIP voice-service configuration mode.
Step 4	**sip** **Example:** `Router(conf-voi-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.

	Command or Action	Purpose
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.

Configuring P-Called-Party-Id Support on an Individual Dial Peer

To configure P-Called-Party-Id support on an individual dial peer, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *tag* **voip**
4. **voice-class sip call-route p-called-party-id**
5. **voice-class sip random-request-uri validate**
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**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	Purpose
Step 3	**dial-peer voice** *tag* **voip** **Example:** `Router(config)# dial-peer voice 2611 voip`	Defines the dial peer, specifies the method of voice encapsulation, and enters dial peer voice configuration mode.
Step 4	**voice-class sip call-route p-called-party-id** **Example:** `Router(config-dial-peer)# voice-class sip call-route p-called-party-id`	Enables the routing of calls based on the PCPID header on this dial peer.
Step 5	**voice-class sip random-request-uri validate** **Example:** `Router(config-dial-peer)# voice-class sip random-request-uri validate`	Enables the validation of the random string in the Request URI of the incoming INVITE message on this dial peer.
Step 6	**exit** **Example:** `Router(config-dial-peer)# exit`	Exits the current mode.

Configuring Privacy Support on a Cisco Unified Border Element

To configure privacy support on a Cisco Unified Border Element, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **sip**
5. **privacy** *privacy-option*
6. **privacy-policy** *privacy-policy-option*
7. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
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-voi-serv)# sip`	Enters voice service VoIP SIP configuration mode.
Step 5	**privacy** *privacy-option* **Example:** `Router(conf-serv-sip)# privacy id`	Enables the privacy settings for the header.
Step 6	**privacy-policy** *privacy-policy-option* **Example:** `Router(conf-serv-sip)# privacy-policy passthru`	Specifies the privacy policy to use when passing the privacy header from one SIP leg to the next.
Step 7	**exit** **Example:** `Router(conf-serv-sip)# exit`	Exits the current mode.

Configuring Privacy Support on an Individual Dial Peer

To configure privacy support on an individual dial peer, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *tag* **voip**
4. **voice-class sip privacy** *privacy-option*
5. **voice-class sip privacy-policy** *privacy-policy-option*
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**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.
Step 3	**dial-peer voice** *tag* **voip** **Example:** `Router(config)# dial-peer voice 2611 voip`	Defines the dial peer, specifies the method of voice encapsulation, and enters dial peer voice configuration mode.
Step 4	**voice-class sip privacy** *privacy-option* **Example:** `Router(config-dial-peer)# voice-class sip privacy id`	Enables the privacy settings for the header on this dial peer.
Step 5	**voice-class sip privacy-policy** *privacy-policy-option* **Example:** `Router(config-dial-peer)# voice-class sip privacy-policy passthru`	Specifies the privacy policy to use when passing the privacy header from one SIP leg to the next, on this dial peer.
Step 6	**exit** **Example:** `Router(config-dial-peer)# exit`	Exits the current mode.

Configuring Random-Contact Support on a Cisco Unified Border Element

To configure random-contact support on a Cisco Unified Border Element, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **sip-ua**
4. **credentials username** *username* **password** *password* **realm** *domain-name*
5. **registrar ipv4:** *destination-address* **random-contact expires** *expiry*
6. **exit**
7. **voice service voip**
8. **sip**
9. **random-contact**
10. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**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.
Step 3	**sip-ua** **Example:** `Router(config)# sip-ua`	Enters SIP user-agent configuration mode.
Step 4	**credentials username** *username* **password** *password* **realm** *domain-name* **Example:** `Router(config-sip-ua)# credentials username 123456 password cisco realm cisco`	Sends a SIP registration message from the Cisco Unified Border Element.
Step 5	**registrar ipv4:** *destination-address* **random-contact expires** *expiry*	Enables the SIP gateways to register E.164 numbers on behalf of analog telephone voice ports (FXS), IP phone virtual voice

	Command or Action	Purpose
	Example: `Router(config-sip-ua)# registrar ipv4:10.1.2.2 random-contact expires 200`	ports (EFXS), and Skinny Client Control Protocol (SCCP) phones with an external SIP proxy or SIP registrar. • The **random-contact** keyword configures the Cisco Unified Border Element to send the random string from the REGISTER message to the registrar.
Step 6	**exit** **Example:** `Router(config-sip-ua)# exit`	Exits the current mode.
Step 7	**voice service voip** **Example:** `Router(config)# voice service voip`	Enters VoIP voice-service configuration mode.
Step 8	**sip** **Example:** `Router(conf-voi-serv)# sip`	Enters voice service VoIP SIP configuration mode.
Step 9	**random-contact** **Example:** `Router(conf-serv-sip)# random-contact`	Enables random-contact support on a Cisco Unified Border Element.
Step 10	**exit** **Example:** `Router(conf-serv-sip)# exit`	Exits the current mode.

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

	Command or Action	Purpose
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.
Step 3	**sip-ua** **Example:** `Router(config)# sip-ua`	Enters SIP user-agent configuration mode.
Step 4	**credentials username** *username* **password** *password* **realm** *domain-name* **Example:** `Router(config-sip-ua)# credentials username 123456 password cisco realm cisco`	Sends a SIP registration message from the Cisco Unified Border Element.
Step 5	**registrar ipv4:** *destination-address* **random-contact expires** *expiry* **Example:** `Router(config-sip-ua)# registrar ipv4:10.1.2.2 random-contact expires 200`	Enables the SIP gateways to register E.164 numbers on behalf of FXS, EFXS, and SCCP phones with an external SIP proxy or SIP registrar. • The **random-contact** keyword configures the Cisco Unified Border Element to send the random string from the REGISTER message to the registrar.

	Command or Action	Purpose
Step 6	**exit** **Example:** `Router(config-sip-ua)# exit`	Exits the current mode.
Step 7	**dial-peer voice** *tag* **voip** **Example:** `Router(config)# dial-peer voice 2611 voip`	Defines the dial peer, specifies the method of voice encapsulation, and enters dial peer voice configuration mode.
Step 8	**voice-class sip random-contact** **Example:** `Router(config-dial-peer)# voice-class sip random-contact`	Enables random-contact support on this dial peer.
Step 9	**exit** **Example:** `Router(config-dial-peer)# exit`	Exits the current mode.

CHAPTER 19

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

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 www.cisco.com/go/cfn. 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

Note With CSCty41575, 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 (Cisco UBE) 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 Cisco UBE does not process because, currently, unsupported payload types are not negotiated by Cisco UBE. 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 Cisco UBE so that both the remote ends can negotiate media independent of Cisco UBE.

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

- Flow-through—Cisco UBE 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—Cisco UBE neither plays a part in media negotiation nor does it terminate and reoriginate media. Media negotiation and media exchange is completely end-to-end.

Unsupported Headers

You can configure Cisco Unified Border Element (Cisco UBE) to pass through unsupported headers (headers Cisco UBE cannot understand) such as SERVER, CALL-INFO, SUPPORTED, ALLOW-EVENTS, RESOURCE-PRIORITY and so on.

Non-mandatory Headers

You can configure Cisco UBE to pass through headers that are not mandatory (headers that Cisco UBE does not pass through by default). You can configure a list of headers to be passed across. The list can contain any header except the mandatory headers shown in the table below.

Table 32: Mandatory Headers List

Mandtory Headers List		
ALSO	AUTHORIZATION	CALLID
CC_DIVERSION	CC_REDIRECT	CONTACT
CONTENT_DISP	CONTENT_ENCODING	CONTENT_LENGTH
CONTENT_TYPE	CISCO_GCID	CISCO_GUID

Mandtory Headers List		
CSEQ	DATE	FROM
MAX_FORWARDS	MIME_VER	MIME_VER_VAL
PRIVACY	PRIVACY_ASSERTED_ID	PRIVACY_PREFERRED_ID
PROXY_AUTH	PROXY_AUTHENTICATE	RECORD_ROUTE
ROUTE	RTP_STAT	SESSION_EXPIRES
TIMESTAMP	TO	USER_AGENT
VIA	WWW_AUTHENTICATE	

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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**voice service voip** **Example:** `Device(config)# voice service voip`	Enters voice service VoIP configuration mode.
Step 4	**sip** **Example:** `Device(conf-voi-serv)# sip`	Enters SIP configuration mode.

Step 5	**pass-thru** {**content** {**sdp** | **unsupp**} | **headers** {**unsupp** | *list-tag*}}
	Example:
	`Device(conf-serv-sip)# pass-thru content unsupp`
		Passes the Session Description Protocol (SDP) transparently from in-leg to the out-leg with no media negotiation.

Step 6	**end**
	Example:
	`Device(conf-serv-sip)# end`
		Ends the current configuration session and returns to privileged EXEC mode.

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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**dial-peer voice** *tag* **voip** **Example:** `Device(config)# dial-peer voice 2 voip`	Enters dial peer VoIP configuration mode.
Step 4	**voice-class sip pass-thru** {**content** {**sdp** | **unsupp**} | **headers** {**unsupp** | **list** *tag*}} [**system**] **Example:** `Device(config-dial-peer)# voice-class sip pass-thru content sdp`	Passes the Session Description Protocol (SDP) transparently from in-leg to the out-leg with no media negotiation.

Step 5	**end**
	Example:
	`Device(config-dial-peer)# end`
		Ends the current configuration session and returns to privileged EXEC mode.

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice class sip-hdr-passthrulist** *list-tag*
4. **passthru-hdr** *header-name*
5. **passthru-hdr-unsupp**
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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**voice class sip-hdr-passthrulist** *list-tag* **Example:** `Device(config)# voice class sip-hdr-passthrulist 101`	Configures list of headers to be passed through and enters voice class configuration mode.
Step 4	**passthru-hdr** *header-name* **Example:** `Device(config-class)# passthru-hdr Resource-Priority`	Adds header name to the list of headers to be passed through. Repeat this step for every non-mandatory header.
Step 5	**passthru-hdr-unsupp** **Example:** `Device(config-class)# passthru-hdr-unsupp`	Adds the unsupported headers to the list of headers to be passed through.

	Command or Action	Purpose
Step 6	**exit** **Example:** `Device(config-class)# exit`	Exits the current configuration session and returns to global configuration mode.
Step 7	**dial-peer voice** *tag* **voip** **Example:** `Device(config)# dial-peer voice 1 voip`	Enters dial peer voice configuration mode.
Step 8	**description** *string* **Example:** `Device(config-dial-peer)# description inbound-dialpeer`	Adds descriptive information about the dial peer.
Step 9	**session protocol sipv2** **Example:** `Device(config-dial-peer)# session protocol sipv2`	Configures the IETF Session Initiation Protocol (SIP) for the dial peer.
Step 10	**voice-class sip pass-thru headers** *list-tag* **Example:** `Device(config-dial-peer)# voice-class sip pass-thru headers 101`	Enables call routing based on the destination route string for a dial peer.

Step 11	**end**
	Example:
	`Device(config-dial-peer)# end`
		Exits the current configuration mode and returns to privileged EXEC mode.

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-passthrulist 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

Related Topic	Document Title
Voice commands	Cisco IOS Voice Command Reference
Cisco IOS commands	Cisco IOS Master Command List, All Releases
SIP configuration tasks	SIP Configuration Guide, Cisco IOS Release 15M&T

Technical Assistance

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

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 33: Feature Information for Configurable Pass-Through of SIP INVITE Parameters

Feature Name	Releases	Feature Information
Configurable Unsupported Header using Pass-Through List	15.4(1)T	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-unsupp** .

Feature Name	Releases	Feature Information
Configurable Route-String Header Pass-Through using a Pass Through List	15.3(3)M	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: **passthru-hdr**, **voice class sip-hdr-passthrulist**.
Configurable Pass-Through of SIP INVITE Parameters	15.0(1)M	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: **pass-thru** and **voice-class sip pass-thru**.

CHAPTER 20

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

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 www.cisco.com/go/cfn. 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.

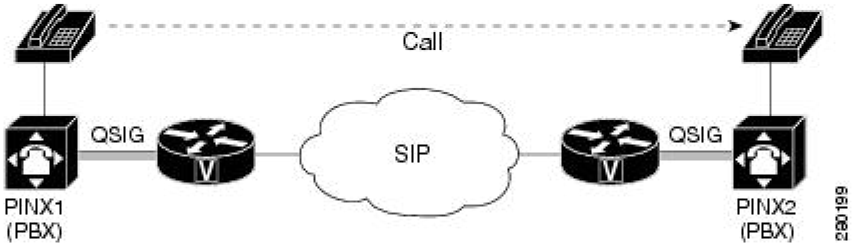
Q.931 tunneling over Cisco IOS SIP gateways was introduced as the ability to transparently tunnel only QSIG messages--the FACILITY-based Q.931 messages. Beginning with Cisco IOS Release 12.4(15)XZ and Cisco IOS Release 12.4(20)T, tunneling of all Q.931 messages (SETUP, ALERTING, CONNECT, and RELEASE 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).

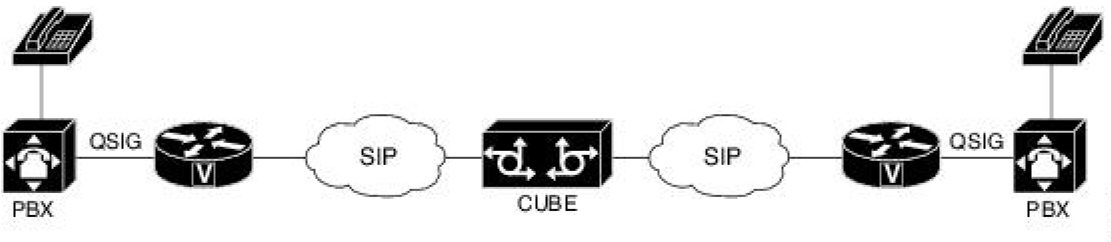
Figure 5: Tunneling QSIG (or Q.931) Messages Across a SIP Trunk



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

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

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

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.

• QSIG FACILITY/NOTIFY/INFO	<-->	SIP INFO
• QSIG SETUP	<-->	SIP INVITE
• QSIG ALERTING	<-->	SIP 180 RINGING
• QSIG PROGRESS	<-->	SIP 183 PROGRESS
• QSIG CONNECT	<-->	SIP 200 OK
• QSIG DISCONNECT	<-->	SIP BYE/CANCEL/4*xx* --6*xx* Response

How to Transparently Tunnel QSIG over SIP

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

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

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

Use the **signaling forward**command at the global configuration level to configure the feature for the entire gateway. You can also enable the QSIG tunneling feature for only a specific interface. If you enable this feature at both the global and dial peer configuration level and the option specified for the interface is different than for the gateway, the interface setting will override the global setting.

Configuring Signaling Forward Settings for a Gateway

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

Signaling Forward Settings for a Gateway

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

Note To override the global setting for a specific interface, use the **signaling forward** command at the dial-peer level (see the Configuring Signaling Forward Settings for an Interface, on page 166).

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

	Command or Action	Purpose
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.
Step 3	voice service voip **Example:** `Router(config)# voice service voip`	Enters voice-service configuration mode and specifies a voice-encapsulation type globally.

Step 4	Do one of the following:
	• **signaling forward** *message-type*
	Example:
	`Router(conf-voi-serv)# signaling forward rawmsg`
	Example:
	Example:
	`Router(conf-voi-serv)# signaling forward unconditional`
		Enables tunneling of QSIG raw messages (application-qsig) only.
		or
		Enables tunneling of all QSIG message bodies unconditionally.

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 169).

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

	Command or Action	Purpose
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.
Step 3	**dial-peer voice** *number* **voip** **Example:** `Router(config)# dial-peer voice 3 voip`	Enters voice-service configuration mode and specifies a voice-encapsulation type for a specific interface.

Step 4	Do one of the following:
	• **signaling forward** *message-type*
	Example:
	`Router(config-dial-peer)# signaling forward rawmsg`
	Example:
	Example:
	`Router(config-dial-peer)# signaling forward unconditional`
		Enables tunneling of QSIG raw messages (application-qsig) only.
		or
		Enables tunneling of all QSIG message bodies unconditionally.

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:

```
!
```

```
voice service voip
 signaling forward rawmsg
 sip
  rel1xx require "100rel"
!
```

Tunneling QSIG Messages Unconditionally over SIP Example

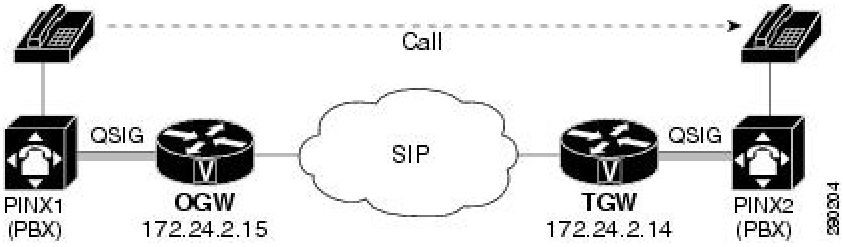
The following example shows how to configure transparent tunneling of QSIG messages unconditionally through a SIP TDM gateway on a SIP trunk at either the OGW or TGW:

```
!
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)



Configuration for OGW (172.24.2.15) Tunneling only QSIG Raw Mmessages

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

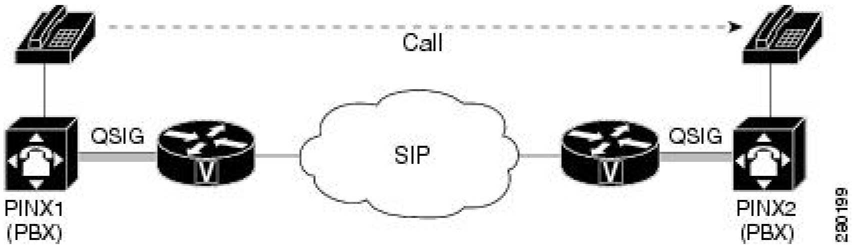
Configuration for TGW (172.24.2.14) Tunneling only QSIG Raw Mmessages

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

Tunneling QSIG Messages Unconditionally over SIP on an 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 34: Feature Information for Transparent Tunneling of QSIG and Q.931 over SIP TDM Gateway and SIP-SIP Cisco Unified Border Element

Feature Name	Releases	Feature Information
Transparent Tunneling of QSIG and Q.931 over SIP TDM Gateway and SIP-SIP Cisco Unified Border Element	12.4(15)XZ 12.4(20)T	This feature adds support for transparent tunneling of all Q.931 messages over SIP and for the Transparent Tunneling of QSIG and Q.931 over a SIP-SIP Cisco Unified Border Element. Transparent tunneling is accomplished by encapsulating QSIG or Q.931 messages within SIP message bodies. These messages are encapsulated using "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. This feature uses no new or modified commands.

History Table for the Cisco Unifired Border Element (Enterprise)

Table 35: Feature Information for Transparent Tunneling of QSIG and Q.931 over SIP TDM Gateway and SIP-SIP Cisco Unified Border Element

Feature Name	Releases	Feature Information
Transparent Tunneling of QSIG and Q.931 over SIP TDM Gateway and SIP-SIP Cisco Unified Border Element	Cisco IOS XE Release 3.1S	This feature adds support for transparent tunneling of all Q.931 messages over SIP and for the Transparent Tunneling of QSIG and Q.931 over a SIP-SIP Cisco Unified Border Element. Transparent tunneling is accomplished by encapsulating QSIG or Q.931 messages within SIP message bodies. These messages are encapsulated using "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. This feature uses no new or modified commands.

CHAPTER 21

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

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 www.cisco.com/go/cfn. 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

	Command or Action	Purpose
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.
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 Agenet 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. An account on Cisco.com is not required. Feature History Table entry for the Cisco Unified Border Element.

Table 36: Feature Information for SIP Diversion Header Enhancements

Feature Name	Releases	Feature Information
SIP Diversion Header Enhancements	12.4(22)T	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**

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

Table 37: Feature Information for SIP Diversion Header Enhancements

Feature Name	Releases	Feature Information
SIP Diversion Header Enhancements	Cisco IOS XE Release 3.1S	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**

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

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 www.cisco.com/go/cfn. 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 3.1or 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: http://www.cisco.com/en/US/docs/ios/voice/sip/configuration/guide/sip_cg-msg_tmr_rspns.html#wp1073292

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 38: Feature Information for SIP History-info Header

Feature Name	Releases	Feature Information
SIP History-info Header	12.4(22)T	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: **history-info**and **voice-class sip history-info**

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

Table 39: Feature Information for SIP History-info Header

Feature Name	Releases	Feature Information
SIP History-info Header	Cisco IOS XE Release 3.1S	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: **history-info**and **voice-class sip history-info**.

CHAPTER 23

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

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 www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for SIP Ability to Send a SIP Registration Message on a Border Element

- Configure a registrar in sip UA configuration mode.

Cisco Unified Border Element

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

Cisco Unified Border Element (Enterprise)

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

Configuring SIP Ability to Send a SIP Registration Message on a Border Element

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**sip-ua** **Example:** `Device(config)# sip-ua`	Enters sip user-agent configuration mode.
Step 4	**credentials username** *username* **password** *password* **realm** *domain-name* **Example:** `Device(config-sip-ua)# credentials username alex password test realm cisco.com`	Enters SIP digest credentials in sip-ua configuration mode.

	Command or Action	Purpose
Step 5	**exit** **Example:** `Device(config-sip-ua)# exit`	Exits the current mode.

Step 6	**end**
	Example:
	`Device(config)# end`
		Returns to privileged EXEC mode.

Feature Information for Sending a SIP Registration Message from a 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 40: Feature Information for Sending a SIP Registration Message from a Cisco Unified Border Element

Feature Name	Releases	Feature Information
SIP: Ability to Send a SIP Registration Message on a Border Element	12.4(24)T	Provides the ability to send a SIP Registration Message from Cisco Unified Border Element. The following command was modified: **credentials** (SIP UA)
SIP: Ability to Send a SIP Registration Message on a Border Element	Cisco IOS XE Release 2.5	Provides the ability to send a SIP Registration Message from Cisco Unified Border Element. The following command was modified: **credentials** (SIP UA)

CHAPTER 24

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

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 www.cisco.com/go/cfn. 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

	Command or Action	Purpose
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.
Step 3	**voice service voip** **Example:** `Router(config)# voice service voip`	Enters voice service VoIP configuration mode.
Step 4	**sip** **Example:** `Router(conf-voi-serv)# sip`	Enters SIP configuration mode.
Step 5	**reset timer expires 183** **Example:** `Router(conf-serv-sip)# reset timer expires 183`	Enables resetting of the Expires timer upon receipt of SIP 183 messages globally.
Step 6	**exit** **Example:** `Router(conf-serv-sip)# exit`	Exits the current mode.

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

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

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. An account on Cisco.com is not required.

Feature History Table entry for the Cisco Unified Border Element.

Table 41: Feature Information for Support for Expires Timer Reset on Receiving or Sending SIP 183 Message

Feature Name	Releases	Feature Information
Support for Expires Timer Reset on Receiving or Sending SIP 183 Message	15.0(1)XA 15.1(1)T	This feature enables support for resetting the Expires timer upon receipt of SIP 183 messages on Cisco Unified Communications Manager Express (Cisco Unified CME), a Cisco IOS voice gateway, or a Cisco Unified Border Element (Cisco UBE). The following commands were introduced or modified: **reset timer expires**and **voice-class sip reset timer expires.**

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

Table 42: Feature Information for Support for Expires Timer Reset on Receiving or Sending SIP 183 Message

Feature Name	Releases	Feature Information
Support for Expires Timer Reset on Receiving or Sending SIP 183 Message	Cisco IOS XE Release 3.1S	This feature enables support for resetting the Expires timer upon receipt of SIP 183 messages on Cisco Unified Communications Manager Express (Cisco Unified CME), a Cisco IOS voice gateway, or a Cisco Unified Border Element (Cisco UBE). The following commands were introduced or modified: **reset timer expires**and **voice-class sip reset timer expires.**

CHAPTER 25

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

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 43: Feature Information for Dynamic REFER Handling

Feature Name	Releases	Feature Information
REFER Consume (Enhancements)	IOS 15.5(1)T IOS XE 3.14.0 S	REFER Consume (Enhancements) provides additional configurations to conditionally forward the REFER message. The following commands were introduced: **refer consume**.
Dynamic REFER Handling	IOS 15.2(1)T IOS XE Release 3.7S	The Dynamic REFER handling feature provides configurations to pass across or consume the REFER message The following commands were introduced: **referto-passing**, **voice-class sip referto-passing**.

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.

supplementary service refer	Results
yes	REFER is passed through from the in leg to the out leg

supplementary service refer	Results
no	INVITE is sent towards refer-to dial-peer

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:
   - **referto-passing** in Global VoIP SIP configuration mode.
   - **voice-class sip referto-passing [system]** in dial-peer configuration mode.
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	Configure REFER passthrough: • **supplementary-service sip refer** in global VoIP configuration mode. • **supplementary-service sip refer** in dial-peer configuration mode. **Example:**	Configures REFER passthrough. A REFER is sent towards the inbound dial peer

	Command or Action	Purpose

	In Global VoIP configuration mode:
	`Device(config)# voice service voip`
	`Device(conf-voi-serv)# supplementary-service sip refer`
	Example:
	In dial-peer configuration mode:
	`Device(config)# dial-peer voice 22 voip`
	`Device(config-dial-peer)# supplementary-service sip refer`	

Step 4	Configure unmodified Refer-to:
	• **referto-passing** in Global VoIP SIP configuration mode.
	• **voice-class sip referto-passing [system]** in dial-peer configuration mode.
	Example:
	In Global VoIP configuration mode:
	`Device(config)# voice service voip`
	`Device(conf-voi-serv)# sip`
	`Device(conf-serv-sip)# referto-passing`
	Example:
	In dial-peer configuration mode:
	`Device(config)# dial-peer voice 22 voip`
	`Device(config-dial-peer)# voice-class sip referto-passing`
		(Optional)
		Ensures that the refer-to header is unmodified and not changed to the IP address during passthrough

Step 5	**end**	Exits to privileged EXEC mode.

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 44: Configurations for REFER Consumption

supplementary service refer	refer consume	Results
yes	no	REFER is sent towards inbound dial-peer
yes	yes	INVITE is sent towards refer-to dial-peer
no	no	INVITE is sent towards refer-to dial-peer
no	yes	INVITE is sent towards refer-to dial-peer

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. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

Step 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.
	Example:
	In global VoIP configuration mode:
	`Device(config)# voice service voip`
	`Device(conf-voi-serv)# no supplementary-service sip refer`
	Example:
	In dial-peer configuration mode:
	`Device(config)# dial-peer voice 22 voip`
	`Device(config-dial-peer)# no supplementary-service sip refer`
		Configures REFER consumption. An INVITE is sent towards the Refer-to dial peer.

	Command or Action	Purpose

Step 4	**refer consume** in global VoIP configuration mode.
	Example:
	In dial-peer configuration mode:
	`Device(config)# dial-peer voice 22 voip`
	`Device(config-dial-peer)# refer consume`
		Configures REFER consumption.

Step 5	**supplementary-service media-renegotiate** in global VoIP configuration mode.
	Example:
	In global VoIP configuration mode:
	`Device(config)# voice service voip`
	`Device(conf-voi-serv)# supplementary-service media-renegotiate`
		(Optional)
		Enables end-to-end media renegotiation during the call transfer in REFER consumption mode.

Step 6	**end**	Exits to privileged EXEC mode.

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**

CHAPTER 26

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

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 www.cisco.com/go/cfn. 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 <TBD> 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 (RFC3361) to get a SIP server address, and this can be used by any vendor DHCP server. Only one address is supported, which is in the IPv4 address format. Multiple IPv4 address entries are not supported. Also, there is no support for a DNS name in this or for any port number given behind the IPv4 address.
- DHCP Option 125 (RFC 3925) provides vendor-specific information and its interpretation is associated with the enterprise identity. The primary and secondary phone numbers and domain are obtained using Option 125, which is vendor-specific. As long as other customers use the same format as in the Next Generation Network (NGN) DHCP specification, they can use this feature.
- A primary or contract number is required in suboption 202 of DHCP Option 125. There can be only one instance of the primary number and not multiple instances.
- Multiple secondary or numbers in suboption 203 of DHCP Option 125 are supported. Up to five numbers are accepted and the rest ignored. Also, they have to follow the contract number in the DHCP packet data.
- Authentication is not supported for REGISTER and INVITE messages sent from a Cisco Unified Border Element that uses DHCP provisioning
- The DHCP provisioning of SIP Parameters is supported only over one DHCP interface.
- The DHCP option is available only to be configured for the primary registrar. It will not be available for a secondary registrar.

Information About Configurable SIP Parameters via DHCP

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

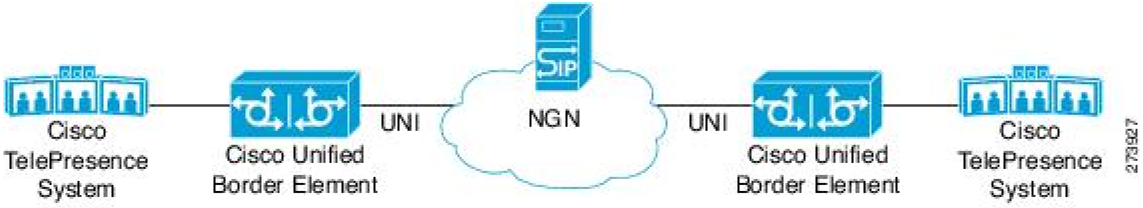
Cisco Unified Border Element Support for Configurable SIP Parameters via DHCP

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


Cisco TelePresence System
Cisco Unified Border Element
UNI
SIP
NGN
UNI
Cisco Unified Border Element
Cisco TelePresence System
273927

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

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

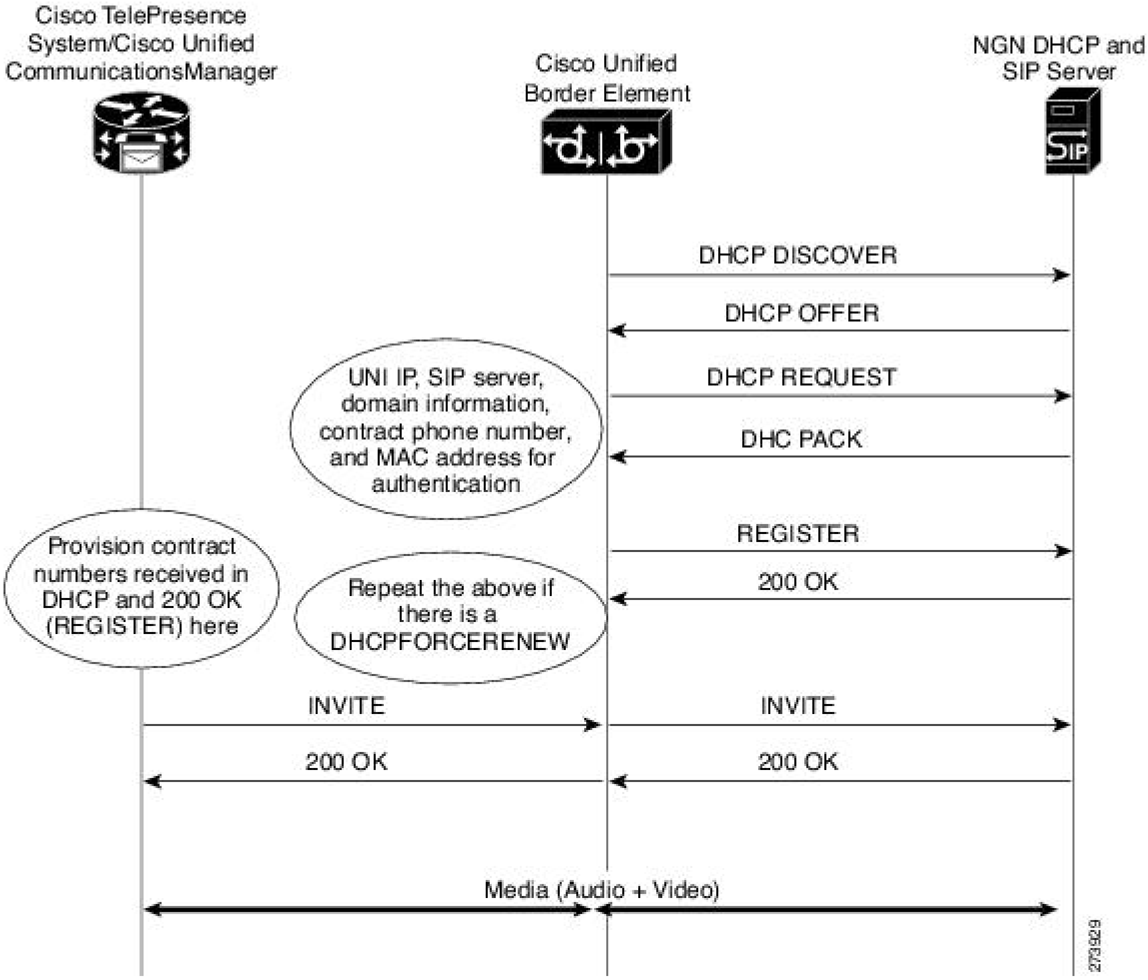
- IP address for Cisco Unified Border Element’s UNI interface facing NGN
- SIP server address using option 120
- Option 125 vendor specific information to get:
  - Pilot number (also called primary or contract number), there is only one pilot number in DHCPACK, and REGISTER is done only for the pilot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

DHCP-SIP Call Flow

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

The figure below shows the DHCP and SIP messages involved in obtaining the SIP parameters and using them for REGISTER and INVITE.

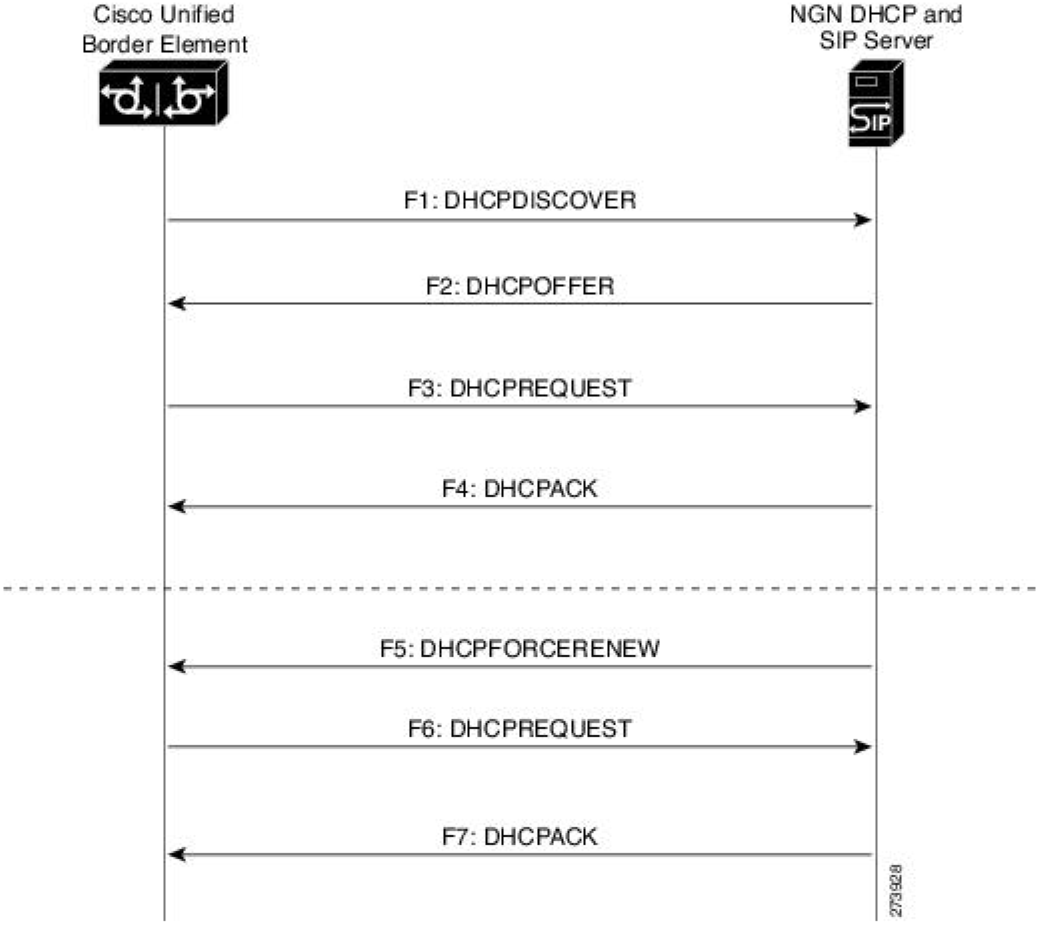
Figure 10: DHCP-SIP Call Flow


Cisco TelePresence System/Cisco Unified CommunicationsManager
Cisco Unified Border Element
NGN DHCP and SIP Server
DHCP DISCOVER
DHCP OFFER
UNI IP, SIP server, domain information, contract phone number, and MAC address for authentication
DHCP REQUEST
DHC PACK
REGISTER
Provision contract numbers received in DHCP and 200 OK (REGISTER) here
200 OK
Repeat the above if there is a DHCPFORCERENEW
INVITE
INVITE
200 OK
200 OK
Media (Audio + Video)
273929

DHCP Message Details

The DHCP call flow involved in obtaining Cisco Unified Border Element provision information, including the IP address for UNI interface and SIP information such as phone number, domain, and SIP server, is shown in the figure below.

Figure 11: DHCP Message Details



The DHCP messages involved in provisioning the SIP parameters are described in Steps 1 to 6.

1. F1: The Cisco Unified Border Element DHCP client sends a DHCPDISCOVER message to find the available NGN DHCP servers on the network and obtain a valid IPv4 address. The Cisco Unified Border Element DHCP client identity (computer name) and MAC address are included in this message.
2. F2: The Cisco Unified Border Element DHCP client receives a DHCPOFFER message from each available NGN DHCP server. The DHCPOFFER message includes the offered DHCP server's IPv4 address, the DHCP client's MAC address, and other configuration parameters.
3. F3: The Cisco Unified Border Element DHCP client selects an NGN DHCP server and its IPv4 address configuration from the DHCPOFFER messages it receives, and sends a DHCPREQUEST message requesting its usage. Note that this is where Cisco Unified Border Element requests SIP server information via DHCP Option 120 and vendor- identifying information via DHCP Option 125.

4 F4: The chosen NGN DHCP server assigns its IPv4 address configuration to the Cisco Unified Border Element DHCP client by sending a DHCPACK message to it. The Cisco Unified Border Element DHCP client receives the DHCPACK message. This is where the SIP server address, phone number and domain name information are received via DHCP options 120 and 125. The Cisco Unified Border Element will use the information for registering the phone number and routing INVITE messages to the given SIP server.

5 F5: When NGN has a change of information or additional information (such as changing SIP server address from 1.1.1.1 to 2.2.2.2) for assigning to Cisco Unified Border Element, the DHCP server initiates DHCPFORCERENEW to the Cisco Unified Border Element. If the authentication is successful, the Cisco Unified Border Element DHCP client accepts the DHCPFORCERENEW and moves to the next stage of sending DHCPREQUEST. Otherwise DHCPFORCERENEW is ignored and the current information is retained and used.

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

How to Configure SIP Parameters via DHCP

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

	Command or Action	Purpose
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.
Step 3	**interface type number** **Example:** `Router(config)# interface gigabitethernet 0/0`	Configures an interface type and enters interface configuration mode.
Step 4	**ip dhcp client request sip-server-address** **Example:** `Router(config-if)# ip dhcp client request sip-server-address`	Configures the DHCP client to request a SIP server address from a DHCP server.
Step 5	**ip dhcp client request vendor-identifying-specific** **Example:** `Router(config-if)# ip dhcp client request vendor-identifying-specific`	Configures the DHCP client to request vendor-specific information from a DHCP server.
Step 6	**ip address dhcp** **Example:** `Router(config-if)#` **ip address dhcp**	Acquires an IP address on the interface from the DHCP.

	Command or Action	Purpose
Step 7	**exit** **Example:** `Router(config-if)# exit`	Exits the current mode.

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

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface type number** **Example:** `Router(config)# interface gigabitethernet 0/0`	Configures an interface type and enters interface configuration mode.
Step 4	**sip-ua** **Example:** `Router(config-if)# sip-ua`	Enters SIP user-agent configuration mode.
Step 5	**dhcp interface type number** **Example:** `Router(sip-ua)# dhcp interface gigabitethernet 0/0`	Assigns a specific interface for DHCP provisioning of SIP parameters. • Multiple interfaces on the CUBE can be configured with DHCP--this command specifies the DHCP interface used with SIP.
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.

	Command or Action	Purpose
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

	Command or Action	Purpose
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.
Step 3	**voice service voip** **Example:** `Router(config)# voice service voip`	Enters voice service VoIP configuration mode and specifies VoIP as the voice-encapsulation type.
Step 4	**sip** **Example:** `Router(config-voi-srv)# sip`	Enters voice service SIP configuration mode.
Step 5	**outbound-proxy dhcp** **Example:** `Router(conf-serv-sip)# outbound-proxy dhcp`	Configures the DHCP client to request a SIP server address from a DHCP server.
Step 6	**exit** **Example:** `Router(config-serv-sip)# exit`	Exits the current mode.

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

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

```
Router> enable
Router# configure terminal

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

Configuring a SIP Outbound Proxy Server 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.

Note 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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**dial-peer voice number voip** **Example:** `Router(config)# dial-peer voice 10 voip`	Defines a dial peer, specifies VoIP as the method of voice encapsulation, and enters dial peer configuration mode.
Step 4	**session protocol sipv2** **Example:** `Router(config-dial-peer)# session protocol sipv2`	Enters the session protocol type as SIP.
Step 5	**voice-class sip outbound-proxy dhcp** **Example:** `Router(config-dial-peer)# voice-class sip outbound-proxy dhcp`	Configures the SIP server received from the DHCP server as a SIP outbound proxy server.
Step 6	**session target dhcp** **Example:** `Router(config-dial-peer)# session target dhcp`	Specifies that the DHCP protocol is used to determine the IP address of the session target.
Step 7	**exit** **Example:** `Router(config-dial-peer)# exit`	Exits the current mode.

Configuring a SIP Outbound Proxy Server in Dial Peer Configuration Mode Example

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

```
Router> enable
Router# configure terminal
Router(config)# dial-peer voice 11 voip
Router(config-dial-peer)# session protocol sipv2

Router(config-dial-peer)# voice-class sip outbound-proxy dhcp
Router(config-dial-peer)# session target dhcp
Router(config-dial-peer)# exit
```

Feature Information for Configurable SIP Parameters via DHCP

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 45: Feature Information for Configurable SIP Parameters via DHCP

Feature Name	Releases	Feature Information
Configurable SIP Parameters via DHCP	12.4(22)YB 15.0(1)M	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**.

Feature History Table for the ASR.

Table 46: Feature Information for Configurable SIP Parameters via DHCP

Feature Name	Releases	Feature Information
Configurable SIP Parameters via DHCP	IOS XE Release <TBD>	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**.

CHAPTER 27

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

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 www.cisco.com/go/cfn. 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 47: Feature Information for the Multiple Registrars on SIP Trunks Feature

Feature Name	Releases	Feature Information
Multiple Registrars on SIP Trunks	15.0(1)XA 15.1(1)T	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**.

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

Table 48: Feature Information for the Multiple Registrars on SIP Trunks Feature

Feature Name	Releases	Feature Information
Multiple Registrars on SIP Trunks	Cisco IOS XE Release 3.1S	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**.

CHAPTER 28

Handle Multiple Early Dialog Messages

In a VoIP/SIP network, services such as call forward trigger multiple early dialog creation on Cisco UBE. SIP forking proxy will fork the SIP invite request to multiple endpoints and send out multiple forked invite responses to Cisco UBE. The Handle Multiple Early Dialog Messages feature enables Cisco UBE to respond to the forked invite responses.

Note A SIP forking proxy is a proxy sever that routes messages to more than one destination.

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 www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Handle Multiple Early Dialog Messages

This feature does not support the following calls:

- SIP-H323
- Media Anti-trombone
- Session Description Protocol (SDP) Passthrough

- SRTP-RTP interworking and SRTP passthrough
- RSVP and RSVP interworking
- TCL and VXML application

Information About Handle Early Dialog Messages

Multiple Early Dialog Support

The Handle Multiple Early Dialog Messages feature is enabled on Cisco UBE by default. When a service such as call forward triggers multiple early dialog creation on Cisco UBE, the SIP forking proxy will fork the SIP invite request to multiple endpoints and multiple invite responses are sent out to Cisco UBE. Cisco UBE handles the forked invite responses on the outbound call-leg and updates the peer (inbound) call-leg with an early dialog UPDATE message. This message renegotiates the media information, and Cisco UBE maps the appropriate dialog and responds to the forked responses.

Note UPDATE and PRACK (rel1xx) support is a prerequisite for this feature.

Verifying the Handle Multiple Early Dialog Messages Feature

Perform this task to verify the multiple early dialog messages support on Cisco UBE. The **show** commands can be entered in any order.

SUMMARY STEPS

1. **enable**
2. **show call active voice compact**
3. **show call active voice brief**
4. **show voip rtp connections**

DETAILED STEPS

Step 1 **enable**

Example:

```
Router> enable
```

Enables privileged EXEC mode.

Step 2 **show call active voice compact**

Example:

```
Router# show call active voice compact

<callID> A/O FAX T<sec> Codec type Peer Address IP R<ip>:<udp>
Total call-legs: 2
42 ANS T9 g711ulaw VOIP P1000 10.0.1.10:20796
43 ORG T9 g711ulaw VOIP P2000 10.0.2.20:21252
```

Displays a compact version of the voice calls in progress.

Step 3 **show call active voice brief**

Example:

```
Router#  show voice active voice brief | inc tx

dur hh:mm:ss tx:<packets>/<bytes> rx:<packets>/<bytes> dscp:<packets violation> media:<packets
violation>
Tele <int> (callID) [channel_id] tx:<tot>/<v>/<fax>ms <codec> noise:<l> acom:<l> i/o:<l>/<l> dBm
speeds(bps): local <rx>/<tx> remote <rx>/<tx>
tx: <audio pkts>/<audio bytes>,<video pkts>/<video bytes>,<t120 pkts>/<t120 bytes>
dur 00:00:10 tx:507/81120 rx:510/81600 dscp:0 media:0
dur 00:00:10 tx:510/81600 rx:507/81120 dscp:0 media:0
```

Displays a truncated version of the active voice or video call information.

Step 4 **show voip rtp connections**

Example:

```
Router# show voip rtp connections

VoIP RTP active connections :
No. CallId dstCallId LocalRTP RmtRTP LocalIP      RemoteIP
1   42     43          18440    20796  9.44.44.44 9.44.46.21
2   43     42          22668    21252  9.44.44.44 9.44.46.25
Found 2 active RTP connections
```

Displays RTP-named event packets.

Troubleshooting Tips

The following commands can help troubleshoot the Handle Multiple Early Dialog Messages feature:

- **debug ccsip all**
- **debug voip ccapi inout**

Feature Information for Handle Multiple Early Dialog Messages

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 49: Feature Information for Handle Multiple Early Dialog Messages

Feature Name	Releases	Feature Information
Handle Multiple Early Dialog Messages	15.2(2)T	In a VoIP/SIP network, services such as call forward trigger multiple early dialog creation on Cisco UBE. SIP forking proxy will fork the SIP invite request to multiple endpoints and send out multiple forked invite responses to Cisco UBE. The Handle Multiple Early Dialog Messages feature enables Cisco UBE to respond to the forked invite responses. No commands were introduced or modified by this feature.

CHAPTER 29

Monitoring of Phantom Packets

The Monitoring of Phantom Packets feature allows you to configure port ranges specific to the VoIP Real-Time Transport Protocol (RTP) layer. This allows the VoIP RTP layer to safely drop packets without proper sessions (phantom packets) received on these ports of the Cisco Unified Border Element (CUBE) or Voice time-division multiplexing (TDM) gateways. Because the ports are configured specifically for the VoIP RTP layer, there is no need to punt the packets to the RP (control plane) in case the packets were intended for some other application, thus reducing performance issues.

Restrictions of Monitoring of Phantom Packets

- The authentication, authorization, and accounting (AAA) default port range of 21645 to 21844 must not be configured.
- Up to ten port range entries can be defined under a single media-address range.
- The minimum port must be numerically lower than the maximum port.
- Port ranges should not overlap.
- Address ranges should not overlap.
- Address ranges and single addresses should not overlap
- Where a range of addresses are defined in a single command, they will share any port ranges assigned. If there is a requirement to have different port ranges for different media addresses, then the addresses must be configured separately.
- The interface used for media and signaling should be different.

- The media address and the signaling address should not be identical. If the media address and the signaling address are identical, and the Cisco IOS XE based router platform (Cisco ASR 1000 Series Aggregation Services Router, Cisco 4000 Series Integrated Services Routers, or Cisco Cloud Services Router 1000V Series) selects an ephemeral port to send out signaling packets, the port may overlap with the port range of the media address. As a result, the signaling packets do not get punted up to the RP, and get dropped by the media packet filter. This may result in events such as incomplete TCP handshakes during the second leg of a call through CUBE or Voice Gateways.

Information About Monitoring of Phantom Packets

Monitoring of Phantom Packets

The Monitoring of Phantom Packets feature allows you to configure port ranges specific to the VoIP Real-Time Transport Protocol (RTP) layer. This configuration allows the VoIP RTP layer to safely drop packets without proper sessions (phantom packets) received on the ports of the Cisco Unified Border Element (CUBE) or Voice time-division multiplexing (TDM) gateways. Because the ports are configured specifically for the VoIP RTP layer, there is no need to punt the packets to the UDP process in case the packets were intended for some other application, thus reducing performance issues.

A phantom packet is a valid RTP packet meant for the CUBE or Voice TDM gateway without an existing session on the respective gateways. When a phantom packet is received by the VoIP RTP layers of the gateways, the packet is punted to the UDP process to check if it is required by any other applications causing performance issues, especially when a large number of such packets are received. A malicious attacker can also send a large number of phantom packets. The packet is punted to the UDP process because UDP port ranges are shared by many applications other than VoIP RTP and the VoIP RTP layer cannot drop the packet assuming the packet is for itself.

This feature allows you to configure port ranges specific to the VoIP RTP layer. If a phantom packet is received on the configured port, the VoIP RTP layer can safely drop the packet. If a phantom packet is received on any other port, the VoIP RTP layer punts the packet to the UDP process.

How to Configure Monitoring of Phantom Packets

Configuring Monitoring of Phantom Packets

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **media-address range** *starting-ip-address ending-ip-address*
5. **port-range** *starting-port-number ending-port-number*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**voice service voip** **Example:** `Device(config)# voice service voip`	Specifies VoIP encapsulation and enters voice-service configuration mode.

Step 4	**media-address range** *starting-ip-address ending-ip-address*
	Example:
	Using IPv4 addresses:
	`Device(conf-voi-serv)# media-address range 10.1.1.1 10.1.1.254`
	Example:
	Using IPv6 addresses:
	`Device(conf-voi-serv)# media-address range 2001:DB8:1::1 2001:DB8:1::17`
		Configures an IPv4 or IPv6 media address range.

Step 5	**port-range** *starting-port-number ending-port-number* **Example:** `Device(cfg-media-addr-range)# port-range 32766 32768`	Configures a port range.

Step 6	**end**
	Example:
	`Router(cfg-media-addr-range)# end`
		Exits voice-service configuration mode and returns to privileged EXEC mode.

Configuration Examples For Monitoring of Phantom Packets

```
Device(config)# voice service voip
Device(conf-voi-serv))# media-address range 10.1.1.1 10.1.1.254
Device(cfg-media-addr-range)# port-range 32766 32768
Device(cfg-media-addr-range)# port-range 16384 16386
Device(cfg-media-addr-range)# exit

Device(conf-voi-serv))# media-address range 2001:DB8:1::1 2001:DB8:1::17
Device(cfg-media-addr-range)# port-range 32766 32768
Device(cfg-media-addr-range)# port-range 16384 16386
Device(cfg-media-addr-range)# end
```

Additional References for Configurable Pass-Through of SIP INVITE Parameters

Related Documents

Related Topic	Document Title
Voice commands	Cisco IOS Voice Command Reference
Cisco IOS commands	Cisco IOS Master Command List, All Releases
SIP configuration tasks	SIP Configuration Guide, Cisco IOS Release 15M&T

Technical Assistance

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

Feature Information for Monitoring of Phantom Packets

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 50: Feature Information for Monitoring of Phantom Packets

Feature Name	Releases	Feature Information
Monitoring of Phantom Packets	Cisco IOS XE Release 3.9S 15.4(1)T	This feature allows you to configure port ranges specific to the VoIP Real-Time Transport Protocol (RTP) layer and drop phantom RTP packets (RTP packets that are configured in valid port range but for which there is no matching call or session). The following commands were introduced: **port-range**, **media-address range**.

CHAPTER 30

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-IP gateway) for V.150.1 calls to traverse a CUBE in SDP passthrough flow-through mode.

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 www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About VER.150.1 MER Support in SDP Passthrough Mode

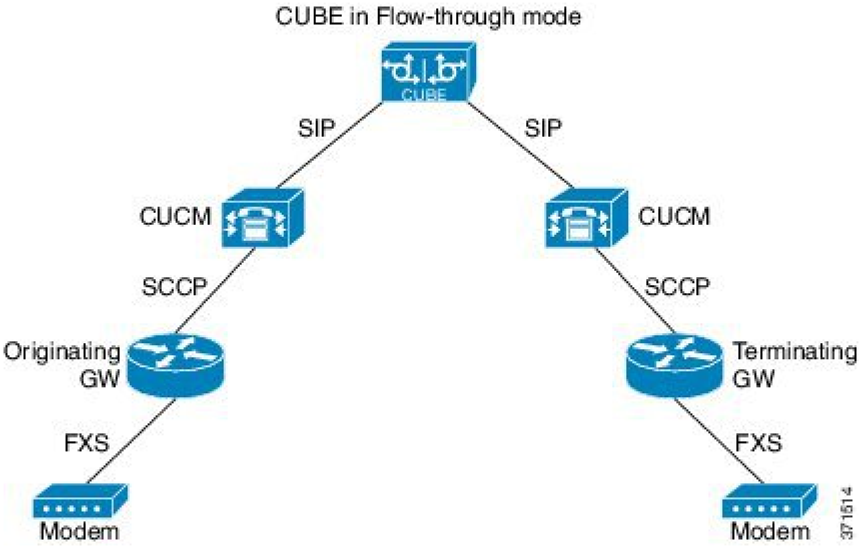
V.150.1 MER Support in SDP Passthrough Mode

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).

Modem Relay Topology

Figure 12: Topology—Modem Relay



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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

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 (conf-voi-serv)#sip`
	`Device (conf-serv-sip)#pass-thru content sdp mode non-rtp`
	`Device (conf-serv-sip)#end`	

Step 4	**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:
010363: *Jan 31 12:34:00.148: //31/14B4F1000000/SIP/Function/sipSPI_ipip_IsSDPPassthruEnabled:
010364: *Jan 31 12:34:00.148:
//31/14B4F1000000/SIP/Info/critical/8192/sipSPI_ipip_IsSDPPassthruEnabled:  - 1
010365: *Jan 31 12:34:00.148: //31/14B4F1000000/SIP/Function/sipSPI_ipip_SetSDPPassthruMode:
010366: *Jan 31 12:34:00.148: //31/14B4F1000000/SIP/Info/info/128/sipSPI_ipip_SetSDPPassthruMode:
SDP Passthru Mode is set to - 1

011365: *Jan 31 12:34:02.604: //31/14B4F1000000/SIP/Function/sipSPIGetStream:
011366: *Jan 31 12:34:02.604:
//32/14B4F1000000/SIP/Info/info/128/sipSPI_ipip_UpdatePthruStreamRtcpInfo: Setting stream xmit
function to voip_udp_xmit
011367: *Jan 31 12:34:02.604: //32/14B4F1000000/SIP/Function/sipSPIGetRSVPIPTos
```

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 51: Feature Information for V.150.1 MER Support for SDP Passthrough

Feature Name	Releases	Feature Information
V.150.1 MER Support for SDP Passthrough	15.4(2)T	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**