Cisco Unified Border Element (Enterprise) Protocol-Independent Features and Setup Configuration Guide, Cisco IOS XE Release 2

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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

© 2011 Cisco Systems, Inc. All rights reserved.

CONTENTS

Cisco Unified Border Element Enterprise Protocol-Independent Features and Setup

This Cisco Unified Border Element (Enterprise) is a special Cisco IOS XE software image that runs on Cisco ASR1000. It provides a network-to-network interface point for billing, security, call admission control, quality of service, and signaling interworking. This chapter describes basic gateway functionality, software images, topology, and summarizes supported features.

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 feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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 Enterprise Protocol-Independent Features and Setup

This chapter contains the following configuration topics:

Cisco UBE (Enterprise) Prerequisites and Restrictions

Dial Plan Management

- Dial Peer Configuration on Voice Gateway Routers http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/dial_peer/dpeer_c.html

- Translation Rules

http://www.cisco.com/en/US/docs/ios/voice/command/reference/vr_t3.html#wp1651612

- ENUM support
- Configuring Tool Command Language (Tcl)

http://www.cisco.com/en/US/products/sw/voicesw/ps2192/products_programming_reference_guides_list.html

- Cisco Service Advertisement Framework (SAF)

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps8802/ps10587/ps10591/ps10621/product_bulletin_c25-561938.html#wp9000293

Configuring Call Admissions Control

- VoIP Call Admissions Control

http://www.cisco.com/en/US/docs/ios/solutions_docs/voip_solutions/CAC.html

Resource Reservation Protocol (RSVP)

- Interworking Between RSVP Capable and RSVP Incapable Networks
- Cisco Resource Reservation Protocol Agent

Dual-Tone Multifrequency (DTMF) Support and Interworking

- SIP--INFO Method for DTMF Tone Generation
- DTMF Events through SIP Signaling
- Configuring SIP DTMF Features

http://www.cisco.com/en/US/docs/ios/12_3/sip/configuration/guide/chapter8.html

- H.323 RFC2833 - SIP NOTIFY

http://www.cisco.com/en/US/docs/ios/voice/sip/configuration/guide/sip_cg-dtmf_ps6441_TSD_Products_Configuration_Guide_Chapter.html#wp1062375

Codec Negotiation

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

Transcoding

- iLBC Support for SIP and H.323
- Negotiation of an Audio Codec From a List of Codecs on Each Leg of a SIP-to-SIP Call on the Cisco UBE

Payload Type Interoperability

- Interworking Between RSVP Capable and RSVP Incapable Networks
- Modem Pass Through Capability for Individual Dial Peers

http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/dial_peer/dp_confg.html#wp1068501

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

Transrating

- DSP Based Functionality on the Cisco UBE (Enterprise) Including Transcoding and Transrating

Voice Quality Controls

- QoS Marking Settings on dial-peers

http://www.cisco.com/en/US/docs/ios/voice/command/reference/vr_i1.html#wp1109014

Fax/modem Support

- Modem passthrough
- T.38 Fax Relay

http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/cisco_ios_fax_services_over_ip_application_guide/t38.html

- Cisco Fax Relay

http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/cisco_ios_fax_services_over_ip_application_guide/cisrly.html

H.323 Video

- Cisco Unified Border Element Videoconferencing

SIP Video

- SIP Video Calls with Flow Around Media
- RTP Media Loopback for SIP Calls
- Configuring RTP Media Loopback for SIP Calls

Telepresence

- SIP Video Support for Telepresence Calls

Security Features

- Toll Fraud Prevention

http://www.cisco.com/en/US/docs/ios/ios_xe/voice_cube_-_ent/configuration/guide/vb_ch2_xe.html

- Access lists (ACLs)

http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_tech_note09186a00809dc487.shtml?

- CAC (call spike)

http://www.cisco.com/en/US/docs/ios/voice/command/reference/vr_c3.html#wp1210005?

- SIP--Ability to Send a SIP Registration Message on a Border Element
- SIP Parameter Modification

- SIP--SIP Stack Portability
- Session Refresh with Reinvites
- CDR

http://www.cisco.com/en/US/docs/ios/voice/cube/configuration/guide/vb-gw-overview_ps5640_TSD_Products_Configuration_Guide_Chapter.html#wp1166707

- Transport Layer Security (TLS)
- Interworking of Secure RTP calls for SIP and H.323
- SIP SRTP Fallback to Nonsecure RTP
- VRF aware H.323 and SIP

IPv4 and IPv6 Interworking

- VoIP for IPv6

RSVP Interworking

- Interworking Between RSVP Capable and RSVP Incapable Networks

Collocated Services

- Software Media Termination Point
- Cisco Unified Communication Trusted Firewall Control
- Cisco Unified Communication Trusted Firewall Control-Version II
- Cisco Unified Border Element with Gatekeeper

http://www.cisco.com/en/US/docs/ios/voice/cubegk/configuration/guide/ve_book/ve_book.html

- Toll Fraud Prevention, page 4

Toll Fraud Prevention

When a Cisco router platform is installed with a voice-capable Cisco IOS software image, appropriate features must be enabled on the platform to prevent potential toll fraud exploitation by unauthorized users. Deploy these features on all Cisco router Unified Communications applications that process voice calls, such as Cisco Unified Communications Manager Express (CME), Cisco Survivable Remote Site Telephony (SRST), Cisco Unified Border Element (UBE), Cisco IOS-based router and standalone analog and digital PBX and public-switched telephone network (PSTN) gateways, and Cisco contact-center VoiceXML gateways. These features include, but are not limited to, the following:

- Disable secondary dial tone on voice ports--By default, secondary dial tone is presented on voice ports on Cisco router gateways. Use private line automatic ringdown (PLAR) for foreign exchange office (FXO) ports and direct-inward-dial (DID) for T1/E1 ports to prevent secondary dial tone from being presented to inbound callers.
- Cisco router access control lists (ACLs)--Define ACLs to allow only explicitly valid sources of calls to the router or gateway, and therefore to prevent unauthorized Session Initiation Protocol (SIP) or H.323 calls from unknown parties to be processed and connected by the router or gateway.
- Close unused SIP and H.323 ports--If either the SIP or H.323 protocol is not used in your deployment, close the associated protocol ports. If a Cisco voice gateway has dial peers configured to route calls outbound to the PSTN using either time division multiplex (TDM) trunks or IP, close the unused H.323 or SIP ports so that calls from unauthorized endpoints cannot connect calls. If the protocols are used and the ports must remain open, use ACLs to limit access to legitimate sources.

- Change SIP port 5060--If SIP is actively used, consider changing the port to something other than well-known port 5060.
- SIP registration--If SIP registration is available on SIP trunks, turn on this feature because it provides an extra level of authentication and validation that only legitimate sources can connect calls. If it is not available, ensure that the appropriate ACLs are in place.
- SIP Digest Authentication--If the SIP Digest Authentication feature is available for either registrations or invites, turn this feature on because it provides an extra level of authentication and validation that only legitimate sources can connect calls.
- Explicit incoming and outgoing dial peers--Use explicit dial peers to control the types and parameters of calls allowed by the router, especially in IP-to-IP connections used on CME, SRST, and Cisco UBE. Incoming dial peers offer additional control on the sources of calls, and outgoing dial peers on the destinations. Incoming dial peers are always used for calls. If a dial peer is not explicitly defined, the implicit dial peer 0 is used to allow all calls.
- Explicit destination patterns--Use dial peers with more granularity than.T for destination patterns to block disallowed off-net call destinations. Use class of restriction (COR) on dial peers with specific destination patterns to allow even more granular control of calls to different destinations on the PSTN.
- Translation rules--Use translation rules to manipulate dialed digits before calls connect to the PSTN to provide better control over who may dial PSTN destinations. Legitimate users dial an access code and an augmented number for PSTN for certain PSTN (for example, international) locations.
- Tcl and VoiceXML scripts--Attach a Tcl/VoiceXML script to dial peers to do database lookups or additional off-router authorization checks to allow or deny call flows based on origination or destination numbers. Tcl/VoiceXML scripts can also be used to add a prefix to inbound DID calls. If the prefix plus DID matches internal extensions, then the call is completed. Otherwise, a prompt can be played to the caller that an invalid number has been dialed.
- Host name validation--Use the "permit hostname" feature to validate initial SIP Invites that contain a fully qualified domain name (FQDN) host name in the Request Uniform Resource Identifier (Request URI) against a configured list of legitimate source hostnames.
- Dynamic Domain Name Service (DNS)--If you are using DNS as the "session target" on dial peers, the actual IP address destination of call connections can vary from one call to the next. Use voice source groups and ACLs to restrict the valid address ranges expected in DNS responses (which are used subsequently for call setup destinations).

For more configuration guidance, see the " Cisco IOS Unified Communications Toll Fraud Prevention " paper.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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

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 feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

Cisco Unified Border Element

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

Cisco Unified Border Element (Enterprise)

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

Information About SIP INFO Method for DTMF Tone Generation

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

How to Review SIP INFO Messages

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

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

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

Prerequisites

The following are general prerequisites for SIP functionality:

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

Restrictions

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

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

Configuring for SIP INFO Method for DTMF Tone Generation

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

Troubleshooting Tips

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

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

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

```
Router# show sip-ua statistics
SIP Response Statistics (Inbound/Outbound)
Informational:
Trying 1/1, Ringing 0/0,
Forwarded 0/0, Queued 0/0,
SessionProgress 0/1
Success:
OkInvite 0/1, OkBye 1/0,
OkCancel 0/0, OkOptions 0/0,
OkPrack 0/0, OkPreconditionMet 0/0
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:

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

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.

ISR Feature table entry

Table 1 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**.

ASR Feature table entry

Table 2 Feature Information for SIP: INFO Method for DTMF Tone Generation

Feature Name	Releases	Feature Information
SIP: INFO Method for DTMF Tone Generation	IOS XE Release 2.5	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**.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams,

and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

DTMF Events through SIP Signaling

The DTMF Events through SIP Signaling feature provides the following:

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

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

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

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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 DTMF Events through SIP Signaling

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 DTMF Events through SIP Signaling

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

Configuring DTMF Events through SIP Signaling

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode or any 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	**sip-ua** **Example:** `Router(config)# sip-ua`	Enters SIP user-agent configuration mode.

	Command or Action	Purpose
Step 4	**timers notify** *number* **Example:** `Router(config-sip-ua)# timers notify 100`	Sets the amount of time that the user agent waits before retransmitting the Notify message. The argument is as follows: • *number* --Time, in milliseconds, to wait before retransmitting. Range: 100 to 1000. Default: 500.
Step 5	**retry notify** *number* **Example:** `Router(config-sip-ua)# retry notify 6`	Sets the number of times that the Notify message is retransmitted to the user agent that initiated the transfer or Refer request. The argument is as follows: • *number* --Number of retries. Range: 1 to 10. Default: 10.
Step 6	**exit** **Example:** `Router(config-sip-ua)# exit`	Exits the current mode.

• Verifying SIP DTMF Support, page 15

Verifying SIP DTMF Support

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

SUMMARY STEPS

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

DETAILED STEPS

Step 1 **show running-config**

Use this command to show dial-peer configurations.

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

Example:

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

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

Example:

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

Step 2 **show sip-ua retry**

Use this command to display SIP retry statistics.

Example:

```
Router# show sip-ua retry
SIP UA Retry Values
invite retry count = 6 response retry count = 1
bye retry count = 1 cancel retry count = 1
prack retry count = 10 comet retry count = 10
reliable 1xx count = 6 notify retry count = 10
```

Step 3 **show sip-ua statistics**

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

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

Example:

```
Router# show sip-ua statistics
SIP Response Statistics (Inbound/Outbound)
Informational:
```

```
Trying 4/2, Ringing 2/1,
Forwarded 0/0, Queued 0/0,
SessionProgress 0/0
Success:
OkInvite 1/2, OkBye 0/1,
OkCancel 1/0, OkOptions 0/0,
OkPrack 2/0, OkPreconditionMet 0/0,
OkNotify 1/0, 202Accepted 0/1
Redirection (Inbound only):
MultipleChoice 0, MovedPermanently 0,
MovedTemporarily 0, SeeOther 0,
UseProxy 0, AlternateService 0
Client Error:
BadRequest 0/0, Unauthorized 0/0,
PaymentRequired 0/0, Forbidden 0/0,
NotFound 0/0, MethodNotAllowed 0/0,
NotAcceptable 0/0, ProxyAuthReqd 0/0,
ReqTimeout 0/0, Conflict 0/0, Gone 0/0,
LengthRequired 0/0, ReqEntityTooLarge 0/0,
ReqURITooLarge 0/0, UnsupportedMediaType 0/0,
BadExtension 0/0, TempNotAvailable 0/0,
CallLegNonExistent 0/0, LoopDetected 0/0,
TooManyHops 0/0, AddrIncomplete 0/0,
Ambiguous 0/0, BusyHere 0/0
RequestCancel 1/0, NotAcceptableMedia 0/0
Server Error:
InternalError 0/1, NotImplemented 0/0,
BadGateway 0/0, 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) /* Traffic Statistics
Invite 3/2, Ack 3/2, Bye 1/0,
Cancel 0/1, Options 0/0,
Prack 0/2, Comet 0/0,
Notify 0/1, Refer 1/0
Retry Statistics                             /* Retry Statistics
Invite 0, Bye 0, Cancel 0, Response 0,
Prack 0, Comet 0, Reliable1xx 0, Notify 0
```

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

Example:

```
Router# show sip-ua statistics
SIP Response Statistics (Inbound/Outbound)
Informational:
Trying 1/1, Ringing 0/0,
Forwarded 0/0, Queued 0/0,
SessionProgress 0/1
Success:
OkInvite 0/1, OkBye 1/0,
OkCancel 0/0, OkOptions 0/0,
OkPrack 0/0, OkPreconditionMet 0/0
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
```

Step 4 **show sip-ua status**

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

Example:

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

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

Example:

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

```
 Timespec line (t=) required
 Media supported: audio image
 Network types supported: IN
 Address types supported: IP4
 Transport types supported: RTP/AVP udptl
```

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

Example:

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

Step 5 **show sip-ua timers**

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

Example:

```
Router# show sip-ua timers
SIP UA Timer Values (millisecs)
trying 500, expires 300000, connect 500, disconnect 500
comet 500, prack 500, rel1xx 500, notify 500
```

Step 6 **show voip rtp connections**

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

Step 7 **show sip-ua calls**

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

The following sample output shows that the DTMF method isSIP-KPML.

Example:

```
router# show sip-ua calls
SIP UAC CALL INFO
Call 1
SIP Call ID                : 57633F68-2BE011D6-8013D46B-B4F9B5F6@172.18.193.251
   State of the call       : STATE_ACTIVE (7)
   Substate of the call    : SUBSTATE_NONE (0)
   Calling Number          :
   Called Number           : 8888
   Bit Flags               : 0xD44018 0x100 0x0
   CC Call ID              : 6
   Source IP Address (Sig ): 192.0.2.1
   Destn SIP Req Addr:Port : 192.0.2.2:5060
   Destn SIP Resp Addr:Port: 192.0.2.3:5060
   Destination Name        : 192.0.2.4.250
   Number of Media Streams : 1
   Number of Active Streams: 1
```

```
    RTP Fork Object         : 0x0
    Media Mode              : flow-through
    Media Stream 1
      State of the stream      : STREAM_ACTIVE
      Stream Call ID           : 6
      Stream Type              : voice-only (0)
      Negotiated Codec         : g711ulaw (160 bytes)
     Codec Payload Type       : 0
      Negotiated Dtmf-relay    : sip-kpml
      Dtmf-relay Payload Type  : 0
      Media Source IP Addr:Port: 192.0.2.5:17576
      Media Dest IP Addr:Port  : 192.0.2.6:17468
      Orig Media Dest IP Addr:Port : 0.0.0.0:0
    Number of SIP User Agent Client(UAC) calls: 1
 SIP UAS CALL INFO
    Number of SIP User Agent Server(UAS) calls: 0
```

Troubleshooting Tips

- To enable debugging for RTP named-event packets, use the **debug voip rtp** command.
- To enable KPML debugs, use the **debug kpml** command.
- To enable SIP debugs, use the **debug ccsip** command.
- Collect debugs while the call is being established and during digit presses.
- If an established call is not sending digits through KPML, use the **show sip-ua calls** command to ensure SIP-KPML is included in the negotiation process.

Feature Information for DTMF Events through SIP Signaling

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

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

ISR Feature History Entry.

Table 3 Feature Information for Configuring DTMF Events through SIP Signaling

Feature Name	Releases	Feature Information
DTMF Events through SIP Signaling	12.2(11)T 12.2(8)YN 12.2(15)T 12.2(11)YV 12.2(11)T,	The DTMF Events through SIP Signaling feature provides the following: • DTMF event notification for SIP messages. • Capability of receiving hookflash event notification through the SIP NOTIFY method. • Third-party call control, or other signaling mechanisms, to provide enhanced services, such as calling card and messaging services. • Communication with the application outside of the media connection. The following commands were introduced or modified: **timers notify** and **retry notify**.

ASR Feature History Entry.

Table 4 Feature Information for Configuring DTMF Events through SIP Signaling

Feature Name	Releases	Feature Information
DTMF Events through SIP Signaling	Cisco IOS XE Release 2.5	The DTMF Events through SIP Signaling feature provides the following: • DTMF event notification for SIP messages. • Capability of receiving hookflash event notification through the SIP NOTIFY method. • Third-party call control, or other signaling mechanisms, to provide enhanced services, such as calling card and messaging services. • Communication with the application outside of the media connection. The following commands were introduced or modified: **timers notify** and **retry notify**.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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

Negotiation of an Audio Codec from a List of Codecs

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

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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.

Benefits

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

- You can configure dissimilar Voice Class Codec configurations on the incoming and outgoing dial peers.
- Both normal transcoding and high-density transcoding are supported with the Voice Class Codec configuration.
- Mid-call codec changes for supplementary services are supported with the Voice Class Codec configuration. Transcoder resources are dynamically inserted or deleted when required.

- Reinvite-based supplementary services invoked from the Cisco Unified Communications Manager (CUCM), like call hold, call resume, music on hold (MOH), call transfer, and call forward are supported with the Voice Class Codec configuration.
- T.38 fax and fax passthru switchover with Voice Class Codec configuration are supported.
- Reinvite-based call hold and call resume for Secure Real-Time Transfer protocol (SRTP) and Real-Time Protocol (RTP) interworking on Cisco UBE are supported with the Voice Class Codec configuration.

Prerequisites for Negotiation of an Audio Codec from a List of Codecs

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

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

Cisco Unified Border Element

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

Cisco Unified Border Element (Enterprise)

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

Restrictions for Negotiation of an Audio Codec from a List of Codecs

The Negotiation of an Audio Codec from a List of Codecs on Each Leg of a SIP-to-SIP Call on the Cisco Unified Border Element feature has the following limitations:

- Mid-call insertion or deletion of the transcoder with voice class codec for H323-H323 and H323-SIP is not supported.
- Voice class codec is not supported for video calls.

Disabling Codec Filtering

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

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

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

SUMMARY STEPS

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

DETAILED STEPS

	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 10 voip`	Enters dial peer voice configuration mode.
Step 4	**voice-class codec** *tag* [**offer-all**] **Example:** `Router(config-dial-peer)# voice-class codec 10 offer-all`	Adds all the configured voice class codec to the outgoing offer from the Cisco UBE.
Step 5	**end** **Example:** `Router(config-dial-peer)# end`	Exits the dial peer voice configuration mode.

Troubleshooting Negotiation of an Audio Codec from a List of Codecs

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

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

Verifying Negotiation of an Audio Codec from a List of Codecs

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

SUMMARY STEPS

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

DETAILED STEPS

Step 1 **enable**

Enables privileged EXEC mode.

Step 2 **show call active voice brief**

Displays a truncated version of call information for voice calls in progress.

Example:

```
Router# show call active voice brief
<ID>: <CallID> <start>ms.<index> +<connect> pid:<peer_id> <dir> <addr> <state>
  dur hh:mm:ss tx:<packets>/<bytes> rx:<packets>/<bytes>
 IP <ip>:<udp> rtt:<time>ms pl:<play>/<gap>ms lost:<lost>/<early>/<late>
  delay:<last>/<min>/<max>ms <codec>
 media inactive detected:<y/n> media cntrl rcvd:<y/n> timestamp:<time>
 long duration call detected:<y/n> long duration call duration :<sec> timestamp:<time>
  MODEMPASS <method> buf:<fills>/<drains> loss <overall%> <multipkt>/<corrected>
   last <buf event time>s dur:<Min>/<Max>s
 FR <protocol> [int dlci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
  <codec> (payload size)
 ATM <protocol> [int vpi/vci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
  <codec> (payload size)
 Tele <int> (callID) [channel_id] tx:<tot>/<v>/<fax>ms <codec> noise:<l> acom:<l> i/o:<l>/<l> dBm
  MODEMRELAY info:<rcvd>/<sent>/<resent> xid:<rcvd>/<sent> total:<rcvd>/<sent>/<drops>
```

```
         speeds(bps): local <rx>/<tx> remote <rx>/<tx>
 Proxy <ip>:<audio udp>,<video udp>,<tcp0>,<tcp1>,<tcp2>,<tcp3> endpt: <type>/<manf>
 bw: <req>/<act> codec: <audio>/<video>
  tx: <audio pkts>/<audio bytes>,<video pkts>/<video bytes>,<t120 pkts>/<t120 bytes>
 rx: <audio pkts>/<audio bytes>,<video pkts>/<video bytes>,<t120 pkts>/<t120 bytes>
Telephony call-legs: 0
SIP call-legs: 2
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 2
Multicast call-legs: 0
Total call-legs: 4
1243 : 11 971490ms.1 +-1 pid:1 Answer 1230000 connecting
 dur 00:00:00 tx:415/66400 rx:17/2561
 IP 192.0.2.1:19304 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off
 media inactive detected:n media contrl rcvd:n/a timestamp:n/a
 long duration call detected:n long duration call duration:n/a timestamp:n/a
1243 : 12 971500ms.1 +-1 pid:2 Originate 3210000 connected
 dur 00:00:00 tx:5/10 rx:4/8
 IP 9.44.26.4:16512 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g729br8 TextRelay: off
 media inactive detected:n media contrl rcvd:n/a timestamp:n/a
 long duration call detected:n long duration call duration:n/a timestamp:n/a
0    : 13 971560ms.1 +0 pid:0 Originate  connecting
 dur 00:00:08 tx:415/66400 rx:17/2561
 IP 192.0.2.2:2000 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off
 media inactive detected:n media contrl rcvd:n/a timestamp:n/a
 long duration call detected:n long duration call duration:n/a timestamp:n/a
0    : 15 971570ms.1 +0 pid:0 Originate  connecting
 dur 00:00:08 tx:5/10 rx:3/6
 IP 192.0.2.3:2000 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g729br8 TextRelay: off
 media inactive detected:n media contrl rcvd:n/a timestamp:n/a
 long duration call detected:n long duration call duration:n/a timestamp:n/a
Telephony call-legs: 0
SIP call-legs: 2
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 2
Multicast call-legs: 0
Total call-legs: 4
```

Step 3 **show voip rtp connections**

Displays Real-Time Transport Protocol (RTP) connections.

Example:

```
Router# show voip rtp connections
VoIP RTP active connections :
No. CallId     dstCallId  LocalRTP RmtRTP     LocalIP                                RemoteIP
1     11         12         16662    19304    192.0.2.1
192.0.2.2
2     12         11         17404    16512    192.0.2.2
192.0.2.3
3     13         14         18422    2000     192.0.2.4
9.44.26.3
4     15         14         16576    2000     192.0.2.6
192.0.2.5
Found 4 active RTP connections
```

Step 4 **show sccp connections**

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

Example:

```
Router# show sccp connections
sess_id    conn_id      stype mode     codec   sport rport ripaddr
5          5            xcode sendrecv g729b   16576 2000  192.0.2.3
```

```
5          6            xcode sendrecv g711u   18422 2000  192.0.2.4
Total number of active session(s) 1, and connection(s) 2
```

Step 5 **show dspfarm dsp active**

Displays active DSP information about the DSP farm service.

Example:

```
Router# show dspfarm dsp active
SLOT DSP VERSION  STATUS CHNL USE   TYPE    RSC_ID BRIDGE_ID PKTS_TXED PKTS_RXED
0    1   27.0.201 UP     1    USED  xcode   1      0x9        5         8
0    1   27.0.201 UP     1    USED  xcode   1      0x8        2558      17
Total number of DSPFARM DSP channel(s) 1
```

Feature Information for Negotiation of an Audio Codec from a List of Codecs

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 ISR

Table 5 Feature Information for Negotiation of an Audio Codec from a List of Codecs on Each Leg of a SIP-to-SIP Call on the Cisco Unified Border Element

Feature Name	Releases	Feature Information
Negotiation of an Audio Codec from a List of Codecs on Each Leg of a SIP-to-SIP Call on the Cisco Unified Border Element	15.1(2)T	The Negotiation of an Audio Codec from a List of Codecs on Each Leg of a SIP-to-SIP Call on the Cisco Unified Border Element feature supports negotiation of an audio codec using the Voice Class Codec and Codec Transparent infrastructure on the Cisco UBE. The following command was introduced or modified: **voice-class codec (dial peer).**

Feature History Table entry for the ASR

Table 6 Feature Information for Negotiation of an Audio Codec from a List of Codecs on Each Leg of a SIP-to-SIP Call on the Cisco Unified Border Element

Feature Name	Releases	Feature Information
Negotiation of an Audio Codec from a List of Codecs on Each Leg of a SIP-to-SIP Call on the Cisco Unified Border Element	Cisco IOS XE Release 2.5	The Negotiation of an Audio Codec from a List of Codecs on Each Leg of a SIP-to-SIP Call on the Cisco Unified Border Element feature supports negotiation of an audio codec using the Voice Class Codec and Codec Transparent infrastructure on the Cisco UBE. The following command was introduced or modified: **voice-class codec (dial peer)**.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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

iLBC Support for SIP and H.323

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

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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 iLBC Support for SIP and H.323

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 iLBC Support for SIP and H.323

The iLBC Support for SIP and H.323 feature is supported on the following:

- IP-to-IP gateways with no transcoding and conferencing
- All c5510 DSP-based platforms

Information About iLBC Support for SIP and H.323

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

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

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

How to Configure an iLBC Codec

- Configuring an iLBC Codec on a Dial Peer, page 32
- Configuring an iLBC Codec in the Voice Class, page 34
- Verifying iLBC Support for SIP and H.323, page 36

Configuring an iLBC Codec on a Dial Peer

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

SUMMARY STEPS

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

DETAILED STEPS

	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 10 voip`	Enters dial-peer configuration mode for the VoIP dial peer designated by *tag*.

Step 4	**rtp payload-type cisco-codec-ilbc** [*number*
	
	Example:
	
	`Router(config-dial-peer)# rtp payload-type cisco-codec-ilbc 100`
		Identifies the payload type of a Real-Time Transport Protocol (RTP) packet. Keyword and argument are as follows:
		
		• **cisco-codec-ilbc** [*number*]--Payload type is for internet Low Bit Rate Codec (iLBC). Range: 96 to 127. Default: 116.
		
		Note Do not use the following numbers because they have preassigned values: 96, 97, 100, 117, 121 to 123, and 125 to 127. If you use these values, the command will fail. You must first reassign the value in use to a different unassigned number, for example:
		
		`rtp payload-type nse 105`
		`rtp payload-type cisco-codec-ilbc 100`

Step 5	**codec ilbc** [**mode** *frame_size* [**bytes** *payload_size*]] **Example:** `Router(config-dial-peer)# codec ilbc mode 30 bytes 200`	Specifies the voice coder rate of speech for a dial peer. Keywords and arguments are as follows: • **mode** *frame_size* --The iLBC operating frame mode that will be encapsulated in each packet. Valid entries are 20 (20ms frames for 15.2kbps bit rate) or 30 (30ms frames for 13.33 kbps bit rate). Default is 20. • **bytes** *payload_size* --Number of bytes in an RTP packet. For mode 20, valid values are 38 (default), 76, 114, 152, 190, and 228. For mode 30, valid values are 50(default), 100, 150, and 200.

	Command or Action	Purpose
Step 6	**exit** **Example:** `Router(config-dial-peer)# exit`	Exits the current mode.

Configuring an iLBC Codec in the Voice Class

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

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

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters 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	**voice class codec** *tag* **Example:** `Router(config)# voice class codec 99`	Enters voice-class configuration mode and assigns an identification tag number for a codec voice class. The argument is as follows: • *tag* --Unique identifier on the router. Range is 1 to 10000.
Step 4	**codec preference** *value* **ilbc** [**mode** *frame_size*] [**bytes** *payload_size*] **Example:** `Router(config-voice-class)# codec preference 1 ilbc 30 200`	Specifies a list of preferred codecs to use on a dial peer. Keywords and arguments are as follows: • *value* --Order of preference, with 1 being the most preferred and 14 being the least preferred. • **mode** *frame_size* --The iLBC operating frame mode that will be encapsulated in each packet. Valid entries are 20 (20ms frames for 15.2kbps bit rate) or 30 (30ms frames for 13.33 kbps bit rate). Default is 20. • **bytes** *payload_size* --Number of bytes in an RTP packet. For mode 20, valid values are 38 (default), 76, 114, 152, 190, and 228. For mode 30, valid values are 50(default), 100, 150, and 200.
Step 5	**exit** **Example:** `Router(config-voice-class)# exit`	Exits the current mode.
Step 6	**dial-peer voice** *tag* **voip** **Example:** `Router(config)# dial-peer voice 16 voip`	Enters dial-peer configuration mode for the specified VoIP dial peer.
Step 7	**voice-class codec** *tag* **Example:** `Router(config-dial-peer)# voice-class codec 99`	Assigns a previously configured codec selection preference list (the codec voice class that you defined in step 3) to the specified VoIP dial peer. **Note** The **voice-class codec**command in dial-peer configuration mode contains a hyphen. The **voice class** command in global configuration mode does not contain a hyphen.
Step 8	**exit** **Example:** `Router(config-dial-peer)# exit`	Exits the current mode.

Verifying iLBC Support for SIP and H.323

You can use the following commands to check iLBC status:

- **show voice call summary**
- **show voice call status**
- **show voice dsmp stream**
- **show call active voice**
- **show call history voice**
- **show voice dsp and its extensions**
- **show dial-peer voice**
- **show voice dsp channel operational-status**

Feature Information for iLBC Support for SIP and H.323

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 7 Feature Information for iLBC Support for SIP and H.323

Feature Name	Releases	Feature Information
iLBC Support for SIP and H.323	12.2(11)T 12.2(15)T	The iLBC is a standard, high-complexity speech codec suitable for robust voice communication over IP. The iLBC has built-in error correction functionality that helps the codec perform in networks with high-packet loss. This codec is supported on both Session Initiation Protocol (SIP) and H.323. The following commands were introduced or modified: **codec ilbc**, **codec preference**, and **rtp payload-type**.

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

Table 8 Feature Information for iLBC Support for SIP and H.323

Feature Name	Releases	Feature Information
iLBC Support for SIP and H.323	Cisco IOS XE Release 2.5	The iLBC is a standard, high-complexity speech codec suitable for robust voice communication over IP. The iLBC has built-in error correction functionality that helps the codec perform in networks with high-packet loss. This codec is supported on both Session Initiation Protocol (SIP) and H.323. The following commands were introduced or modified: **codec ilbc**, **codec preference**, and **rtp payload-type**.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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.

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.

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:** `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	**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 alex password test realm cisco.com`	Enters SIP digest credentials in sip-ua configuration mode.
Step 5	**exit** **Example:** `Router(config-sip-ua)# exit`	Exits the current mode.
Step 6	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.

- Feature Information for Sending a SIP Registration Message from a Cisco Unified Border Element, page 42

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.

Feature History Table entry for the Cisco Unified Border Element.

Table 9 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)

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

Table 10 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	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)

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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

SIP Parameter Modification

Cisco Unified Border Element

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

Cisco Unified Border Element (Enterprise)

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

Note

- This feature applies to outgoing SIP messages.
- This feature is disabled by default.
- Removal of mandatory headers is not supported.
- This feature allows removal of entire MIME bodies from SIP messages. Addition of MIME bodies is not supported.

The SIP Parameter modification feature allow customers to add, remove, or modify the SIP parameters in the SIP messages going out of a border element. The SIP message is generated from the standard signaling stack, but runs the message through a parser which can add, delete or modify specific parameters. This allows interoperability with additional third party devices that require specific SIP message formats. All SIP methods and responses are supported, profiles can be added either in dial-peer level or global level. Basic Regular Expression support would be provided for modification of header values. SDP parameters can also be added, removed or modified.

This feature is applicable only for outgoing SIP messages. Changes to the messages are applied just before they are sent out, and the SIP SPI code does not remember the changes. Because there are no restrictions on the changes that can be applied, users must be careful when configuring this feature - for example, the call might fail if a regular expression to change the To tag value is configured.

In releases prior to Cisco IOS Release 15.1(3)S1, outgoing SIP messages used to have non-token characters in server and user-agent SIP headers. In Cisco IOS Release 15.1(3)S1 and later releases, server and user-agent SIP headers have only token characters. Token characters can be a alphanumeric character, hyphen (-), dot (.), exclamation mark (!), percent (%), asterisk (*), underscore (_), plus sign (+), grave (`), apostrophe ('), or a tilde (~).

The **all** keyword is used to apply rules on all requests and responses.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service** *number* **voip**
4. **voice-class sip-profiles** *group-number*
5. **response** *option* **sip-header** *option* ADD *word* CR
6. **exit**
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**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** *number* **voip** **Example:** `Router(config)# voice service 1 voip`	Enters VoIP voice-service configuration mode.
Step 4	**voice-class sip-profiles** *group-number* **Example:** `Router(config)# voice-class sip profiles 42`	Establishes individual sip profiles defined by a group-number. Valid group-numbers are from 1 to 1000.
Step 5	**response** *option* **sip-header** *option* ADD *word* CR **Example:** `Router(config)# request INVITE sip-header supported remove`	Add, change, or delete any SIP or SDP header in voice class or sip-profile submode.

	Command or Action	Purpose
Step 6	**exit** **Example:** `Router(config-dial-peer)# exit`	Exits the current mode.
Step 7	**end** **Example:** `Router(config-voi-srv)# end`	Returns to privileged EXEC mode.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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.

Example

```
!
!
!
voice service voip
allow-connections sip to sip
redirect ip2ip
sip
early-offer forced
midcall-signaling passthru
sip-profiles 1
!
!
!
voice class sip-profiles 1
request INVITE sip-header Supported remove
request INVITE sip-header Min-SE remove
request INVITE sip-header Session-Expires remove
request INVITE sip-header Unsupported modify "Unsupported:" "timer"
!
!
!
```

Feature Information for Configuring SIP Parameter Modification

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 11 Feature Information for Configuring SIP Parameter Modification

Feature Name	Releases	Feature Information
SIP Parameter Modification	12.4(15)XZ 12.4(20)T	Allows users to change the standard SIP messages sent from the Cisco SIP stack for better interworking with different SIP entities. This feature introduces or modifies the following commands: **voice class sip-profiles**, **voice-class sip profiles**

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

Table 12 Feature Information for Configuring SIP Parameter Modification

Feature Name	Releases	Feature Information
SIP Parameter Modification	Cisco IOS XE Release 2.5	Allows users to change the standard SIP messages sent from the Cisco SIP stack for better interworking with different SIP entities. This feature introduces or modifies the following commands: **voice class sip-profiles**, **voice-class sip profiles**

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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.

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.

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: sess 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.

>

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.

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.

	Command or Action	Purpose
Step 6	**exit** **Example:** `Router(conf-serv-sip)# exit`	Exits the current mode.
Step 7	**end** **Example:** `Router(conf-serv-sip) end`	Returns to privileged EXEC mode.

• Feature Information for Session Refresh with Reinvites, page 55

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 History Table for the ASR

Table 13 Feature Information for Session Refresh with Reinvites

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. **midcall-signaling**

Feature History Table for the ISR

Table 14 Feature Information for Session Refresh with Reinvites

Feature Name	Releases	Feature Information
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. **midcall-signaling**

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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

SIP Stack Portability

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

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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 Stack Portability

Cisco Unified Border Element

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

Cisco Unified Border Element (Enterprise)

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

Information About SIP Stack Portability

The SIP Stack Portability feature implements the following capabilities to the Cisco IOS SIP gateway stack:

- It receives inbound Refer message requests both within a dialog and outside of an existing dialog from the user agents (UAs).
- It sends and receives SUBSCRIBE or NOTIFY message requests via UAs.
- It receives unsolicited NOTIFY message requests without having to subscribe to the event that was generated by the NOTIFY message request.
- It supports outbound delayed media.

It sends an INVITE message request without Session Description Protocol (SDP) and provides SDP information in either the PRACK or ACK message request for both initial call establishment and mid-call re-INVITE message requests.

- It sets SIP headers and content body in requests and responses.

The stack applies certain rules and restrictions for a subset of headers and for some content types (such as SDP) to protect the integrity of the stack's functionality and to maintain backward compatibility. When receiving SIP message requests, it reads the SIP header and any attached body without any restrictions.

To make the best use of SIP call-transfer features, you should understand the following concepts:

SIP Call-Transfer Basics

Basic Terminology of SIP Call Transfer

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

Refer Message Request

The SIP Refer message request provides call-transfer capabilities to supplement the SIP BYE and ALSO message requests already implemented on Cisco IOS SIP gateways. The Refer message request has three main roles:

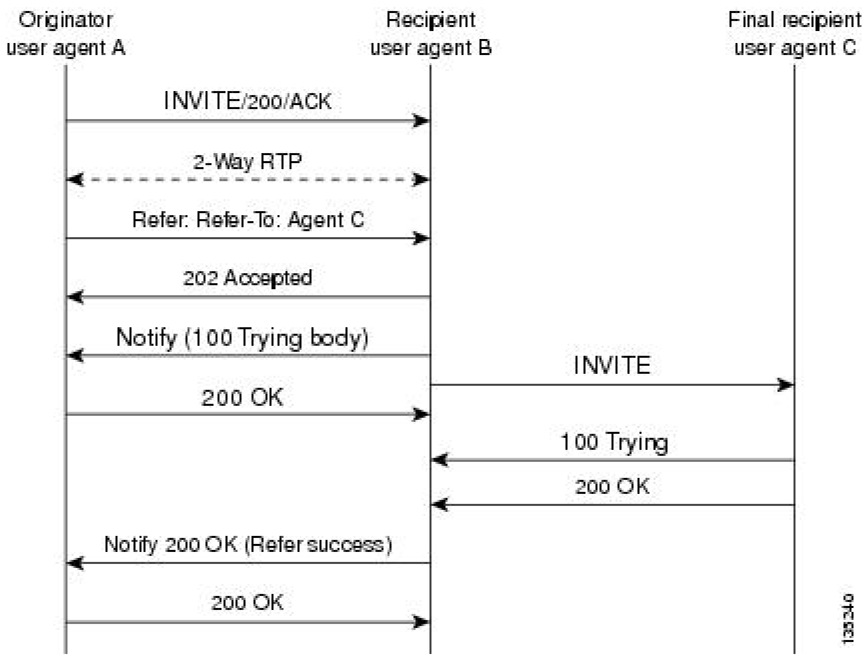
- Originator--User agent that initiates the transfer or Refer request.
- Recipient--User agent that receives the Refer request and is transferred to the final-recipient.
- Final-Recipient--User agent introduced into a call with the recipient.

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

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

The figure below represents the call flow of a successful Refer transaction initiated within the context of an existing call.

Figure 1 Successful Refer transaction



Refer-To Header

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

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

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

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

All other headers present in the Refer-To are ignored, and are not sent in the triggered INVITE.

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

Referred-By Header

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

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

NOTIFY Message Request

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

The NOTIFY message must do the following:

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

Two Cisco IOS commands pertain to the NOTIFY message request:

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

Note For information on these commands, see the *Cisco IOS Voice Command Reference* .

Types of SIP Call Transfer Using the Refer Message Request

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

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

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

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

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

Blind Call-Transfer Process

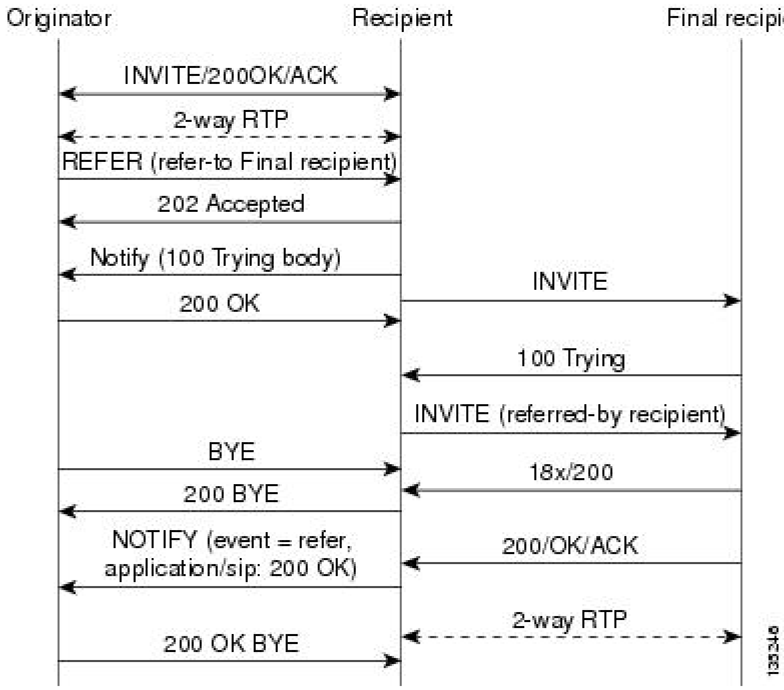
A blind, or unattended, transfer is one in which the transferring phone connects the caller to a destination line before ringback begins. This is different from a consultative, or attended, transfer in which one of the transferring parties either connects the caller to a ringing phone (ringback heard)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

Blind transfer works as described in the Types of SIP Call Transfer Using the Refer Message Request, page 60. The process is as follows:

1. Originator (user agent that initiates the transfer or Refer request) does the following:
    a. Sets up a call with recipient (user agent that receives the Refer request)
    b. Issues a Refer request to recipient
2. Recipient does the following:
    a. Sends an INVITE request to final recipient (user agent introduced into a call with the recipient)
    b. Returns a SIP 202 (Accepted) response to originator
    c. Notifies originator of the outcome of the Refer transaction--whether final recipient was successfully (SIP 200 OK) contacted or not (SIP 503 Service Unavailable)
3. If successful, a call is established between recipient and final recipient.
4. The original signaling relationship between originator and recipient terminates when either of the following occurs:
5. One of the parties sends a Bye request.
6. Recipient sends a Bye request after successful transfer (if originator does not first send a Bye request after receiving an acknowledgment for the NOTIFY message).

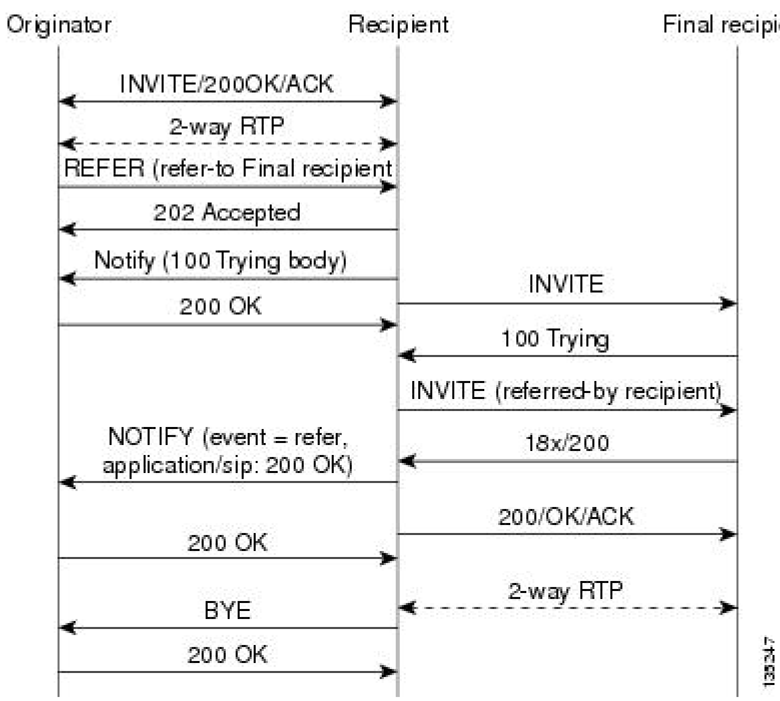
The figure below shows a successful blind or unattended call transfer in which the originator initiates a Bye request to terminate signaling with the recipient.

Figure 2 Successful Blind or Unattended Transfer--Originator Initiating a Bye Request



The figure below shows a successful blind or unattended call transfer in which the recipient initiates a Bye request to terminate signaling with the originator. A NOTIFY message is always sent by the recipient to the originator after the final outcome of the call is known.

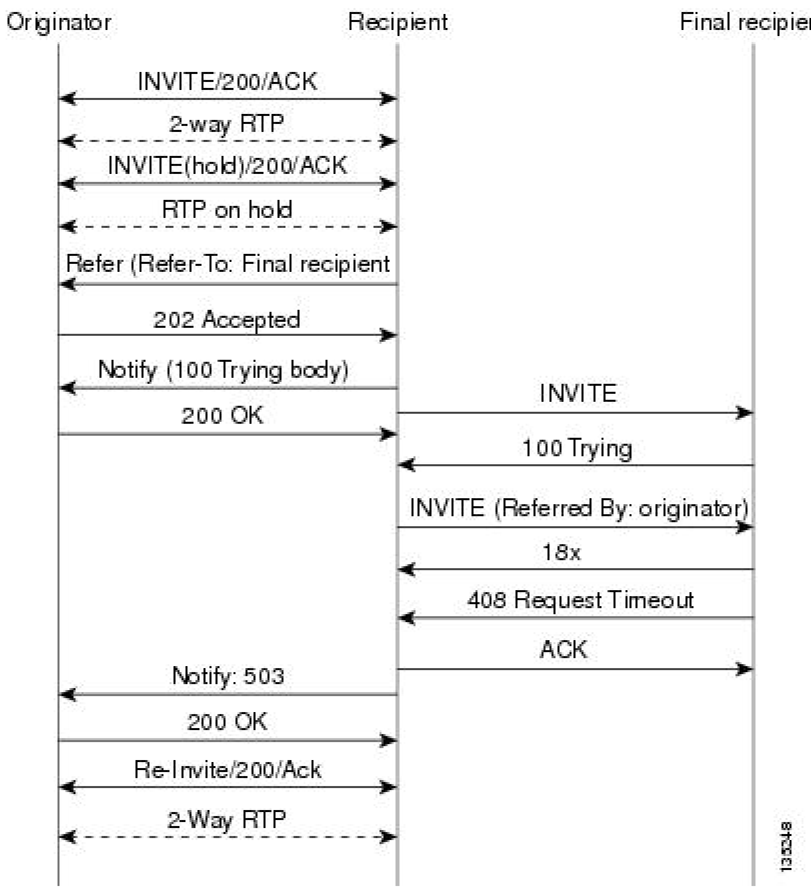
Figure 3 Successful Blind or Unattended Transfer--Recipient Initiating a Bye Request



If a failure occurs with the triggered INVITE to the final recipient, the call between originator and recipient is not disconnected. Rather, with blind transfer the process is as follows:

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

Figure 4 Failed Blind Transfer--Originator Returns to Original Call with Recipient



Attended Transfer

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

1. Originator does the following:
   - **a** Sets up a call with recipient.

  b. Places recipient on hold.
  c. Establishes a call to final recipient.
  d. Sends recipient a Refer message request with an overloaded Replaces header in the Refer-To header.
2. Recipient does the following:
  a. Sends a triggered INVITE request to final recipient. (Request includes the Replaces header, identifying the call leg between the originator and the final recipient.)
  b. Recipient returns a SIP 202 (Accepted) response to originator. (Response acknowledges that the INVITE has been sent.)
3. Final recipient establishes a direct signaling relationship with recipient. (Replaces header indicates that the initial call leg is to be shut down and replaced by the incoming INVITE request.)
4. Recipient notifies originator of the outcome of the Refer transaction. (Outcome indicates whether or not the final recipient was successfully contacted.)
5. Recipient terminates the session with originator by sending a Bye request.

Replaces Header

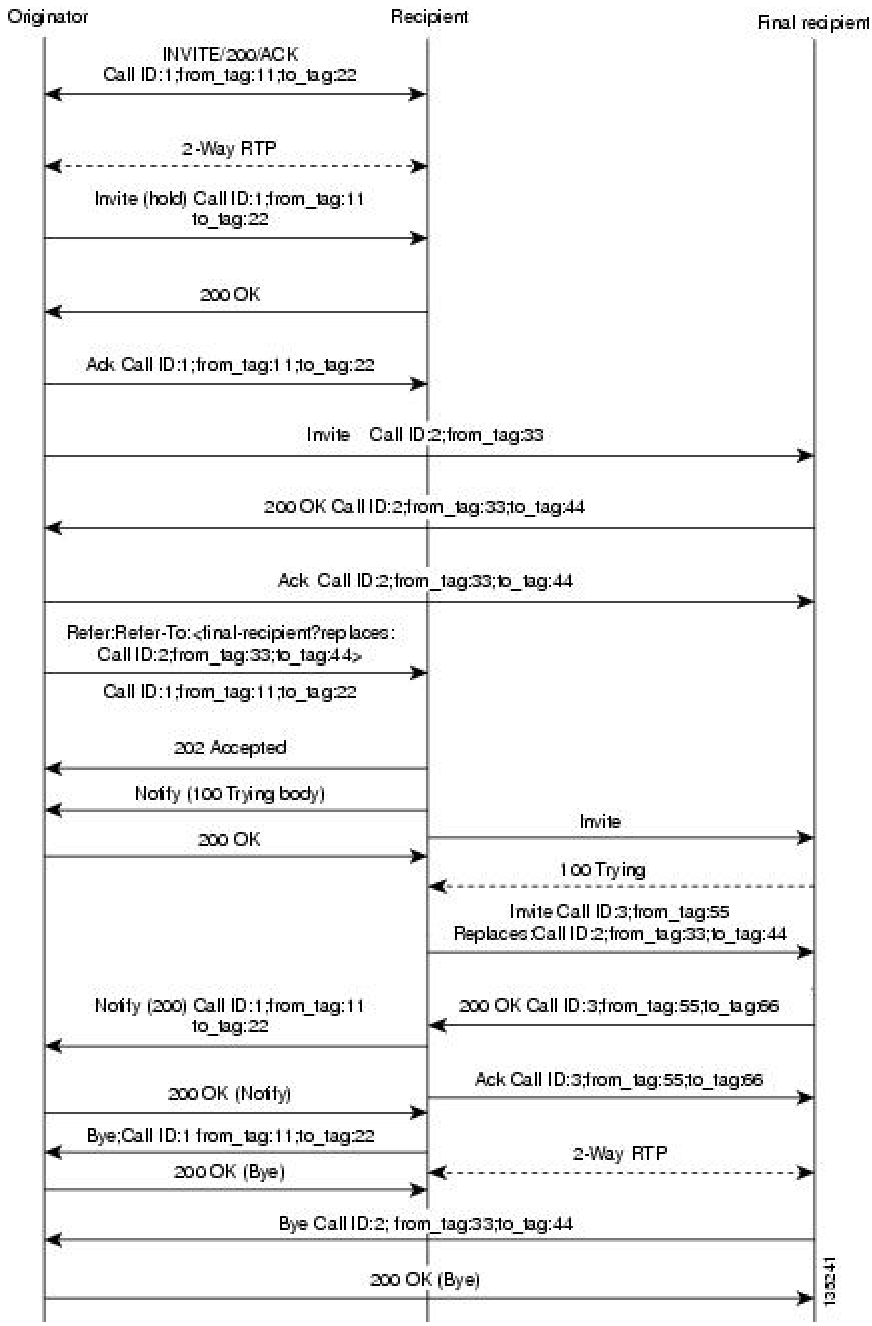
The Replaces header is required in attended transfers. It indicates to the final recipient that the initial call leg (identified by the Call-ID header and tags) is to be shut down and replaced by the incoming INVITE request. The final recipient sends a Bye request to the originator to terminate its session.

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

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

The figure below shows a call flow for a successful attended transfer.

Figure 5 ***Successful Attended Transfer***



Attended Transfer with Early Completion

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

The process for attended transfer with early completion is as follows (see the figure below):

1 Originator does the following:

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

2 Recipient does the following:

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

3 Final recipient establishes a direct signaling relationship with recipient.

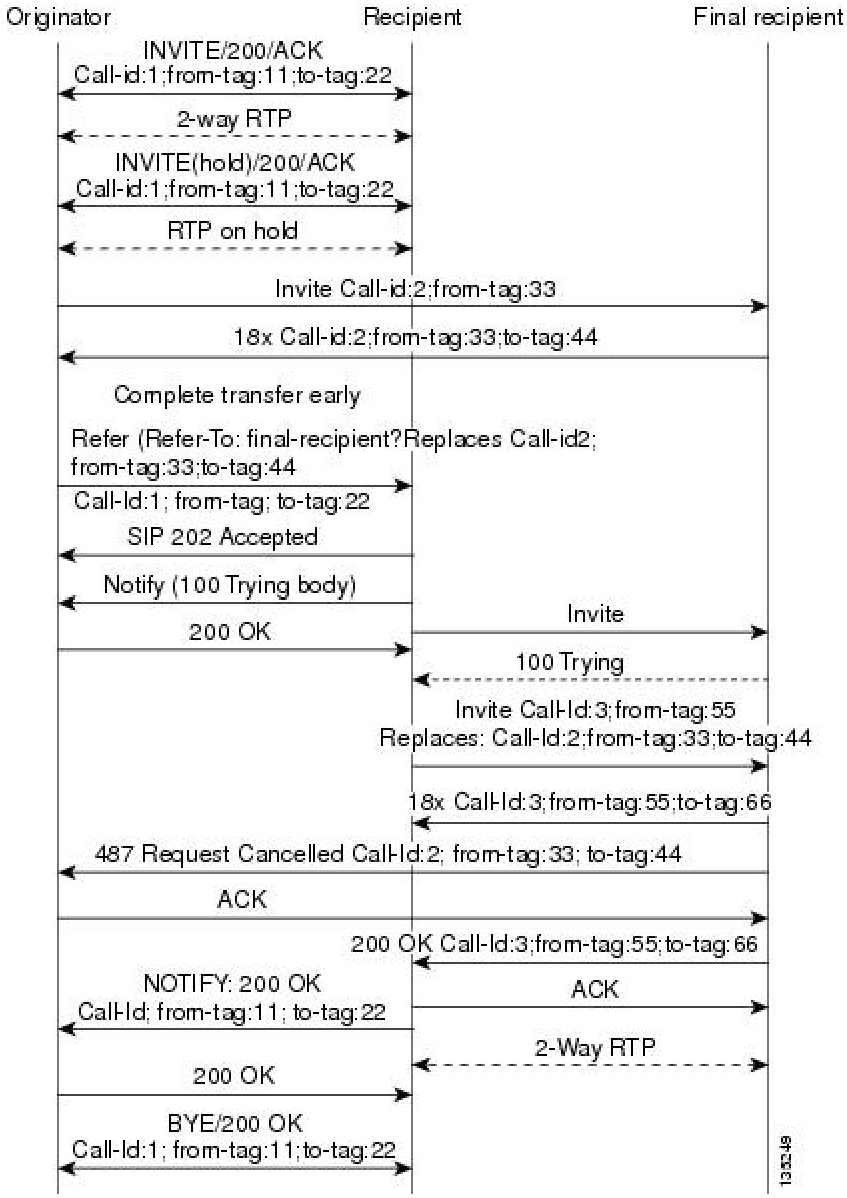
4 Final recipient tries to match the Call-ID header and the To or From tag in the Replaces header of the incoming INVITE with an active call leg in its call control block. If a matching active call leg is found, final recipient replies with the same status as the found call leg. However, it then terminates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

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

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

2 Recipient or originator terminates the session by sending a Bye request.

Figure 6 Attended Transfer with Early Completion



VSA for Call Transfer

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

Referred-By Header

For consistency with existing billing models, Referred-By and Requested-By headers are populated in call history tables as a VSA. Cisco VSAs are used for VoIP call authorization. The new VSA tag **supp-svc-xfer-by**helps to associate the call legs for call-detail-record (CDR) generation. The call legs can be originator-to-recipient or recipient-to-final-recipient.

The VSA tag **supp-svc-xfer-by** contains the user@host portion of the SIP URL of the Referred-By header for transfers performed with the Refer message request. For transfers performed with the Bye/Also message request, the tag contains user@host portion of the SIP URL of the Requested-By header. For each call on the gateway, two RADIUS records are generated: start and stop. The **supp-svc-xfer-by**VSA is generated only for stop records and is generated only on the recipient gateway--the gateway receiving the Refer or Bye/Also message.

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

Business Group Field

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

Note For information on VSAs, see the RADIUS VSA Voice Implementation Guide .

Feature Information for SIP Stack Portability

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 ASR

Table 15 Feature Information for SIP Stack Portability

Feature Name	Releases	Feature Information
SIP Stack Portability	Cisco IOS XE Release 2.5	Implements capabilities to the SIP gateway Cisco IOS stack involving user-agent handling of messages, handling of unsolicited messages, support for outbound delayed media, and SIP headers and content in requests and responses The following commands were introduced or modified: **None**

Feature History Table for the ISR

Table 16 Feature Information for SIP--SIP Stack Portability

Feature Name	Releases	Feature Information
SIP Stack Portability	12.4(2)T	Implements capabilities to the SIP gateway Cisco IOS stack involving user-agent handling of messages, handling of unsolicited messages, support for outbound delayed media, and SIP headers and content in requests and responses The following commands were introduced or modified: **None**

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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

Support for Software Media Termination Point

The Support for Software Media Termination Point (MTP) feature bridges the media streams between two connections allowing Cisco Unified Communications Manager (Cisco UCM) to relay calls that are routed through SIP or H.323 endpoints via Skinny Call Control Protocol (SCCP) commands. These commands allow Cisco UCM to establish an MTP for call signaling.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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 Support for Software Media Termination Point

This feature extends the software MTP support to the Cisco Unified Border Element (Enterprise). Software MTP is an essential component of large-scale deployments of Cisco UCM. This feature enables new capabilities so that the Cisco UBE can function as an Enterprise Edge Cisco Session Border Controller for large-scale deployments that are moving to SIP trunking.

How to Configure Support for Software Media Termination Point

Prerequisites

- For the software MTP to function properly, codec and packetization must be configured the same way on both in call legs and out call legs.

Cisco Unified Border Element (Enterprise)

- Cisco IOS XE Release 2.6 or a later release must be installed and running on your Cisco ASR 1000 Series Router.

Restrictions

- RSVP Agent is not supported in software MTP.
- Hardware MTP for repacketization is not supported.
- Call Threshold is not supported for standalone software MTP.
- Per-call debugging is not supported.

Configuring Support for Software Media Termination Point

To enable and configure the Support for Software Media Termination Point feature, perform the following task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **sccp local** *interface-type interface-number* [**port** *port-number*]
4. **sccp ccm** {*ipv4-address* | *ipv6-address* | *dns*} **identifier** *identifier-number* [**port** *port-number*] **version** *version-number*
5. **sccp**
6. **sccp ccm group** *group-number*
7. **associate ccm** *identifier-number* **priority** *number*
8. **associate profile** *profile-identifier* **register** *device-name*
9. **dspfarm profile** *profile-identifier* {**conference** | **mtp** | **transcode**} [**security**]
10. **maximum sessions** {**hardware** | **software**} *number*
11. **associate application sccp**
12. **no shutdown**

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	**sccp local** *interface-type interface-number* [**port** *port-number*] **Example:** `Router(config)# sccp local gigabitethernet0/0/0`	Selects the local interface that SCCP applications (transcoding and conferencing) use to register with Cisco UCM. • *interface type* --Can be an interface address or a virtual-interface address such as Ethernet. • *interface number* --Interface number that the SCCP application uses to register with Cisco UCM. • (Optional) **port** *port-number*--Port number used by the selected interface. Range is 1025 to 65535. Default is 2000.
Step 4	**sccp ccm** {*ipv4-address* | *ipv6-address* | *dns*} **identifier** *identifier-number* [**port** *port-number*] **version** *version-number* **Example:** `Router(config)# sccp ccm 10.1.1.1 identifier 1 version 7.0+`	Adds a Cisco UCM server to the list of available servers and sets the following parameters: • *ipv4-address* --IP version 4 address of the Cisco UCM server. • *ipv6-address* --IP version 6 address of the Cisco UCM server. • *dns* --DNS name. • **identifier** --Specifies the number that identifies the Cisco UCM server. Range is 1 to 65535. • **port** *port-number* (Optional)--Specifies the TCP port number. Range is 1025 to 65535. Default is 2000. • **version** *version-number* --Cisco UCM version. Valid versions are 3.0, 3.1, 3.2, 3.3, 4.0, 4.1, 5.0.1, 6.0, and 7.0+. There is no default value.
Step 5	**sccp** **Example:** `Router(config)# sccp`	Enables the Skinny Client Control Protocol (SCCP) and its related applications (transcoding and conferencing).

	Command or Action	Purpose
Step 6	**sccp ccm group** *group-number* **Example:** `Router(config)# sccp ccm group 10`	Creates a Cisco UCM group and enters SCCP Cisco UCM configuration mode. • *group-number* --Identifies the Cisco UCM group. Range is 1 to 50.
Step 7	**associate ccm** *identifier-number* **priority** *number* **Example:** `Router(config-sccp-ccm)# associate ccm 10 priority 3`	Associates a Cisco UCM with a Cisco UCM group and establishes its priority within the group: • *identifier-number* --Identifies the Cisco UCM. Range is 1 to 65535. There is no default value. • **priority** *number* --Priority of the Cisco UCM within the Cisco UCM group. Range is 1 to 4. There is no default value. The highest priority is 1.
Step 8	**associate profile** *profile-identifier* **register** *device-name* **Example:** `Router(config-sccp-ccm)# associate profile 1 register MTP0011`	Associates a DSP farm profile with a Cisco UCM group: • *profile-identifier* --Identifies the DSP farm profile. Range is 1 to 65535. There is no default value. • **register** *device-name* --Device name in Cisco UCM. A maximum of 15 characters can be entered for the device name.
Step 9	**dspfarm profile** *profile-identifier* {**conference** | **mtp** | **transcode**} [**security**] **Example:** `Router(config-sccp-ccm)# dspfarm profile 1 mtp`	Enters DSP farm profile configuration mode and defines a profile for DSP farm services: • *profile-identifier* --Number that uniquely identifies a profile. Range is 1 to 65535. There is no default. • **conference** --Enables a profile for conferencing. • **mtp** --Enables a profile for MTP. • **transcode** --Enables a profile for transcoding. • **security** (Optional)-- Enables a profile for secure DSP farm services.
Step 10	**maximum sessions** {**hardware** | **software**} *number* **Example:** `Router(config-dspfarm-profile)# maximum sessions software 10`	Specifies the maximum number of sessions that are supported by the profile. • **hardware** --Number of sessions that MTP hardware resources can support. • **software** --Number of sessions that MTP software resources can support. • *number* --Number of sessions that are supported by the profile. Range is 0 to x. Default is 0. The x value is determined at run time depending on the number of resources available with the resource provider.

	Command or Action	Purpose
Step 11	**associate application sccp** **Example:** `Router(config-dspfarm-profile)# associate application sccp`	Associates SCCP to the DSP farm profile.
Step 12	**no shutdown** **Example:** `Router(config-dspfarm-profile)# no shutdown`	Changes the status of the interface to the UP state.

- Examples, page 75
- Troubleshooting Tips, page 75

Examples

The following example shows a sample configuration for the Support for Software Media Termination Point feature:

```
sccp local GigabitEthernet0/0/1
sccp ccm 10.13.40.148 identifier 1 version 6.0
sccp
!
sccp ccm group 1
 bind interface GigabitEthernet0/0/1
 associate ccm 1 priority 1
 associate profile 6 register RR_RLS6
!
 dspfarm profile 6 mtp
 codec g711ulaw
 maximum sessions software 100
 associate application SCCP
!
!
gateway
media-inactivity-criteria all
timer receive-rtp 400
```

Troubleshooting Tips

To verify and troubleshoot this feature, use the following **show** commands:

- To verify information about SCCP, use the **show sccp** command:

```
Router# show sccp

SCCP Admin State: UP
Gateway IP Address: 10.13.40.157, Port Number: 2000
IP Precedence: 5
User Masked Codec list: None
Call Manager: 10.13.40.148, Port Number: 2000
```

```
                Priority: N/A, Version: 6.0, Identifier: 1
                Trustpoint: N/A
```

- To verify information about the DSPfarm profile, use the **show dspfarm profile** command:

```
Router# show dspfarm profile 6

Dspfarm Profile Configuration
 Profile ID = 6, Service = MTP, Resource ID = 1
 Profile Description :
 Profile Service Mode : Non Secure
 Profile Admin State : UP
 Profile Operation State : ACTIVE
 Application : SCCP   Status : ASSOCIATED
 Resource Provider : NONE   Status : NONE
 Number of Resource Configured : 100
 Number of Resource Available : 100
 Hardware Configured Resources : 0
 Hardware Available Resources : 0
 Software Resources : 100
 Codec Configuration
 Codec : g711ulaw, Maximum Packetization Period : 30
```

- To display statistics for the SCCP connections, use the **show sccp connections** command:

```
Router# show sccp connections

sess_id    conn_id    stype mode     codec   ripaddr         rport sport
16808048   16789079     mtp   sendrecv g711u 10.13.40.20     17510 7242
16808048   16789078     mtp   sendrecv g711u 10.13.40.157     6900 18050
```

- To display information about RTP connections, use the **show rtpspi call** command:

```
Router# show rtpspi call
RTP Service Provider info:
No. CallId dstCallId Mode      LocalRTP RmtRTP LocalIP    RemoteIP   SRTP
    22     19        Snd-Rcv   7242     17510  0x90D080F  0x90D0814    0
    19     22        Snd-Rcv   18050    6900   0x90D080F  0x90D080F    0
```

- To display information about VoIP RTP connections, use the **show voip rtp connections** command:

```
Router# show voip rtp connections
VoIP RTP Port Usage Information
Max Ports Available: 30000, Ports Reserved: 100, Ports in Use: 102
Port range not configured, Min: 5500, Max: 65499
VoIP RTP active connections :
No. CallId     dstCallId  LocalRTP  RmtRTP   LocalIP         RemoteIP
1     114        117        19822    24556  10.13.40.157     10.13.40.157
2     115        116        24556    19822  10.13.40.157     10.13.40.157
3     116        115        19176    52625  10.13.40.157     10.13.40.20
4     117        114        16526    52624  10.13.40.157     10.13.40.20
```

- Additional, more specific, **show** commands that can be used include the following:
  - **show sccp connection callid**
  - **show sccp connection connid**
  - **show sccp connection sessionid**
  - **show rtpspi call callid**
  - **show rtpspi stat callid**
  - **show voip rtp connection callid**
  - **show voip rtp connection type**
- To isolate specific problems, use the **debug sccp** command:
  - **debug sccp** [**all** | **config** | **errors** | **events** | **keepalive** | **messages** | **packets** | **parser** | **tls**]

Feature Information for Support for Software Media Termination Point

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 Historey Table for the ASR

Table 17 Feature Information for Support for Software Media Termination Point

Feature Name	Releases	Feature Information
Support for Software Media Termination Point	Cisco IOS XE Release 2.6 S	Software Media Termination Point (MTP) provides the capability for Cisco Unified Communications Manager (Cisco UCM) to interact with a voice gateway via Skinny Client Control Protocol (SCCP) commands. These commands allow the Cisco UCM to establish an MTP for call signaling.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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

Additional References

The following sections provide references related to the Cisco Unified Border Element (Enterprise) Configuration Guide.

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Cisco IOS Voice commands	*Cisco IOS Voice Command Reference*
Cisco IOS Voice Configuration Library	For more information about Cisco IOS voice features, including feature documents, and troubleshooting information--at http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/cisco_ios_voice_configuration_library_glossary/vcl.htm
Cisco IOS Release 15.0	Cisco IOS Release 15.0 Configuration Guides
Cisco IOS Release 12.2	Cisco IOS Voice, Video, and Fax Configuration Guide, Release 12.2

Related Topic	Document Title
internet Low Bitrate Codec (iLBC) Documents	• Codecs section of the Dial Peer Configuration on Voice Gateway Routers Guide http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/dial_peer/ dp_ovrvw.html • Dial Peer Features and Configuration section of the Dial Peer Configuration on Voice Gateway Routers Guide http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/dial_peer/ dp_confg.html
Related Application Guides	• *Cisco Unified Communications Manager and Cisco IOS Interoperability Guide* • *Cisco IOS SIP Configuration Guide* • Cisco Unified Communications Manager (CallManager) Programming Guides
Troubleshooting and Debugging guides	• Cisco IOS Debug Command Reference, Release 12.4 at http://www.cisco.com/en/US/docs/ios/debug/command/reference/db_book.html • *Troubleshooting and Debugging VoIP Call Basics* at http://www.cisco.com/en/US/tech/tk1077/technologies_tech_note09186a0080094045.shtml • *VoIP Debug Commands* at http://www.cisco.com/en/US/docs/routers/access/1700/1750/software/configuration/guide/debug.html

Standards

Standard	Title
ITU-T G.711	--

MIBs

MIB	MIBs Link
• CISCO-PROCESS MIB • CISCO-MEMORY-POOL-MIB • CISCO-SIP-UA-MIB • DIAL-CONTROL-MIB • CISCO-VOICE-DIAL-CONTROL-MIB • CISCO-DSP-MGMT-MIB • IF-MIB • IP-TAP-MIB • TAP2-MIB • USER-CONNECTION-TAP-MIB	To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 1889	*RTP: A Transport Protocol for Real-Time Applications*
RFC 2131	*Dynamic Host Configuration Protocol*
RFC 2132	*DHCP Options and BOOTP Vendor Extensions*
RFC 2198	*RTP Payload for Redundant Audio Data*
RFC 2327	*SDP: Session Description Protocol*
RFC 2543	*SIP: Session Initiation Protocol*
RFC 2543-bis-04	*SIP: Session Initiation Protocol, draft-ietf-sip-rfc2543bis-04.txt*
RFC 2782	*A DNS RR for Specifying the Location of Services (DNS SRV)*
RFC 2833	*RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*
RFC 3203	*DHCP reconfigure extension*
RFC 3261	*SIP: Session Initiation Protocol*
RFC 3262	*Reliability of Provisional Responses in Session Initiation Protocol (SIP)*
RFC 3323	*A Privacy Mechanism for the Session Initiation Protocol (SIP)*

RFC	Title
RFC 3325	*Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks*
RFC 3515	*The Session Initiation Protocol (SIP) Refer Method*
RFC 3361	*Dynamic Host Configuration Protocol (DHCP-for-IPv4) Option for Session Initiation Protocol (SIP) Servers*
RFC 3455	*Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)*
RFC 3608	*Session Initiation Protocol (SIP) Extension Header Field for Service Route Discovery During Registration*
RFC 3711	*The Secure Real-time Transport Protocol (SRTP)*
RFC 3925	Vendor-Identifying Vendor Options for Dynamic Host Configuration Protocol version 4 (DHCPv4)

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/cisco/web/support/index.html

Glossary

AMR-NB --Adaptive Multi Rate codec - Narrow Band.

Allow header --Lists the set of methods supported by the UA generating the message.

bind -- In SIP, configuring the source address for signaling and media packets to the IP address of a specific interface.

call --In SIP, a call consists of all participants in a conference invited by a common source. A SIP call is identified by a globally unique call identifier. A point-to-point IP telephony conversation maps into a single SIP call.

call leg --A logical connection between the router and another endpoint.

CLI --command-line interface.

Content-Type header --Specifies the media type of the message body.

CSeq header --Serves as a way to identify and order transactions. It consists of a sequence number and a method. It uniquely identifies transactions and differentiates between new requests and request retransmissions.

delta --An incremental value. In this case, the delta is the difference between the current time and the time when the response occurred. **dial peer**--An addressable call endpoint.

dial peer --An addressable call endpoint.

DNS --Domain Name System. Used to translate H.323 IDs, URLs, or e-mail IDs to IP addresses. DNS is also used to assist in locating remote gatekeepers and to reverse-map raw IP addresses to host names of administrative domains.

DNS SRV --Domain Name System Server. Used to locate servers for a given service.

DSP --Digital Signal Processor.

DTMF --dual-tone multifrequency. Use of two simultaneous voice-band tones for dialing (such as touch-tone).

EFXS --IP phone virtual voice ports.

FQDN --fully qualified domain name. Complete domain name including the host portion; for example, *serverA.companyA.com* .

FXS --analog telephone voice ports.

gateway --A gateway allows SIP or H.323 terminals to communicate with terminals configured to other protocols by converting protocols. A gateway is the point where a circuit-switched call is encoded and repackaged into IP packets.

H.323 --An International Telecommunication Union (ITU-T) standard that describes packet-based video, audio, and data conferencing. H.323 is an umbrella standard that describes the architecture of the conferencing system and refers to a set of other standards (H.245, H.225.0, and Q.931) to describe its actual protocol.

iLBC --internet Low Bitrate Codec.

INVITE--A SIP message that initiates a SIP session. It indicates that a user is invited to participate, provides a session description, indicates the type of media, and provides insight regarding the capabilities of the called and calling parties.

IP-- Internet Protocol. A connectionless protocol that operates at the network layer (Layer 3) of the OSI model. IP provides features for addressing, type-of-service specification, fragmentation and reassemble, and security. Defined in RFC 791. This protocol works with TCP and is usually identified as TCP/IP. See TCP/IP.

ISDN --Integrated Services Digital Network.

Minimum Timer --Configured minimum value for session interval accepted by SIP elements (proxy, UAC, UAS). This value helps minimize the processing load from numerous INVITE requests.

Min-SE --Minimum Session Expiration. The minimum value for session expiration.

multicast --A process of transmitting PDUs from one source to many destinations. The actual mechanism (that is, IP multicast, multi-unicast, and so forth) for this process might be different for LAN technologies.

originator --User agent that initiates the transfer or Refer request with the recipient.

PDU --protocol data units. Used by bridges to transfer connectivity information.

PER --Packed Encoding Rule.

proxy --A SIP UAC or UAS that forwards requests and responses on behalf of another SIP UAC or UAS.

proxy server --An intermediary program that acts as both a server and a client for the purpose of making requests on behalf of other clients. Requests are serviced internally or by passing them on, possibly after translation, to other servers. A proxy interprets and, if necessary, rewrites a request message before forwarding it.

recipient --User agent that receives the Refer request from the originator and is transferred to the final recipient.

redirect server --A server that accepts a SIP request, maps the address into zero or more new addresses, and returns these addresses to the client. It does not initiate its own SIP request or accept calls.

re-INVITE --An INVITE request sent during an active call leg.

Request URI --Request Uniform Resource Identifier. It can be a SIP or general URL and indicates the user or service to which the request is being addressed.

RFC --Request For Comments.

RTP --Real-Time Transport Protocol (RFC 1889)

SCCP --Skinny Client Control Protocol.

SDP--Session Description Protocol. Messages containing capabilities information that are exchanged between gateways.

session --A SIP session is a set of multimedia senders and receivers and the data streams flowing between the senders and receivers. A SIP multimedia conference is an example of a session. The called party can be invited several times by different calls to the same session.

session expiration --The time at which an element considers the call timed out if no successful INVITE transaction occurs first.

session interval --The largest amount of time that can occur between INVITE requests in a call before a call is timed out. The session interval is conveyed in the Session-Expires header. The UAS obtains this value from the Session-Expires header of a 2*xx* INVITE response that it sends. Proxies and UACs determine this value from the Session-Expires header in a 2*xx* INVITE response they receive.

SIP --Session Initiation Protocol. An application-layer protocol originally developed by the Multiparty Multimedia Session Control (MMUSIC) working group of the Internet Engineering Task Force (IETF). Their goal was to equip platforms to signal the setup of voice and multimedia calls over IP networks. SIP features are compliant with IETF RFC 2543, published in March 1999.

SIP URL --Session Initiation Protocol Uniform Resource Locator. Used in SIP messages to indicate the originator, recipient, and destination of the SIP request. Takes the basic form of *user@host* , where *user* is a name or telephone number, and *host* is a domain name or network address.

SPI --service provider interface.

socket listener -- Software provided by a socket client to receives datagrams addressed to the socket.

stateful proxy --A proxy in keepalive mode that remembers incoming and outgoing requests.

TCP --Transmission Control Protocol. Connection-oriented transport layer protocol that provides reliable full-duplex data transmissions. TCP is part of the TCP/IP protocol stack. See also TCP/IP and IP.

TDM --time-division multiplexing.

UA --user agent. A combination of UAS and UAC that initiates and receives calls. See **UAS**and **UAC**.

UAC --user agent client. A client application that initiates a SIP request.

UAS --user agent server. A server application that contacts the user when a SIP request is received and then returns a response on behalf of the user. The response accepts, rejects, or redirects the request.

UDP -- User Datagram Protocol. Connectionless transport layer protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by other protocols. UDP is defined in RFC-768.

URI --Uniform Resource Identifier. Takes a form similar to an e-mail address. It indicates the user's SIP identity and is used for redirection of SIP messages.

URL --Universal Resource Locator. Standard address of any resource on the Internet that is part of the World Wide Web (WWW).

User Agent --A combination of UAS and UAC that initiates and receives calls. See **UAS and UAC.**

VFC --Voice Feature Card.

VoIP --Voice over IP. The ability to carry normal telephone-style voice over an IP-based Internet with POTS-like functionality, reliability, and voice quality. VoIP is a blanket term that generally refers to the Cisco standards-based approach (for example, H.323) to IP voice traffic.