Cisco Unified Border Element (Enterprise) Protocol-Independent Features and Setup Configuration Guide, Cisco IOS XE Release 3S (Cisco ASR 1000)

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.

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.

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

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-xml/ios/voice/dialpeer/configuration/15-1mt/vd-15-1mt-book.html
- Translation Rules — http://www.cisco.com/en/US/docs/ios-xml/ios/voice/vcr5/vcr-t3.html#GUID-62D8FEDA-D685-40FB-A70D-1794E8150036
- 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-xml/ios/voice/sip/configuration/15-1mt/Configuring_SIP_DTMF_Features.html
- H.323 RFC2833 - SIP NOTIFY

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-xml/ios/voice/vcr2/vcr-i1.html#GUID-2FC584E4-49EB-455F-BA0B-B1EB68515CCF

Fax/modem Support

- Modem passthrough
- T.38 Fax Relay — http://www.cisco.com/en/US/docs/ios-xml/ios/voice/fax/configuration/15-1mt/vf-cfg-t38-fxrly.html
- Cisco Fax Relay — http://www.cisco.com/en/US/docs/ios-xml/ios/voice/fax/configuration/15-1mt/vf-cfg-fx-relay.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
- Access lists (ACLs)
- CAC (call spike) — http://www.cisco.com/en/US/docs/ios-xml/ios/voice/vcr1/vcr-c3.html#GUID-ED81C161-885D-4BEC-A6A0-D4C9886AEA2F
- SIP--Ability to Send a SIP Registration Message on a Border Element
- SIP Parameter Modification
- SIP--SIP Stack Portability
- Session Refresh with Reinvites
- CDR
- 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

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.

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-to-SIP Extended Feature Functionality for Session Border Controllers

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

- Call Admission Control (based on CPU, memory, and total calls)
- Delayed Media Call
- ENUM support
- Configuring SIP Error Message Pass Through
- Interoperability with Cisco Unified Communications Manager 5.0 and BroadSoft
- Lawful Intercept
- Media Inactivity
- Modem Passthrough over VoIP, page 8
- TCP and UDP interworking
- Tcl scripts with SIP NOTIFY VoiceXML with SIP-to-SIP
- Transport Layer Security (TLS)

Finding Feature Information

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

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

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

Cisco Unified Border Element

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

Cisco Unified Border Element (Enterprise)

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

Modem Passthrough over VoIP

The Modem Passthrough over VoIP feature provides the transport of modem signals through a packet network by using pulse code modulation (PCM) encoded packets.

Prerequisites for the Modem Passthrough over VoIP Feature

- VoIP enabled network.
- Cisco IOS Release 12.1(3)T must run on the gateways for the Modem Passthrough over VoIP feature to work.
- Network suitability to pass modem traffic. The key attributes are packet loss, delay, and jitter. These characteristics of the network can be determined by using the Cisco IOS feature Service Assurance Agent.

Cisco Unified Border Element

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

Cisco Unified Border Element (Enterprise)

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

Restrictions for the Modem Passthrough over VoIP Feature

Cisco Unified Border Element (Enterprise)

- If call started as g729, upon modem tone (2100Hz) detection both the outgoing gateway (OGW) and the trunking gateway (TGW) will genearate NSE packets towards peer side and up speed to g711 as Cisco UBE(Enterprise) passes these packets to the peer side.

Note That OGW and TGW display the new codec, but the Cisco UBE (Enterprise) continues to show the original codec g729 in the show commands.

Information about Configuring Modem Passthrough over VoIP

The Modem Passthrough over VoIP feature performs the following functions:

- Represses processing functions like compression, echo cancellation, high-pass filter, and voice activity detection (VAD).
- Issues redundant packets to protect against random packet drops.
- Provides static jitter buffers of 200 milliseconds to protect against clock skew.
- Discriminates modem signals from voice and fax signals, indicating the detection of the modem signal across the connection, and placing the connection in a state that transports the signal across the network with the least amount of distortion.
- Reliably maintains a modem connection across the packet network for a long duration under *normal* network conditions.

For further details, the functions of the Modem Passthrough over VoIP feature are described in the following sections.

Modem Tone Detection

The gateway is able to detect modems at speeds up to V.90.

Passthrough Switchover

When the gateway detects a data modem, both the originating gateway and the terminating gateway roll over to G.711. The roll over to G.711 disables the high-pass filter, disables echo cancellation, and disables VAD. At the end of the modem call, the voice ports revert to the prior configuration and the digital signal processor (DSP) goes back to the state before switchover. You can configure the codec by selecting the **g711alaw** or **g711ulaw** option of the **codec** command.

See also the How to Configure Modem Passthrough over VoIP, page 10 section in this document.

Controlled Redundancy

You can enable payload redundancy so that the Modem Passthrough over VoIP switchover causes the gateway to emit redundant packets.

Packet Size

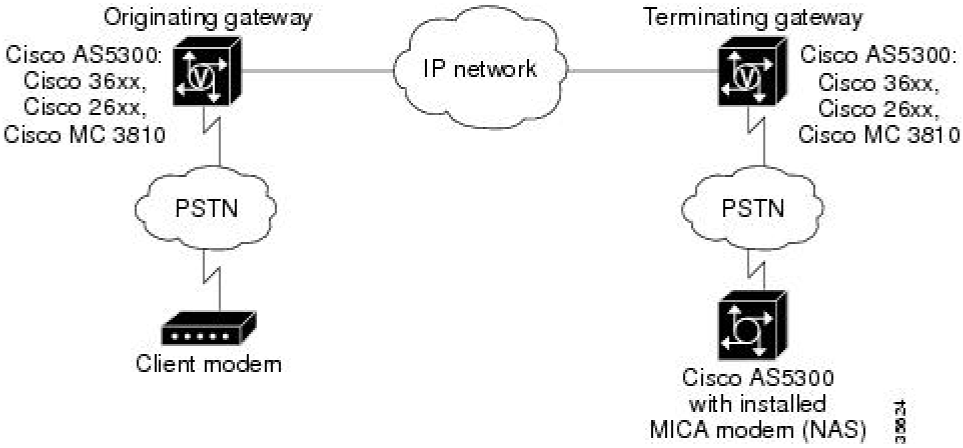
When redundancy is enabled, 10-ms sample-sized packets are sent. When redundancy is disabled, 20-ms sample-sized packets are sent.

Clock Slip Buffer Management

When the gateway detects a data modem, both the originating gateway and the terminating gateway switch from dynamic jitter buffers to static jitter buffers of 200-ms depth. The switch from dynamic to static is to compensate for Public Switched Telephone Network (PSTN) clocking differences at the originating gateway and the terminating gateway. At the conclusion of the modem call, the voice ports revert to dynamic jitter buffers.

The figure below illustrates the connection from the client modem to a MICA technologies modem network access server (NAS).

Figure 1 Modem Passthrough Connection



How to Configure Modem Passthrough over VoIP

You can configure the Modem Passthrough over VoIP feature on a specific dial peer in two ways, as follows:

- Globally in the voice-service configuration mode
- Individually in the dial-peer configuration mode on a specific dial peer

By default, modem passthrough over VoIP capability and redundancy are disabled.

Tip You need to configure modem passthrough in both the originating gateway and the terminating gateway for the Modem Passthrough over VoIP feature to operate. If you configure only one of the gateways in a pair, the modem call will not connect successfully.

Redundancy can be enabled in one or both of the gateways. When only a single gateway is configured for redundancy, the other gateway receives the packets correctly, but does not produce redundant packets.

See the following sections for the Modem Passthrough over VoIP feature. The two configuration tasks can configure separately or together. If both are configured, the dial-peer configuration takes precedence over the global configuration. Consequently, a call matching a particular dial-peer will first try to apply the modem passthrough configuration on the dial-peer. Then, if a specific dial-peer is not configured, the router will use the global configuration:

- Configuring Modem Passthrough over VoIP Globally, page 11
- Configuring Modem Passthrough over VoIP for a Specific Dial Peer, page 12
- Troubleshooting Tips, page 14

Configuring Modem Passthrough over VoIP Globally

For the Modem Passthrough over VoIP feature to operate, you need to configure modem passthrough in both the originating gateway and the terminating gateway so that the modem call matches a voip dial-peer on the gateway.

The default behavior for the voice-service configuration mode is **no modem passthrough**. This default behavior implies that modem passthrough is disabled for all dial peers on the gateway by default.

When using the **voice service voip** and **modem passthrough nse** commands on a terminating gateway to globally set up fax or modem passthrough with NSEs, you must also ensure that each incoming call will be associated with a VoIP dial peer to retrieve the global fax or modem configuration. You associate calls with dial peers by using the **incoming called-number** command to specify a sequence of digits that incoming calls can match.

To configure the Modem Passthrough over VoIP feature for all the connections of a gateway, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. **enable**
2. **voice service voip**
3. **modem passthrough nse** [**payload-type** *number*] **codec** {**g711ulaw** | **g711alaw**} [**redundancy**] [**maximum-sessions** *value*]
4. **exit**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**voice service voip** **Example:** `Device(config)# voice service voip`	Enters voice-service configuration mode. Configures voice service for all the connections for the gateways.

	Command or Action	Purpose
Step 3	**modem passthrough nse** [**payload-type** *number*] **codec** {**g711ulaw** | **g711alaw**} [**redundancy**] [**maximum-sessions** *value*] **Example:** `Device(config)# Router(conf-voi-serv)# modem passthrough nse payload-type 97 codec g711alaw redundancy maximum-sessions 3`	Configures the Modem Passthrough over VoIP feature The default behavior is **no modem passthrough**. The payload type is an optional parameter for the **nse** keyword. Use the same **payload-type** *number* for both the originating gateway and the terminating gateway. The **payload-type** *number*can be set from 96 to 119. If you do not specify the **payload-type** *number*, the *number*defaults to 100. When the **payload-type** is 100, and you use the **show running-config**command, the **payload-type** parameter does not appear. Use the same codec type for both the originating gateway and the terminating gateway. **g711ulaw** codec is required for T1, and **g711alaw** codec is required for E1. The **redundancy** keyword is an optional parameter for sending redundant packets for modem traffic. The **maximum-sessions** keyword is an optional parameter for the **redundancy**keyword. This parameter determines the maximum simultaneous modem passthrough sessions with **redundancy**.
Step 4	**exit** **Example:** `Device(conf-voi-serv)# exit`	Exits voice-service configuration mode.
Step 5	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode.

Configuring Modem Passthrough over VoIP for a Specific Dial Peer

To enable Modem Passthrough on the VoIP dial peers on both the originating and terminating gateway, configure modem passthrough globally or explicitly on the dial peer.

For modem passthrough to operate, you must define VoIP dial peers on both gateways to match the call, for example, by using a destination pattern or an incoming called number. The modem passthrough parameters associated with those dial peers then will apply to the call.

Note When modem passthrough is configured individually for a specific dial peer, that configuration for the specific dial peer takes precedence over the global configuration.

To configure the Modem Passthrough over VoIP feature for a specific dial peer, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. **enable**
2. **dial-peer voice** *number* **voip**
3. **modem passthrough** {**system** | **nse** [**payload-type** *number*] **codec** {**g711ulaw** | **g711alaw**} [**redundancy**]}
4. **exit**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**dial-peer voice** *number* **voip** **Example:** `Device(config)# dial-peer voice 5 voip`	Enters dial-peer configuration mode. Configures a specific dial peer in dial-peer configuration mode.

Step 3	**modem passthrough** {**system** | **nse** [**payload-type** *number*] **codec** {**g711ulaw** | **g711alaw**}[**redundancy**]}
	Example:
	`Device(config-dial-peer)# modem passthrough nse payload-type 97 codec g711alaw redundancy`
		Configures the Modem Passthrough over VoIP feature for a specific dial peer. The default behavior for the Modem Passthrough for VoIP feature in dial-peer configuration mode is **modem passthrough system**. As required, the gateway defaults to **no modem passthrough**.
		When the **system** keyword is enabled, the following parameters are not available: **nse**, **payload-type**, **codec**, and **redundancy**. Instead the values from the global configuration are used.
		The payload type is an optional parameter for the **nse** keyword. Use the same **payload-type** *number* for both the originating gateway and the terminating gateway. The **payload-type** *number*can be set from 96 to 119. If you do not specify the **payload-type** *number*, the *number*defaults to 100. When the **payload-type** is 100, and you use the **show running-config**command, the **payload-type** parameter does not appear.
		Use the same codec type for both the originating gateway and the terminating gateway. **g711ulaw** codec is required for T1, and **g711alaw** codec is required for E1.
		The **redundancy** keyword is an optional parameter for sending redundant packets for modem traffic.

	Command or Action	Purpose
Step 4	**exit** **Example:** `Device(config-dial-peer)# exit`	Exits dial-peer configuration mode and returns to the global configuration mode.
Step 5	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode.

Troubleshooting Tips

To troubleshoot the Modem Passthrough over VoIP feature, perform the following steps:

- Make sure that you can make a voice call.
- Make sure that Modem Passthrough over VoIP is configured on both the originating gateway and the terminating gateway.
- Make sure that both the originating gateway and the terminating gateway have the same named signaling event (NSE) **payload-type** *number*.
- Make sure that both the originating gateway and the terminating gateway have the same **maximum-sessions** *value* when the two gateways are configured in the voice-service configuration mode.
- Use the **debug vtsp dsp** and **debug vtsp session** commands to debug a problem.

Verifying Modem Passthrough over VoIP

To verify that the Modem Passthrough over VoIP feature is enabled, perform the following steps:

SUMMARY STEPS

1. Enter the **show run** command to verify the configuration.
2. Enter the **show dial-peer voice** command to verify that Modem Passthrough over VoIP is enabled.

DETAILED STEPS

Step 1 Enter the **show run** command to verify the configuration.

Step 2 Enter the **show dial-peer voice** command to verify that Modem Passthrough over VoIP is enabled.

Monitoring and Maintaining Modem Passthrough over VoIP

To monitor and maintain the Modem Passthrough over VoIP feature, use the following commands in privileged EXEC mode:

Command	Purpose
Device# **show call active voice brief**	Displays information for the active call table or displays the voice call history table. The brief option displays a truncated version of either option.
Device# **show dial-peer voice 15 summary**	Displays configuration information for dial peers. The *number* argument specifies a specific dial peer from 1 to 32767. The summary option displays a summary of all dial peers.

Configuration Examples

The following is sample configuration for the Modem Passthrough over VoIP feature:

```
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
voice service voip
     modem passthrough nse codec g711ulaw redundancy maximum-session 5
!
!
resource-pool disable
!
!
!
!
!
ip subnet-zero
ip ftp source-interface Ethernet0
ip ftp username lab
ip ftp password lab
no ip domain-lookup
!
isdn switch-type primary-5ess
cns event-service server
!
!
!
!
!
mta receive maximum-recipients 0
!
!
controller T1 0
 framing esf
 clock source line primary
 linecode b8zs
 pri-group timeslots 1-24
!
controller T1 1
 shutdown
 clock source line secondary 1
!
controller T1 2
 shutdown
!
controller T1 3
 shutdown
!
!
!
interface Ethernet0
 ip address 1.1.2.2 255.0.0.0
 no ip route-cache
 no ip mroute-cache
!
interface Serial0:23
 no ip address
 encapsulation ppp
 ip mroute-cache
 no logging event link-status
 isdn switch-type primary-5ess
 isdn incoming-voice modem
 no peer default ip address
 no fair-queue
 no cdp enable
 no ppp lcp fast-start
!
interface FastEthernet0
 ip address 26.0.0.1 255.0.0.0
 no ip route-cache
 no ip mroute-cache
 load-interval 30
 duplex full
 speed auto
 no cdp enable
!
ip classless
ip route 17.18.0.0 255.255.0.0 1.1.1.1
no ip http server
!
!
!
!
voice-port 0:D
!
dial-peer voice 1 pots
 incoming called-number 55511..
 destination-pattern 020..
 direct-inward-dial
 port 0:D
 prefix 020
!
dial-peer voice 2 voip
 incoming called-number 020..
 destination-pattern 55511..
 modem passthrough nse codec g711ulaw redundancy
 session target ipv4:26.0.0.2
!
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
line vty 0 4
 login
!
!
end
```

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

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

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

Table 1 Feature Information for Configuring SIP-to-SIP Extended Feature Functionality for Session Border Controllers

Feature Name	Releases	Feature Information
SIP-to-SIP Extended Feature Functionality for Session Border Controllers	12.4(6)T	The SIP-to-SIP Extended Feature Functionality for Session Border Controllers (SBCs) enables the SIP-to-SIP functionality to conform with RFC 3261 to interoperate with SIP User Agents (UAs). In Cisco IOS Release 12.4(6)S, this feature was implemented on the Cisco Unified Border Element The following commands were introduced or modified: **modem passthrough (dial-peer)**; **modem passthrough (voice-service)**; **show call active voice voice**; **show call history voice voice**; **show dial-peer voice**; **voice service**.
SIP-to-SIP Extended Feature Functionality for Session Border Controllers	Cisco IOS XE Release 3.1S Cisco IOS XE Release 3.3S	The SIP-to-SIP Extended Feature Functionality for Session Border Controllers (SBCs) enables the SIP-to-SIP functionality to conform with RFC 3261 to interoperate with SIP User Agents (UAs). In Cisco IOS Release 12.4(6)S, this feature was implemented on the Cisco Unified Border Element (Enterprise). The following commands were introduced or modified: **modem passthrough (dial-peer)**; **modem passthrough (voice-service)**; **show call active voice voice**; **show call history voice voice**; **show dial-peer voice**; **voice service**.

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.

Bandwidth-Based Call Admission Control

The Bandwidth-Based Call Admission Control (CAC) feature provides the functionality to reject SIP calls when the bandwidth accounted by the SIP signaling layer exceeds the aggregate bandwidth threshold for VoIP media traffic—voice, video, and fax. This functionality helps you prevent Quality of Service (QoS) degradation of VoIP media traffic for existing calls when the bandwidth allocated for VoIP traffic is fully utilized. The Bandwidth-Based Call Admission Control feature is supported on Session Initiation Protocol (SIP) trunks of the Time Division Multiplexing (TDM) SIP gateway and the Cisco Unified Border Element (Cisco UBE).

Midcall media renegotiation can also be rejected if the configured maximum bandwidth threshold for the VoIP media traffic is exceeded. The call continues as per the previously negotiated media codecs if midcall media renegotiation is rejected.

The excess subscription of the bandwidth allocated for VoIP traffic results in VoIP media packets being dropped or delayed, irrespective of the VoIP call to which they belong. Under such circumstances, it is better to deny new calls to prevent QoS deterioration for existing VoIP call traffic. The existing traffic congestion resolution mechanisms do not differentiate between media packets of existing calls (admitted) and new calls (oversubscribed). Similarly, existing call signaling is unaware of the media traffic congestion. The Bandwidth-Based Call Admission Control feature fills this gap by rejecting new SIP calls when the bandwidth allocated for VoIP traffic is fully utilized. The actual bandwidth usage is not measured and policed. The lower-level QoS policies control the traffic characteristics for the specified traffic class.

Note The Bandwidth-Based Call Admission Control feature is applicable only to VoIP traffic.

Finding Feature Information

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

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

Restrictions for Bandwidth-Based Call Admission Control

- Cisco UBE, configured with the Bandwidth-Based Call Admission Control feature, will not reject the call if the bandwidth of the SDP answer is greater than the bandwidth of the SDP offer.
- Layer 2 overhead is not included in the bandwidth calculation.
- A midcall delayed-offer (DO) to DO call is disconnected if the bandwidth requested in an offer message (200 OK) exceeds the threshold bandwidth.
- Real Time Transport Control Protocol (RTCP) and RTP Named Telephone Event (RTP-NTE) bandwidth requirement is not computed.
- The Bandwidth-Based Call Admission Control feature does not support:
    - Cisco fax relay.
    - Filtering of codecs to accommodate calls within the available bandwidth.
    - Media flow-around, Session Description Protocol (SDP) pass-through, out-of-box low-density transcoding, high-density transcoding, video transcoding, and midcall consumption functionalities.
    - Non-SIP call legs.
    - SIP-to-H32X call flows (SIP-H320, H320-SIP, SIP-H324, H324-SIP).
    - Subinterfaces for bandwidth-based CAC on an interface.

Information About Bandwidth-Based Call Admission Control

- Maximum Bandwidth Calculation, page 20
- Bandwidth Tables, page 21

Maximum Bandwidth Calculation

The bandwidth requirement for each SIP call leg is calculated using the codec information available in the SDP. Here, the actual media bandwidth used is not measured.

Bandwidth in Kbps (Kilo bits per second) = [codec bytes + RTP header (12) + UDP (8) + IP Header (20 or 40)] * Packets per seconds * 8/1000

Where, codec bytes = Codec payload size, in bytes, for a given packetization interval.

RTP header = Size of the RTP header, in bytes.

UDP = Size of the UDP header, in bytes.

IP Header = Size of the IP header, in bytes. The IPV4 header is 20 bytes and the IPV6 header is 40 bytes.

Packets per second = Number of RTP packets sent or received per second. This value is as per the negotiated packetization interval. The SDP media attribute "ptime" indicates the number of packets per second.

Bandwidth Tables

This section provides the sample maximum bandwidth calculation for audio and fax calls.

Table 2 Audio Bandwidth Table

Codec and Bit Rate (Kbps)	Codec Sample Size in Bytes	Voice Payload Size in Bytes	Voice Payload Size in Milliseconds	Packets Per Second	Bandwidth for IPv4 (excluding Layer 2) in Kbps	Bandwidth for IPv6 (excluding Layer 2) in Kbps
G.711 (64 Kbps)	80	160	20	50	80	88
G.729 (8 Kbps)	10	20	20	50	24	32
G.723.1 (6.3 Kbps)	24	24	30	33.3	17	22
G.723.1 (5.3 Kbps)	20	20	30	33.3	16	21
G.726 (32 Kbps)	20	80	20	50	48	56
G.726 (24 Kbps)	15	60	20	50	40	48
G.726 (16 Kbps)	10	40	20	50	32	40
G.728 (16 Kbps)	10	40	20	50	32	40
G722_64k (64 Kbps)	80	160	20	50	80	88
ilbc_mode_20 (15.2 Kbps)	38	38	20	50	31	39
ilbc_mode_30 (13.33 Kbps)	50	50	30	33.3	24	29
gsm (13 Kbps)	33	33	20	50	30	37
gsm (12 Kbps)	32	32	20	50	29	37

G.Clear (64 Kbps)	80	160	20	50	80	88
GSM AMR	—	—	—	—	15	15
ISAC (32 Kbps)	—	—	—	—	37	37
Aacld (mpeg4)	—	—	—	—	Derived from the SDP bandwidth attribute (TIAS)	Derived from the SDP bandwidth attribute (TIAS)

Table 3 Fax Bandwidth Table

T.38 Fax Bit Rate	Redundancy	Maximum Bandwidth in Kbps
2400	None	8
2400	Redundancy	17
9600 (default)	None	16
9600 (default)	Redundancy	46
14400	None	20
14400	Redundancy	65
33600	None	40
33600	Redundancy	142

How to Configure Bandwidth-Based Call Admission Control

- Configuring Bandwidth-Based Call Admission Control at the Interface Level, page 23
- Configuring Bandwidth-Based Call Admission Control at the Dial Peer Level, page 24
- Configuring the Bandwidth-Based Call Admission Control SIP Error Response Code Mapping, page 26
- Verifying Bandwidth-Based Call Admission Control, page 28
- Troubleshooting Tips, page 30

Configuring Bandwidth-Based Call Admission Control at the Interface Level

You can configure the Bandwidth-Based Call Admission Control feature at the interface level to reject SIP calls when the bandwidth required for the call exceeds the aggregate bandwidth threshold.

You can configure the Bandwidth-Based Call Admission Control feature for the following interfaces:

- ATM
- Ethernet (Fast Ethernet, Gigabit Ethernet)
- Loopback
- Serial

Note Cisco recommends that you configure a bind media to associate a specific interface for SIP calls. Otherwise, the interface used for the calls will be determined based on the best local address that can access the remote media source address (for early offer calls) or the remote signaling source address (for delayed offer calls). When you use a Loopback interface to configure CAC, you must configure an additional bind-to-bind media with the Loopback interface at the global level or the dial peer level. Configure the **bind media source-interface loopback** *number* command in service SIP configuration mode to configure a bind media.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **call threshold interface** *type number* **int-bandwidth** {**class-map** *name* [**l2-overhead** *percentage*] | **low** *low-threshold* **high** *high-threshold*} [**midcall-exceed**]
4. **end**

DETAILED STEPS

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

	Command or Action	Purpose

Step 3	**call threshold interface** *type number* **int-bandwidth** {**class-map** *name* [**l2-overhead** *percentage*] | **low** *low-threshold* **high** *high-threshold*} [**midcall-exceed**]
	Example:
	`Device(config)# call threshold interface GigabitEthernet 0/0 int-bandwidth low 1000 high 20000 midcall-exceed`
	or
	`Device(config)# call threshold interface GigabitEthernet 0/0 int-bandwidth class-map voip-traffic l2-overhead 20 midcall-exceed`
		Configures the Bandwidth-Based Call Admission Control feature at the interface level to reject SIP calls when the bandwidth required for the calls exceed the aggregate bandwidth threshold.
		• You can configure the **call threshold interface** *type number* **low** *low-threshold* **high** *high-threshold* [**midcall-exceed**] command to apply call admission control to reject SIP calls once the accounted bandwidth reaches the *high-threshold* value and continues to be above the *low-threshold* value.
		• You can configure the **call threshold interface** *type number* **int-bandwidth class-map** *name* [**l2-overhead** *percentage*] [**midcall-exceed**] command to use the bandwidth value provisioned in the QoS policy under the interface for VoIP media traffic for CAC. See the Modular Quality of Service Command-Line Interface Overview document at http://www.cisco.com/en/US/docs/ios/12_2/qos/configuration/guide/qcfmdcli.html for information on the usage of the QoS policy with Call Admission Control.
		• SIP calls are rejected when the calculated aggregate bandwidth of VoIP media traffic on the specified interface exceeds the configured bandwidth threshold.

Step 4	**end**
	Example:
	`Device(config)# end`
		Exits global configuration mode and enters privileged EXEC mode.

Configuring Bandwidth-Based Call Admission Control at the Dial Peer Level

You can configure the Bandwidth-Based Call Admission Control feature at the dial peer level to reject SIP calls when the bandwidth required for the calls exceeds the aggregate bandwidth threshold.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *tag* **voip**
4. **session protocol sipv2**
5. **max-bandwidth** *bandwidth-value* [**midcall-exceed**]
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**dial-peer voice** *tag* **voip** **Example:** `Device(config)# dial-peer voice 44 voip`	Enters dial peer voice configuration mode.
Step 4	**session protocol sipv2** **Example:** `Device(config-dial-peer)# session protocol sipv2`	Configures the Bandwidth-Based Call Admission Control feature for SIP dial peers only.
Step 5	**max-bandwidth** *bandwidth-value* [**midcall-exceed**] **Example:** `Device(config-dial-peer)# max-bandwidth 24 midcall-exceed`	Configures the Bandwidth-Based Call Admission Control feature at the dial peer level to reject SIP calls when the bandwidth required for the calls exceed the aggregate bandwidth threshold. • Configuring the **midcall-exceed** keyword allows exceeding the bandwidth threshold during mid-call media renegotiation. Media renegotiation exceeding the bandwidth threshold is rejected by default.

Step 6	**end**
	Example:
	`Device(config-dial-peer)# end`
		Exits dial peer configuration mode and enters privileged EXEC mode.

Configuring the Bandwidth-Based Call Admission Control SIP Error Response Code Mapping

Mapping of the call rejection cause code to a specific SIP error response code is known as error response code mapping. The cause code for the call rejected because of the bandwidth-based CAC can be mapped to a SIP error response code between 400 to 600. The default SIP error response code is 488.

You can configure SIP error response codes for calls rejected by the Bandwidth-Based Call Admission Control feature at the global level, dial peer level, or both.

- Configuring Bandwidth-Based Call Admission Control SIP Error Response Code Mapping at the Global Level, page 26
- Configuring Bandwidth-Based Call Admission Control SIP Error Response Code Mapping at the Dial Peer Level, page 27

Configuring Bandwidth-Based Call Admission Control SIP Error Response Code Mapping at the Global Level

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **sip**
5. **error-code-override cac-bandwidth failure** *sip-status-code-number*
6. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**voice service voip** **Example:** `Device(config)# voice service voip`	Enters voice-service configuration mode.
Step 4	**sip** **Example:** `Device(conf-voi-serv)# sip`	Enters service SIP configuration mode.
Step 5	**error-code-override cac-bandwidth failure** *sip-status-code-number* **Example:** `Device(conf-serv-sip)# error-code-override cac-bandwidth failure 500`	Configures bandwidth-based CAC SIP error response code mapping at the global level.

Step 6	**end**
	Example:
	`Device(conf-serv-sip)# end`
		Exits service SIP configuration mode and enters privileged EXEC mode.

Configuring Bandwidth-Based Call Admission Control SIP Error Response Code Mapping at the Dial Peer Level

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *tag* {**pots** | **voatm** | **vofr** | **voip**}
4. **voice-class sip error-code-override cac-bandwidth failure** {*sip-status-code-number* | **system**}
5. **end**

DETAILED STEPS

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

Step 3	**dial-peer voice** *tag* {**pots** | **voatm** | **vofr** | **voip**}
	Example:
	`Device(config)# dial-peer voice 88 voip`
		Enters dial peer voice configuration mode.

Step 4	**voice-class sip error-code-override cac-bandwidth failure** {*sip-status-code-number* | **system**}
	Example:
	`Device(config-dial-peer)# voice-class sip error-code-override cac-bandwidth failure 500`
		Configures bandwidth-based CAC SIP error response code mapping at the dial peer level.

Step 5	**end**
	Example:
	`Device(config-dial-peer)# end`
		Exits dial peer configuration mode and enters privileged EXEC mode.

Verifying Bandwidth-Based Call Admission Control

Perform this task to verify the configuration for the Bandwidth-Based Call Admission Control feature on Cisco UBE. The **show** commands need not be entered in any specific order.

SUMMARY STEPS

1. **enable**
2. **show call threshold config**
3. **show call threshold status**
4. **show call threshold stats**
5. **show dial-peer voice**

DETAILED STEPS

Step 1 **enable**

Example:

```
Device>enable
```

Enables privileged EXEC mode.

Step 2 **show call threshold config**

Example:

```
Device# show call threshold config

Some resource polling interval:
  CPU_AVG interval: 60
  Memory interval:  5

IF                  Type            Value   Low     High    Enable
-----               ----            -----   ----    ----    ------
GigabitEthernet0/0  int-bandwidth   0       100     400      N/A
```

Displays the current call threshold configuration at the interface level for all resources.

Step 3 **show call threshold status**

Example:

```
Device# show call threshold status

Status  IF                  Type            Value   Low     High    Enable
------  ---                 ------          ----    ----    ----    -----
Avail   GigabitEthernet0/0  int-bandwidth   0       100     400      N/A
```

Displays the availability status of resources that are configured when the Bandwidth-Based Call Admission Control feature is enabled at an interface level.

Step 4 **show call threshold stats**

Example:

```
Device# show call threshold stats

Total resource check: 2
successful: 1
 failed:   1

1: ------------------------
  Failed resources: int-bandwidth,
  related interface: GigabitEthernet0/0; related option:N/A
  Recorded time: 04:49:39 UTC Wed Dec 8 2010
2: ------------------------
Successful
  All resources are available for this check.
  Recorded time: 04:29:39 UTC Wed Dec 8 2010
```

Displays the statistics of resources that are configured when the Bandwidth-Based Call Admission Control feature is enabled at an interface level.

Step 5 **show dial-peer voice**

Example:

```
Device# show dial-peer voice

incoming called-number = `2000', connections/maximum = 0/unlimited,
bandwidth/maximum = 0/400,
…….
Successful Calls = 0, Failed Calls = 0, Incomplete Calls = 0
Accepted Calls = 3, Refused Calls = 0,
Bandwidth CAC Accepted Calls = 3, Bandwidth CAC Refused Calls = 0
```

Displays information for the voice dial peer.

Troubleshooting Tips

The following commands can help troubleshoot the Bandwidth-Based Call Admission Control feature:

- **debug ccsip all**
- **debug voice ccapi all**

Configuration Examples for Bandwidth-Based Call Admission Control

Example: Configuring Bandwidth-Based Call Admission Control at the Interface Level

The following example shows how to configure Cisco UBE to reject new SIP calls if the accounted VoIP media bandwidth on Gigabit Ethernet interface 0/0 exceeds 400 Kbps of bandwidth and continues to have a bandwidth above 100 Kbps:

```
Device> enable
Device# configure terminal
Device(config)# call threshold interface GigabitEthernet 0/0 int-bandwidth  low 100 high
400
```

The following example shows how to configure Cisco UBE to reject new SIP calls if the VoIP media bandwidth on Gigabit Ethernet interface 0/0 exceeds the configured bandwidth for priority traffic in the “voip_traffic” class:

```
Device>enable
Device# configure terminal
Device(config)# class-map match-all voip-traffic

Device(config-cmap)# policy-map voip-policy
Device(config-pmap)# class voip-traffic
Device(config-pmap-c)# priority 440
Device(config-pmap-c)# end

Device# enaconfigure terminalble
Device(config)# call threshold interface GigabitEthernet 0/0 int-bandwidth class-map voip-
traffic l2-overhead 10
```

Note Layer 2 overhead of 10 percent in the **call threshold** command indicates that the IP bandwidth, excluding Layer 2, is 90 percent of the configured priority bandwidth.

Example: Configuring Bandwidth-Based Call Admission Control at the Dial Peer Level

The following example shows how to configure Cisco UBE to reject calls once the accounted aggregate bandwidth of active calls exceeds 400 Kbps for a SIP dial peer:

```
Device> enable
Device# configure terminal
Device(config)# dial-peer voice 2000 voip
Device(config)# session protocol sipv2
Device(config-dial-peer)# max-bandwidth 400
```

Example: Configuring the Bandwidth-Based Call Admission Control SIP Error Response Code Mapping at the Global Level

The following example shows how to configure Cisco UBE for bandwidth-based CAC SIP error response code mapping at the global level:

```
Device> enable
Device# configure terminal
Device(config)# voice service voip
Device(conf-voi-serv)# sip
Device(conf-serv-sip)# error-code-override cac-bandwidth 500
```

Example: Configuring the Bandwidth-Based Call Admission Control SIP Error Response Code Mapping at the Dial Peer Level

The following example shows how to configure Cisco UBE for bandwidth-based CAC SIP error response code mapping at the dial peer level:

```
Device> enable
Device# configure terminal
Device(config)# dial-peer voice 88 voip
Device(config-dial-peer)# voice-class sip error-code-override cac-bandwidth failure 500
```

Feature Information for Bandwidth-Based Call Admission Control

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

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

Table 4 Feature Information for Bandwidth-Based Call Admission Control

Feature Name	Releases	Feature Information
Bandwidth-Based Call Admission Control	15.2(2)T	The Bandwidth-Based Call Admission Control feature provides the functionality to reject SIP calls when the bandwidth accounted by the SIP signaling layer exceeds the aggregate bandwidth threshold for VoIP media traffic—voice, video, and fax. This functionality helps prevent QoS degradation of VoIP media traffic for existing calls when the bandwidth allocated for VoIP traffic is fully utilized. The following commands were introduced or modified: **call threshold interface**, **error-code-override**, **max-bandwidth**, **show call threshold**, **voice-class sip**

Feature Name	Releases	Feature Information
Bandwidth-Based Call Admission Control	Cisco IOS XE Release 3.7S	The Bandwidth-Based Call Admission Control feature provides the functionality to reject SIP calls when the bandwidth accounted by the SIP signaling layer exceeds the aggregate bandwidth threshold for VoIP media traffic—voice, video, and fax. This functionality helps prevent QoS degradation of VoIP media traffic for existing calls when the bandwidth allocated for VoIP traffic is fully utilized. The following commands were introduced or modified: **call threshold interface**, **error-code-override**, **max-bandwidth**, **show call threshold**, **voice-class sip**

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.

Interworking Between RSVP Capable and RSVP Incapable Networks

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

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

Finding Feature Information

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

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 Interworking Between RSVP Capable and RSVP Incapable Networks

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

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

Cisco Unified Border Element

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

Cisco Unified Border Element (Enterprise)

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

Restrictions for Interworking Between RSVP Capable and RSVP Incapable Networks

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

- Segmented RSVP is not supported.
- Interoperability between Cisco UBE and Cisco Unified Communications Manager is not available.
- RSVP-enabled video calls are not supported.

How to Configure Interworking Between RSVP Capable and RSVP Incapable Networks

- Configuring RSVP on an Interface, page 36
- Configuring Optional RSVP on the Dial Peer, page 37
- Configuring Mandatory RSVP on the Dial Peer, page 39
- Configuring Midcall RSVP Failure Policies, page 40
- Configuring DSCP Values, page 42
- Configuring an Application ID, page 43
- Configuring Priority, page 44

Configuring RSVP on an Interface

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type slot* / *port* **Example:** `Device(config)# interface FastEthernet 0/1`	Configures an interface type and enters interface configuration mode.
Step 4	**ip rsvp bandwidth** [*reservable-bw* [*max-reservable-bw*] [**sub-pool** *reservable-bw*]] **Example:** `Device(config-if)# ip rsvp bandwidth 10000 100000`	Enables RSVP for IP on an interface.

Step 5	**end**
	Example:
	`Device(config-if)# end`
		(Optional) Exits interface configuration mode and returns to privileged EXEC mode.

Configuring Optional RSVP on the Dial Peer

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

SUMMARY STEPS

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

DETAILED STEPS

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

	Command or Action	Purpose
Step 5	**req-qos** {**controlled-load** | **guaranteed-delay**} [**audio** | **video**] [**bandwidth** [**default** *bandwidth-value*] [**max** *bandwidth-value*]] **Example:** `Device(config-dial-peer)# req-qos controlled-load`	Configures the desired quality of service (QoS) to be used. • Calls continue even if there is a failure in bandwidth reservation. **Note** Configure the **req-qos** commandusing the same keyword that you used to configure the **acc-qos** command, either **controlled-load** or **guaranteed-delay**. That is, if you configured **acc-qos controlled-load** command in the previous step, then use the **req-qos controlled-load** command here.

Step 6	**end**
	Example:
	`Device(config-dial-peer)# end`
		(Optional) Exits dial peer voice configuration mode and returns to privileged EXEC mode.

Configuring Mandatory RSVP on the Dial Peer

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

SUMMARY STEPS

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

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**dial-peer voice** *tag* **voip** **Example:** `Device(config)# dial-peer 77 voip`	Enters dial peer voice configuration mode.
Step 4	**acc-qos** {**best-effort** | **controlled-load** | **guaranteed-delay**} [**audio** | **video**] **Example:** `Device(config-dial-peer)# acc-qos best-effort`	Configures mandatory RSVP on the dial-peer. • Keywords are as follows: ◦ **best-effort**--Indicates that Resource Reservation Protocol (RSVP) makes no bandwidth reservation. This is the default. ◦ **controlled-load**--Indicates that RSVP guarantees a single level of preferential service, presumed to correlate to a delay boundary. The controlled load service uses admission (or capacity) control to ensure that preferential service is received even when the bandwidth is overloaded. ◦ **guaranteed-delay**--Indicates that RSVP reserves bandwidth and guarantees a minimum bit rate and preferential queueing if the bandwidth reserved is not exceeded.

Step 5	**req-qos** {**best-effort** [**audio** | **video**] | {**controlled-load** | **guaranteed-delay**} [**audio** | **video**] [**bandwidth** [**default** *bandwidth-value*] [**max** *bandwidth-value*]]}
	Example:
	`Device(config-dial-peer)# req-qos controlled-load`
		Configures mandatory RSVP on the dial-peer.
		• Calls continue even if there is a drop in the bandwidth reservation.

Step 6	**end**
	Example:
	`Device(config-dial-peer)# end`
		(Optional) Exits dial peer voice configuration mode and returns to privileged EXEC mode.

Configuring Midcall RSVP Failure Policies

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**dial-peer voice** *tag* **voip** **Example:** `Device(config)# dial-peer voice 66 voip`	Enters dial peer voice configuration mode.
Step 4	**voice-class sip rsvp-fail-policy** {**video** | **voice**} **post-alert** {**optional keep-alive** | **mandatory** {**keep-alive** | **disconnect retry** *retry-attempts*}} **interval** *seconds* **Example:** `Device(config-dial-peer)# voice-class sip rsvp-fail-policy voice post-alert mandatory keep-alive interval 50`	Enables call handling policies for a midcall RSVP failure. • Keywords are as follows: ◦ **optional keep-alive**--The keepalive messages are sent when RSVP fails only if RSVP negotiation is optional. ◦ **mandatory keep-alive**--The keepalive messages are sent when RSVP fails only if RSVP negotiation is mandatory. **Note** Keepalive messages are sent at 30-second intervals when a postalert call fails to negotiate RSVP regardless of the RSVP negotiation setting (mandatory or optional).

	Command or Action	Purpose

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

Configuring DSCP Values

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. - Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**dial-peer voice** *tag* **voip** **Example:** `Device(config)# dial-peer voice 66 voip`	Enters dial peer voice configuration mode.

	Command or Action	Purpose

Step 4	**ip qos dscp** {*dscp-value* | *set-af* | *set-cs* | **default** | **ef**} {**signaling** | **media** [**rsvp-pass** | **rsvp-fail**] | **video**[**rsvp-none**| **rsvp-pass** | **rsvp-fail**]}
	Example:
	`Device(config-dial-peer)# ip qos dscp af11 media rsvp-pass`
		Configures DSCP values based on RSVP status.
		• Keywords are as follows:
		◦ **media rsvp-pass**--Specifies that the DSCP value applies to media packets with successful RSVP reservations.
		◦ **media rsvp-fail**--Specifies that the DSCP value applies to packets (media or video) with failed RSVP reservations.
		◦ The default DSCP value for all media (voice and fax) packets is **ef**.
		Note You must configure the DSCP values for all cases: **media rsvp-pass** and **media rsvp-fail**.

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

Configuring an Application ID

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

SUMMARY STEPS

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

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**dial-peer voice** *tag* **voip** **Example:** `Device(config)# dial-peer voice 66 voip`	Enters dial peer voice configuration mode.
Step 4	**ip qos policy-locator** {**video** | **voice**} [**app** *app-string*] [**guid** *guid-string*] [**sapp** *subapp-string*] [**ver** *version-string*] **Example:** `Device(config-dial-peer)# ip qos policy-locator voice`	Configures a QoS policylocator (application ID) used to deploy RSVP policies for specifying bandwidth reservations on Cisco IOS Session Initiation Protocol (SIP) devices.

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

Configuring Priority

Perform this task to configure priorities for call preemption.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**dial-peer voice** *tag* **voip** **Example:** `Device(config)# dial-peer voice 66 voip`	Enters dial peer voice configuration mode.
Step 4	**ip qos defending-priority** *defending-pri-value* **Example:** `Device(config-dial-peer)# ip qos defending-priority 66`	Configures the RSVP defending priority value for determining QoS.
Step 5	**ip qos preemption-priority** *preemption-pri-value* **Example:** `Device(config-dial-peer)# ip qos preemption-priority 75`	Configures the RSVP preemption priority value for determining QoS.

Step 6	**end**
	Example:
	`Device(config-dial-peer)# end`
		(Optional) Exits dial peer configuration mode and returns to privileged EXEC mode.

Troubleshooting for Interworking Between RSVP Capable and RSVP Incapable Networks Feature

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

- **debug call rsvp-sync events**

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

Verifying Interworking Between RSVP Capable and RSVP Incapable Networks

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show sip-ua calls** **Example:** `Device# show sip-ua calls`	(Optional) Displays active user agent client (UAC) and user agent server (UAS) information on SIP calls.

	Command or Action	Purpose
Step 3	**show ip rsvp installed** **Example:** `Device# show ip rsvp installed`	(Optional) Displays RSVP-related installed filters and corresponding bandwidth information.
Step 4	**show ip rsvp reservation** **Example:** `Device# show ip rsvp reservation`	(Optional) Displays RSVP-related receiver information currently in the database.
Step 5	**show ip rsvp interface detail** [*interface-type number*] **Example:** `Device# show ip rsvp interface detail GigabitEthernet 0/0`	(Optional) Displays the interface configuration for hello.
Step 6	**show sccp connections details** **Example:** `Device# show sccp connections details`	(Optional) Displays SCCP connection details, such as call-leg details.
Step 7	**show sccp connections rsvp** **Example:** `Device# show sccp connections rsvp`	(Optional) Displays information about active SCCP connections that are using RSVP.
Step 8	**show sccp connections internal** **Example:** `Device# show sccp connections internal`	(Optional) Displays the internal SCCP details, such as time-stamp values.
Step 9	**show sccp** [**all** | **connections** | **statistics**] **Example:** `Device# show sccp statistics`	(Optional) Displays SCCP information, such as administrative and operational status.

Feature Information for Interworking Between RSVP Capable and RSVP Incapable Networks

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

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

Feature History Table entry for the Cisco Unified Border Element.

Table 5 Feature Information for Interworking Between RSVP Capable and RSVP Incapable Network

Feature Name	Releases	Feature Information
Interworking Between RSVP Capable and RSVP Incapable Networks	15.0(1)XA 15.1(1)T	The Interworking Between RSVP Capable and RSVP Incapable Networks feature provides precondition-based RSVP support for basic audio call and supplementary services on the Cisco UBE. The following commands were introduced or modified: **acc-qos**, **ip qos defending-priority**, **ip qos dscp**, **ip qos policy-locator**, **ip qos preemption-priority, req-qos**, **voice-class sip rsvp-fail-policy**,
Interworking Between RSVP Capable and RSVP Incapable Networks	Cisco IOS XE Release 3.1S	The nterworking Between RSVP Capable and RSVP Incapable Networks feature provides precondition-based RSVP support for basic audio call and supplementary services on the Cisco UBE. The following commands were introduced or modified: **acc-qos**, **ip qos defending-priority**, **ip qos dscp**, **ip qos policy-locator**, **ip qos preemption-priority**, **req-qos**, **voice-class sip rsvp-fail-policy**,

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.

Cisco Resource Reservation Protocol Agent

The Cisco RSVP Agent feature enables the call admission control (CAC) mechanism based on the Resource Reservation Protocol (RSVP), which is applicable to any network topology and which eases the restriction of a traditional hub-and-spoke topology.

Finding Feature Information

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

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 Cisco Resource Reservation Protocol Agent

Cisco Unified Border Element

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

Cisco Unified Border Element (Enterprise)

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

Configuring Cisco Resource Reservation Protocol Agent

To enable this feature, see the " Unified CM RSVP-Enabled Locations " section in the " Call Admission Control" chapter of the Cisco Unified Communications SRND Based on Cisco Unified Communications Manager 7.x Guide at the following URL:

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/7x/cac.html#wp1043949

Detailed command information for the **dspfarm profile**, **ip rsvp bandwidth**, **maximum sessions**, **switchover method immediate**, **switchback method guard timeout**, and **timer receiver-rtp**commands are located in the Cisco IOS Voice Command Reference

Feature Information for Cisco Resource Reservation Protocol Agent

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

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

Table 6 Feature Information for Cisco RSVP Agent

Feature Name	Releases	Feature Information
Cisco Resource Reservation Protocol (RSVP) Agent	12.4(4)T	Enables the CAC mechanism based on the RSVP agent. The following commands were introduced or modified: **dspfarm profile**, **ip rsvp bandwidth**, **maximum sessions**, **switchover method immediate**, **switchback method guard timeout**, and **timer receiver-rtp**.
Cisco Resource Reservation Protocol (RSVP) Agent	Cisco IOS XE Release 3.3S	Enables the CAC mechanism based on the RSVP agent. The following commands were introduced or modified: **dspfarm profile**, **ip rsvp bandwidth**, **maximum sessions**, **switchover method**, and **timer receiver-rtp**.

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

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

Prerequisites for SIP INFO Method for DTMF Tone Generation

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

Cisco Unified Border Element

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

Cisco Unified Border Element (Enterprise)

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

Restrictions for SIP INFO Methods for DTMF Tone Generation

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

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

Information About SIP INFO Method for DTMF Tone Generation

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

How to Review SIP INFO Messages

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

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

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

Configuring for SIP INFO Method for DTMF Tone Generation

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

Troubleshooting Tips

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

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

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

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

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

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

Feature Information for SIP INFO Method for DTMF Tone Generation

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

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

Table 7 Feature Information for SIP: INFO Method for DTMF Tone Generation

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

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

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

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:** `Device> 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:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**sip-ua** **Example:** `Device(config)# sip-ua`	Enters SIP user-agent configuration mode.

	Command or Action	Purpose
Step 4	**timers notify** *number* **Example:** `Device(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:** `Device(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:** `Device(config-sip-ua)# exit`	Exits the current mode.

- Verifying SIP DTMF Support, page 63

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:

```
Device# 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:

```
Device# 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:

```
Device# 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:

```
Device# 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:

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

Step 4 **show sip-ua status**

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

Example:

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

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

Example:

```
Device# show sip-ua status
SIP User Agent Status
SIP User Agent for UDP : ENABLED
SIP User Agent for TCP : ENABLED
SIP User Agent bind status(signaling): DISABLED
SIP User Agent bind status(media): DISABLED
SIP 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:

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

Step 5 **show sip-ua timers**

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

Example:

```
Device# 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:

```
Device# 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.

Table 8 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**.
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**.

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

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 3.7S 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:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**dial-peer voice** *tag* **voip** **Example:** `Device(config)# dial-peer voice 10 voip`	Enters dial peer voice configuration mode.
Step 4	**voice-class codec** *tag* [**offer-all**] **Example:** `Device(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:
	`Device(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:

```
Device# 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:

```
Device# 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:

```
Device# 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:

```
Device# 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.

Table 9 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 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 3.7S	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)**.

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.

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

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

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

Finding Feature Information

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

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.

Symmetric and Asymmetric Calls

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

- A symmetric endpoint accepts and sends the same payload type.

- An asymmetric endpoint can accept and send different payload types.

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

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

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

Cisco Unified Border Element

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

Cisco Unified Border Element (Enterprise)

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

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

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

- H323-to-H323 and H323-to-SIP calls.
- All transcoded calls.
- Secure Real-Time Protocol (SRTP) pass-through calls.
- Flow-around calls.
- Asymmetric payload types are not supported on early-offer (EO) call legs in a delayed-offer to early-offer (DO-EO) scenario.
- Multiple *m* lines with the same dynamic payload types, where *m* is:

m = audio <media-port1> RTP/AVP XXX m = video <media-port2> RTP/AVP XXX

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

Configuring Dynamic Payload Support at the Global Level

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

SUMMARY STEPS

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

DETAILED STEPS

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

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

Step 5	**asymmetric payload** {**dtmf** | **dynamic-codecs** | **full** | **system**}
	Example:
	`Device(conf-serv-sip)# asymmetric payload full`
		Configures global SIP asymmetric payload support.
		Note The **dtmf** and **dynamic-codecs** keywords are internally mapped to the **full** keyword to provide asymmetric payload type support for audio and video codecs, DTMF, and NSEs.

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

Configuring Dynamic Payload Support for a Dial Peer

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

SUMMARY STEPS

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

DETAILED STEPS

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

Step 5	**end**
	Example:
	`Device(config-dial-peer)# end`
		(Optional) Exits dial peer voice configuration mode and enters privileged EXEC mode.

Verifying Dynamic Payload Interworking for DTMF and Codec Packets Support

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

SUMMARY STEPS

1. **enable**
2. **show call active voice compact**
3. **show call active voice**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show call active voice compact** **Example:** `Device# show call active voice compact`	(Optional) Displays a compact version of call information.
Step 3	**show call active voice** **Example:** `Device# show call active voice`	(Optional) Displays call information for voice calls in progress.

Troubleshooting Tips

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

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

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

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

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

Table 10 Feature Information for Dynamic Payload Interworking for DTMF and Codec Packets Support

Feature Name	Releases	Feature Information
Dynamic Payload Type Interworking for DTMF and Codec Packets for SIP-to-SIP Calls	15.0(1)XA 15.1(1)T	The Dynamic Payload Type Interworking for DTMF and Codec Packets for SIP-to-SIP Calls feature provides dynamic payload type interworking for DTMF and codec packets for SIP-to-SIP calls. The following commands were introduced or modified: **asymmetric payload** and **voice-class sip asymmetric payload**.
Dynamic Payload Type Interworking for DTMF and Codec Packets for SIP-to-SIP Calls	Cisco IOS Release XE 3.1S	The Dynamic Payload Type Interworking for DTMF and Codec Packets for SIP-to-SIP Calls feature provides dynamic payload type interworking for DTMF and codec packets for SIP-to-SIP calls. The following commands were introduced or modified: **asymmetric payload** and **voice-class sip asymmetric payload**.

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

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

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:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**dial-peer voice** *tag* **voip** **Example:** `Device(config)# dial-peer voice 10 voip`	Enters dial-peer configuration mode for the VoIP dial peer designated by *tag*.

Step 4	**rtp payload-type cisco-codec-ilbc** [*number*
	Example:
	`Device(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:** `Device(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:** `Device(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:** `Device> enable`	Enters privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**voice class codec** *tag* **Example:** `Device(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:** `Device(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:** `Device(config-voice-class)# exit`	Exits the current mode.
Step 6	**dial-peer voice** *tag* **voip** **Example:** `Device(config)# dial-peer voice 16 voip`	Enters dial-peer configuration mode for the specified VoIP dial peer.
Step 7	**voice-class codec** *tag* **Example:** `Device(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:** `Device(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.

Table 11 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 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**.

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.

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

The DSP-Based Functionality on the Cisco UBE (Enterprise) Including Transcoding and Transrating of dspfarm feature provides transcoding support for DSPs that are located on the same box as the Cisco ASR.

Finding Feature Information

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

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

- To enable this feature, you must have Cisco IOS XE Release 3.2S or a later release installed and running on your Cisco ASR 1000 Series Router.

Restrictions for DSP-Based Functionality on the Cisco UBE Enterprise Including Transcoding and Transrating

- Out-of-box transcoding is not supported.
- Cisco Unified Communications Manager transcoding is not supported.
- Transcoding calls are not check-pointed, when failover happens, these calls will not be persevered. The expected behavior is for the SPA card to reset the DSPs and start the firmware download.

Information About DSP-Based Functionality on Cisco UBE Enterprise Including Transcoding and Transrating

To configure transcoding on the Cisco UBE it was required that architecture a Cisco Unified Communications Manager was required to setup the transcoding streams through SCCP protocol for both inbox and out-of-box transcoding. The result is a significant amount of overhead for the inbox transcoding case with SCCP messaging and additional 2 RTPSPI and VOIP RTP ports associated with the SCCP transcoding call leg. The DSP-based functionality feature avoids addition resource overhead for inbox transcoding by having DSMP streams setup via VOIP FPI by the SPI legs bypassing the requirement for SCCP client, SCCP server and RTPSPI streams for inbox transcoding. The transcoding conversion in the Cisco UBE (Enterprise) is completed in the Ucode library. The DSP farm profile guarantees the configured resources for the most complex codec that is configured.

DTMF interoperability for transcoding calls is supported for the following call flows:

- RFC2833 <—> OOB
- RFC2833 <—> RFC2833
- Inband Tone <—> RFC2833

Note Inband <—> OOB is not supported currently by the CUBE (Enterprise).

How to Configure DSP-Based Functionality on Cisco UBE Enterprise Including Transcoding and Transrating

To configure DSP-Based Functionality on the Cisco UBE (Enterprise) Including Transcoding and Transrating perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dspfarm profile**
   - Cisco Unified Border Element
   - Cisco Unified Border Element (Enterprise)
4. **codec** {*codec-type* | **pass-through**}
5. **maximum sessions** *number*
6. **associate application** {**cube** | **sbc** | **sccp**}
7. **no shutdown**
8. **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	**dspfarm profile**
	• Cisco Unified Border Element
	• Cisco Unified Border Element (Enterprise)
	Example:
	dspfarm profile*profile-identifier* { **conference** | **mtp** | **transcode** [**security**]
	`Device(config)# dspfarm profile 1 transcode security`
	Example:
	dspfarm profile*profile-identifier* **transcode**
	`Device# dspfarm profile 2 transcode`
		Enters the DSP farm profile configuration mode and defines a profile for digital signal processor (DSP) farm services.
		Note SRTP support on the Cisco Unified Border Element is provided via a transcoding profile. SRTP support on the Cisco Unified Border Element (Enterprise) is provided through library.

	Command or Action	Purpose

Step 4	**codec** {*codec-type* | **pass-through**}
	Example:
	`Device (config-dspfarm-profile)# codec g711ulaw`
		Specifies the codecs supported by a DSP farm profile. Repeat this step for each codec supported by the profile.
		Note Hardware MCPO support only G.711 a-law and G.711 u-law. If you configure a profile as a hardware MTP, and you want to change the codec to other than G.711, you must first remove the hardware MTP by using the no maximum sessions hardware command.
		Note Only one codec is supported for each MTP profile. To support multiple codecs, you must define a separate MTP profile for each codec.

Step 5	**maximum sessions** *number* **Example:** `Device (config-dspfarm-profile)# maximum sessions 768`	Specifies the maximum number of sessions that are supported by the profile. • *number* --Range is determined by the available registered DSP resources. Default is 0. **Note** The hardware and software keywords apply only to MTP profiles.

Step 6	**associate application** {**cube** | **sbc** | **sccp**}
	Example:
	`Device(config-dspfarm-profile)# associate application cube`
		Associates the application to the DSP profile.

Step 7	**no shutdown** **Example:** `Device (config-dspfarm-profile)# no shutdown`	Enables the profile, allocates DSP farm resources, and associates the application.
Step 8	**exit** **Example:** `Device (config-dspfarm-profile)# exit`	Exits DSP farm profile configuration mode.

- Verifying DSP Farm Configuration, page 98

Verifying DSP Farm Configuration

To verify DSP-based functionality on Cisco UBE (Enterprise) including Transcoding and Transrating of dspfarm feature use the following commands:

- **show voice dsp group** — Displays the DSP resource allocation, the total number of credits, and number of credits and channels in use.
- **show dspfarm dsp** — Display the dsps allocated to the dspfarm.

- **show dspfarm dsp stats** -—– Displays statistics for each dsp session.

Feature Information for DSP-based functionality on Cisco UBE Enterprise including Transcoding and Transrating

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

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

Table 12 Feature Information for DSP-based functionality on Cisco UBE including Transocoding and Transrating

Feature Name	Releases	Feature Information
DSP Based Functionality on the Cisco UBE (Enterprise) Including Transcoding and Transrating	Cisco IOS XE Release 3.2S	Provides transcoding support for DSPs that are located on the same box as the Cisco UBE (Enterprise). The following commands were modified: **associate application**, **codec**, and **dspfarm profile**.

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.

Acoustic Shock Protection

Acoustic Shock Protection (ASP) is a voice circuit-breaker feature that is designed to protect users, especially those wearing headsets, from exposure to loud, sustained, and piercing tones, such as those produced by a fax machine. It is a workplace-safety feature for voice calls. When the tone is present at the input of the ASP module, the audio path in the affected direction is muted to protect the listener, and a gentle alert tone is played out for as long as the tone persists. ASP may be inserted in either or both directions of a call, that is, applied to incoming packets to protect the ears of a listener on the Time-Division Multiplexing (TDM) gateway, applied to incoming PSTN calls (microphone signal) to protect the ears of listeners at the other end of the call, or applied to both simultaneously.

Finding Feature Information

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

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

Restrictions for ASP

- Supported on PVDM3 only.
- Supported only on flex codec complexity.
- No support for H.32x video call, complex forking calls, and fax and modem calls.
- No support for TDM hairpin call.
- The configuration under dial peer has higher priority than the configuration at the global level.
- No support for conference calls, IP/SIP phones, and the Skinny Client Control Protocol (SCCP).
- CLI supports enabling ASP but not disabling ASP.
- No support for dynamically enabling or disabling ASP during a call.

Information About ASP

Acoustic Shock Protection

Acoustic Shock Protection (ASP) is an adaptive signal processing algorithm on the Digital Signal Processor (DSP) that analyzes incoming audio for the presence of offending tones that might harm humans. Offending tones include signals that are:

- Loud
- Tonal (energy concentrated around a single frequency)
- Persistent (lasts longer than a few tens of milliseconds)

If an offending tone is present, the audio path in that direction is muted temporarily, and a quiet, alerting signal is played out to the listener side. The call is never dropped; only the audio is muted temporarily. If or when the tone disappears from the input, the mute is removed. ASP does not disrupt low-frequency tones (below 650 Hz) such as ringback, dial, and so forth. Since ASP is designed to mute only single-frequency tones, it allows multi-tone signals such as Dual Tone Multi-Frequency (DTMF) to pass unhindered. ASP is supported on TDM gateways (TDM-VoIP and TDM-TDM) and on the Cisco Unified Border Element (Cisco UBE).

Note ASP is for voice calls only and not for faxes and modems.

Some of the best practices for ASP are as follows:

- Use default values
- Use ASP on dial peers where you are certain that people (not faxes) are listening.
- Do not use ASP on dial peers associated with fax machines, modems, or TTY/TDD devices. Use fax-relay or modem-relay modes on dial peers dedicated to such devices.
- ASP is designed for deployment in situations where customers have experienced acoustic shock safety issues. If there are issues like false triggering (for example, ASP alerts on regular voices), then you must turn off ASP. You can choose from three detector sensitivity modes: slow, auto, or fast. Fast mode is a highly sensitive hair-trigger. Auto mode is recommended. Slow mode lets more tone leak through, but has better rejection of false triggers.

How to Configure ASP

Creating the Media Profile for ASP

Perform this task to create a media profile to configure acoustic shock protection.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **media profile asp** *tag*
4. **mode** *mode*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**media profile asp** *tag* **Example:** `Device(config)# media profile asp 5`	Creates the media profile to configure ASP and enters media profile configuration mode. The range for the media profile tag is from 1 to 10000.
Step 4	**mode** *mode* **Example:** `Device(cfg-mediaprofile)# mode auto`	Sets the ASP sensitivity mode to preset = auto (which is default). Auto mode provides a good tradeoff between ASP speed and false trigger rejection. The other modes are: • slow—Presets ASP sensitivity mode to 1. This mode provides slower detection speed for reduced chance of false triggers. • fast—Presets ASP sensitivity mode to 2. This mode provides faster detection speed but higher chance of false triggers. • expert—This mode exposes direct control of individual ASP parameters and is recommended for test use only.

	Command or Action	Purpose

Step 5	**end**
	Example:
	`Device(config)# end`
		Returns to privileged EXEC mode.

Creating the Media Profile to Enable ASP

After the media profile is created, you must create a media class to enable acoustic shock protection. Perform this task to create a media class.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **media class** *tag*
4. **asp profile** *tag*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**media class** *tag* **Example:** `Device(config)# media class 2`	Creates the media class to enable the acoustic shock protection feature and enters media class configuration mode. The range for the media class tag is from 1 to 10000.

	Command or Action	Purpose
Step 4	**asp profile** *tag* **Example:** `Device(cfg-mediaclass)# asp profile 200`	Applies the media profile to the media class. The range for the media profile ASP tag is from 1 to 10000.

Step 5	**end**
	Example:
	`Device(cfg-mediaclass)# end`
		Returns to privileged EXEC mode.

Configuring the Media Class at a Dial Peer Level for ASP

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *tag* **pots**
4. **media-class** *tag*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**dial-peer voice** *tag* **pots** **Example:** `Device(config)# dial-peer voice 20 pots`	Defines a particular dial peer and enters dial-peer voice configuration mode. The range for the dial-peer voice tag is from 1 to 1073741823.

	Command or Action	Purpose
Step 4	**media-class** *tag* **Example:** `Device(config-dial-peer)# media-class 2`	Applies the media class to the specific dial peer. The range for the media class tag number is from 1 to 10000.

Step 5	**end**
	Example:
	`Device(config-dial-peer)# end`
		Returns to privileged EXEC mode.

Configuring the Media Class Globally for ASP

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **media service**
4. **enhancement**
5. **tdm** *tag*
6. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**media service** **Example:** `Device(config)# media service`	Enters media service configuration mode.
Step 4	**enhancement** **Example:** `Device(cfg-mediaservice)# enhancement`	Enters the submode enhance of media service.
Step 5	**tdm** *tag* **Example:** `Device(cfg-service-enhance)# tdm 2`	Applies the TDM call globally. The range for the media class tag number is from 1 to 10000.

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

Verifying ASP

Perform this task to verify the voice quality metrics.

SUMMARY STEPS

1. **enable**
2. **show call active voice stats | b pid:**

DETAILED STEPS

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

Step 2 **show call active voice stats | b pid:**

Example:

Device# **show call active voice stats | b pid:1300**

```
11EC : 5 09:14:25.971 PDT Thu Jul 28 2011.1 +1130 pid:1300 Answer 1300 active dur 00:01:36 tx:
17/321 rx:17/321 dscp:0 media:0
DSP/TX: PK=17, SG=0, NS=1, DU=90570, VO=320
DSP/RX: PK=17, SG=0, CF=1, RX=90570, VO=320, BS=0, BP=0, LP=0, EP=0
….
DSP/DL: RT=0, ED=0
MIC Direction:
DSP/NR: NR=1, ND=0, LV=257, IN=1, PN=0, ON=0
DSP/AS: AE=1, AD=0, AV=0, AM=0, NT=0, DT=0, TT=0, TD=0, LF=0, LD=0
EAR Direction:
DSP/NR: NR=0, ND=0, LV=0, IN=0, PN=0, ON=0
DSP/AS: AE=0, AD=0, AV=0, AM=0, NT=0, DT=0, TT=0, TD=0, LF=0, LD=0
11EC : 6 09:14:25.973 PDT Thu Jul 28 2011.2 +1130 pid:2300 Originate 2300 active dur 00:01:36 tx:
17/457 rx:17/321 dscp:0 media:0
Telephony call-legs: 1
SIP call-legs: 0
H323 call-legs: 1
```

Displays information about digital signal processing (DSP) voice quality metrics.

Troubleshooting Tips

The following commands can help troubleshoot ASP:

- **debug voip hpi all**
- **debug voip dsmp all**
- **debug voip dsm all**
- **debug voip vtsp all**
- **debug vpm dsp all**

Configuration Examples for the Acoustic Shock Protection Feature

Example: Enabling ASP Globally

```
media profile asp 6
!
media class 1
  asp profile 6
!
media service
  enhancement
    tdm 1
```

Example: Enabling ASP on a Dial Peer

```
media profile asp 4
!
media class 1
```

```
  asp profile 4
!
dial-peer voice 2100 pots
  destination-pattern 2100
  incoming called-number 1100
  media-class 1
  port 0/2/0:1
  forward-digits all
 dial-peer voice 1300 voip
 destination-pattern 1300 session target ipv4:1.2.146.102 media-class 1
```

Feature Information for Acoustic Shock Protection

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

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

Table 13 Feature Information for Acoustic Shock Protection

Feature Name	Releases	Feature Information
Acoustic Shock Protection	15.2(2)T, 15.2(3)T	Acoustic Shock Protection (ASP) is a voice circuit-breaker feature that is designed to protect users, especially those wearing headsets, from exposure to loud, sustained, and piercing tones, such as those produced by a fax machine. It is a workplace-safety feature for voice calls. ASP is supported on TDM gateways and on Cisco UBE. The following commands were introduced or modified: **media profile asp**, **media service**.

Feature Name	Releases	Feature Information
Acoustic Shock Protection	Cisco IOS XE Release 3.6S	Acoustic Shock Protection (ASP) is a voice circuit-breaker feature that is designed to protect users, especially those wearing headsets, from exposure to loud, sustained, and piercing tones, such as those produced by a fax machine. It is a workplace-safety feature for voice calls. ASP is supported on TDM gateways and on Cisco UBE. In Cisco IOS XE Release 3.6S, this feature was implemented on the Cisco Unified Border Element (Enterprise) The following commands were introduced or modified: **media profile asp**, **media service**.

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.

Noise Reduction

Noise Reduction (NR) is a voice enhancement process that improves the quality of incoming speech that has already been corrupted with background noise; for example, a voice conference participant speaking on a cell-phone in a car. NR works best with steady state broadband noises like engine noise but not as well with impulsive noises like nearby chatter.

Finding Feature Information

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

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 Noise Reduction

Cisco Unified Border Element

- Cisco IOS Release 15.2(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 3.6S or a later release must be installed and running on your Cisco ASR 1000 Series Router.

Restrictions for NR

- Supported only on PVDM3.
- Supported only on flex codec complexity.

- No support for H.32x video call, complex forking calls, and fax and modem calls.
- No support for Time-Division Multiplexing (TDM) hairpin call.
- Configurations under POTS dial peer has higher priority over VoIP dial peer for NR.
- Configurations under the dial peer has higher priority than configurations at the global level.
- No support for conference calls, IP/SIP phones, and the Skinny Client Control Protocol (SCCP).
- CLI supports enabling NR but not disabling NR.
- No support for dynamically enabling or disabling NR during a call.

Information About NR

Noise Reduction

Noise Reduction (NR) is an adaptive signal processing algorithm on the Digital Signal Processor (DSP) that analyzes incoming audio, extracts a fingerprint of the background noise during talker pauses, and then performs ongoing spectral subtraction of this noise after a short training period (a few seconds). NR constantly adapts to changes in background noises over time.

NR can affect music on hold signals by making the music quieter. NR may disrupt fax/modem/TDD devices, although it is designed to self-disable in those cases. Use modem-relay mode for reliable fax/modem transmission. NR is supported on TDM gateways (TDM-VoIP and TDM-TDM) and on the Cisco Unified Border Element (Cisco UBE).

Some of the best practices for NR are as follows:

- Use default values.
- Do not use NR on dial peers associated with fax machines. Use fax or modem-relay modes for those dial peers.
- NR, when used without dynamic user control of intensity (as is the case with gateways), must be used at a low intensity (default or lower) since it is always on. High intensity is dramatic for demonstrations with loud background noises, but the NR process itself will degrade “normal” calls if NR is run at high intensity.

How to Configure NR

Creating the Media Profile for NR

Perform this task to create a media profile to configure noise reduction parameters.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **media profile nr** *tag*
4. **intensity** *level*
5. **noisefloor** *level*
6. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**media profile nr** *tag* **Example:** `Device(config)# media profile nr 2`	Creates the media profile to configure noise reduction parameters and enters media profile configuration mode. The range for the media profile tag is from 1 to 10000.
Step 4	**intensity** *level* **Example:** `Device(cfg-mediaprofile)# intensity 2`	Configures the intensity level or depth of the noise reduction process. The range is from 0 to 6.
Step 5	**noisefloor** *level* **Example:** `Device(cfg-mediaprofile)# noisefloor -50`	Configures the noise level, in dBm, above which NR will operate. NR will allow noises quieter than this level to pass without processing. The range is from -58 to -20.

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

Creating the Media Class to Enable NR

After the media profile is created, you must create a media class to enable noise reduction. Perform this task to create a media class.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **media class** *tag*
4. **nr profile** *tag*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**media class** *tag* **Example:** `Device(config)# media class 2`	Creates the media class to enable the noise reduction feature and enters media class configuration mode. The range for the media class tag is from 1 to 10000.
Step 4	**nr profile** *tag* **Example:** `Device(cfg-mediaclass)# nr profile 200`	Applies the media profile to the media class. The range for the media profile NR tag is from 1 to 10000.

Step 5	**end**
	Example:
	`Device(config)# end`
		Returns to privileged EXEC mode.

Configuring the Media Class at a Dial Peer Level for NR

Perform this task to configure the media class for a dial peer.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *tag* **pots**
4. **media-class** *tag*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**dial-peer voice** *tag* **pots** **Example:** `Device(config)# dial-peer voice 20 pots`	Defines a particular dial peer and enters the dial-peer voice configuration mode. The range for the dial-peer voice tag is from 1 to 1073741823.
Step 4	**media-class** *tag* **Example:** `Device(config-dial-peer)# media-class 2`	Applies the media class to the specific dial peer. The range for the media class tag number is from 1 to 10000.

Step 5	**end**
	Example:
	`Device(config-dial-peer)# end`
		Returns to the privileged EXEC mode.

Configuring the Media Class Globally for NR

Perform this task to configure a media class globally.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **media service**
4. **enhancement**
5. **tdm** *tag*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**media service** **Example:** `Device(config)# media service`	Enters media service configuration mode.
Step 4	**enhancement** **Example:** `Device(cfg-mediaservice)# enhancement`	Enters the submode enhance of media service.
Step 5	**tdm** *tag* **Example:** `Device(cfg-service-enhance)# tdm 2`	Applies the TDM call globally. The range for the media class tag number is from 1 to 10000.

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

Verifying NR

Perform this task to verify the voice quality metrics.

SUMMARY STEPS

1. **enable**
2. **show call active voice stats | b pid:**

DETAILED STEPS

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

Step 2 **show call active voice stats | b pid:**

Example:

```
Device# show call active voice stats | b pid:1300
```

```
11EC : 5 09:14:25.971 PDT Thu Jul 28 2011.1 +1130 pid:1300 Answer 1300 active dur 00:01:36 tx:
17/321 rx:17/321 dscp:0 media:0
DSP/TX: PK=17, SG=0, NS=1, DU=90570, VO=320
DSP/RX: PK=17, SG=0, CF=1, RX=90570, VO=320, BS=0, BP=0, LP=0, EP=0
….
DSP/DL: RT=0, ED=0
MIC Direction:
DSP/NR: NR=1, ND=0, LV=257, IN=1, PN=0, ON=0
DSP/AS: AE=1, AD=0, AV=0, AM=0, NT=0, DT=0, TT=0, TD=0, LF=0, LD=0
EAR Direction:
DSP/NR: NR=0, ND=0, LV=0, IN=0, PN=0, ON=0
DSP/AS: AE=0, AD=0, AV=0, AM=0, NT=0, DT=0, TT=0, TD=0, LF=0, LD=0
11EC : 6 09:14:25.973 PDT Thu Jul 28 2011.2 +1130 pid:2300 Originate 2300 active dur 00:01:36 tx:
17/457 rx:17/321 dscp:0 media:0
Telephony call-legs: 1
SIP call-legs: 0
H323 call-legs: 1
```

Displays information about digital signal processing (DSP) voice quality metrics.

Troubleshooting Tips

The following commands can help troubleshoot NR:

- **debug voip hpi all**
- **debug voip dsmp all**
- **debug voip dsm all**
- **debug voip vtsp all**
- **debug vpm dsp all**

Configuration Examples for the NR feature

Example: Enabling NR globally

```
media profile nr 1
 intensity 1
!
media profile nr 2
!
media profile nr 3
 intensity 2
!
media profile nr 4
 intensity 3
!
media profile nr 5
 intensity 2
!
media profile nr 7
 intensity 2
!
media profile asp 6
!
media class 1
 nr profile 5
 asp profile 6
!
media service
 enhancement
  tdm 1
```

Example: Enabling NR on a Dial Peer

```
media profile nr 1
 intensity 1
!
media profile nr 2
 intensity 2
!
media profile nr 3
 intensity 2
!
media profile asp 4
!
media class 1
 nr profile 2
 asp profile 4
!
dial-peer voice 2100 pots
 destination-pattern 2100
 incoming called-number 1100
 media-class 1
 port 0/2/0:1
 forward-digits all
```

```
dial-peer voice 1300 voip
 destination-pattern 1300
 session target ipv4:1.2.146.102
 media-class 1
```

Feature Information for Noise Reduction

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

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

Table 14 Feature Information for Noise Reduction

Feature Name	Releases	Feature Information
Noise Reduction	15.2(2)T, 15.2(3)T	Noise Reduction (NR) is a voice enhancement or restoration process that improves the quality of incoming speech that has already been corrupted with background noise. NR is supported on TDM gateways and on the Cisco UBE. The following commands were introduced or modified: **intensity**, **media profile nr**, **media service**, and **noisefloor**.

Feature Name	Releases	Feature Information
Noise Reduction	Cisco IOS XE Release 3.6S	Noise Reduction (NR) is a voice enhancement or restoration process that improves the quality of incoming speech that has already been corrupted with background noise. NR is supported on TDM gateways and on Cisco UBE. In Cisco IOS XE Release 3.6S, this feature was implemented on the Cisco Unified Border Element (Enterprise). The following commands were introduced or modified: **intensity**, **media profile nr**, **media service**, **noisefloor**.

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 Ability to Send a SIP Registration Message on a Border Element

Finding Feature Information

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

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

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

- Configure a registrar in sip UA configuration mode.

Cisco Unified Border Element

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

Cisco Unified Border Element (Enterprise)

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

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

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

SUMMARY STEPS

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

DETAILED STEPS

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

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

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

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

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

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

Table 15 Feature Information for Sending a SIP Registration Message from a Cisco Unified Border Element

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

SIP Parameter Modification

Finding Feature Information

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

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.

Prereqisites for SIP Parameter Modification

- 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.

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.

Configuring SIP Parameter Modification

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

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

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.

	Command or Action	Purpose
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** o*ption* 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.
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.

Example: Configuring SIP Parameter Modification

```
!
!
!
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.

Table 16 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**
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**

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.

Session Refresh with Reinvites

Finding Feature Information

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

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

Prerequisites for Session Refresh with Reinvites

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

Cisco Unified Border Element

- Cisco IOS Release 12.4(20)T or a later release must be installed and running on your Cisco Unified Border Element.

Cisco Unified Border Element (Enterprise)

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

Information about Session Refresh with Reinvites

Configuring support for session refresh with reinvites expands the ability of the Cisco Unified Border Element to receive a REINVITE message that contains either a session refresh parameter or a change in media via a new SDP and ensure the session does not time out. The **midcall-signaling** command distinguishes between the way a Cisco Unified Communications Express and Cisco Unified Border

Element releases signaling messages. Most SIP-to-SIP video and SIP-to-SIP ReInvite-based supplementary services features require the Configuring Session Refresh with Reinvites feature to be configured.

Cisco IOS Release 12.4(15)XZ and Earlier Releases

Session refresh support via OPTIONS method. For configuration information, see the "Enabling In-Dialog OPTIONS to Monitor Active SIP Sessions" section.

Cisco IOS Release 12.4(15)XZ and Later Releases

Cisco Unified BE transparently passes other session refresh messages and parameters so that UAs and proxies can establish keepalives on a call.

How to Configure Session Refresh with Reinvites

- Configuring Session refresh with Reinvites, page 136

Configuring Session refresh with Reinvites

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

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

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **sip**
5. **midcall-signaling passthru**
6. **exit**
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. - Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice service voip** **Example:** `Router(config)# voice service voip`	Enters VoIP voice-service configuration mode.
Step 4	**sip** **Example:** `Router(conf-voi-serv)# sip`	Enters SIP configuration mode.
Step 5	**midcall-signaling passthru** **Example:** `Router(conf-serv-sip)# midcall-signaling passthru`	Passes SIP messages from one IP leg to another IP leg.
Step 6	**exit** **Example:** `Router(conf-serv-sip)# exit`	Exits the current mode.

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

Feature Information for Session Refresh with Reinvites

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

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

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

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

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:

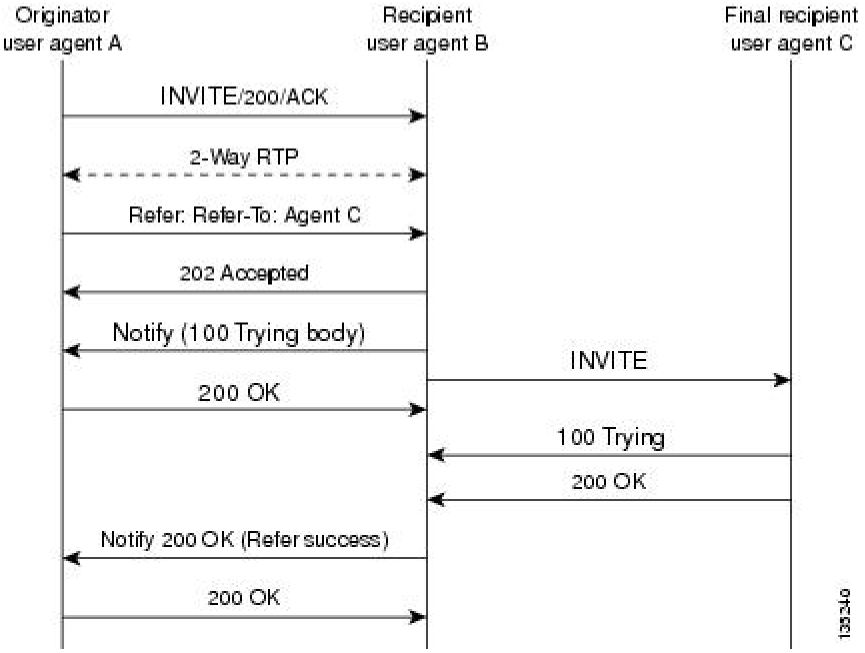
- Originator--User agent that initiates the transfer or Refer request.
- Recipient--User agent that receives the Refer request and is transferred to the final-recipient.
- Final-Recipient--User agent introduced into a call with the recipient.

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 2 ***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

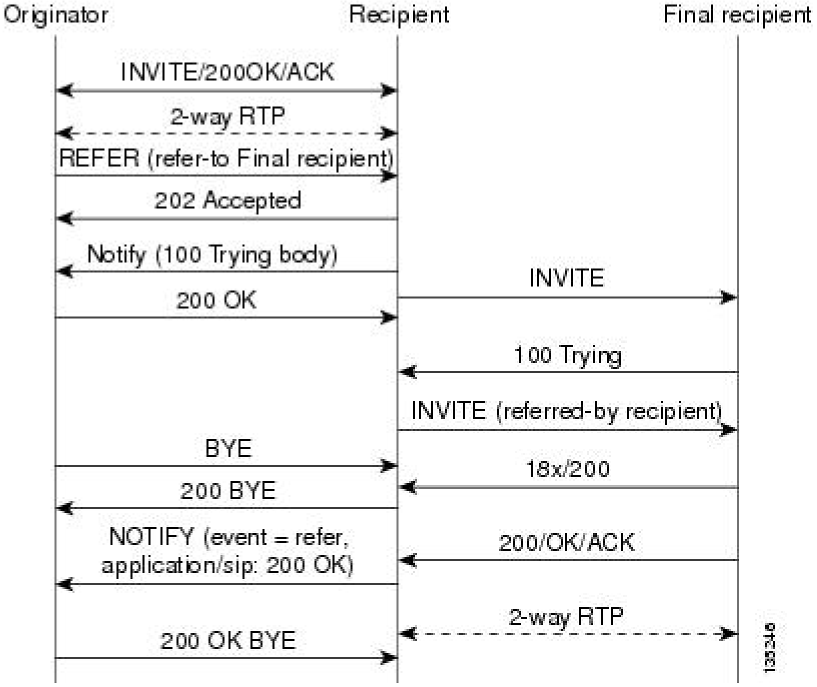
A blind, or unattended, transfer is one in which the transferring phone connects the caller to a destination line before ringback begins. This is different from a consultative, or attended, transfer in which one of the transferring parties either connects the caller to a ringing phone (ringback heard) 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 142. 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).

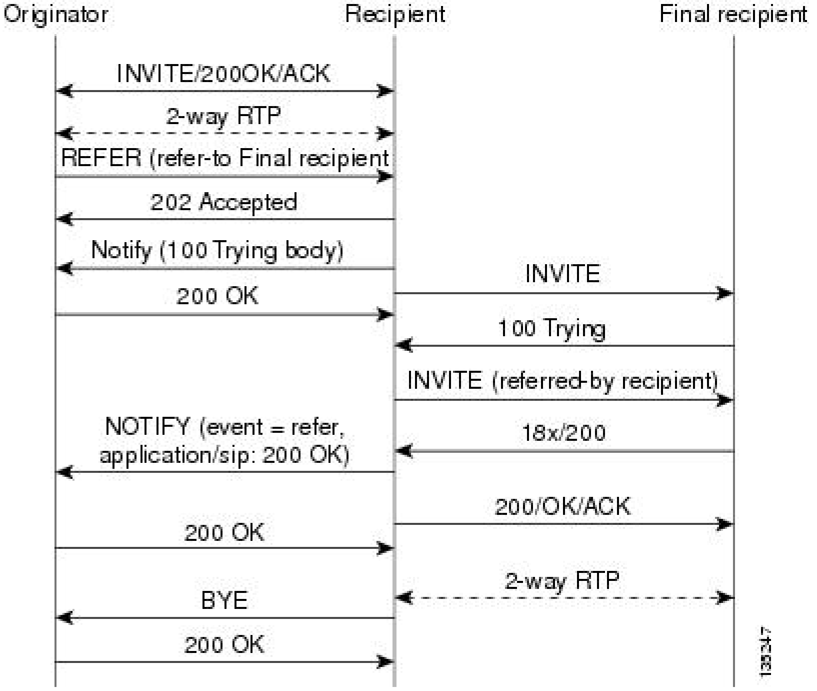
The figure below shows a successful blind or unattended call transfer in which the originator initiates a Bye request to terminate signaling with the recipient.

Figure 3 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 4 Successful Blind or Unattended Transfer--Recipient Initiating a Bye Request

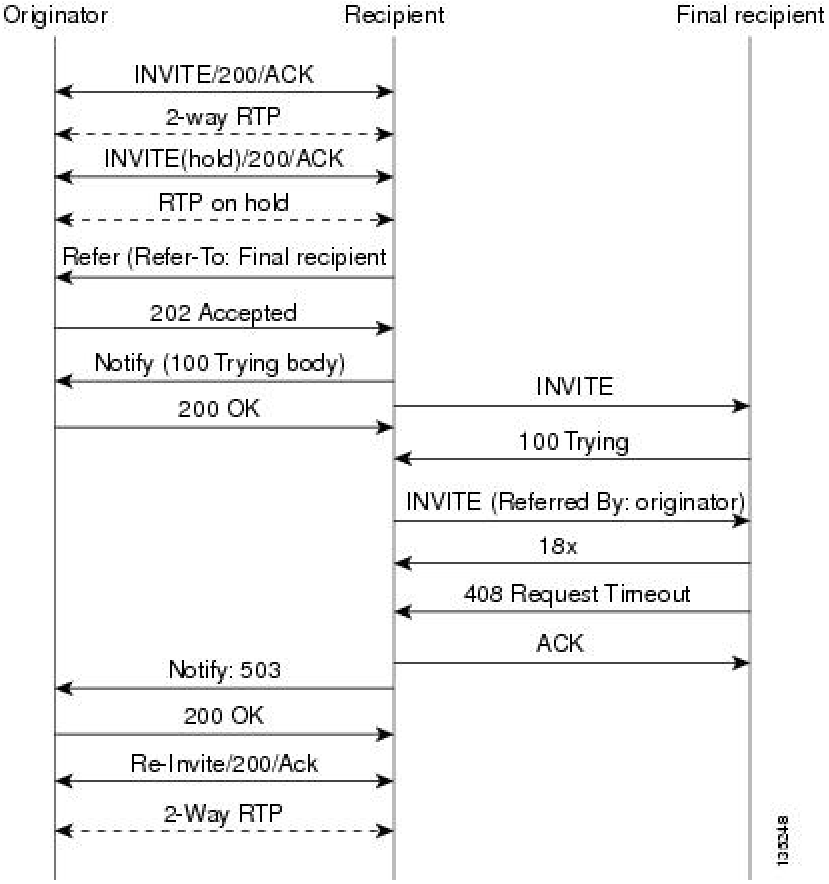


If a failure occurs with the triggered INVITE to the final recipient, the call between originator and recipient is not disconnected. Rather, with blind transfer the process is as follows:

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 5 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

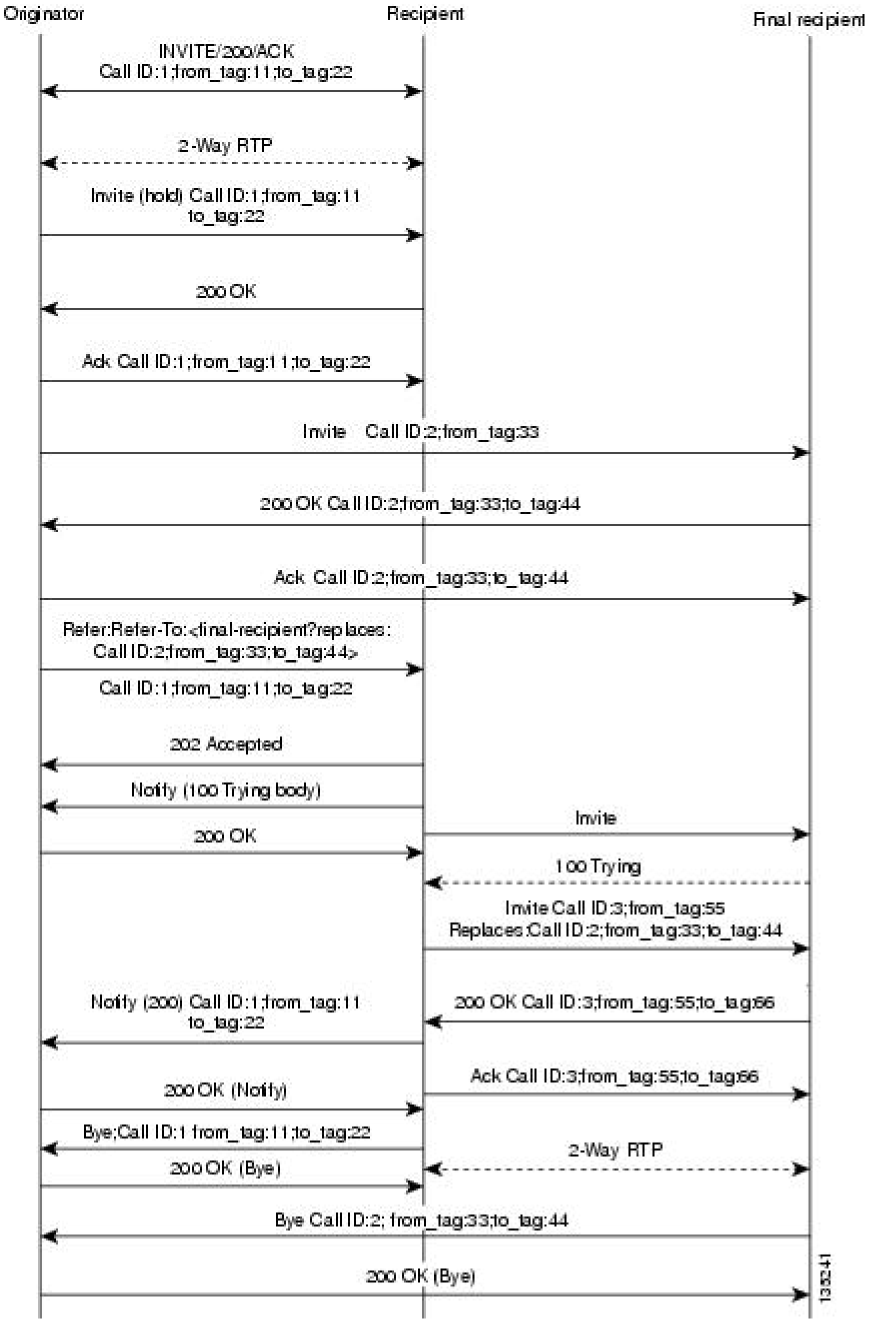
The Replaces header is required in attended transfers. It indicates to the final recipient that the initial call leg (identified by the Call-ID header and tags) is to be shut down and replaced by the incoming INVITE request. The final recipient sends a Bye request to the originator to terminate its session.

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 6 ***Successful Attended Transfer***


Originator
Recipient
Final recipient
INVITE/200/ACK
Call ID:1;from_tag:11;to_tag:22
2-Way RTP
Invite (hold) Call ID:1;from_tag:11
to_tag:22
200 OK
Ack Call ID:1;from_tag:11;to_tag:22
Invite Call ID:2;from_tag:33
200 OK Call ID:2;from_tag:33;to_tag:44
Ack Call ID:2;from_tag:33;to_tag:44
Refer:Refer-To:<final-recipient?replaces:
Call ID:2;from_tag:33;to_tag:44>
Call ID:1;from_tag:11;to_tag:22
202 Accepted
Notify (100 Trying body)
Invite
200 OK
100 Trying
Invite Call ID:3;from_tag:55
Replaces:Call ID:2;from_tag:33;to_tag:44
Notify (200) Call ID:1;from_tag:11
to_tag:22
200 OK Call ID:3;from_tag:55;to_tag:66
Ack Call ID:3;from_tag:55;to_tag:66
200 OK (Notify)
Bye;Call ID:1 from_tag:11;to_tag:22
2-Way RTP
200 OK (Bye)
Bye Call ID:2; from_tag:33;to_tag:44
200 OK (Bye)
135241

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):

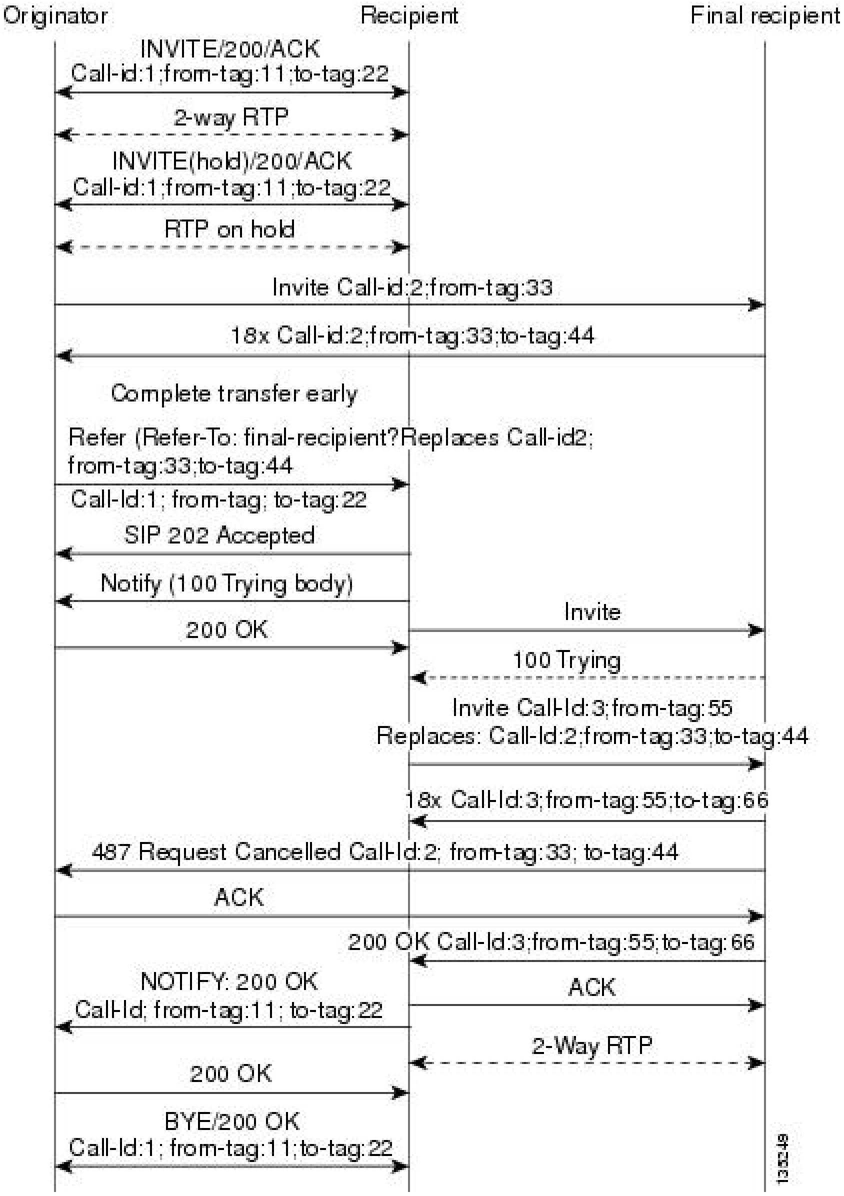
1. Originator does the following:
   - **a** Sets up a call with recipient.
   - **b** Places the recipient on hold.
   - **c** Contacts the final recipient.
   - **d** After receiving an indication that the final recipient is ringing, sends recipient a Refer message request with an overloaded Replaces 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 7 Attended Transfer with Early Completion


Originator
Recipient
Final recipient
INVITE/200/ACK
Call-id:1;from-tag:11;to-tag:22
2-way RTP
INVITE(hold)/200/ACK
Call-id:1;from-tag:11;to-tag:22
RTP on hold
Invite Call-id:2;from-tag:33
18x Call-id:2;from-tag:33;to-tag:44
Complete transfer early
Refer (Refer-To: final-recipient?Replaces Call-id2;
from-tag:33;to-tag:44
Call-Id:1; from-tag; to-tag:22
SIP 202 Accepted
Notify (100 Trying body)
Invite
200 OK
100 Trying
Invite Call-Id:3;from-tag:55
Replaces: Call-Id:2;from-tag:33;to-tag:44
18x Call-Id:3;from-tag:55;to-tag:66
487 Request Cancelled Call-Id:2; from-tag:33; to-tag:44
ACK
200 OK Call-Id:3;from-tag:55;to-tag:66
NOTIFY: 200 OK
Call-Id; from-tag:11; to-tag:22
ACK
2-Way RTP
200 OK
BYE/200 OK
Call-Id:1; from-tag:11;to-tag:22
135249

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.

Table 17 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 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**

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.

Interworking of Secure RTP calls for SIP and H.323

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

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

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

Finding Feature Information

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

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 Interworking of Secure RTP calls for SIP and H.323

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

- Establish a working IP network and configure VoIP.

Note For information about configuring VoIP, see Enhancements to the Session Initiation Protocol for VoIP on Cisco Access Platforms at the following URL: http://www.cisco.com/en/US/docs/ios/12_2t/12_2t11/feature/guide/ftsipgv1.html

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

Cisco Unified Border Element

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

Cisco Unified Border Element (Enterprise)

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

Restrictions for Interworking of Secure RTP calls for SIP and H.323

- The SIP gateway does not support codecs other than those listed in the table titled "SIP Codec Support by Platform and Cisco IOS Release" in the "Enhanced Codec Support for SIP Using Dynamic Payloads" section of the Configuring SIP QoS Features module at the following URL: http://www.cisco.com/en/US/docs/ios/voice/sip/configuration/guide/sip_cg-qos.html
- SIP requires that all times be sent in GMT.

Feature Information for Configuring Interworking of Secure RTP Calls 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.

Table 18 Feature Information for Configuring Support for Expires Timer Reset on Receiving or Sending SIP 183 Message

Feature Name	Releases	Feature Information
Interworking of Secure RTP calls for SIP and H.323	12.4(20)T	This feature provides an option for a Secure RTP (SRTP) call to be connected from H.323 to SIP and from SIP to SIP. Additionally, this feature extends SRTP fallback support from the Cisco IOS voice gateway to the Cisco Unified Border Element. This feature uses no new or modified commands.
Interworking of Secure RTP calls for SIP and H.323	Cisco IOS XE Release 3.1S	This feature provides an option for a Secure RTP (SRTP) call to be connected from H.323 to SIP and from SIP to SIP. Additionally, this feature extends SRTP fallback support from the Cisco IOS voice gateway to the Cisco Unified Border Element. This feature uses no new or modified commands.

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.

Cisco UBE Support for SRTP-RTP Internetworking

The Cisco Unified Border Element Support for SRTP-RTP Internetworking feature allows secure enterprise-to-enterprise calls and provides operational enhancements for Session Initiation Protocol (SIP) trunks from Cisco Unified Call Manager and Cisco Unified Call Manager Express. Support for Secure Real-Time Transport Protocol (SRTP)-Real-Time Transport Protocol (RTP) internetworking between one or multiple Cisco Unified Border Elements (Cisco UBEs) is enabled for SIP-SIP audio calls.

In Cisco IOS Release 15.2(1) and Cisco IOS XE Release 3.7S, the SRTP-RTP Interworking feature was extended to support supplementary services on Cisco UBEs.

Prerequisites for CUBE Support for SRTP-RTP Internetworking

- The Cisco Unified Border Element Support for SRTP-RTP Internetworking feature is supported in Cisco Unified CallManager 7.0 and later releases.

Cisco Unified Border Element

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

Cisco Unified Border Element (Enterprise)

- Cisco IOS XE Release 3.7S or a later release must be installed and running on your Cisco ASR 1000 Series Router.

Restrictions for CUBE Support for SRTP-RTP Internetworking

The following features are not supported by the Cisco Unified Border Element Support for SRTP-RTP Internetworking feature:

- Asymmetric SRTP fallback configurations
- Call admission control (CAC) support
- Rotary SIP-SIP
- SRTCP-RTCP interworking
- SRTP-RTP and SRTP-SRTP video calls
- Transcoding for SRTP-SRTP audio calls

Information About CUBE for SRTP-RTP Internetworking

To configure support for SRTP-RTP internetworking, you should understand the following concepts:

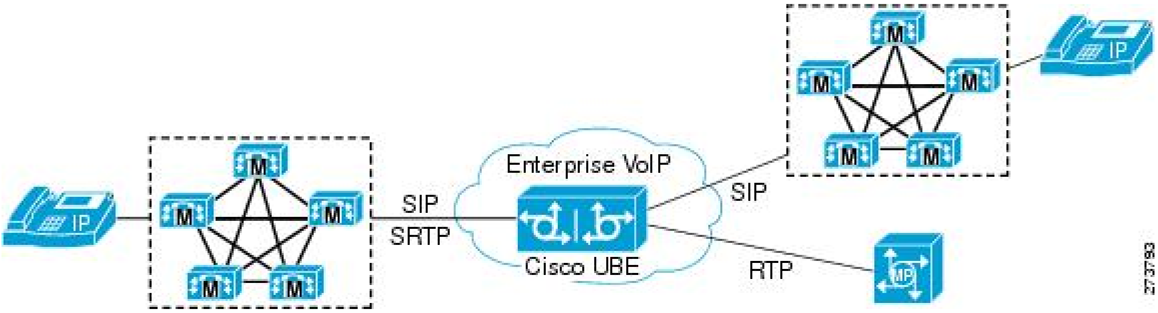
- CUBE Support for SRTP-RTP Internetworking, page 158
- TLS on the Cisco Unified Border Element, page 159
- Supplementary Services Support on the Cisco UBE for RTP-SRTP Calls, page 160

CUBE Support for SRTP-RTP Internetworking

The Cisco Unified Border Element Support for SRTP-RTP Internetworking feature connects SRTP Cisco Unified CallManager domains with the following:

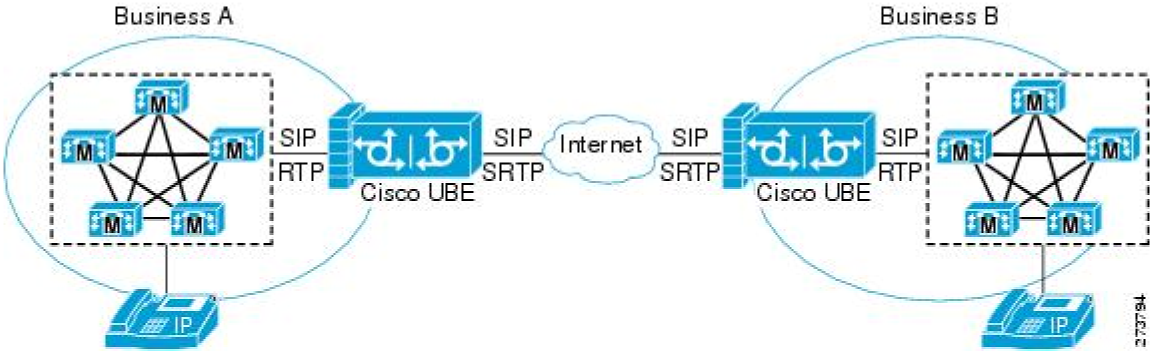
- RTP Cisco Unified CallManager domains. Domains that do not support SRTP or have not been configured for SRTP, as shown in the figure below.
- RTP Cisco applications or servers. For example, Cisco Unified MeetingPlace, Cisco WebEx, or Cisco Unity, which do not support SRTP, or have not been configured for SRTP, or are resident in a secure data center, as shown in the figure below.
- RTP to third-party equipment. For example, IP trunks to PBXs or virtual machines, which do not support SRTP.

Figure 8 SRTP Domain Connections



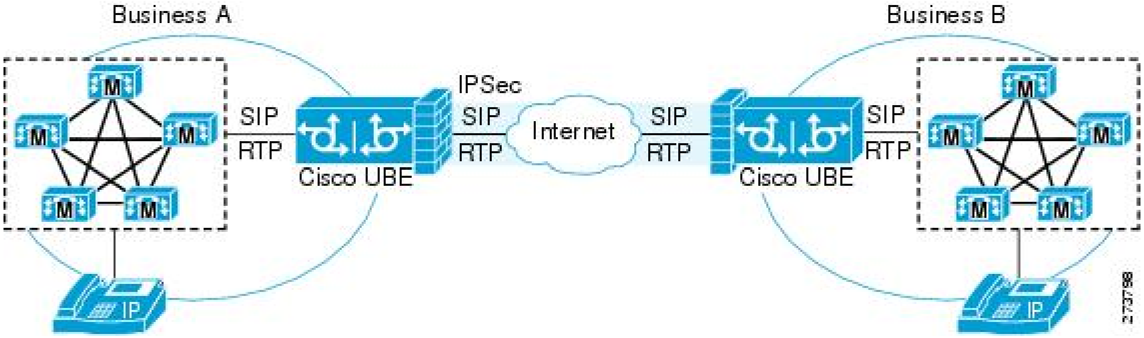
The Cisco Unified Border Element Support for SRTP-RTP Internetworking feature connects SRTP enterprise domains to RTP SIP provider SIP trunks. SRTP-RTP internetworking connects RTP enterprise networks with SRTP over an external network between businesses. This provides flexible secure business-to-business communications without the need for static IPsec tunnels or the need to deploy SRTP within the enterprise, as shown in the figure below.

Figure 9 Secure Business-to-Business Communications



SRTP-RTP internetworking also connects SRTP enterprise networks with static IPsec over external networks, as shown inthe figure below.

Figure 10 SRTP Enterprise Network Connections



SRTP-RTP internetworking on the Cisco UBE in a network topology uses single-pair key generation. Existing audio and dual-tone multifrequency (DTMF) transcoding is used to support voice calls. SRTP-RTP internetworking support is provided in both flow-through and high-density mode. SRTP-SRTP pass-through is not impacted.

SRTP is configured on one dial peer and RTP is configured on the other dial peer using the **srtp** and **srtp fallback** commands. The dial-peer configuration takes precedence over the global configuration on the Cisco UBE.

Fallback handling occurs if one of the call endpoints does not support SRTP. The call can fall back to RTP-RTP, or the call can fail, depending on the configuration. Fallback takes place only if the **srtp fallback** command is configured on the respective dial peer. RTP-RTP fallback occurs when no transcoding resources are available for SRTP-RTP internetworking.

TLS on the Cisco Unified Border Element

The Cisco Unified Border Element Support for SRTP-RTP Internetworking feature allows Transport Layer Security (TLS) to be enabled or disabled between the Skinny Call Control Protocol (SCCP) server and the

SCCP client. By default, TLS is enabled, which provides added protection at the transport level and ensures that SRTP keys are not easily accessible. Once TLS is disabled, the SRTP keys are not protected.

SRTP-RTP internetworking is available with normal and universal transcoders. The transcoder on the Cisco Unified Border Element is invoked using SCCP messaging between the SCCP server and the SCCP client. SCCP messages carry the SRTP keys to the digital signal processor (DSP) farm at the SCCP client. The transcoder can be within the same router or can be located in a separate router. TLS should be disabled only when the transcoder is located in the same router. To disable TLS, configure the **no** form of the **tls** command in dsp farm profile configuration mode. Disabling TLS improves CPU performance.

Supplementary Services Support on the Cisco UBE for RTP-SRTP Calls

The Supplementary Services Support on Cisco UBE for RTP-SRTP Calls feature supports the following supplementary services on the Cisco UBE:

- Midcall codec change with voice class codec configuration for SRTP-RTP and SRTP pass-through calls.
- Reinvite-based call hold.
- Reinvite-based call resume.
- Music on hold (MoH) invoked from the Cisco Unified Communications Manager (Cisco UCM), where the call leg changes between SRTP and RTP for an MoH source.

  Reinvite-based call forward.
- Reinvite-based call transfer.
- Call transfer based on a REFER message, with local consumption or pass-through of the REFER message on the Cisco UBE.
- Call forward based on a 302 message, with local consumption or pass-through of the 302 message on the Cisco UBE.
- T.38 fax switchover.
- Fax pass-through switchover.
- DO-EO for SRTP-RTP calls.
- DO-EO for SRTP pass-through calls.

When the initial SRTP-RTP or SRTP pass-through call is established on the Cisco UBE, a call can switch between SRTP and RTP for various supplementary services that can be invoked on the end points. Transcoder resources are used to perform SRTP-RTP conversion on Cisco UBE. When the call switches between SRTP and RTP, the transcoder is dynamically inserted, deleted, or modified. Both normal transcoding and high-density (optimized) transcoding are supported.

For call transfers involving REFER and 302 messages (messages that are locally consumed on Cisco UBE), end-to-end media renegotiation is initiated from Cisco UBE only when you configure the supplementary-service media-renegotiate command in voice service voip configuration mode.

When supplementary services are invoked from the end points, the call can switch between SRTP and RTP during the call duration. Hence, Cisco recommends that you configure such SIP trunks for SRTP fallback.

How to Configure Cisco UBE Support for SRTP-RTP Internetworking

Configuring Cisco UBE Support for SRTP-RTP Internetworking

Configuring the Certificate Authority

Perform the steps described in this section to configure the certificate authority.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip http server**
4. **crypto pki server** *cs-label*
5. **database level complete**
6. **grant auto**
7. **no shutdown**
8. **exit**

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**ip http server** **Example:** `Device(config)# ip http server`	Enables the HTTP server on your IPv4 or IPv6 system, including the Cisco web browser user interface.
Step 4	**crypto pki server** *cs-label* **Example:** `Device(config)# crypto pki server 3854-cube`	Enables a Cisco IOS certificate server and enters certificate server configuration mode. • In the example, 3854-cube is specified as the name of the certificate server.
Step 5	**database level complete** **Example:** `Device(cs-server)# database level complete`	Controls what type of data is stored in the certificate enrollment database. • In the example, each issued certificate is written to the database.
Step 6	**grant auto** **Example:** `Device(cs-server)# grant auto`	Specifies automatic certificate enrollment.
Step 7	**no shutdown** **Example:** `Device(cs-server)# no shutdown`	Reenables the certificate server. • Create and enter a new password when prompted.
Step 8	**exit** **Example:** `Device(cs-server)# exit`	Exits certificate server configuration mode.

Configuring a Trustpoint for the Secure Universal Transcoder

Perform the task in this section to configure, authenticate, and enroll a trustpoint for the secure universal transcoder.

Before you configure a trustpoint for the secure universal transcoder, you should configure the certificate authority, as described in the Configuring the Certificate Authority, page 161.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** *name*
4. **enrollment url** *url*
5. **serial-number**
6. **revocation-check** *method*
7. **rsakeypair** *key-label*
8. **end**
9. **crypto pki authenticate** *name*
10. **crypto pki enroll** *name*
11. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**crypto pki trustpoint** *name* **Example:** `Device(config)# crypto pki trustpoint secdsp`	Declares the trustpoint that the router uses and enters ca-trustpoint configuration mode. • In the example, the trustpoint is named secdsp.
Step 4	**enrollment url** *url* **Example:** `Device(ca-trustpoint)# enrollment url http://10.13.2.52:80`	Specifies the enrollment parameters of a certification authority (CA). • In the example, the URL is defined as http://10.13.2.52:80.

	Command or Action	Purpose
Step 5	**serial-number** **Example:** `Device(ca-trustpoint)# serial-number`	Specifies whether the router serial number should be included in the certificate request.
Step 6	**revocation-check** *method* **Example:** `Device(ca-trustpoint)# revocation-check crl`	Checks the revocation status of a certificate. • In the example, the certificate revocation list checks the revocation status.
Step 7	**rsakeypair** *key-label* **Example:** `Device(ca-trustpoint)# rsakeypair 3845-cube`	Specifies which key pair to associate with the certificate. • In the example, the key pair 3845-cube generated during enrollment is associated with the certificate.

Step 8	**end**
	Example:
	`Device(ca-trustpoint)# end`
		Exits ca-trustpoint configuration mode.

Step 9	**crypto pki authenticate** *name* **Example:** `Device(config)# crypto pki authenticate secdsp`	Authenticates the CA. • Accept the trustpoint CA certificate if prompted.
Step 10	**crypto pki enroll** *name* **Example:** `Device(config)# crypto pki enroll secdsp`	Obtains the certificate for the router from the CA. • Create and enter a new password if prompted. • Request a certificate from the CA if prompted.
Step 11	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode.

Configuring DSP Farm Services

Perform the task in this section to configure DSP farm services.

Before you configure DSP farm services, you should configure the trustpoint for the secure universal transcoder, as described in the Configuring a Trustpoint for the Secure Universal Transcoder, page 162.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice-card** *slot*
4. **dspfarm**
5. **dsp services dspfarm**
6. Repeat Steps 3, 4, and 5 to configure a second voice card.
7. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**voice-card** *slot* **Example:** `Device(config)# voice-card 0`	Configures a voice card and enters voice-card configuration mode. • In the example, voice card 0 is configured.
Step 4	**dspfarm** **Example:** `Device(config-voicecard)# dspfarm`	Adds a specified voice card to those participating in a DSP resource pool.
Step 5	**dsp services dspfarm** **Example:** `Device(config-voicecard)# dsp services dspfarm`	Enables DSP farm services for a particular voice network module.
Step 6	Repeat Steps 3, 4, and 5 to configure a second voice card.	--

	Command or Action	Purpose
Step 7	**exit** **Example:** `Device(config-voicecard)# exit`	Exits voice-card configuration mode.

Associating SCCP to the Secure DSP Farm Profile

Perform the task in this section to associate SCCP to the secure DSP farm profile.

Before you associate SCCP to the secure DSP farm profile, you should configure DSP farm services, as described in the Configuring DSP Farm Services, page 164.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **sccp local** *interface-type interface-number*
4. **sccp ccm** *ip-address* **identifier** *identifier-number* **version** *version-number*
5. **sccp**
6. **associate ccm** *identifier-number* **priority** *priority-number*
7. **associate profile** *profile-identifier* **register** *device-name*
8. **dspfarm profile** *profile-identifier* **transcode universal security**
9. **trustpoint** *trustpoint-label*
10. **codec** *codec-type*
11. Repeat Step 10 to configure reuired codecs.
12. **maximum sessions** *number*
13. **associate application sccp**
14. **no shutdown**
15. **exit**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**sccp local** *interface-type interface-number* **Example:** `Device(config)# sccp local GigabitEthernet 0/0`	Selects the local interface that SCCP applications (transcoding and conferencing) use to register with Cisco CallManager. • In the example, the following parameters are set: ◦ GigabitEthernet is defined as the interface type that the SCCP application uses to register with Cisco CallManager. ◦ The interface number that the SCCP application uses to register with Cisco CallManager is specified as 0/0.
Step 4	**sccp ccm** *ip-address* **identifier** *identifier-number* **version** *version-number* **Example:** `Device(config)# sccp ccm 10.13.2.52 identifier 1 version 5.0.1`	Adds a Cisco Unified Communications Manager server to the list of available servers. • In the example, the following parameters are set: ◦ 10.13.2.52 is configured as the IP address of the Cisco Unified Communications Manager server. ◦ The number 1 identifies the Cisco Unified Communications Manager server. ◦ The Cisco Unified Communications Manager version is identified as 5.0.1.
Step 5	**sccp** **Example:** `Device(config)# sccp`	Enables SCCP and related applications (transcoding and conferencing) and enters SCCP Cisco CallManager configuration mode.
Step 6	**associate ccm** *identifier-number* **priority** *priority-number* **Example:** `Device(config-sccp-ccm)# associate ccm 1 priority 1`	Associates a Cisco Unified CallManager with a Cisco CallManager group and establishes its priority within the group. • In the example, the following parameters are set: ◦ The number 1 identifies the Cisco Unified CallManager. ◦ The Cisco Unified CallManager is configured with the highest priority within the Cisco CallManager group.

	Command or Action	Purpose
Step 7	**associate profile** *profile-identifier* **register** *device-name* **Example:** `Device(config-sccp-ccm)# associate profile 1 register sxcoder`	Associates a DSP farm profile with a Cisco CallManager group. • In the example, the following parameters are set: ◦ The number 1 identifies the DSP farm profile. ◦ Sxcoder is configured as the user-specified device name in Cisco Unified CallManager.
Step 8	**dspfarm profile** *profile-identifier* **transcode universal security** **Example:** `Device(config-sccp-ccm)# dspfarm profile 1 transcode universal security`	Defines a profile for DSP farm services and enters DSP farm profile configuration mode. • In the example, the following parameters are set: ◦ Profile 1 is enabled for transcoding. ◦ Profile 1 is enabled for secure DSP farm services.
Step 9	**trustpoint** *trustpoint-label* **Example:** `Device(config-dspfarm-profile)# trustpoint secdsp`	Associates a trustpoint with a DSP farm profile. • In the example, the trustpoint to be associated with the DSP farm profile is labeled secdsp.
Step 10	**codec** *codec-type* **Example:** `Device(config-dspfarm-profile)# codec g711ulaw`	Specifies the codecs that are supported by a DSP farm profile. • In the example, the g711ulaw codec is specified.
Step 11	Repeat Step 10 to configure reuired codecs.	--
Step 12	**maximum sessions** *number* **Example:** `Device(config-dspfarm-profile)# maximum sessions 84`	Specifies the maximum number of sessions that are supported by the profile. • In the example, a maximum of 84 sessions are supported by the profile. The maximum number of sessions depends on the number of DSPs available for transcoding.
Step 13	**associate application sccp** **Example:** `Device(config-dspfarm-profile)# associate application sccp`	Associates SCCP to the DSP farm profile.

	Command or Action	Purpose
Step 14	**no shutdown** **Example:** `Device(config-dspfarm-profile)# no shutdown`	Allocates DSP farm resources and associates them with the application.
Step 15	**exit** **Example:** `Device(config-dspfarm-profile)# exit`	Exits DSP farm profile configuration mode.

Registering the Secure Universal Transcoder to the CUBE

Perform the task in this section to register the secure universal transcoder to the Cisco Unified Border Element. The Cisco Unified Border Element Support for SRTP-RTP Internetworking feature supports both secure transcoders and secure universal transcoders.

Before you register the secure universal transcoder to the Cisco Unified Border Element, you should associated SCCP to the secure DSP farm profile, as described in the Associating SCCP to the Secure DSP Farm Profile, page 166.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **sdspfarm transcode sessions** *number*
5. **sdspfarm tag** *number device-name*
6. **em logout** *time1 time2 time3*
7. **max-ephones** *max-ephones*
8. **max-dn** *max-directory-numbers*
9. **ip source-address** *ip-address*
10. **secure-signaling trustpoint** *label*
11. **tftp-server-credentials trustpoint** *label*
12. **create cnf-files**
13. **no sccp**
14. **sccp**
15. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. - Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device> configure terminal`	Enters global configuration mode.
Step 3	**telephony-service** **Example:** `Device(config)# telephony-service`	Enters telephony-service configuration mode.
Step 4	**sdspfarm transcode sessions** *number* **Example:** `Device(config-telephony)# sdspfarm transcode sessions 84`	Specifies the maximum number of transcoding sessions allowed per Cisco CallManager Express router. - In the example, a maximum of 84 DSP farm sessions are specified.
Step 5	**sdspfarm tag** *number device-name* **Example:** `Device(config-telephony)# sdspfarm tag 1 sxcoder`	Permits a DSP farm to be to registered to Cisco Unified CallManager Express and associates it with an SCCP client interface's MAC address. - In the example, DSP farm 1 is associated with the sxcoder device.
Step 6	**em logout** *time1 time2 time3* **Example:** `Device(config-telephony)# em logout 0:0 0:0 0:0`	Configures three time-of-day-based timers for automatically logging out all Extension Mobility feature users. - In the example, all users are logged out from Extension Mobility after 00:00.
Step 7	**max-ephones** *max-ephones* **Example:** `Device(config-telephony)# max-ephones 4`	Sets the maximum number of Cisco IP phones to be supported by a Cisco CallManager Express router. - In the example, a maximum of four phones are supported by the Cisco CallManager Express router.

	Command or Action	Purpose
Step 8	**max-dn** *max-directory-numbers* **Example:** `Device(config-telephony)# max-dn 4`	Sets the maximum number of extensions (ephone-dns) to be supported by a Cisco Unified CallManager Express router. • In the example, a maximum of four extensions is allowed.
Step 9	**ip source-address** *ip-address* **Example:** `Device(config-telephony)# ip source-address 10.13.2.52`	Identifies the IP address and port through which IP phones communicate with a Cisco Unified CallManager Express router. • In the example, 10.13.2.52 is configured as the router IP address.
Step 10	**secure-signaling trustpoint** *label* **Example:** `Device(config-telephony)# secure-signaling trustpoint secdsp`	Specifies the name of the Public Key Infrastructure (PKI) trustpoint with the certificate to be used for TLS handshakes with IP phones on TCP port 2443. • In the example, PKI trustpoint secdsp is configured.
Step 11	**tftp-server-credentials trustpoint** *label* **Example:** `Device(config-telephony)# tftp-server-credentials trustpoint scme`	Specifies the PKI trustpoint that signs the phone configuration files. • In the example, PKI trustpoint scme is configured.
Step 12	**create cnf-files** **Example:** `Device(config-telephony)# create cnf-files`	Builds the XML configuration files that are required for IP phones in Cisco Unified CallManager Express.
Step 13	**no sccp** **Example:** `Device(config-telephony)# no sccp`	Disables SCCP and its related applications (transcoding and conferencing) and exits telephony-service configuration mode.
Step 14	**sccp** **Example:** `Device(config)# sccp`	Enables SCCP and related applications (transcoding and conferencing).

	Command or Action	Purpose

Step 15	**end**
	Example:
	`Device(config)# end`
		Exits global configuration mode.

Configuring SRTP-RTP Internetworking Support

Perform the task in this section to enable SRTP-RTP internetworking support between one or multiple Cisco Unified Border Elements for SIP-SIP audio calls. In this task, RTP is configured on the incoming call leg and SRTP is configured on the outgoing call leg.

Before you configure the Cisco Unified Border Element Support for SRTP-RTP Internetworking feature, you should register the secure universal transcoder to the Cisco Unified Border Element, as described in the Registering the Secure Universal Transcoder to the CUBE, page 169.

Note The Cisco Unified Border Element Support for SRTP-RTP Internetworking feature is available only on platforms that support transcoding on the Cisco Unified Border Element. The feature is also available only on secure Cisco IOS images on the Cisco Unified Border Element.

>

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *tag* **voip**
4. **destination-pattern** *string*
5. **session protocol sipv2**
6. **session target ipv4:** *destination-address*
7. **incoming called-number** *string*
8. **codec** *codec*
9. **end**
10. **dial-peer voice** *tag* **voip**
11. Repeat Steps 4, 5, 6, and 7 to configure a second dial peer.
12. **srtp**
13. **codec** *codec*
14. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**dial-peer voice** *tag* **voip** **Example:** `Device(config)# dial-peer voice 201 voip`	Defines a particular dial peer, to specify the method of voice encapsulation, and enters dial peer voice configuration mode. • In the example, the following parameters are set: ◦ Dial peer 201 is defined. ◦ VoIP is shown as the method of encapsulation.
Step 4	**destination-pattern** *string* **Example:** `Device(config-dial-peer)# destination-pattern 5550111`	Specifies either the prefix or the full E.164 telephone number to be used for a dial peer string. • In the example, 5550111 is specified as the pattern for the telephone number.
Step 5	**session protocol sipv2** **Example:** `Device(config-dial-peer)# session protocol sipv2`	Specifies a session protocol for calls between local and remote routers using the packet network. • In the example, the **sipv2** keyword is configured so that the dial peer uses the IEFTF SIP.
Step 6	**session target ipv4:** *destination-address* **Example:** `Device(config-dial-peer)# session target ipv4:10.13.25.102`	Designates a network-specific address to receive calls from a VoIP or VoIPv6 dial peer. • In the example, the IP address of the dial peer to receive calls is configured as 10.13.25.102.

	Command or Action	Purpose
Step 7	**incoming called-number** *string* **Example:** `Device(config-dial-peer)# incoming called-number 5550111`	Specifies a digit string that can be matched by an incoming call to associate the call with a dial peer. • In the example, 5550111 is specified as the pattern for the E.164 or private dialing plan telephone number.
Step 8	**codec** *codec* **Example:** `Device(config-dial-peer)# codec g711ulaw`	Specifies the voice coder rate of speech for the dial peer. • In the example, G.711 mu-law at 64,000 bps, is specified as the voice coder rate for speech.

Step 9	**end**
	Example:
	`Device(config-dial-peer)#end`
		Exits dial peer voice configuration mode.

Step 10	**dial-peer voice** *tag* **voip** **Example:** `Device(config)# dial-peer voice 200 voip`	Defines a particular dial peer, to specify the method of voice encapsulation, and enters dial peer voice configuration mode. • In the example, the following parameters are set: ◦ Dial peer 200 is defined. ◦ VoIP is shown as the method of encapsulation.
Step 11	Repeat Steps 4, 5, 6, and 7 to configure a second dial peer.	--
Step 12	**srtp** **Example:** `Device(config-dial-peer)# srtp`	Specifies that SRTP is used to enable secure calls for the dial peer.
Step 13	**codec** *codec* **Example:** `Device(config-dial-peer)# codec g711ulaw`	Specifies the voice coder rate of speech for the dial peer. • In the example, G.711 mu-law at 64,000 bps, is specified as the voice coder rate for speech.

	Command or Action	Purpose
Step 14	**exit** **Example:** `Device(config-dial-peer)# exit`	Exits dial peer voice configuration mode.

- Troubleshooting Tips, page 175

Troubleshooting Tips

The following commands can help troubleshoot Cisco Unified Border Element support for SRTP-RTP internetworking:

- **show crypto pki certificates**
- **show sccp**
- **show sdspfarm**

Enabling SRTP on the Cisco UBE

You can configure SRTP with the fallback option so that a call can fall back to RTP if SRTP is not supported by the other call end. Enabling SRTP is required for supporting nonsecure supplementary services such as MoH, call forward, and call transfer.

- Enabling SRTP Globally, page 175
- Enabling SRTP on a Dial Peer, page 176
- Troubleshooting Tips, page 178

Enabling SRTP Globally

Perform this task to enable SRTP globally.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **srtp fallback**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**voice service voip** **Example:** `Device(config)# voice service voip`	Enters voice-service configuration mode and specifies VoIP encapsulation as the voice-encapsulation type.
Step 4	**srtp fallback** **Example:** `RoDeviceuter(conf-voi-serv)# srtp fallback`	Enables call fallback to nonsecure mode. **Note** If the secure SIP trunk is towards the Cisco UCM, you must configure the **srtp negotiate cisco** command in voice-service configuration mode for a non-Cisco fallback to work.
Step 5	**exit** **Example:** `Device(conf-voi-serv)# exit`	Exits voice service configuration mode.

Example: Enabling SRTP Globally

```
Device(config)# voice service voip
Device(conf-voi-serv)# srtp fallback
Device(conf-voi-serv)# exit
```

Enabling SRTP on a Dial Peer

Perform this task to enable SRTP on a dial peer.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *tag* **voip**
4. **srtp fallback**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. - Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**dial-peer voice** *tag* **voip** **Example:** `Device(config)# dial-peer voice 10 voip`	Defines a particular dial peer to specify VoIP as the method of voice encapsulation and enters dial peer voice configuration mode.
Step 4	**srtp fallback** **Example:** `Device(config-dial-peer)# srtp fallback`	Enables specific dial-peer calls to fall back to nonsecure mode. **Note** If the secure SIP trunk is towards the Cisco UCM, you must configure the **srtp negotiate cisco** command in dial peer voice configuration mode for a non-Cisco fallback to work.
Step 5	**exit** **Example:** `Device(config-dial-peer)# exit`	Exits dial peer voice configuration mode.

Example: Enabling SRTP on a Dial Peer

```
Device(config)# dial-peer voice 10 voip
Device(config-dial-peer)# srtp fallback
Device(config-dial-peer)# exit
```

Troubleshooting Tips

The following commands can help troubleshoot SRTP-RTP supplementary services support on Cisco UBE:

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

Verifying SRTP-RTP Supplementary Services Support on the Cisco UBE

Perform this task to verify the configuration for SRTP-RTP supplementary services support on the Cisco UBE. The **show** commands need not be entered in any specific order.

SUMMARY STEPS

1. **enable**
2. **show call active voice brief**
3. **show sccp connection**
4. **show dspfarm dsp active**

DETAILED STEPS

Step 1 **enable**

Enables privileged EXEC mode.

Example:

```
Device> enable
```

Step 2 **show call active voice brief**

Displays call information for voice calls in progress.

Example:

```
Device# show call active voice brief
Telephony call-legs: 0
SIP call-legs: 2
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 2
ulticast call-legs: 0
Total call-legs: 4
0    : 1 12:49:45.256 IST Fri Jun 3 2011.1 +29060 pid:1 Answer 10008001 connected
 dur 00:01:19 tx:1653/271092 rx:2831/464284 dscp:0 media:0
 IP 10.45.40.40:7892 SRTP: on 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    : 2 12:49:45.256 IST Fri Jun 3 2011.2 +29060 pid:22 Originate 20009001 connected
 dur 00:01:19 tx:2831/452960 rx:1653/264480 dscp:0 media:0
 IP 10.45.40.40:7893 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    : 3 12:50:14.326 IST Fri Jun 3 2011.1 +0 pid:0 Originate  connecting
```

```
 dur 00:01:19 tx:2831/452960 rx:1653/264480 dscp:0 media:0
 IP 10.45.34.252:2000 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    : 5 12:50:14.326 IST Fri Jun 3 2011.2 +0 pid:0 Originate  connecting
 dur 00:01:19 tx:1653/271092 rx:2831/464284 dscp:0 media:0
 IP 10.45.34.252:2000 SRTP: on 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
```

Step 3 **show sccp connection**

Displays SCCP connection details.

Example:

```
Device# show sccp connection
sess_id    conn_id      stype mode     codec   sport rport ripaddr conn_id_tx

65537      4          s-xcode sendrecv g711u   17124 2000  10.45.34.252
65537      8            xcode sendrecv g711u   30052 2000  10.45.34.252

Total number of active session(s) 1, and connection(s) 2
```

Step 4 **show dspfarm dsp active**

Displays active DSP information about the DSP farm service.

Example:

```
Device# show dspfarm dsp active
SLOT DSP VERSION  STATUS CHNL USE   TYPE    RSC_ID BRIDGE_ID PKTS_TXED PKTS_RXED

0    1   30.0.209 UP     1    USED  xcode   1      4         2876      1706
0    1   30.0.209 UP     1    USED  xcode   1      5         1698      2876

Total number of DSPFARM DSP channel(s) 1
```

Configuration Examples for CUBE Support for SRTP-RTP Internetworking

- SRTP-RTP Internetworking Example, page 179

SRTP-RTP Internetworking Example

The following example shows how to configure Cisco Unified Border Element support for SRTP-RTP internetworking. In this example, the incoming call leg is RTP and the outgoing call leg is SRTP.

```
enable
 configure terminal
 ip http server
 crypto pki server 3845-cube
  database level complete
  grant auto
  no shutdown
%PKI-6-CS_GRANT_AUTO: All enrollment requests will be automatically granted.
% Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key or type Return to exit
Password:
Re-enter password:
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
% SSH-5-ENABLED: SSH 1.99 has been enabled
% Exporting Certificate Server signing certificate and keys...
% Certificate Server enabled.
%PKI-6-CS_ENABLED: Certificate server now enabled.
!
crypto pki trustpoint secdsp
 enrollment url http://10.13.2.52:80
 serial-number
 revocation-check crl
 rsakeypair 3845-cube
 exit
!
crypto pki authenticate secdsp
Certificate has the following attributes:
 Fingerprint MD5: CCC82E9E 4382CCFE ADA0EB8C 524E2FC1
 Fingerprint SHA1: 34B9C4BF 4841AB31 7B0810AD 80084475 3965F140
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
crypto pki enroll secdsp
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this password to the CA
Administrator in order to revoke your certificate. For security reasons your password
will not be saved in the configuration. Please make a note of it.
Password:
Re-enter password:
% The subject name in the certificate will include: 3845-CUBE
% The serial number in the certificate will be: FHK1212F4MU
% Include an IP address in the subject name? [no]:
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate secdsp verbose' command will show the fingerprint.
CRYPTO_PKI:  Certificate Request Fingerprint MD5: 56CE5FC3 B8411CF3 93A343DA 785C2360
CRYPTO_PKI:  Certificate Request Fingerprint SHA1: EE029629 55F5CA10 21E50F08 F56440A2
DDC7469D
%PKI-6-CERTRET: Certificate received from Certificate Authority
!
voice-card 0
 dspfarm
 dsp services dspfarm
 voice-card 1
 dspfarm
 dsp services dspfarm
 exit
!
sccp local GigabitEthernet 0/0
sccp ccm 10.13.2.52 identifier 1 version 5.0.1
sccp
SCCP operational state bring up is successful.sccp ccm group 1
 associate ccm 1 priority 1
 associate profile 1 register sxcoder
 dspfarm profile 1 transcode universal security
  trustpoint secdsp
  codec g711ulaw
  codec g711alaw
  codec g729ar8
  codec g729abr8
  codec g729r8
  codec ilbc
  codec g729br8
  maximum sessions 84
  associate application sccp
  no shutdown
  exit
!
telephony-service
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface EDSP0, changed state to upsdspfarm units 1
 sdspfarm transcode sessions 84
 sdspfarm tag 1 sxcoder
 em logout 0:0 0:0 0:0
 max-ephones 4
 max-dn 4
 ip source-address 10.13.2.52
Updating CNF files
CNF-FILES: Clock is not set or synchronized, retaining old versionStamps
CNF files updating complete
 secure-signaling trustpoint secdsp
 tftp-server-credentials trustpoint scme
CNF-FILES: Clock is not set or synchronized, retaining old versionStamps
CNF files update complete (post init)
 create cnf-files
CNF-FILES: Clock is not set or synchronized, retaining old versionStamps
 no sccp
!
sccp
SCCP operational state bring up is successful.
end
%SDSPFARM-6-REGISTER: mtp-1:sxcoder IP:10.13.2.52 Socket:1 DeviceType:MTP has registered.
%SYS-5-CONFIG_I: Configured from console by console
dial-peer voice 201 voip
 destination-pattern 5550111
 session protocol sipv2
 session target ipv4:10.13.25.102
 incoming called-number 5550112
 codec g711ulaw
!
dial-peer voice 200 voip
 destination-pattern 5550112
 session protocol sipv2
 session target ipv4:10.13.2.51
 incoming called-number 5550111
 srtp
 codec g711ulaw
```

Feature Information for CUBE Support for SRTP-RTP Internetworking

Table 19 Feature Information for Cisco Unified Border Element Support for SRTP-RTP Internetworking

Feature Name	Releases	Feature Information
Cisco Unified Border Element Support for SRTP-RTP Internetworking	12.4(22)YB , 15.0(1)M	This feature allows secure enterprise-to-enterprise calls. Support for SRTP-RTP internetworking between one or multiple Cisco Unified Border Elements is enabled for SIP-SIP audio calls. The following sections provide information about this feature: The following command was introduced: **tls**.

Feature Name	Releases	Feature Information
Supplementary Services Support on Cisco UBE for RTP-SRTP Calls	15.2(1)T	The SRTP-RTP Internetworking feature was enhanced to support supplementary services for SRTP-RTP calls on Cisco UBE.
Supplementary Services Support on Cisco UBE for RTP-SRTP Calls	Cisco IOS XE Release 3.7S	The SRTP-RTP Internetworking feature was enhanced to support supplementary services for SRTP-RTP calls on Cisco UBE.

SIP SRTP Fallback to Nonsecure RTP

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

Finding Feature Information

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

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 SRTP Fallback to Nonsecure RTP

Cisco Unified Border Element

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

Cisco Unified Border Element (Enterprise)

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

Configuring SIP SRTP Fallback to Nonsecure RTP

To enable this feature, see the "Configuring SIP Support for SRTP" section of the Cisco IOS SIP Configuration Guide, Release 15.1 at the following URL: http://www.cisco.com/en/US/docs/ios/voice/sip/configuration/guide/sip_cg-srtp_ps10592_TSD_Products_Configuration_Guide_Chapter.html

Detailed command information for the **srtp**, **srtp negotiate**, and **voice-class sip srtp negotiate**commands is located in the Cisco IOS Voice Command Reference http://www.cisco.com/en/US/docs/ios/voice/command/reference/vr_book.html

Feature Information for SIP SRTP Fallback to Nonsecure RTP

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

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

Table 20 Feature Information for SIP SRTP Fallback to Nonsecure RTP

Feature Name	Releases	Feature Information
SIP SRTP Fallback to Nonsecure RTP	12.4(22)T	The SIP SRTP Fallback to Nonsecure RTP feature enables a Cisco IOS Session Initiation Protocol (SIP) gateway to fall back from SRTP to RTP by accepting or sending an RTP/AVP(RTP) profile in response to an RTP/SAVP(SRTP) profile. This feature also allows inbound and outbound SRTP calls with nonsecure SIP signaling schemes (such as SIP URL) and provides the administrator the flexibility to configure TLS, IPsec, or any other security mechanism used in the lower layers for secure signaling of crypto attributes. The following commands were introduced or modified: **srtp (voice)**, **srtp negotiate**, and **voice-class sip srtp negotiate**

Feature Name	Releases	Feature Information
SIP SRTP Fallback to Nonsecure RTP	Cisco IOS XE Release 3.1S	The SIP SRTP Fallback to Nonsecure RTP feature enables a Cisco IOS Session Initiation Protocol (SIP) gateway to fall back from SRTP to RTP by accepting or sending an RTP/AVP(RTP) profile in response to an RTP/SAVP(SRTP) profile. This feature also allows inbound and outbound SRTP calls with nonsecure SIP signaling schemes (such as SIP URL) and provides the administrator the flexibility to configure TLS, IPsec, or any other security mechanism used in the lower layers for secure signaling of crypto attributes. The following commands were introduced or modified: **srtp (voice)**, **srtp negotiate**, and **voice-class sip srtp negotiate**

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.

VoIP for IPv6

This document describes VoIP in IPv6 (VoIPv6), a feature that adds IPv6 capability to existing VoIP features. This feature adds dual-stack (IPv4 and IPv6) support on voice gateways and media termination points (MTPs), IPv6 support for Session Initiation Protocol (SIP) trunks, and support for Skinny Client Control Protocol (SCCP)-controlled analog voice gateways. In addition, the Session Border Controller (SBC) functionality of connecting a SIP IPv4 or H.323 IPv4 network to a SIP IPv6 network is implemented on a Cisco Unified Border Element to facilitate migration from VoIPv4 to VoIPv6.

Finding Feature Information

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

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 VoIP for IPv6

- Cisco Express Forwarding for IPv6 must be enabled.
- Virtual routing and forwarding (VRF) is not supported in IPv6 calls.

Cisco Unified Border Element

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

Cisco Unified Border Element (Enterprise)

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

Information About VoIP for IPv6

- SIP Voice Gateways in VoIPv6, page 188
- MTP Used with Voice Gateways in VoIPv6, page 188

SIP Voice Gateways in VoIPv6

SIP is a simple, ASCII-based protocol that uses requests and responses to establish communication among the various components in the network and to ultimately establish a conference between two or more endpoints.

For further information about this feature and information about configuring the SIP voice gateway for VoIPv6, see the Configuring a SIP Voice Gateway for IPv6, page 188.

MTP Used with Voice Gateways in VoIPv6

Cisco IOS MTP trusted relay point (TRP) supports media interoperation between IPv4 and IPv6 networks.

How to Configure VoIP for IPv6

- Configuring a SIP Voice Gateway for IPv6, page 188
- Configuring H.323 IPv4-to-SIPv6 Connections in a Cisco Unified Border Element, page 202
- Configuring MTP Used with Voice Gateways, page 204

Configuring a SIP Voice Gateway for IPv6

SIP is a simple, ASCII-based protocol that uses requests and responses to establish communication among the various components in the network and to ultimately establish a conference between two or more endpoints.

Users in a SIP network are identified by unique SIP addresses. A SIP address is similar to an e-mail address and is in the format of sip:userID@gateway.com. The user ID can be either a username or an E.164 address. The gateway can be either a domain (with or without a hostname) or a specific Internet IPv4 or IPv6 address.

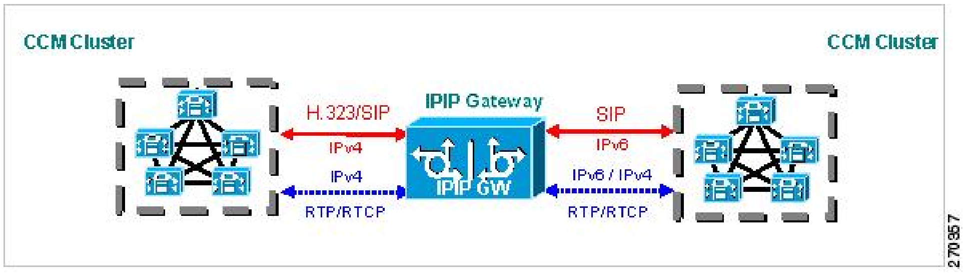
A SIP trunk can operate in one of three modes: SIP trunk in IPv4-only mode, SIP trunk in IPv6-only mode, and SIP trunk in dual-stack mode, which supports both IPv4 and IPv6.

A SIP trunk uses the Alternative Network Address Transport (ANAT) mechanism to exchange multiple IPv4 and IPv6 media addresses for the endpoints in a session. ANAT is automatically enabled on SIP trunks in dual-stack mode. The ANAT Session Description Protocol (SDP) grouping framework allows user agents (UAs) to include both IPv4 and IPv6 addresses in their SDP session descriptions. The UA is then able to use any of its media addresses to establish a media session with a remote UA.

A Cisco Unified Border Element can interoperate between H.323/SIP IPv4 and SIP IPv6 networks in media flow-through mode. In media flow-through mode, both signaling and media flows through the Cisco

Unified Border Element, and the Cisco Unified Border Element performs both signaling and media interoperation between H.323/SIP IPv4 and SIP IPv6 networks (see the figure below).

Figure 11 H.323/SIP IPv4--SIP IPv6 Interoperating in Media Flow-Through Mode



Shutting Down or Enabling VoIPv6 Service on Cisco Gateways

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **shutdown** [**forced**]

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**voice service voip** **Example:** `Device(config)# voice service voip`	Enters voice service VoIP configuration mode.
Step 4	**shutdown** [**forced**] **Example:** `Device(config-voi-serv)# shutdown forced`	Shuts down or enables VoIP call services.

Shutting Down or Enabling VoIPv6 Submodes on Cisco Gateways

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **sip**
5. **call service stop** [**forced**] [**maintain-registration**

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**voice service voip** **Example:** `Device(config)# voice service voip`	Enters voice service VoIP configuration mode.
Step 4	**sip** **Example:** `Device(config-voi-serv)# sip`	Enters SIP configuration mode.
Step 5	**call service stop** [**forced**] [**maintain-registration** **Example:** `Device(config-serv-sip)# call service stop`	Shuts down or enables VoIPv6 for the selected submode.

Configuring the Protocol Mode of the SIP Stack

SIP service should be shut down before configuring the protocol mode. After configuring the protocol mode as IPv6, IPv4, or dual-stack, SIP service should be reenabled.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **sip-ua**
4. **protocol mode ipv4** | **ipv6** | **dual-stack** [**preference** {**ipv4** | **ipv6**}]}

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**sip-ua** **Example:** `Device(config)# sip-ua`	Enters SIP user agent configuration mode.

Step 4	**protocol mode ipv4** | **ipv6** | **dual-stack** [**preference** {**ipv4** | **ipv6**}]}
	Example:
	`Device(config-sip-ua)# protocol mode dual-stack`
		Configures the Cisco IOS SIP stack in dual-stack mode.

Example: Configuring the SIP Trunk

This example shows how to configure the SIP trunk to use dual-stack mode, with IPv6 as the preferred mode. The SIP service must be shut down before any changes are made to protocol mode configuration.

```
Device(config)# sip-ua
Device(config-sip-ua)# protocol mode dual-stack preference ipv6
```

- Disabling ANAT Mode, page 192

Disabling ANAT Mode

ANAT is automatically enabled on SIP trunks in dual-stack mode. Perform this task to disable ANAT in order to use a single-stack mode.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **sip**
5. **no anat**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**voice service voip** **Example:** `Device(config)# voice service voip`	Enters voice service VoIP configuration mode.
Step 4	**sip** **Example:** `Device(config-voi-serv)# sip`	Enters SIP configuration mode.
Step 5	**no anat** **Example:** `Device(conf-serv-sip)# no anat`	Disables ANAT on a SIP trunk.

Configuring the Source IPv6 Address of Signaling and Media Packets

Users can configure the source IPv4 or IPv6 address of signaling and media packets to a specific interface's IPv4 or IPv6 address. Thus, the address that goes out on the packet is bound to the IPv4 or IPv6 address of the interface specified with the **bind** command.

The **bind** command also can be configured with one IPv6 address to force the gateway to use the configured address when the bind interface has multiple IPv6 addresses. The bind interface should have both IPv4 and IPv6 addresses to send out ANAT.

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **sip**
5. **bind** {**control** | **media** | **all**} **source interface** *interface-id* [**ipv6-address** *ipv6-address*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**voice service voip** **Example:** `Device(config)# voice service voip`	Enters voice service VoIP configuration mode.
Step 4	**sip** **Example:** `Device(config-voi-serv)# sip`	Enters SIP configuration mode.
Step 5	**bind** {**control** | **media** | **all**} **source interface** *interface-id* [**ipv6-address** *ipv6-address* **Example:** `Device(config-serv-sip)# bind control source- interface FastEthernet 0/0`	Binds the source address for signaling and media packets to the IPv6 address of a specific interface.

Example: Configuring the Source IPv6 Address of Signaling and Media Packets

```
Device(config)# voice service voip
Device(config-voi-serv)# sip
Device(config-serv-sip)# bind control source-interface fastEthernet 0/0
```

Configuring the SIP Server

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **sip-ua**
4. sip-server {**dns:** *host-name*] | **ipv4:** *ipv4-address* | **ipv6:** **[**ipv6-address**]** **:**[*port-nums*]}
5. **keepalive target** {{**ipv4 :** *address* | **ipv6 :** *address*}[**:** *port*] | **dns :** *hostname* **} [tcp [tls]]** | **udp**] [**secondary**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**sip-ua** **Example:** `Device(config)# sip-ua`	Enters SIP user agent configuration mode.

Step 4	sip-server {**dns:** *host-name*] | **ipv4:** *ipv4-address* | **ipv6:** **[**ipv6-address**]** **:**[*port-nums*]}
	Example:
	`Device(config-sip-ua)# sip-server ipv6:[2001:DB8:0:0:8:800:200C:417A]`
		Configures a network address for the SIP server interface.

Step 5	**keepalive target** {{**ipv4 :** *address* | **ipv6 :** *address*}[**:** *port*] | **dns :** *hostname* **}** **[tcp [tls]]** | **udp**] [**secondary**] **Example:** `Device(config-sip-ua)# keepalive target ipv6:[2001:DB8:0:0:8:800:200C:417A`	Identifies SIP servers that will receive keepalive packets from the SIP gateway.

Example: Configuring the SIP Server

```
Device(config)# sip-ua
Device(config-sip-ua)# sip-server ipv6:[2001:DB8:0:0:8:800:200C:417A]
```

Configuring the Session Target

Perform this task to configure the session target.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *tag* {**mmoip** | **pots** | **vofr** | **voip**}
4. **destination pattern** [+ *string* **T**
5. **session target** {**ipv4:** *destination-address*| **ipv6: [** *destination-address* **]**| **dns : s.** | **d.** | **e.** | **u.**] *host-name* | **enum:***table -num* | **loopback:rtp** | **ras**| **sip-server**} [**:** *port*

DETAILED STEPS

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

Step 3	**dial-peer voice** *tag* {**mmoip** | **pots** | **vofr** | **voip**}
	Example:
	`Device(config)# dial-peer voice 29 voip`
		Defines a particular dial peer, specifies the method of voice encapsulation, and enters dial peer configuration mode.

Step 4	**destination pattern** [+ *string* **T** **Example:** `Device(config-dial-peer)# destination-pattern 7777`	Specifies either the prefix or the full E.164 telephone number to be used for a dial peer.

	Command or Action	Purpose
Step 5	**session target** {**ipv4:** *destination-address*| **ipv6: [** *destination-address* **]**| **dns : s.** | **d.** | **e.** | **u.**] *host-name* | **enum:***table -num* | **loopback:rtp** | **ras**| **sip-server**} [**:** *port* **Example:** `Device(config-dial-peer)# session target [ipv6:2001:DB8:0:0:8:800:200C:417A]`	Designates a network-specific address to receive calls from a VoIP or VoIPv6 dial peer.

Example: Configuring the Session Target

```
Device(config)# dial-peer voice 29 voip
Device(config-dial-peer)# destination-pattern 7777
Device(config-dial-peer)# session target ipv6:[2001:DB8:0:0:8:800:200C:417A]
```

Configuring SIP Register Support

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **sip-ua**
4. **registrar** {**dns:** *address* | **ipv4:** *destination-address* [**:** *port*] | **ipv6:** *destination-address* **:** *port*] } **aor-domain expires** *seconds* [**tcp tls**]] **type** [**secondary**] [**scheme** *string*]
5. **retry register** *retries*
6. **timers register** *milliseconds*

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**sip-ua** **Example:** `Device(config)# sip-ua`	Enters SIP user agent configuration mode.
Step 4	**registrar** {**dns:** *address* | **ipv4:** *destination-address* [**:** *port*] | **ipv6:** *destination-address* **:** *port*] } **aor-domain expires** *seconds* [**tcp tls**]] **type** [**secondary**] [**scheme** *string*] **Example:** `Device(config-sip-ua)# registrar ipv6: [2001:DB8::1:20F:F7FF:FE0B:2972] expires 3600 secondary`	Enables SIP gateways to register E.164 numbers on behalf of analog telephone voice ports, IP phone virtual voice ports, and SCCP phones with an external SIP proxy or SIP registrar.
Step 5	**retry register** *retries* **Example:** `Device(config-sip-ua)# retry register 10`	Configures the total number of SIP register messages that the gateway should send.
Step 6	**timers register** *milliseconds* **Example:** `Device(config-sip-ua)# timers register 500`	Configures how long the SIP UA waits before sending register requests.

Example: Configuring SIP Register Support

```
Device(config)# sip-ua
Device(config-sip-ua)# registrar ipv6:[2001:DB8:0:0:8:800:200C:417A] expires 3600
secondary
Device(config-sip-ua)# retry register 10
Device((config-sip-ua)#  timers register 500
```

Configuring Outbound Proxy Server Globally on a SIP Gateway

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **sip**
5. **outbound-proxy** {**ipv4:** *ipv4-address* | **ipv6:** *ipv6-address* | **dns:** *host* **:** *domain*} [**:** *port-number*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. - Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**voice service voip** **Example:** `Device(config)# voice service voip`	Enters voice service VoIP configuration mode.
Step 4	**sip** **Example:** `Device(config-voi-serv)# sip`	Enters sip configuration mode.
Step 5	**outbound-proxy** {**ipv4:** *ipv4-address* | **ipv6:** *ipv6-address* | **dns:** *host* **:** *domain*} [**:** *port-number*] **Example:** `Device(config-serv-sip)#outbound-proxy ipv6 [2001:DB8:0:0:8:800:200C:417A]`	Specifies the SIP outbound proxy globally for a Cisco IOS voice gateway using an IPv6 address.

Verifying SIP Gateway Status

SUMMARY STEPS

1. **show sip-ua calls**
2. **show sip-ua connections**
3. **show sip-ua status**

DETAILED STEPS

Step 1 **show sip-ua calls**

The **show sip-ua calls** command displays active user agent client (UAC) and user agent server (UAS) information on SIP calls:

```
Device# show sip-ua calls
SIP UAC CALL INFO
    Call 1
    SIP Call ID : 8368ED08-1C2A11DD-80078908-BA2972D0@2001::21B:D4FF:FED7:B000
        State of the call       : STATE_ACTIVE (7)
        Substate of the call    : SUBSTATE_NONE (0)
        Calling Number          : 2000
        Called Number           : 1000
        Bit Flags               : 0xC04018 0x100 0x0
CC Call ID              : 2
   Source IP Address (Sig ): 2001:DB8:0:ABCD::1
   Destn SIP Req Addr:Port : 2001:DB8:0:0:FFFF:5060
   Destn SIP Resp Addr:Port: 2001:DB8:0:1:FFFF:5060
   Destination Name        : 2001::21B:D5FF:FE1D:6C00
   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           : 2
     Stream Type              : voice-only (0)
     Stream Media Addr Type   : 1709707780
     Negotiated Codec         :  (20 bytes)
     Codec Payload Type       : 18
     Negotiated Dtmf-relay    : inband-voice
     Dtmf-relay Payload Type  : 0
     Media Source IP Addr:Port: [2001::21B:D4FF:FED7:B000]:16504
     Media Dest IP Addr:Port  : [2001::21B:D5FF:FE1D:6C00]:19548
Options-Ping    ENABLED:NO    ACTIVE:NO
   Number of SIP User Agent Client(UAC) calls: 1
SIP UAS CALL INFO
   Number of SIP User Agent Server(UAS) calls: 0
```

Step 2 **show sip-ua connections**

Use the **show sip-ua connections** command to display SIP UA transport connection tables:

Example:

```
Device# show sip-ua connections udp brief
Total active connections      : 1
No. of send failures          : 0
No. of remote closures        : 0
No. of conn. failures         : 0
No. of inactive conn. ageouts : 0
Router# show sip-ua connections udp detail

Total active connections      : 1
No. of send failures          : 0
No. of remote closures        : 0
No. of conn. failures         : 0
No. of inactive conn. ageouts : 0
---------Printing Detailed Connection Report---------
Note:
 ** Tuples with no matching socket entry
    - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port>'
      to overcome this error condition
 ++ Tuples with mismatched address/port entry
    - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port> id <connid>'
      to overcome this error condition
Remote-Agent:2001::21B:D5FF:FE1D:6C00, Connections-Count:1
  Remote-Port Conn-Id Conn-State  WriteQ-Size
  =========== ======= =========== ===========
         5060       2 Established           0
```

Step 3 **show sip-ua status**

Use the **show sip-ua status** command to display the status of the SIP UA:

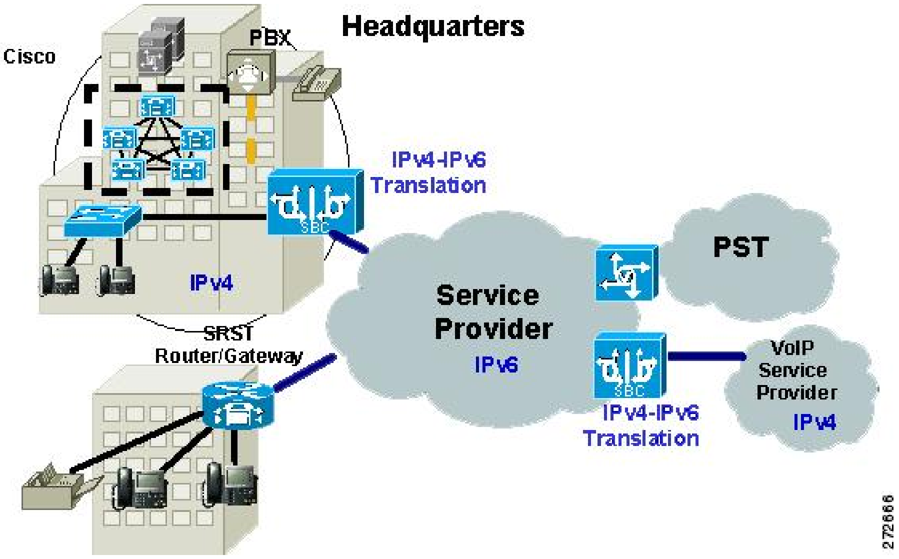
Example:

```
Device# show sip-ua status
SIP User Agent Status
SIP User Agent for UDP : ENABLED
SIP User Agent for TCP : ENABLED
SIP User Agent for TLS over 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 : 70
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
Reason Header will override Response/Request Codes: DISABLED
Out-of-dialog Refer: DISABLED
Presence support is DISABLED
protocol mode is ipv6
SDP application configuration:
 Version line (v=) required
 Owner line (o=) required
 Timespec line (t=) required
 Media supported: audio video image
 Network types supported: IN
 Address types supported: IP4 IP6
 Transport types supported: RTP/AVP udptl
```

Configuring H.323 IPv4-to-SIPv6 Connections in a Cisco Unified Border Element

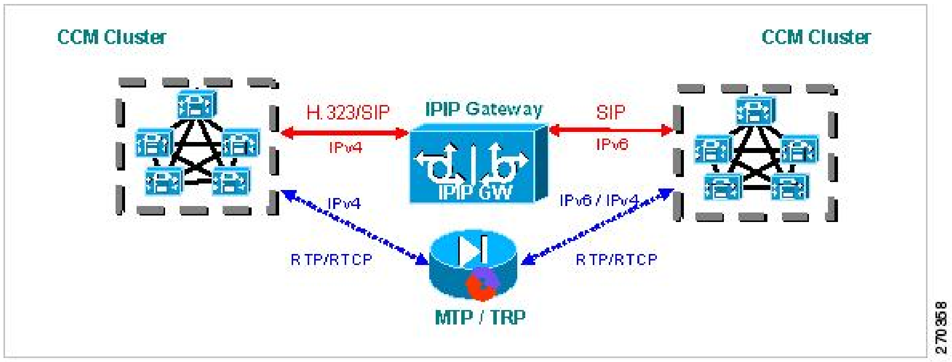
An organization with an IPv4 network can deploy a Cisco Unified Border Element on the boundary to connect with the service provider's IPv6 network (see the figure below).

Figure 12 Cisco Unified Border Element Interoperating IPv4 Networks with IPv6 Service Provider



A Cisco Unified Border Element can interoperate between H.323/SIP IPv4 and SIP IPv6 networks in media flow-through mode. In media flow-through mode, both signaling and media flows through the Cisco Unified Border Element, and the Cisco Unified Border Element performs both signaling and media interoperation between H.323/SIP IPv4 and SIP IPv6 networks (see the figure below).

Figure 13 IPv4 to IPv6 Media Interoperating Through Cisco IOS MTP



The Cisco Unified Border Element feature adds IPv6 capability to existing VoIP features. This feature adds dual-stack support on voice gateways and MTP, IPv6 support for SIP trunks, and SCCP-controlled analog voice gateways. In addition, the SBC functionality of connecting SIP IPv4 or H.323 IPv4 network to a SIP IPv6 network is implemented on an Cisco Unified Border Element to facilitate migration from VoIPv4 to VoIPv6.

Cisco Unified Border Element must be configured in IPv6-only or dual-stack mode to support IPv6 calls.

Note A Cisco Unified Border Element interoperates between H.323/SIP IPv4 and SIP IPv6 networks only in media flow-through mode.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**voice service voip** **Example:** `Device(config)# voice service voip`	Enters voice service VoIP configuration mode.
Step 4	**allow-connections** *from type* **to** *to type* **Example:** `Device(config-voi-serv)# allow-connections h323 to sip`	Allows connections between specific types of endpoints in a VoIPv6 network. Arguments are as follows: • *from-type* --Type of connection. Valid values: **h323**, **sip**. • *to-type* --Type of connection. Valid values: **h323**, **sip**.

Example: Configuring H.323 IPv4-to-SIPv6 Connections in a Cisco Unified Border Element

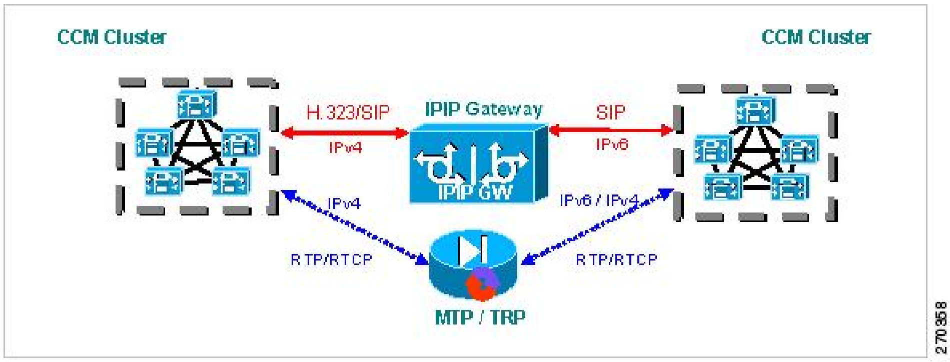
```
Device(config)# voice service voip
Device(config-voi-serv)# allow-connections h323 to sip
```

Configuring MTP Used with Voice Gateways

Cisco IOS MTP trusted relay point (TRP) supports media interoperation between IPv4 and IPv6 networks (see the figure below). This functionality is used when an IPv4 phone (registered to Cisco Unified Communications Manager, formerly known as Cisco Unified Call Manager) communicates with an IPv6 phone (registered to another Cisco Unified Communications Manager). In this case, one of the Cisco Unified Communications Managers inserts a Cisco IOS MTP to perform the IPv4-to-IPv6 media translation between the phones.

MTP for IPv4-to-IPv6 media translation operates only in dual-stack mode. Communication between Cisco IOS MTP and Cisco Unified Communications Manager occurs over SCCP for IPv4 only.

Figure 14 IPv4 to IPv6 Media Interoperating Through Cisco IOS MTP



The VoIPv6 feature includes IPv4 and IPv6 dual-stack support on voice gateways and MTP, IPv6 support for SIP trunks, and SCCP-controlled analog phones. In addition, connecting a SIP IPv4 or H.323 IPv4 network to a SIP IPv6 network is implemented on Cisco Unified Border Element.

- Configuring MTP for IPv4-to-IPv6 Translation, page 204

Configuring MTP for IPv4-to-IPv6 Translation

MTP for IPv4-to-IPv6 media translation operates in dual-stack mode only. A SIP trunk can be configured over IPv4 only, over IPv6 only, or in dual-stack mode. In dual-stack mode, ANAT is used to describe both IPv4 and IPv6 media capabilities.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **sccp ccm** {*ipv4-address* | *ipv6-address* | *dns*} **identifier** *identifier-number* [**priority** *priority*] [**port** *port-number*] [**version** *version-number*]
4. **sccp ccm group** *group -number*
5. **associate profile** *profile-identifier* **register** *device -name*
6. **exit**
7. **dspfarm profile** *profile -identifier* {**conference** | **mtp** | **transcode**} [**security**]
8. **codec** {*codec-type* | **pass-through**}
9. **maximum sessions** {**hardware** | **software**} *number*
10. **associate application sccp**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**sccp ccm** {*ipv4-address* | *ipv6-address* | *dns*} **identifier** *identifier-number* [**priority** *priority*] [**port** *port-number*] [**version** *version-number*] **Example:** `Device(config)# sccp ccm 2001:DB8:C18:1::102 identifier 2 version 7.0`	Adds a Cisco Unified CallManager server to the list of available servers and set various parameters--including IP address, IPv6 address, or Domain Name System (DNS) name, port number, and version number. **Note** SCCP communication between Cisco IOS MTP and Cisco Unified Border Element is supported only for an IPv4-only network. Do not use the *ipv6-address* argument with this command if you are configuring for the Cisco Unified Border Element.
Step 4	**sccp ccm group** *group -number* **Example:** `Device(config)# sccp ccm group 1`	Creates a Cisco CallManager group and enters SCCP Cisco CallManager configuration mode

	Command or Action	Purpose
Step 5	**associate profile** *profile-identifier* **register** *device -name* **Example:** `Device(conif-sccp-ccm)# associate profile 5 register MTP3825`	Associates a digital signal processor (DSP) farm profile with a Cisco CallManager group.
Step 6	**exit** **Example:** `Device(config-sip-ua)# exit`	Exits the current configuration mode.
Step 7	**dspfarm profile** *profile -identifier* {**conference** | **mtp** | **transcode**} [**security**] **Example:** `Device(config)# dspfarm profile 5 mtp`	Enters DSP farm profile configuration mode and defines a profile for DSP farm services.

Step 8	**codec** {*codec-type* | **pass-through**}
	Example:
	`Device(config-dspfarm-profile)# codec g711ulaw`
		Specifies the codecs that are supported by a DSP farm profile.

Step 9	**maximum sessions** {**hardware** | **software**} *number* **Example:** `Device(config-dspfarm-profile)# maximum sessions software 100`	Specifies the maximum number of sessions that are supported by the profile.
Step 10	**associate application sccp** **Example:** `Device(config-dspfarm-profile)# associate application sccp`	Associates SCCP to the DSP farm profile.

Example: Configuring MTP for IPv4-to-IPv6 Translation

```
Device(config)# sccp ccm group 1
Device(config-sccp-ccm)#associate profile 5 register MTP3825
Device(config-sccp-ccm)# exit
Device(config)# dspfarm profile 5 mtp
Device(config-dspfarm-profile)# codec g711ulaw
Device(config-dspfarm-profile)# maximum sessions software 100
Device(config-dspfarm-profile)# associate application sccp
```

```
Device# show sccp
sccp ccm group 1
associate profile 5 register MTP3825
!
dspfarm profile 5 mtp
 codec g711ulaw
 maximum sessions software 100
 associate application SCCP
```

Feature Information for VoIP for IPv6

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

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

Table 21 Feature Information for VoIP for IPv6

Feature Name	Releases	Feature Information
Cisco UBE support for IPv6	12.4(22)T	Cisco UBE support for SIP IPv4-IPv6 dual stack and IPv4 and IPv6 capability provides the following functionality: • Translation of SIP IPv4 to IPv6 addresses • Administration and enforcement of policies for the IPv4/IPv6 mode of operation of each component. • Support the following scenarios: H.323 IPv4 to SIP IPv6; SIP IPv4 to SIP IPv6, SIP IPv6 to SIP IPv6 • DTMF: Interworking capability on Cisco UBE (H. 245 Signal, RFC 2833, SIP Notify, Key Press Markup Language,H.323 to SIP, RFC 2833 to G.711 Inband) • IPv6 topology hiding and demarcation • SIP Options-ping
DSCP-Based QoS Support	12.4(22)T	IPv6 supports this feature.

Feature Name	Releases	Feature Information
IPv6 Dual Stack	12.4(22)T	Adds IPv6 capability to existing VoIP features on the Cisco Unified Border Element. Additionally, the SBC functionality of connecting SIP IPv4 or H.323 IPv4 network to SIP IPv6 network is implemented on a Cisco Unified Border Element to facilitate migration from VoIPv4 to VoIPv6. The following commands were introduced or modified: None
IPv6 Dual Stack	Cisco IOS XE Release 3.3S	Adds IPv6 capability to existing VoIP features on the Cisco Unified Border Element (Enterprise). Additionally, the SBC functionality of connecting SIP IPv4 or H.323 IPv4 network to SIP IPv6 network is implemented on a Cisco Unified Border Element to facilitate migration from VoIPv4 to VoIPv6. The following commands were introduced or modified: None
RTP/RTCP over IPv6	12.4(22)T	RTP stack supports the ability to create IPv6 connections using IPv6 unicast and multicast addresses as well as IPV4 connections.
TDM-SIP GW for IPv6	12.4(24)T	IPv6 supports this feature.
Voice Gateway/MTP	12.4(22)T	Support for If an MTP (Media Translation Point) is used for SIP IPv4/IPv6 media translation. The following commands were introduced or modified: None

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

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 215
- Troubleshooting Tips, page 215

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 22 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.

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.

Cisco Unified Communication Trusted Firewall Control

Cisco Unified Communications Trusted Firewall Control pushes intelligent services onto the network through a Trusted Relay Point (TRP) firewall. Firewall traversal is accomplished using Session Traversal Utilities for NAT(STUN) on a TRP collocated with a Cisco Unified Communications Manager Express (Cisco Unified CME) or a Cisco Unified Border Element.

Finding Feature Information

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

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

Prerequisites

Cisco Unified Border Element

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

Cisco Unified Border Element (Enterprise)

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

Configuring Cisco Unified Communication Trusted Firewall Control

To enable this feature, see the "Cisco Unified Communications Trusted Firewall Control" feature guide.

Detailed command information for the **stun**, **stun flowdata agent-id**, **stun flowdata keepalive**, **stun flowdata shared-secret**, **stun usage firewall-traversal flowdata**, **voice-class stun-usage**commands is located in the *Cisco IOS Voice Command Reference*.

Feature Information for Cisco Unified Communication Trusted Firewall Control

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

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

Table 23 Feature Information for Cisco Unified Communication Trusted Firewall Control

Feature Name	Releases	Feature Information
Cisco Unified Communications Trusted Firewall Control	12.4(22)T	Cisco Unified Communications Trusted Firewall Control pushes intelligent services into the network through Trust Relay Point (TRP). The following commands were introduced or modified: **stun**, **stun flowdata agent-id**, **stun flowdata keepalive**, **stun flowdata shared-secret**, **stun usage firewall-traversal flowdata**, **voice-class stun-usage**.

Table 24 Feature Information for Cisco Unified Communication Trusted Firewall Control

Feature Name	Releases	Feature Information
Cisco Unified Communications Trusted Firewall Control	Cisco IOS XE Release 3.3S	Cisco Unified Communications Trusted Firewall Control pushes intelligent services into the network through Trust Relay Point (TRP). The following commands were introduced or modified: **stun**, **stun flowdata agent-id**, **stun flowdata keepalive**, **stun flowdata shared-secret**, **stun usage firewall-traversal flowdata**, **voice-class stun-usage**.

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.

Cisco Unified Communication Trusted Firewall Control-Version II

Cisco Unified Communications Trusted Firewall Control pushes intelligent services onto the network through a Trusted Relay Point (TRP) firewall. TRP is a Cisco IOS service feature, which is similar to the Resource Reservation Protocol (RSVP) agent. Firewall traversal is accomplished using Session Traversal Utilities for NAT (STUN) on a TRP colocated with a Cisco Unified Communications Manager Express (Cisco Unified CME), Cisco Unified Border Element, and Media Termination Points (MTP).

This release introduces the following features:

- Noncolocated firewall for UC SIP trunks
- Support Firewall traversal for Cisco Unified Border Element call flows in which the media flow through the Media Termination Points such as MTP, Transcoder, or Conference bridge with Trust Relay Point (TRP) enabled.
- Firewall traversal for additional Cisco Unified Border Element call flows using STUN.

Finding Feature Information

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

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 Cisco Unified Communication Trusted Firewall Control-Version II

Cisco Unified Border Element

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

Cisco Unified Border Element (Enterprise)

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

Configuring Cisco Unified Communication Trusted Firewall Control-Version II

To enable this feature, see the "Cisco Unified Communications Trusted Firewall Control-Version II" feature guide.

Detailed command information for the **stun flowdata catlife** command is located in the *Cisco IOS Voice Command Reference*.

Feature Information for Cisco Unified Communication Trusted Firewall Control-Version II

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

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

Table 25 Feature Information for Cisco Unified Communication Trusted Firewall Control-Version II

Feature Name	Releases	Feature Information
Cisco Unified Communication Trusted Firewall Control-Version II	15.0(1)T	Cisco Unified Communications Trusted Firewall Control pushes intelligent services into the network through Trust Relay Point (TRP). The following command was introduced: **stun flowdata catlife**.

Table 26 Feature Information for Cisco Unified Communication Trusted Firewall Control-Version II

Feature Name	Releases	Feature Information
Cisco Unified Communication Trusted Firewall Control-Version II	Cisco IOS XE Release 3.3S	Cisco Unified Communications Trusted Firewall Control pushes intelligent services into the network through Trust Relay Point (TRP). The following command was introduced: **stun flowdata catlife**.

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

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 Cisco Unified Communications Trusted Firewall Control - Version III

- Ensure that you have the correct platform to support this feature. Cisco Unified Communications Trusted Firewall Control is supported on the Cisco 1861, 2801, 2811, 2821, 2851, 3825, and 3845 platforms.
- Cisco IOS Release 15.1(2)T
- All k9 images with voice support. Session Timer feature can run on any voice image and does not support the firewall traversal.
- uc-base and securityk9 licenses on Cisco 29xx and 39xx platforms. Session Timer feature does not require securityk9 licenses.

Configuration Prerequisites

The trusted firewall traversal for Cisco Unified CME SIP line side endpoints can be configured using TRP. The TRP must be configured under **voice service voip> stun** with the following information:

- Authorization agent-id
- Shared secret
- CAT ife
- Keepalive interval

The authorization agent-id and shared secret are mandatory commands and the CATlife and Keepalive interval are optional commands and can have default values

In addition, the **stun-usage** command must to be configured as firewall traversal by using CISCO-STUN-FLOWDATA under **voice class stun-usage**

For detail configuration steps, see: http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/feature/guide/EnhancedTrustedFirewallControll.html

Restrictions for Enhanced Firewall Traversal for Cisco Unified Communications

Cisco IOS Release 15.1(2)T implements firewall traversal for media using STUN on TRP and is not supported for:

- RSVP flow support through the Firewall
- Traditional SRST mode
- H.323 trunk support for Unified Communication Trusted Firewall
- Media flow around on Cisco Unified Border Element
- IPv6
- IP Multicast
- Video calls on SCCP and SIP line side

Information About Cisco Unified Communications Trusted Firewall Control - Version III

Before you configure Enhanced Firewall Traversal using STUN, you should understand the following concepts:

Overview of Firewall Traversal for Cisco Unified Communications

In previous releases, firewall traversal implemented a new framework for IOS firewall traversal on Cisco Unified CME and Cisco Unified Border Element for SIP trunks.

For more information on Cisco trusted firewall traversal, see: www.cisco.com/en/US/docs/voice_ip_comm/cucme/feature/guide/EnhancedTrustedFirewallControll.html

SIP Session Timer

The SIP Session Timer (RFC 4028) is the standard SIP keepalive mechanism that keeps the SIP session active. The SIP user agents send periodic re-INVITE or UPDATE requests (referred to as session refresh requests) to keep the session alive. The interval for the session refresh request is determined through a negotiation mechanism. Session Timer is used to allow SIP signaling through the IOS firewall. You must configure Access Control List (ACL) or partial SIP-Application Layer Gateway (ALG) on the Cisco IOS firewall to allow SIP signaling.

After signaling, a pinhole is created. The firewall starts an inactivity timer, so that in case the user agents crashes or reboots during the call or the BYE message is lost, it can remove its states when the timer starts.

For the Cisco Unified CME SIP line side, by default, the endpoint sends periodic REGISTER messages on port 5060.

- A partial SIP-ALG keeps track of the endpoint registration and keeps the signaling pinhole open as far as the registration is active.
- An ACL tracks the User Datagram Protocol (UDP) / Transmission Control Protocol (TCP) messages that travel across the signaling port and keeps the signaling pinhole open.

However, the Cisco Unified CME SIP trunks do not exchange periodic SIP messages.The Cisco IOS firewall control sessions times out if no SIP messages are exchanged. The timed out SIP over UDP sessions are re-established with the next SIP message (for example, BYE). Timed out SIP over TCP sessions are not re-established and the subsequent SIP messages (for example, BYE) will be dropped.

Restrictions and Limitations for SIP Session Timer

SIP session timer does not support the following:

- Media modifications in responses to locally sent ReINVITE for session refresh
- Session timer in early dialog UPDATE

SIP Session Timer on CUBE for SIP-SIP Call Flows

The following table shows who will be sending the session refresh requests for all combinations of User Agent Clients (UAC) / User Agent Server (UAS) support for session timer

Table 27 Session Timer on CUBE for SIP-SIP Call Flows

S.No	UAC Support	UAS Support	Command Line Interface Enabled on IN leg	Command Line Interface Enabled on OUT leg	Action
1	Yes	Yes	Yes	Yes	UAC/UAS will send the session refresh requests and the Call Control Agent will pass it across.
2	Yes	Yes	No	Yes	
3	Yes	Yes	Yes	No	
4	Yes	Yes	No	No	UAC/UAS may send session refresh requests and the Call Control Agent will pass it across.
5	Yes	No	Yes	Yes	If the incoming INVITE has no "refresher" or "refresher=uac", UAC will send the session refresh requests and the Call Control Agent will pass it across. The Call Control Agent will also start the session expiration timer on the IN LEG. If the incoming INVITE has "refresher=uas", the Call Control Agent will send the session refresh requests on the appropriate leg(s).
6	Yes	No	No	Yes	
7	Yes	No	Yes	No	
8	Yes	No	No	No	UAC may send the session refresh requests and the Call Control Agent will pass it across.
9	No	Yes	Yes	Yes	If the 2xx response from UAS has "refresher=uas", UAS will send the session refresh requests and
10	No	Yes	No	Yes	

S.No	UAC Support	UAS Support	Command Line Interface Enabled on IN leg	Command Line Interface Enabled on OUT leg	Action
11	No	Yes	Yes	No	the Call Control Agent will pass it across. The Call Control Agent will also start the session expiration timer on the OUT LEG. If the 2xx response from UAS has no "refresher" or has "refresher=uac", the Call Control Agent will the send session refresh requests on the appropriate call leg(s).
12	No	Yes	No	No	UAS may send the session refresh requests and the Call Control Agent will pass it across.
13	No	No	Yes	Yes	Call Control Agent will send the session refresh requests on the appropriate call leg(s).
14	No	No	No	Yes	
15	No	No	Yes	No	
16	No	No	No	No	No session timer.

Firewall Traversal Deployment Scenarios

This section provides the firewall traversal scenarios for the Cisco Unified CME line side endpoints.

Firewall Traversal for Soft Phone

For Cisco Unified CME line side, you can deploy an IOS firewall that can be collocated or non-collocated with the Cisco Unified CME.

This is a typical TRP-based trusted IOS firewall traversal deployment between a soft phone and the desk phones. In this scenario, a soft phone like CIPC in the data segment is registered to a Cisco Unified CME. When this soft phone communicates to a desktop IP phone in the voice segment that is registered to the same or different Cisco Unified CME, you can deploy an IOS firewall for the traffic sent between the desktop phone and the soft phone on the Cisco Unified CME line side.

Firewall Traversal for Wireless Phone

In this scenario, the TRP-based trusted IOS firewall traversal is deployed between a wireless phone and desktop phones. A wireless (WiFi) phone like Cisco 792xG is registered to a Cisco Unified CME. When the wireless phone communicates to a wired phone that is registered to the same or different Cisco Unified CME, you can deploy an IOS firewall for the traffic sent between the wired and the wireless phone on the Cisco Unified CME line side.

Firewall Traversal for Teleworker

In this scenario, the teleworker phone is registered to a central or branch office and the Cisco Unified CME communicates to a phone which resides inside the central or branch office. You can deploy an IOS firewall for the traffic sent between the central/branch office and the teleworker phone on the Cisco Unified CME line side.

The teleworker can use the Transport Layer Security (TLS) and Secure Real-Time Protocol (SRTP) for making VoIP calls or establish a Virtual Private Network (VPN) tunnel to the central or branch office for making VoIP calls. In TLS/ SRTP case, the VPN engine/concentrator decrypts the signaling packets and passes the packets to the firewall for inspection. Hence, either a partial SIP ALG or ACL, along with TRP, can be deployed. In VPN case, the firewall will not have the key to decrypt the signaling packets. Hence, only ACL along with TRP can be deployed

How to Configure Cisco Unified Communications Trusted Firewall Control - Version III

To configure Firewall traversal for Cisco Unified CME SIP line side endpoints, enable the stun-usage under:

- Voice-register pool or voice-register template and apply under the voice register pool for SIP line side

Configuring Firewall Traversal for Cisco Unified CME SIP Line Side Endpoints

Perform these tasks to configure firewall traversal.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice register pool***phone-tag*
4. **voice-class stun-usage***tag*
5. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**voice register pool***phone-tag* **Example:** `Device(config)# voice register pool 3`	Enters voice register pool configuration mode to set the phone-specific parameters for an SIP phone. • *phone-tag-Unique* sequence number that identifies the phone. Range is version and platform-dependent; type **?** to display range.
Step 4	**voice-class stun-usage***tag* **Example:** `Device(config-voice-register-pool)# voice-class stun-usage 1`	Enables voice-class stun-usage on the voice-register pool. • This command can also be configured in voice-register-template configuration mode and applied to one or more SIP phones. The voice-register pool configuration has priority over the voice-register-template configuration.

Step 5	**end**
	Example:
	`Device(config-voice-register-pool)# end`
		Exits configuration mode and returns to privileged EXEC mode.

Example: Cisco Unified CME SIP Line Side EndPoints

This section provides the following sample configuration:

```
Device# show run
Building configuration...
!
! Last configuration change at 14:20:02 IST Thu Mar 25 2010 by cisco
! NVRAM config last updated at 15:10:47 IST Wed Mar 24 2010 by cisco
!
version 15.1
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
no service password-encryption
!
hostname fidessrst
!
boot-start-marker
boot system tftp://9.13.40.15/kartk/c3845-adventerprisek9_ivs-mz.0_2_0_20091205
boot-end-marker
!
logging buffered 1000000
no logging console
enable secret 5 $1$GbsI$Ah0BLBHzFx4w/Hu7kyhrs1
enable password cisco
!
no aaa new-model
!
no process cpu autoprofile hog
clock timezone IST 5
!
dot11 syslog
ip source-route
!
no ip cef
```

```
!
no ip domain lookup
ip domain name yourdomain.com
no ipv6 cef
!
multilink bundle-name authenticated
!
template 10
!
voice-card 0
 dspfarm
 dsp services dspfarm
!
voice service voip
 notify redirect ip2pots
 no supplementary-service sip moved-temporarily
 no supplementary-service sip refer
 stun
  stun flowdata agent-id 1 boot-count 45
  stun flowdata shared-secret 7 14141B180F0B7B79772B3A26211C564450
  stun flowdata catlife 70 keepalive 30
 sip
  session transport tcp
  registrar server expires max 600 min 60
!
voice class stun-usage 1
 stun usage firewall-traversal flowdata
!
voice register global
 mode cme
 source-address 192.168.0.1 port 5060
 max-dn 100
 max-pool 100
 load 7971 SIP70.8-5-2SR1S
 load 7970 SIP70.8-5-2SR1S
 load 7961 SIP41.8-5-2SR1S
 load 7960-7940 P0S3-8-12-00
 authenticate realm cisco.com
 tftp-path flash:
 create profile sync 0221764396482329
!
voice register dn  2
 number 999999
 pickup-group 333
 name 7970-2
 mwi
!
voice register dn  3
 number 777777
 pickup-group 333
 name 7970-3
 mwi
!
voice register dn  5
 number 2222
 name 7960-Camelot1
 mwi
!
voice register dn  6
 number 4444
 name 7960-Camelot2
 mwi
!
voice register dn  7
 number 6666
 name 7960-Camelot3
 mwi
!
voice register dn  8
 number 8888
 call-forward b2bua all 6666
 name 7960-Camelot4
 mwi
```

```
!
voice register dn  9
 number 101010
 call-forward b2bua all 1111
 name 7960-Camelot5
 mwi
!
voice register dn  10
 number 121212
 call-forward b2bua noan 6666 timeout 3
 name 7960-Camelot6
 mwi
!
voice register dn  11
 number 141414
 call-forward b2bua busy 1111
 name 7960-Camelot7
 huntstop channel 1
 mwi
!
voice register dn  50
number 15253545
name callgen-sip1
mwi
!
voice register dn  51
number 16263646
name callgen-sip2
mwi
voice register template  10
 voice-class stun-usage 1
 softkeys connected  Park Confrn Endcall Hold Trnsfer
!
voice register pool  2
 park reservation-group 1111
 id mac 0022.9059.81D9
 type 7970
 number 1 dn 2
 template 10
 codec g711ulaw
!
voice register pool  50
 id mac 0011.209F.5D60
 type 7960
 number 1 dn 50
 voice-class stun-usage 1
 codec g711ulaw
!
voice register pool  51
 id mac 0011.209F.5D60
 type 7960
 number 1 dn 51
  voice-class stun-usage 1
 codec g711ulaw
license udi pid CISCO3845-MB sn FOC12373868
archive
 log config
  hidekeys
username cisco password 0 cisco
!
redundancy
!
ip ftp username test
ip ftp password test123
!
!
interface GigabitEthernet0/0
 description $ETH-LAN$$ETH-SW-LAUNCH$$INTF-INFO-GE 0/0$
 ip address 7.9.9.120 255.255.0.0
 duplex auto
 speed auto
 media-type rj45
 no keepalive
 no cdp enable
!
interface GigabitEthernet0/1
 ip address 192.168.0.1 255.255.255.0
 duplex auto
 speed auto
 media-type rj45
 no cdp enable
!
ip forward-protocol nd
ip http server
no ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
!
ip route 0.0.0.0 0.0.0.0 7.9.0.1
ip route 9.13.7.0 255.255.255.0 9.13.7.1
ip route 9.13.7.0 255.255.255.0 9.13.38.1
ip route 9.13.40.0 255.255.255.0 9.13.38.1
ip route 10.104.56.0 255.255.255.0 192.168.0.35
!
arp 10.104.56.54 0024.81b5.3302 ARPA
!
!
control-plane
!
call treatment on
!
voice-port 0/0/0
!
voice-port 0/0/1
!
!
mgcp fax t38 ecm
!
gateway
 timer receive-rtp 1200
!
sip-ua
!
!
alias exec showrtp show policy-map type inspect zone-pair sessions
!
line con 0
 exec-timeout 0 0
 login local
line aux 0
line vty 0 4
 access-class 23 in
 privilege level 15
 login local
 transport input telnet
line vty 5 15
 access-class 23 in
 privilege level 15
 login local
 transport input telnet
!
exception data-corruption buffer truncate
scheduler allocate 20000 1000
end
```

Configuring Firewall Traversal for Cisco Unified CME SCCP Line Side Endpoints

To configure Firewall traversal for Cisco Unified CME SCCP line side endpoints, enable the stun-usage under:

- Ephone or ephone-template and apply under the ephone for SCCP line side

Note MTP should be enabled under ephones for SCCP CME line side endpoints

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ephone***phone-tag*
4. **mtp**
5. **voice-class stun-usage***tag*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ephone***phone-tag* **Example:** `Device(config)# ephone 2`	Enters ephone configuration mode to set phone-specific parameters for an SCCP phone. • *phone-tag* —Unique sequence number that identifies the phone. Range is version and platform-dependent; type **?**to display range.
Step 4	**mtp** **Example:** `Device(config-ephone)# mtp`	Enables Media Termination Points (MTP) on this ephone.
Step 5	**voice-class stun-usage***tag* **Example:** `Device(config-ephone)# voice-class stun-usage 10000`	This command can also be configured in ephone-template configuration mode and applied to one or more SCCP phones. The ephone configuration has priority over the ephone-template configuration.

	Command or Action	Purpose

Step 6	**end**
	Example:
	`Device(config-ephone)# end`
		Exits ephone configuration mode and returns to privileged EXEC mode.

Example: Cisco Unified CME SCCP Line Side EndPoints

This section provides the following sample configuration:

```
Device#show run
Building configuration...
!
! Last configuration change at 14:20:02 IST Thu Mar 25 2010 by cisco
! NVRAM config last updated at 15:10:47 IST Wed Mar 24 2010 by cisco
!
version 15.1
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
no service password-encryption
!
hostname fidessrst
!
boot-start-marker
boot system tftp://9.13.40.15/kartk/c3845-adventerprisek9_ivs-mz.0_2_0_20091205
boot-end-marker
!
logging buffered 1000000
no logging console
enable secret 5 $1$GbsI$Ah0BLBHzFx4w/Hu7kyhrs1
enable password cisco
!
no aaa new-model
!
no process cpu autoprofile hog
clock timezone IST 5
!
dot11 syslog
ip source-route
!
no ip cef
!
no ip domain lookup
ip domain name yourdomain.com
no ipv6 cef
!
multilink bundle-name authenticated
!
template 10
!
voice-card 0
 dspfarm
 dsp services dspfarm
!
voice service voip
 notify redirect ip2pots
 no supplementary-service sip moved-temporarily
 no supplementary-service sip refer
 stun
  stun flowdata agent-id 1 boot-count 45
  stun flowdata shared-secret 7 14141B180F0B7B79772B3A26211C564450
  stun flowdata catlife 70 keepalive 30
 sip
  session transport tcp
  registrar server expires max 600 min 60
!
voice class stun-usage 1
```

```
 stun usage firewall-traversal flowdata
!
!
license udi pid CISCO3845-MB sn FOC12373868
archive
 log config
  hidekeys
username cisco password 0 cisco
!
redundancy
!
ip ftp username test
ip ftp password test123
!
!
interface GigabitEthernet0/0
 description $ETH-LAN$$ETH-SW-LAUNCH$$INTF-INFO-GE 0/0$
 ip address 7.9.9.120 255.255.0.0
 duplex auto
 speed auto
 media-type rj45
 no keepalive
 no cdp enable
!
interface GigabitEthernet0/1
 ip address 192.168.0.1 255.255.255.0
 duplex auto
 speed auto
 media-type rj45
 no cdp enable
!
ip forward-protocol nd
ip http server
no ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
!
ip route 0.0.0.0 0.0.0.0 7.9.0.1
ip route 9.13.7.0 255.255.255.0 9.13.7.1
ip route 9.13.7.0 255.255.255.0 9.13.38.1
ip route 9.13.40.0 255.255.255.0 9.13.38.1
ip route 10.104.56.0 255.255.255.0 192.168.0.35
!
arp 10.104.56.54 0024.81b5.3302 ARPA
!
control-plane
!
call treatment on
!
voice-port 0/0/0
!
voice-port 0/0/1
!
!
mgcp fax t38 ecm
!
sccp local GigabitEthernet0/1
sccp ccm 192.168.0.1 identifier 1 version 7.0
sccp
!
gateway
 timer receive-rtp 1200
!
sip-ua
!
telephony-service
 sdspfarm units 3
 sdspfarm transcode sessions 12
 sdspfarm tag 2 HwConference
 sdspfarm tag 3 mtp00230471e381
 video
 srst mode auto-provision all
 srst ephone template 1
 srst dn line-mode dual
 max-ephones 262
 max-dn 500
 ip source-address 192.168.0.1 port 2000
 service directed-pickup gpickup
 max-conferences 8 gain -6
 call-park system application
 moh music-on-hold.au
 transfer-system full-consult
 create cnf-files version-stamp 7960 Mar 24 2010 15:09:20
!
ephone-template  1
voice-class stun-usage 1
 mtp
!
ephone-template  3
 voice-class stun-usage 1
!
ephone-dn  1  dual-line
 number 1000
 name vg1port1
!
ephone-dn  2  dual-line
 number 2000
 name vg1port2
!
ephone-dn  3  dual-line
 number 3000
 name vg2port1
!
ephone-dn  4  dual-line
 number 4000
 name vg2port2
 call-forward all 3000
!
ephone-dn  5  dual-line
 number 1111
 name sccpcamelot1
!
ephone-dn  6  dual-line
 number 3333
 name sccpcamelot2
!
ephone-dn  7  dual-line
 number 717818919
 description 717818919
 name 717818919
!
ephone-dn  8  dual-line
 number 6000
 label 6000
 description 6000
 name 6000
!
ephone-dn  9  dual-line
 number 5000
 label 5000
 description 5000
 name 5000
!
ephone-dn  10  dual-line
!
ephone-dn  11  dual-line
!
ephone-dn  13  dual-line
 number 919886087486
 name blacforestvg0
!
ephone-dn  14  dual-line
 number 919886087487
 name blacforestvg1
!
ephone-dn  15  dual-line
 number 919886087488
 name blacforestvg2
!
ephone-dn  16  dual-line
 number 919886087489
 name blacforestvg3
!
ephone-dn  41  dual-line
 number 9876
 conference meetme
 preference 1
 no huntstop
!
ephone-dn  42  dual-line
 number 9876
 conference meetme
 preference 2
 no huntstop
!
ephone-dn  43  dual-line
 number 9876
 conference meetme
 preference 3
 no huntstop
!
ephone  1
 voice-class stun-usage 1
 device-security-mode none
 mac-address FCAC.3BAE.0000
 max-calls-per-button 2
 mtp
 type anl
 button  1:1
!
ephone  2
 voice-class stun-usage 1
 device-security-mode none
 mac-address FCAC.3BAE.0001
 max-calls-per-button 2
 mtp
 type anl
 button  1:2
!
ephone  3
 voice-class stun-usage 1
 device-security-mode none
 mac-address FCAC.3BAC.0000
 max-calls-per-button 2
 type anl
 button  1:3
!
ephone  4
 voice-class stun-usage 1
 device-security-mode none
 mac-address FCAC.3BAC.0001
 max-calls-per-button 2
 mtp
 type anl
 button  1:4
!
ephone  5
 voice-class stun-usage 1
 device-security-mode none
 mac-address 1234.1234.1111
 max-calls-per-button 2
 mtp
 type 7960
 button  1:5
!
ephone  6
 voice-class stun-usage 1
 device-security-mode none
 mac-address 1234.1234.3333
 ephone-template 3
 max-calls-per-button 2
 codec g729r8 dspfarm-assist
 mtp
 type 7960
 button  1:6
!
ephone  7
 device-security-mode none
 mac-address FCAC.3B79.0001
 ephone-template 1
 max-calls-per-button 2
 type anl
 button  1:14
!
ephone  8
 device-security-mode none
 mac-address 001B.D584.E274
 ephone-template 1
 button  1:7
!
ephone  9
 device-security-mode none
 mac-address FCAC.3B7F.0001
 ephone-template 1
 button  1:8
!
ephone  10
 device-security-mode none
 mac-address FCAC.3B7F.0000
 ephone-template 1
 button  1:9
!
ephone  11
 device-security-mode none
 mac-address FCAC.3B79.0002
 ephone-template 1
 max-calls-per-button 2
 type anl
 button  1:15
!
ephone  13
 device-security-mode none
 mac-address FCAC.3B79.0000
 ephone-template 1
 max-calls-per-button 2
 type anl
 button  1:13
!
ephone  14
 device-security-mode none
 mac-address FCAC.3B79.0003
 ephone-template 1
 max-calls-per-button 2
 type anl
 button  1:16
!
alias exec showrtp show policy-map type inspect zone-pair sessions
!
line con 0
 exec-timeout 0 0
 login local
line aux 0
line vty 0 4
 access-class 23 in
 privilege level 15
 login local
 transport input telnet
line vty 5 15
 access-class 23 in
 privilege level 15
 login local
 transport input telnet
!
```

```
exception data-corruption buffer truncate
scheduler allocate 20000 1000
end
```

Configuring SIP Session Timers

Configuring SIP Sesion Timer Globally

Perform these tasks to configure SIP session timer globally.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **sip**
5. **min-se***string***session-expires***string*
6. **session refresh**
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**voice service voip** **Example:** `Device(config)# voice service voip`	Enters voice-service configuration mode and specifies a voice-encapsulation type.
Step 4	**sip** **Example:** `Device(config-voi-serv)# sip`	Enters SIP configuration mode.

	Command or Action	Purpose
Step 5	**min-se***string***session-expires***string* **Example:** `Device(conf-serv-sip)# min-se 90 session-expires 100`	Configures the minimum session expires (min-se) and session-expires - *min-se* —90 to 86400
Step 6	**session refresh** **Example:** `Device(conf-serv-sip)# session refresh`	Enables SIP session timer globally.

Step 7	**end**
	Example:
	`Device (conf-serv-sip)# end`
		Exits SIP configuration mode and returns to privileged EXEC mode.

Example: SIP Session Timer

This section provides the following sample configuration:

```
Device# show run
show running-config
Building configuration...
Current configuration : 2284 bytes
!
! Last configuration change at 13:50:48 IST Sun Mar 14 2010
! NVRAM config last updated at 16:21:46 IST Fri Mar 12 2010
!
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec localtime show-timezone
no service password-encryption
!
hostname CUBE1-Fides3
!
boot-start-marker
boot-end-marker
!
!
logging buffered 1000000
no logging console
!
no aaa new-model
no process cpu autoprofile hog
clock timezone IST 5
!
ip source-route
!
ip cef
!
no ip domain lookup
ip domain name yourdomain.com
no ipv6 cef
multilink bundle-name authenticated
!
voice service voip
allow-connections sip to sip
sip
min-se 90 session-expires 100
session refresh
!
```

```
voice-card 0
!
license udi pid CISCO2821 sn FHK1143F0UK
archive
log config
hidekeys
no memory lite
username cisco privilege 15 secret 5 $1$p0H/$eUuiG4gFjfFQFVvUzoDd3/
!
redundancy
!
ip ftp username test
ip ftp password test123
!
interface GigabitEthernet0/0
description $ETH-LAN$$ETH-SW-LAUNCH$$INTF-INFO-GE 0/0$
ip address 7.9.9.106 255.255.0.0
duplex auto
speed auto
no cdp enable
!
interface GigabitEthernet0/1
no ip address
shutdown
duplex auto
speed auto
no cdp enable
!
ip forward-protocol nd
!
ip http server
ip http access-class 23
ip http authentication local
ip http timeout-policy idle 60 life 86400 requests 10000
ip route 0.0.0.0 0.0.0.0 7.9.0.1
!
control-plane
!
mgcp fax t38 ecm
!
!
dial-peer voice 100 voip
huntstop
destination-pattern 1000000000
b2bua
session protocol sipv2
session target ipv4:7.9.9.9
incoming called-number 2000000000
voice-class sip session refresh
codec g711ulaw
!
sip-ua
retry invite 2
!
!
gatekeeper
shutdown
line con 0
exec-timeout 0 0
line aux 0
line vty 0 4
access-class 23 in
privilege level 15
login local
transport input telnet
line vty 5 15
access-class 23 in
privilege level 15
login local
transport input telnet
!
exception data-corruption buffer truncate
```

```
scheduler allocate 20000 1000
end
```

Configuring SIP Session Timer on a Dial-Peer

Perform these tasks to configure SIP session timer at the dial peer level.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice***tag***voip**
4. **voice-class sip session refresh**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**dial-peer voice***tag***voip** **Example:** `Device(config)# dial-peer voice 1 voip`	Enters dial peer configuration mode to define a VoIP dial peer.
Step 4	**voice-class sip session refresh** **Example:** `Device(config-dial-peer)# voice-class sip session refresh`	Enables SIP session refresh at dial-peer level.

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

Feature Information for Cisco Unified Communications Trusted Firewall Control - Version III

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

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

Table 28 Feature Information for Cisco Unified Communications Trusted Firewall Control - Version III

Feature Name	Releases	Feature Information
Cisco Unified Communications Trusted Firewall Control - Version III	15.1(2)T	Cisco Unified Communications Trusted Firewall Control using STUN pushes intelligent services into the network through Trust Relay Point (TRP). The following commands were introduced or modified: **session refresh**, and **voice-class sip session refresh**.

Feature Name	Releases	Feature Information
Cisco Unified Communications Trusted Firewall Control - Version III	Cisco IOS XE Release 3.6S	Cisco Unified Communications Trusted Firewall Control using STUN pushes intelligent services into the network through Trust Relay Point (TRP). In Cisco IOS XE Release 3.6S, this feature was implemented on the Cisco Unified Border Element (Enterprise) The following commands were introduced or modified: **session refresh**, and **voice-class sip session refresh**.

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.

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.