Cisco Unified Border Element Protocol-Independent Features and Setup Configuration Guide, Cisco IOS Release 12.4T

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

CONTENTS

Cisco Unified Border Element Protocol-Independent Features and Setup

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

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

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

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

Cisco Unified Border Element Protocol-Independent Features and Setup

This chapter contains the following configuration topics:

Cisco UBE Prerequisites and Restrictions

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

Cisco Unified Border Element Protocol-Independent Features and Setup

Dial Plan Management

- Dial Peer Configuration on Voice Gateway Routers

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

- Translation Rules

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

- ENUM Support
- Configuring Tool Command Language (Tcl)

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

- Cisco Service Advertisement Framework (SAF)

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

Configuring Call Admission Control (CAC)

- VoIP Call Admissions Control

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

- VoIP Call Admission Control Using RSVP

http://www.cisco.com/en/US/docs/ios/12_1t/12_1t5/feature/guide/dt4trsvp.html

RSVP

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

Dual-Tone Multifrequency (DTMF) Support and Interworking

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

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

- H.323 RFC2833 - SIP NOTIFY

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

Codec Negotiation

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

Payload Type Interoperability

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

Cisco Unified Border Element Protocol-Independent Features and Setup

Transcoding

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

Fax/modem Support

- Modem Passthrough
- T.38 Fax Relay

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

- Cisco Fax Relay

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

SIP Video

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

Telepresence

- SIP Video Support for Telepresence Calls

Security Features

- Toll Fraud Prevention

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

- Access lists (ACLs)

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

- CAC (call spike)

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

- SIP--Ability to Send a SIP Registration Message on a Border Element
- SIP Parameter Modification
- SIP--SIP Stack Portability
- Session Refresh with Reinvites
- CDR

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

- Transport Layer Security (TLS)
- Interworking of Secure RTP calls for SIP and H.323
- SIP SRTP Fallback to Nonsecure RTP
- Cisco Unified Communications Trusted Firewall

IPv4 and IPv6 Interworking

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

RSVP Interworking

- Support for Interworking Between RSVP Capable and RSVP Incapable Networks

Collocated Services

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

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

- Toll Fraud Prevention, page 4

Toll Fraud Prevention

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

- Disable secondary dial tone on voice ports--By default, secondary dial tone is presented on voice ports on Cisco router gateways. Use private line automatic ringdown (PLAR) for foreign exchange office (FXO) ports and direct-inward-dial (DID) for T1/E1 ports to prevent secondary dial tone from being presented to inbound callers.
- Cisco router access control lists (ACLs)--Define ACLs to allow only explicitly valid sources of calls to the router or gateway, and therefore to prevent unauthorized Session Initiation Protocol (SIP) or H.323 calls from unknown parties to be processed and connected by the router or gateway.
- Close unused SIP and H.323 ports--If either the SIP or H.323 protocol is not used in your deployment, close the associated protocol ports. If a Cisco voice gateway has dial peers configured to route calls outbound to the PSTN using either time division multiplex (TDM) trunks or IP, close the unused H.323 or SIP ports so that calls from unauthorized endpoints cannot connect calls. If the protocols are used and the ports must remain open, use ACLs to limit access to legitimate sources.
- Change SIP port 5060--If SIP is actively used, consider changing the port to something other than well-known port 5060.
- SIP registration--If SIP registration is available on SIP trunks, turn on this feature because it provides an extra level of authentication and validation that only legitimate sources can connect calls. If it is not available, ensure that the appropriate ACLs are in place.

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

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

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

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

Prerequisites for SIP-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.

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

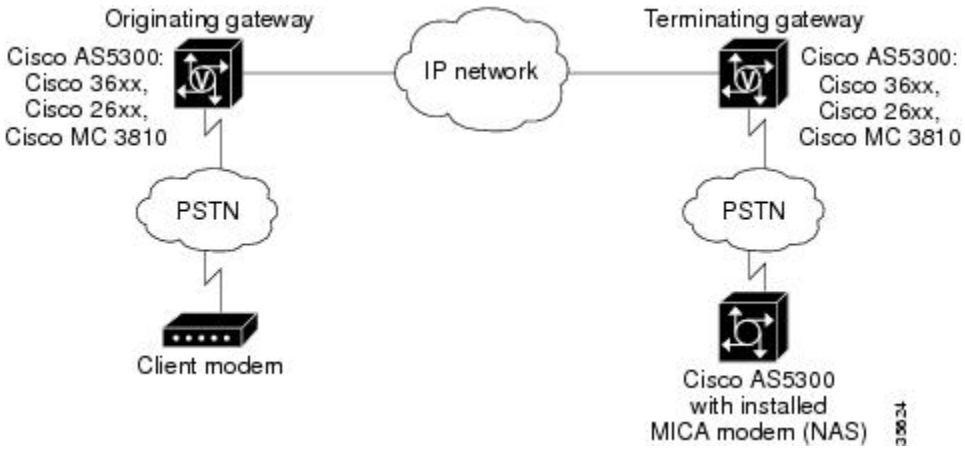
When redundancy is enabled, 10-ms sample-sized packets are sent. When redundancy is disabled, 20-ms sample-sized packets are sent.

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



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.

How to Configure Modem Passthrough over VoIP

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

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.

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:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**voice service voip** **Example:** `Router(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:** `Router(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:** `Router(conf-voi-serv)# exit`	Exits voice-service configuration mode.
Step 5	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

Configuring Modem Passthrough over VoIP for a Specific Dial Peer

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

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.

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

	Command or Action	Purpose
Step 3	**modem passthrough** {**system** | **nse** [**payload-type** *number*] **codec** {**g711ulaw** | **g711alaw**}[**redundancy**]} **Example:** `Router(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.
Step 4	**exit** **Example:** `Router(config-dial-peer)# exit`	Exits dial-peer configuration mode and returns to the global configuration mode.
Step 5	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

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.

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.

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
`Router#` **show call active** {**voice** | **fax**}[**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.
`Router#` **show dial-peer voice** [*number* | **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 for the Cisco Unified Border Element.

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). 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**.

Table 2 Feature Information for Configuring SIP-to-SIP Extended Feature Functionality for Session Border Controllers for the Cisco Unified Border Element (Enterprise).

Feature Name	Releases	Feature Information
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). 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**.

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

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

Prerequisites for 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 20.

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

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:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type slot* / *port* **Example:** `Router(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:** `Router(config-if)# ip rsvp bandwidth 10000 100000`	Enables RSVP for IP on an interface.
Step 5	**end** **Example:** `Router(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:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**dial-peer voice** *tag* **voip** **Example:** `Router(config)# dial-peer 77 voip`	Enters dial peer voice configuration mode.
Step 4	**no acc-qos** {**controlled-load** | **guaranteed-delay**} [**audio** | **video**] **Example:** `Router(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:** `Router(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:** `Router(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:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**dial-peer voice** *tag* **voip** **Example:** `Router(config)# dial-peer 77 voip`	Enters dial peer voice configuration mode.
Step 4	**acc-qos** {**best-effort** | **controlled-load** | **guaranteed-delay**} [**audio** | **video**] **Example:** `Router(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:** `Router(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:** `Router(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:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**dial-peer voice** *tag* **voip** **Example:** `Router(config)# dial-peer voice 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:** `Router(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:** `Router(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:** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**dial-peer voice** *tag* **voip** **Example:** `Router(config)# dial-peer voice 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:** `Router(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:** `Router(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:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**dial-peer voice** *tag* **voip** **Example:** `Router(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:** `Router(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:** `Router(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:** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**dial-peer voice** *tag* **voip** **Example:** `Router(config)# dial-peer voice 66 voip`	Enters dial peer voice configuration mode.
Step 4	**ip qos defending-priority** *defending-pri-value* **Example:** `Router(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:** `Router(config-dial-peer)# ip qos preemption-priority 75`	Configures the RSVP preemption priority value for determining QoS.
Step 6	**end** **Example:** `Router(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:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**show sip-ua calls** **Example:** `Router# show sip-ua calls`	(Optional) Displays active user agent client (UAC) and user agent server (UAS) information on SIP calls.
Step 3	**show ip rsvp installed** **Example:** `Router# show ip rsvp installed`	(Optional) Displays RSVP-related installed filters and corresponding bandwidth information.
Step 4	**show ip rsvp reservation** **Example:** `Router# 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:** `Router# show ip rsvp interface detail GigabitEthernet 0/0`	(Optional) Displays the interface configuration for hello.
Step 6	**show sccp connections details** **Example:** `Router# show sccp connections details`	(Optional) Displays SCCP connection details, such as call-leg details.
Step 7	**show sccp connections rsvp** **Example:** `Router# show sccp connections rsvp`	(Optional) Displays information about active SCCP connections that are using RSVP.
Step 8	**show sccp connections internal** **Example:** `Router# show sccp connections internal`	(Optional) Displays the internal SCCP details, such as time-stamp values.

	Command or Action	Purpose
Step 9	**show sccp** [**all** | **connections** | **statistics**] **Example:** `Router# 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 3 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**,

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

Table 4 Feature Information for Support for Interworking Between RSVP Capable and RSVP Incapable Network

Feature Name	Releases	Feature Information
Interworking Between RSVP Capable and RSVP Incapable Networks	Cisco IOS XE Release 3.1.S	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**,

SIP INFO Method for DTMF Tone Generation

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

Finding Feature Information

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

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

Prerequisites for SIP INFO Method for DTMF Tone Generation

Cisco Unified Border Element

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

Cisco Unified Border Element (Enterprise)

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

Information About SIP INFO Method for DTMF Tone Generation

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

How to Review SIP INFO Messages

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

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

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

Prerequisites

The following are general prerequisites for SIP functionality:

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

Restrictions

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

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

Configuring for SIP INFO Method for DTMF Tone Generation

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

Troubleshooting Tips

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

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

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

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

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

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

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

Feature Information for SIP INFO Method for DTMF Tone Generation

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

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

ISR Feature table entry

Table 5 Feature Information for SIP: INFO Method for DTMF Tone Generation

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

ASR Feature table entry

Table 6 Feature Information for SIP: INFO Method for DTMF Tone Generation

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

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

DTMF Events through SIP Signaling

The DTMF Events through SIP Signaling feature provides the following:

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

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

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

Finding Feature Information

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

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

Prerequisites for DTMF Events through SIP Signaling

Cisco Unified Border Element

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

Cisco Unified Border Element (Enterprise)

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

Restrictions for DTMF Events through SIP Signaling

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

Configuring DTMF Events through SIP Signaling

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode or any other security level set by a system administrator. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**sip-ua** **Example:** `Router(config)# sip-ua`	Enters SIP user-agent configuration mode.

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

• Verifying SIP DTMF Support, page 43

Verifying SIP DTMF Support

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

SUMMARY STEPS

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

DETAILED STEPS

Step 1 **show running-config**

Use this command to show dial-peer configurations.

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

Example:

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

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

Example:

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

Step 2 **show sip-ua retry**

Use this command to display SIP retry statistics.

Example:

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

Step 3 **show sip-ua statistics**

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

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

Example:

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

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

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

Example:

```
Router# show sip-ua statistics
SIP Response Statistics (Inbound/Outbound)
Informational:
Trying 1/1, Ringing 0/0,
Forwarded 0/0, Queued 0/0,
SessionProgress 0/1
Success:
OkInvite 0/1, OkBye 1/0,
OkCancel 0/0, OkOptions 0/0,
OkPrack 0/0, OkPreconditionMet 0/0
OkSubscibe 0/0, OkNotify 0/0,
OkInfo 0/0, 202Accepted 0/0
Redirection (Inbound only):
MultipleChoice 0, MovedPermanently 0,
MovedTemporarily 0, SeeOther 0,
UseProxy 0, AlternateService 0
Client Error:
BadRequest 0/0, Unauthorized 0/0,
PaymentRequired 0/0, Forbidden 0/0,
NotFound 0/0, MethodNotAllowed 0/0,
NotAcceptable 0/0, ProxyAuthReqd 0/0,
ReqTimeout 0/0, Conflict 0/0, Gone 0/0,
LengthRequired 0/0, ReqEntityTooLarge 0/0,
ReqURITooLarge 0/0, UnsupportedMediaType 0/0,
```

```
BadExtension 0/0, TempNotAvailable 0/0,
CallLegNonExistent 0/0, LoopDetected 0/0,
TooManyHops 0/0, AddrIncomplete 0/0,
Ambiguous 0/0, BusyHere 0/0,
BadEvent 0/0
Server Error:
InternalError 0/0, NotImplemented 0/0,
BadGateway 0/0, ServiceUnavail 0/0,
GatewayTimeout 0/0, BadSipVer 0/0
Global Failure:
BusyEverywhere 0/0, Decline 0/0,
NotExistAnywhere 0/0, NotAcceptable 0/0
SIP Total Traffic Statistics (Inbound/Outbound)
    Invite 0/0, Ack 0/0, Bye 0/0,
    Cancel 0/0, Options 0/0,
    Prack 0/0, Comet 0/0,
    Subscribe 0/0, Notify 0/0,
    Refer 0/0, Info 0/0
Retry Statistics
Invite 0, Bye 0, Cancel 0, Response 0, Notify 0
```

Step 4 **show sip-ua status**

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

Example:

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

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

Example:

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

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

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

Example:

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

Step 5 **show sip-ua timers**

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

Example:

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

Step 6 **show voip rtp connections**

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

Step 7 **show sip-ua calls**

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

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

Example:

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

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

Troubleshooting Tips

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

Feature Information for DTMF Events through SIP Signaling

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

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

ISR Feature History Entry.

Table 7 Feature Information for Configuring DTMF Events through SIP Signaling

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

ASR Feature History Entry.

Table 8 Feature Information for Configuring DTMF Events through SIP Signaling

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

Negotiation of an Audio Codec from a List of Codecs

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

Finding Feature Information

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

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

Benefits

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

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

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

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

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

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

Cisco Unified Border Element

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

Cisco Unified Border Element (Enterprise)

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

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

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

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

Disabling Codec Filtering

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

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

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**dial-peer voice** *tag* **voip** **Example:** `Router(config)# dial-peer voice 10 voip`	Enters dial peer voice configuration mode.
Step 4	**voice-class codec** *tag* [**offer-all**] **Example:** `Router(config-dial-peer)# voice-class codec 10 offer-all`	Adds all the configured voice class codec to the outgoing offer from the Cisco UBE.
Step 5	**end** **Example:** `Router(config-dial-peer)# end`	Exits the dial peer voice configuration mode.

Troubleshooting Negotiation of an Audio Codec from a List of Codecs

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

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

Verifying Negotiation of an Audio Codec from a List of Codecs

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

SUMMARY STEPS

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

DETAILED STEPS

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

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

Example:

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

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

Step 3 **show voip rtp connections**

Displays Real-Time Transport Protocol (RTP) connections.

Example:

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

Step 4 **show sccp connections**

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

Example:

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

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

Step 5 **show dspfarm dsp active**

Displays active DSP information about the DSP farm service.

Example:

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

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

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

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

Feature History Table entry for the ISR

Table 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 History Table entry for the ASR

Table 10 Feature Information for Negotiation of an Audio Codec from a List of Codecs on Each Leg of a SIP-to-SIP Call on the Cisco Unified Border Element

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

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

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

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:** `Router> enable` **Example:**	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 voip** **Example:** `Router(config)# voice service voip`	Enters voice service configuration mode.
Step 4	**sip** **Example:** `Router(conf-voi-serv)# sip`	Enters voice service SIP configuration mode.
Step 5	**asymmetric payload** {**dtmf** | **dynamic-codecs** | **full** | **system**} **Example:** `Router(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:** `Router(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:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**dial-peer voice** *tag* **voip** **Example:** `Router(config)# dial-peer voice 77 voip`	Enters dial peer voice configuration mode.
Step 4	**voice-class sip asymmetric payload** {**dtmf** | **dynamic-codecs** | **full** | **system**} **Example:** `Router(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:** `Router(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:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show call active voice compact** **Example:** `Router# show call active voice compact`	(Optional) Displays a compact version of call information.
Step 3	**show call active voice** **Example:** `Router# 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 11 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**.

Table 12 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	IOS 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**.

iLBC Support for SIP and H.323

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

Finding Feature Information

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

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

Prerequisites for iLBC Support for SIP and H.323

Cisco Unified Border Element

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

Cisco Unified Border Element (Enterprise)

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

Restrictions for iLBC Support for SIP and H.323

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

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

Information About iLBC Support for SIP and H.323

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

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

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

How to Configure an iLBC Codec

- Configuring an iLBC Codec on a Dial Peer, page 68
- Configuring an iLBC Codec in the Voice Class, page 70
- Verifying iLBC Support for SIP and H.323, page 72

Configuring an iLBC Codec on a Dial Peer

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

SUMMARY STEPS

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

DETAILED STEPS

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

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

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

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

Configuring an iLBC Codec in the Voice Class

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

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

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

SUMMARY STEPS

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

DETAILED STEPS

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

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

Verifying iLBC Support for SIP and H.323

You can use the following commands to check iLBC status:

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

Feature Information for iLBC Support for SIP and H.323

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

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

Feature History Table entry for the Cisco Unified Border Element.

Table 13 Feature Information for iLBC Support for SIP and H.323

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

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

Table 14 Feature Information for iLBC Support for SIP and H.323

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

SIP Video Calls with Flow Around Media

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

Finding Feature Information

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

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

Prerequisites for SIP Video Calls with Flow Around Media

Cisco Unified Border Element

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

Cisco Unified Border Element (Enterprise)

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

Restrictions for SIP Video Calls with Flow Around Media

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

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

To enable this feature use the **media**command in dial peer, voice class, or voice service configuration mode. For detailed information on the use of this command, see the *Cisco IOS Voice Command Reference* at the following URL: http://www.cisco.com/en/US/docs/ios/voice/command/reference/vr_book.html

Feature Information for Support for SIP Video Calls with Flow Around Media

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 15 Feature Information for SIP Video Calls with Flow Around Media

Feature Name	Releases	Feature Information
SIP Video Calls with Flow Around Media	12.4(15)XZ 12.4(20)T	This feature provides the capability for media packets to pass directly between endpoints without the intervention of the Cisco UBE. The following command was modified by this feature: **media**

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

Table 16 Feature Information for SIP Video Calls with Flow Around Media

Feature Name	Releases	Feature Information
SIP Video Calls with Flow Around Media	Cisco IOS XE Release 3.1S	This feature provides the capability for media packets to pass directly between endpoints without the intervention of the Cisco UBE. The following command was modified by this feature: **media**

Configuring RTP Media Loopback for SIP Calls

Media packets must be enabled to pass through the gateway. Use the **media flow-through** command in dial peer voice or voice service configuration mode to enable the media packets.

Cisco Unified Border Element

- Cisco IOS Release 15.1(4)M or a later release must be installed and running on your Cisco Unified Border Element.

Cisco Unified Border Element (Enterprise)

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

Note

- SRTP, DTLS, and STUN are not supported in loopback mode.
- Fax (midcall transmit function change) is not supported.
- RSVP is not supported.
- Call transfer is not supported.

>

RTP packets are looped back toward the source device when the RTP Media Loopback for SIP Calls feature is configured on a dial peer. The SIP RTP media loopback can be used during Cisco UBE deployments to make test calls to verify the media path between the endpoints and Cisco UBE. In a voice loopback call, an echo is heard at the device originating the call. In a video loopback call, the locally captured video and the audio echo must be rendered at the source device.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *tag* **voip**
4. **destination-pattern** *string*
5. **session protocol sipv2**
6. **session target loopback:rtp**
7. **incoming called-number** *string*
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	**dial-peer voice** *tag* **voip** **Example:** `Router(config)# dial-peer voice 77 voip`	Specifies that the dial peer is a VoIP peer and enters dial peer voice configuration mode.
Step 4	**destination-pattern** *string* **Example:** `Router(config-dial-peer)# destination-pattern 77`	Specifies the prefix or the full E.164 number for the dial peer.
Step 5	**session protocol sipv2** **Example:** `Router(config-dial-peer)# session protocol sipv2`	Specifies the session protocol for calls with the SIP option.
Step 6	**session target loopback:rtp** **Example:** `Router(config-dial-peer)# session target loopback:rtp`	Designates a network-specific address to receive calls from a VoIP dial peer and configures all voice data to loop back to the source.
Step 7	**incoming called-number** *string* **Example:** `Router(config-dial-peer)# incoming called-number 77`	Specifies a digit string that can be matched by an incoming call to associate the call with the dial peer.

	Command or Action	Purpose
Step 8	**exit** **Example:** `Router(config-dial-peer)# exit`	Exits dial peer voice configuration mode and enters global configuration mode.

- Finding Feature Information, page 81
- Configuration Examples for RTP Media Loopback, page 81
- Feature Information for RTP Media Loopback for SIP Calls, page 82

Finding Feature Information

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

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

Configuration Examples for RTP Media Loopback

- Example Configuring Video Loopback with Cisco Telepresence System, page 81
- Example Configuring Video Loopback with Cisco Unified Video Advantage, page 82

Example Configuring Video Loopback with Cisco Telepresence System

The following sample output shows Media Loopback for SIP Calls configured on a Cisco Telepresence System (CTS).

```
!
codec profile 1 aacld
 fmtp "fmtp:96 profile-level-
id=16;streamtype=5;mode=AAChbr;config=B98C00;sizeLength=13;indexLength=3;indexDeltaLength=
3;constantDura
tion=480"
!
codec profile 2 h264
 fmtp "fmtp:112 profile-level-id=4D0028;sprop-parametersets=
R00AKAmWUgDwBDyA,SGE7jyA=;packetization-mode=1"
!
voice class codec 4
 codec preference 1 aacld profile 1
 video codec h264 profile 2
!
dial-peer voice 2000 voip
 destination-pattern 2000
 rtp payload-type cisco-codec-fax-ind 110
 rtp payload-type cisco-codec-aacld 96
 rtp payload-type cisco-codec-video-h264 112
 session protocol sipv2
```

```
 session target loopback:rtp
 incoming called-number 2000
 voice-class codec 4
 voice-class sip bandwidth audio tias-modifier 64000
 voice-class sip bandwidth video tias-modifier 4500000
!
```

Example Configuring Video Loopback with Cisco Unified Video Advantage

The following sample output shows Media Loopback for SIP Calls configured on a Cisco Unified Video Advantage (CUVA).

```
!
codec profile 3 h264
 fmtp "fmtp:98 profile-level-id=420015"
 !
voice class codec 6
 codec preference 1 g711ulaw
 video codec h264 profile 3
 !
dial-peer voice 5000 voip
 description CUVA
 destination-pattern 5000
 rtp payload-type cisco-codec-video-h264 98
 session protocol sipv2
 session target loopback:rtp
 incoming called-number 5000
 voice-class codec 6
 voice-class sip bandwidth video tias-modifier 384000
```

Feature Information for RTP Media Loopback for SIP Calls

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

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

Feature History Table entry for the Cisco Unified Border Element.

Table 17 Feature Information for RTP Media Loopback for SIP Calls

Feature Name	Releases	Feature Information
RTP Media Loopback for SIP Calls	15.1(4)M	RTP packets are looped back toward the source when the RTP Media Loopback for SIP Calls feature is configured on a dial peer. SIP RTP media loopback helps in verifying the media path between the device originating the call and the intermediate device. The following commands were introduced or modified: None.

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

Table 18 Feature Information for RTP Media Loopback for SIP Calls

Feature Name	Releases	Feature Information
RTP Media Loopback for SIP Calls	Cisco IOS XE Release 3.3S	RTP packets are looped back toward the source when the RTP Media Loopback for SIP Calls feature is configured on a dial peer. SIP RTP media loopback helps in verifying the media path between the device originating the call and the intermediate device. The following commands were introduced or modified: None.

Support for Media Flow- Around with SIP Signaling control on CUBE

Finding Feature Information

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

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

Prerequisites

Cisco Unified Border Element

- Cisco IOS Release 15.1(3)T or a later release must be installed and running on your Cisco Unified Border Element.

Cisco Unified Border Element (Enterprise)

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

Configuring Delayed-Offer to Early-Offer Media Flow-Around at the Global Level

Perform this task to configure delayed-offer (DO) to early-offer (EO) media flow-around at the voice service configuration mode.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **media flow-around**
5. **sip**
6. **early offer-forced**
7. **exit**
8. **exit**
9. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice service voip** **Example:** `Router(config)# voice service voip`	Enters voice service configuration mode.
Step 4	**media flow-around** **Example:** `Router(config-voi-serv)# media flow-around`	Enables media flow-around.

	Command or Action	Purpose
Step 5	**sip** **Example:** `Router(config-voi-serv)# sip`	Enters SIP configuration mode.
Step 6	**early offer-forced** **Example:** `Router(config-serv-sip)# early offer-forced`	Forcefully sends SIP EO invites on the Out-Leg(OL).
Step 7	**exit** **Example:** `Router(config-serv-sip)# exit`	Exits SIP configuration mode and returns to voice service configuration mode.
Step 8	**exit** **Example:** `Router(config-voi-serv)# exit`	Exits voice service configuration mode and returns to global configuration mode.
Step 9	**exit** **Example:** `Router(config# exit` **Example:**	Exits global configuration mode and returns to privileged EXEC mode.

Configuring Delayed-Offer to Early-Offer Media Flow-Around for a Dial-Peer

Perform this task to configure DO to EO Media Flow-Around for an individual dial peer.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *number* **voip**
4. **media flow-around**
5. **voice class sip early-offer forced**
6. **exit**
7. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**dial-peer voice** *number* **voip** **Example:** `Router(config)# dial-peer voice 1 voip`	Enters dial peer voice configuration mode for the specified VoIP dial peer.
Step 4	**media flow-around** **Example:** `Router(config-dial-peer)# media flow-around`	Enables media flow-around.
Step 5	**voice class sip early-offer forced** **Example:** `Router(config-dial-peer)# voice class sip early-offer forced`	Forcefully sends SIP EO invites on the Out-Leg.

	Command or Action	Purpose
Step 6	**exit** **Example:** `Router(config-dial-peer)# exit`	Exits dial peer voice configuration mode and returns to global configuration mode.
Step 7	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring Delayed-Offer to Early-Offer Media Flow-Around for High-Density Transcoding Calls

Perform this task to configure Delayed-Offer to Early-Offer Media transcoding high-density calls.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **media transcoder high-density**
5. **sip**
6. **early offer-forced**
7. **exit**
8. **exit**
9. **exit**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice service voip** **Example:** `Router(config)# voice service voip`	Enters voice service configuration mode.
Step 4	**media transcoder high-density** **Example:** `Router(config-voi-serv)# media transcoder high-density`	Enables media transcoder high-density for transcoding high-density media calls.
Step 5	**sip** **Example:** `Router(config-voi-serv)# sip`	Enters SIP configuration mode.
Step 6	**early offer-forced** **Example:** `Router(config-serv-sip)# early offer-forced`	Forcefully sends SIP EO invites on the Out-Leg.
Step 7	**exit** **Example:** `Router(config-serv-sip)# exit`	Exits SIP configuration mode and returns to voice service configuration mode.
Step 8	**exit** **Example:** `Router(config-voi-serv)# exit`	Exits voice service configuration mode and returns to global configuration mode.

	Command or Action	Purpose
Step 9	**exit** **Example:** `Router(config)# exit` **Example:**	Exits global configuration mode and returns to privileged EXEC mode.

Feature Information for Media Flow- Around with SIP Signaling control on Cisco UBE

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

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

ISR Feature table entry

Table 19 Feature Information for Media Flow- Around with SIP Signaling control on Cisco UBE

Feature Name	Releases	Feature Information
Media Flow- Around with SIP Signaling control on CiscoUBE	15.1(3)T	Support for Media Flow-Around for Delayed-Offer to Early-Offer audio calls on Cisco UBE were introduced.The following section provides information about this feature: No new commands were introduced or modified.

ASR Feature table entry

Table 20 Feature Information for Media Flow- Around with SIP Signaling control on CUBE

Feature Name	Releases	Feature Information
Media Flow- Around with SIP Signaling control on CiscoUBE	TBD	Support for Media Flow-Around for Delayed-Offer to Early-Offer audio calls on Cisco UBE were introduced.The following section provides information about this feature: No new commands were introduced or modified.

Configuring Media Antitrombone

Media Trombones are media loops in a SIP entity due to call transfer or call forward. Media loops in Cisco UBE are not detected because Cisco UBE looks at both call types as individual calls and not calls related to each other.

Antitromboning is a media signaling service in SIP entity to overcome the media loops. Antitrombone service has to be enabled only when no media interworking is required in both the out-legs.

To specify media antitrombone for voice class, all VoIP calls, or individual dial peers, perform the tasks in the following sections:

Finding Feature Information

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

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

Prerequisites

Cisco Unified Border Element

- Cisco IOS Release 15.1(3)T or a later release must be installed and running on your Cisco Unified Border Element.

Cisco Unified Border Element (Enterprise)

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

Restrictions

- When media antitrombone service is activated, Cisco UBE does not perform supplementary services such as handling REFER-based call transfers or media services such as SRTP, SNR and call transfers.
- Video codecs are not supported for the normal media handling because the SIP Cisco IOS gateway infrastructure does not support flow-through and flow-around for video.
- Antitrombone will not work if one call leg is flow-through and another call leg is flow-around. Similarly, antitrombone will not work if one call leg is SDP pass-through and another call leg is SDP normal.
- H.323 is not supported.
- Delayed-offer to early-offer (DO-EO) video media flow around is not supported.

Configuring Media Antitrombone for a Voice Class

Perform this task to configure antitrombone service for a voice class.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice class media** *tag*
4. **media anti-trombone**
5. **exit**
6. **exit**

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**voice class media** *tag* **Example:** `Router(config)# voice class media 1`	Enters voice class configuration mode and assigns an identification tag for a media voice class.
Step 4	**media anti-trombone** **Example:** `Router(config-class)# media anti-trombone`	Configures media antitrombone service.
Step 5	**exit** **Example:** `Router(config-dial-peer)# exit`	Exits dial peer configuration mode and enters global configuration mode.
Step 6	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and enters privileged EXEC mode.

Configuring Media Antritrombone at the Global Level

Perform this task to configure media antitrombone service at the voice service configuration mode.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **media anti-trombone**
5. **exit**
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice service voip** **Example:** `Router(config)# voice service voip`	Enters voice service configuration mode.
Step 4	**media anti-trombone** **Example:** `Router(config-voi-serv)# media anti-trombone`	Configures media antitrombone service.
Step 5	**exit** **Example:** `Router(config-voi-serv)# exit`	Exits voice service configuration mode and returns to global configuration mode.
Step 6	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring Media Antitrombone for a Dial Peer

Perform this task to configure media antitrombone at individual dial peer level.

Note

- If both incoming and outgoing dial peers are configured, you must specify the transparent codec on the incoming dial peer.
- The **media anti-trombone** command needs to be enabled for all related dial peers.

>

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *number* **voip**
4. **media anti-trombone**
5. **exit**
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**dial-peer voice** *number* **voip** **Example:** `Router(config)# dial-peer voice 2 voip`	Enters dial peer configuration mode for the specified VoIP dial peer.
Step 4	**media anti-trombone** **Example:** `Router(config-dial-peer)# media antri-trombone`	Configures media antitrombone service.

	Command or Action	Purpose
Step 5	**exit** **Example:** `Router(config-dial-peer)# exit`	Exits dial peer configuration mode and enters global configuration mode.
Step 6	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and enters privileged EXEC mode.

Feature Information for Media Antitrombone

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

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

ISR Feature table entry

Table 21 Feature Information for Media Flow- Around with SIP Signaling control on CUBE

Feature Name	Releases	Feature Information
Media Antitrombone	15.1(3)T	The Media Antitrombone feature is a media signaling service in SIP entity to overcome media loops.

ASR Feature table entry

Table 22 Feature Information for Media Flow- Around with SIP Signaling control on CUBE

Feature Name	Releases	Feature Information
Media Antitrombone	TBD	The Media Antitrombone feature is a media signaling service in SIP entity to overcome media loops.

Finding Feature Information

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

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

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

- Configure a registrar in sip UA configuration mode.

Cisco Unified Border Element

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

Cisco Unified Border Element (Enterprise)

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

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

SUMMARY STEPS

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

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**sip-ua** **Example:** `Router(config)# sip-ua`	Enters sip user-agent configuration mode.
Step 4	**credentials username** *username* **password** *password* **realm** *domain-name* **Example:** `Router(config-sip-ua)# credentials username alex password test realm cisco.com`	Enters SIP digest credentials in sip-ua configuration mode.
Step 5	**exit** **Example:** `Router(config-sip-ua)# exit`	Exits the current mode.
Step 6	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.

- Feature Information for Sending a SIP Registration Message from a Cisco Unified Border Element, page 104

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

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

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

Feature History Table entry for the Cisco Unified Border Element.

Table 23 Feature Information for Sending a SIP Registration Message from a Cisco Unified Border Element

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

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

Table 24 Feature Information for Sending a SIP Registration Message from a Cisco Unified Border Element

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

SIP Parameter Modification

Cisco Unified Border Element

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

Cisco Unified Border Element (Enterprise)

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

Note

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

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

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

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

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice service** *number* **voip** **Example:** `Router(config)# voice service 1 voip`	Enters VoIP voice-service configuration mode.
Step 4	**voice-class sip-profiles** *group-number* **Example:** `Router(config)# voice-class sip profiles 42`	Establishes individual sip profiles defined by a group-number. Valid group-numbers are from 1 to 1000.
Step 5	**response** *option* **sip-header** *option* ADD *word* CR **Example:** `Router(config)# request INVITE sip-header supported remove`	Add, change, or delete any SIP or SDP header in voice class or sip-profile submode.

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

Finding Feature Information

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

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

Example

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

Feature Information for Configuring SIP Parameter Modification

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

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

Feature History Table entry for the Cisco Unified Border Element.

Table 25 Feature Information for Configuring SIP Parameter Modification

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

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

Table 26 Feature Information for Configuring SIP Parameter Modification

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

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

Finding Feature Information

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

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

Session Refresh with Reinvites

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

Cisco Unified Border Element

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

Cisco Unified Border Element (Enterprise)

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

Note

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

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

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

>

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

Cisco IOS Release 12.4(15)XZ and Earlier Releases

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

Cisco IOS Release 12.4(15)XZ and Later Releases

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

SUMMARY STEPS

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

DETAILED STEPS

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

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

- Feature Information for Session Refresh with Reinvites, page 117

Feature Information for Session Refresh with Reinvites

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

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

Feature History Table for the ASR

Table 27 Feature Information for Session Refresh with Reinvites

Feature Name	Releases	Feature Information
Session Refresh with Reinvites	12.4(20)T	Expands the ability of the Cisco Unified BE to control the session refresh parameters and ensure the session does not time out. **midcall-signaling**

Feature History Table for the ISR

Table 28 Feature Information for Session Refresh with Reinvites

Feature Name	Releases	Feature Information
Session Refresh with Reinvites	Cisco IOS XE Release 2.5	Expands the ability of the Cisco Unified BE to control the session refresh parameters and ensure the session does not time out. **midcall-signaling**

SIP Stack Portability

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

Finding Feature Information

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

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

Prerequisites for SIP Stack Portability

Cisco Unified Border Element

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

Cisco Unified Border Element (Enterprise)

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

Information About SIP Stack Portability

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

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

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

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

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

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

SIP Call-Transfer Basics

Basic Terminology of SIP Call Transfer

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

Refer Message Request

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

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

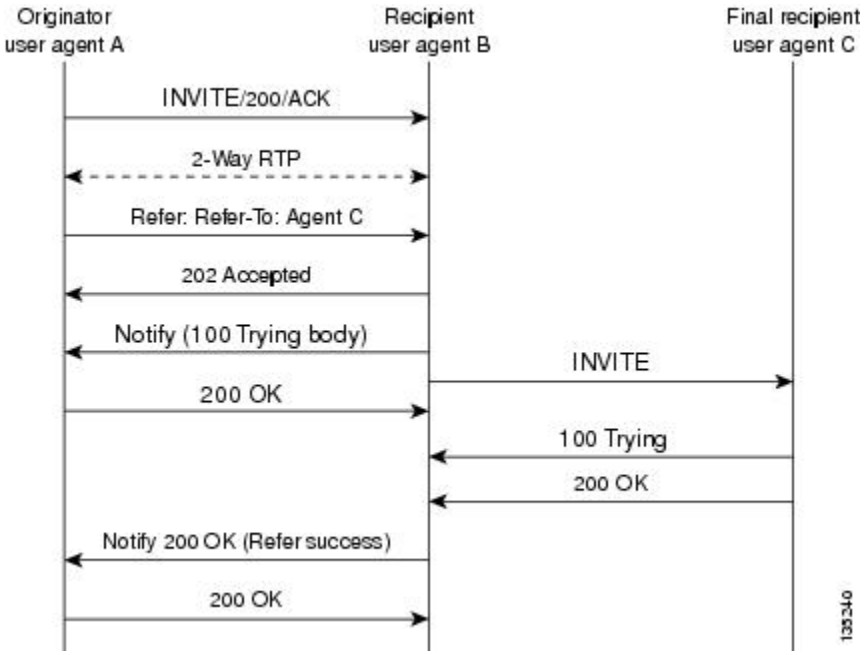
Note A gateway can be a recipient or final recipient, but not an originator.

The Refer message request always begins within the context of an existing call and starts with the *originator* . The originator sends a Refer request to the *recipient* (user agent receiving the Refer request) to initiate a triggered INVITE request. The triggered INVITE request uses the SIP URL contained in the Refer-To header as the destination of the INVITE request. The recipient then contacts the resource in the Refer-To header (*final recipient*), and returns a SIP 202 (Accepted) response to the originator. The recipient also must notify the originator of the outcome of the Refer transaction--whether the final recipient was successfully contacted or not. The notification is accomplished using the SIP NOTIFY message

request, SIP's event notification mechanism. A NOTIFY message with a message body of SIP 200 OK indicates a successful transfer, and a message body of SIP 503 Service Unavailable indicates an unsuccessful transfer. If the call was successful, a call between the recipient and the final recipient results.

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

Figure 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

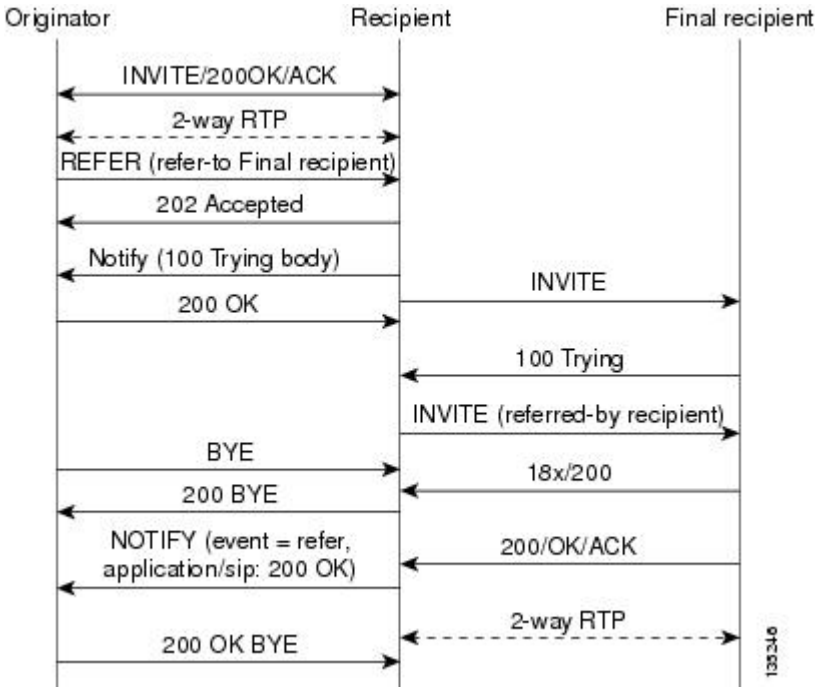
A blind, or unattended, transfer is one in which the transferring phone connects the caller to a destination line before ringback begins. This is different from a consultative, or attended, transfer in which one of the transferring parties either connects the caller to a ringing phone (ringback heard) 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 122. 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).

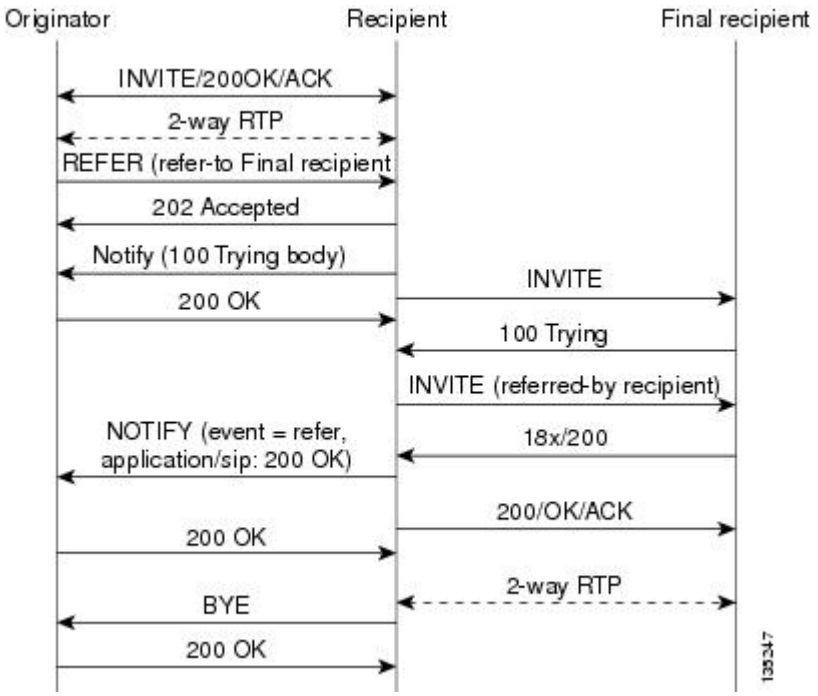
The figure below shows a successful blind or unattended call transfer in which the originator initiates a Bye request to terminate signaling with the recipient.

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.

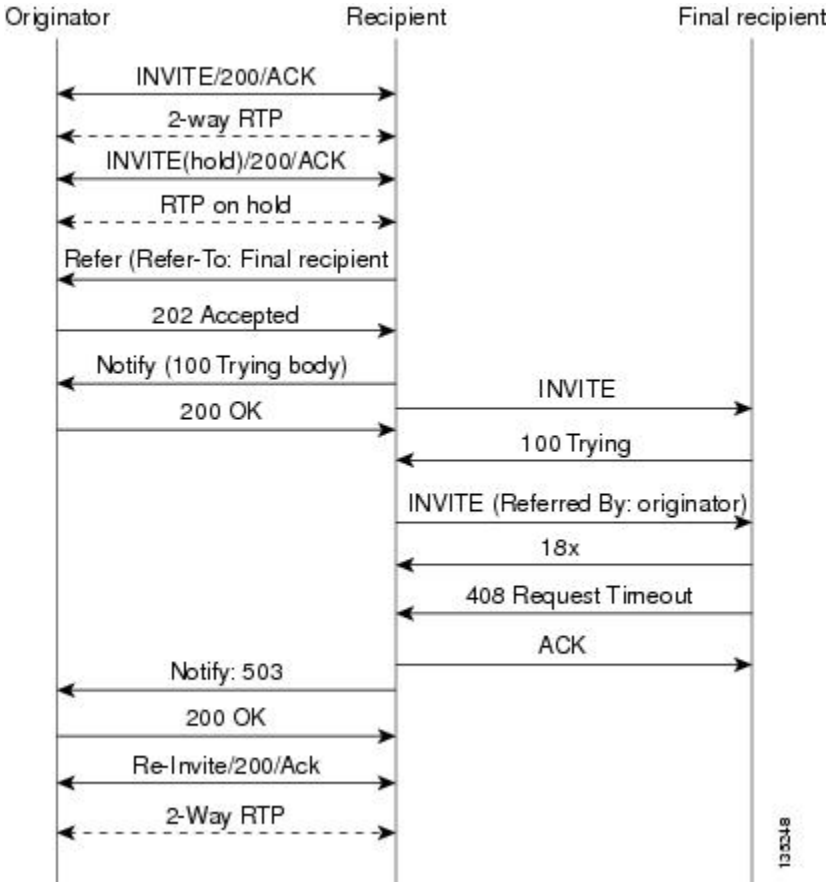
Figure 4 Successful Blind or Unattended Transfer--Recipient Initiating a Bye Request



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

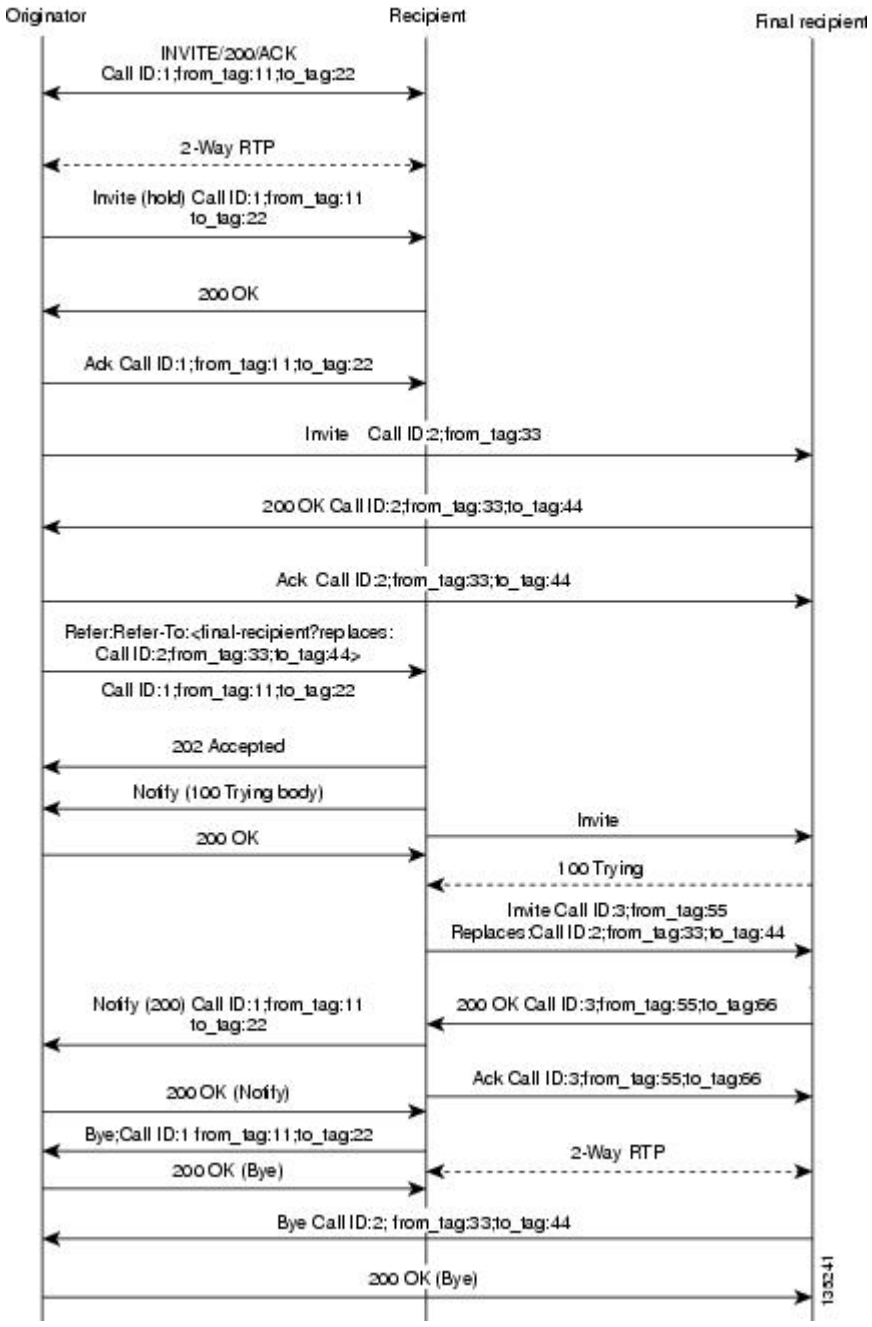
The Replaces header is required in attended transfers. It indicates to the final recipient that the initial call leg (identified by the Call-ID header and tags) is to be shut down and replaced by the incoming INVITE request. The final recipient sends a Bye request to the originator to terminate its session.

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



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):

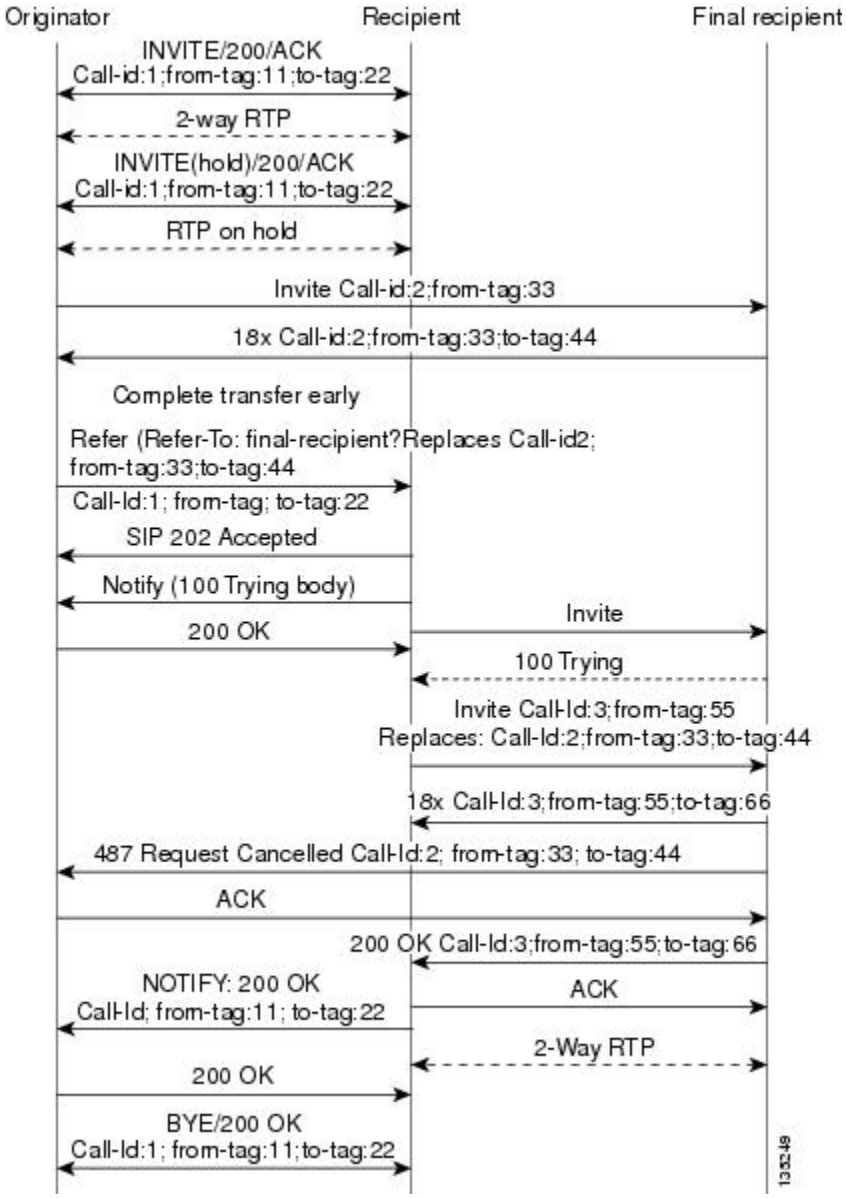
1. Originator does the following:
   a. Sets up a call with recipient.
   b. Places the recipient on hold.
   c. Contacts the final recipient.
   d. After receiving an indication that the final recipient is ringing, sends recipient a Refer message request with an overloaded Replaces header in the Refer-To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



VSA for Call Transfer

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

Referred-By Header

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

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

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

Business Group Field

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

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

Feature Information for SIP Stack Portability

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

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

Feature History Table for the ASR

Table 29 Feature Information for SIP Stack Portability

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

Feature History Table for the ISR

Table 30 Feature Information for SIP--SIP Stack Portability

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

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

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

Prerequisites for 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.

Feature History Table entry for the Cisco Unified Border Element.

Table 31 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.

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

Table 32 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	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.

CUBE 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), the SRTP-RTP Interworking feature was extended to support supplementary services on Cisco UBEs.

Prerequisites for CUBE Support for SRTP-RTP Internetworking

- To enable SRTP-RTP Internetworking feature, you must have Cisco IOS Release 12.4(22)YB or a later release installed and running on your Cisco gateway. For detailed information on platform availability and subsequent releases.
- The Cisco Unified Border Element Support for SRTP-RTP Internetworking feature is supported in Cisco Unified CallManager 7.0 and later releases.

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

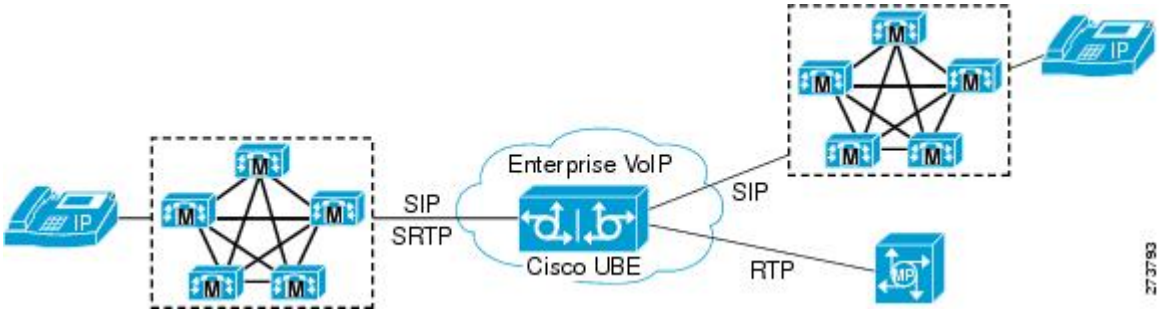
To configure support for SRTP-RTP internetworking, you should understand the following concepts:

CUBE Support for SRTP-RTP Internetworking

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

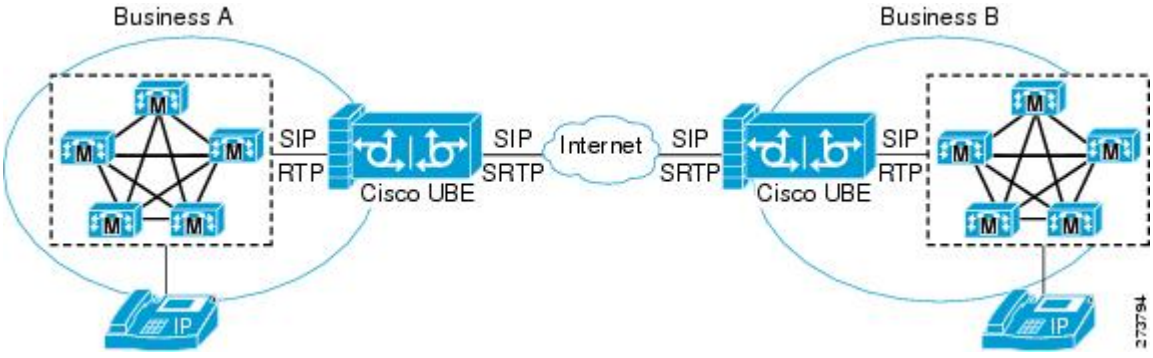
- RTP Cisco Unified CallManager domains. Domains that do not support SRTP or have not been configured for SRTP, as shown in the figure below.
- RTP Cisco applications or servers. For example, Cisco Unified MeetingPlace, Cisco WebEx, or Cisco Unity, which do not support SRTP, or have not been configured 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



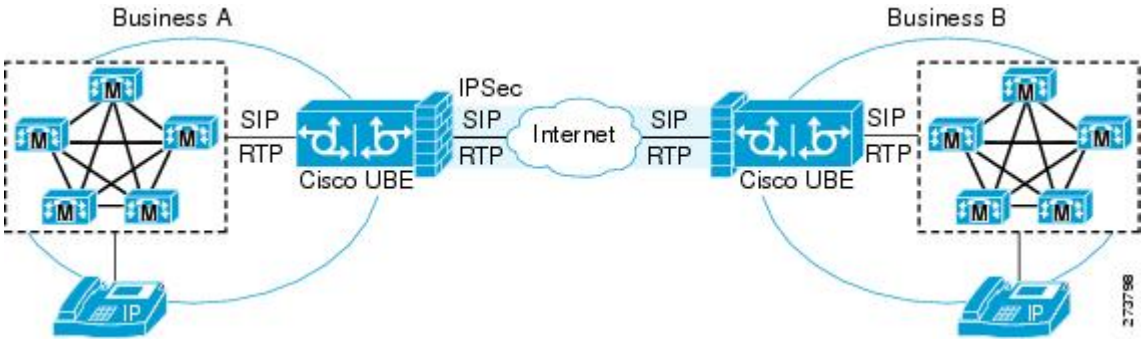
The Cisco Unified Border Element Support for SRTP-RTP Internetworking feature connects SRTP enterprise domains to RTP SIP provider SIP trunks. SRTP-RTP internetworking connects RTP enterprise networks with SRTP over an external network between businesses. This provides flexible secure business-to-business 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 CUBE

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 CUBE Support for SRTP-RTP Internetworking

Configuring CUBE 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:** `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	**ip http server** **Example:** `Router(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:** `Router(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:** `Router(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.

	Command or Action	Purpose
Step 6	**grant auto** **Example:** `Router(cs-server)# grant auto`	Specifies automatic certificate enrollment.
Step 7	**no shutdown** **Example:** `Router(cs-server)# no shutdown`	Reenables the certificate server. • Create and enter a new password when prompted.
Step 8	**exit** **Example:** `Router(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 140.

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:** `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	**crypto pki trustpoint** *name* **Example:** `Router(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:** `Router(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.
Step 5	**serial-number** **Example:** `Router(ca-trustpoint)# serial-number`	Specifies whether the router serial number should be included in the certificate request.
Step 6	**revocation-check** *method* **Example:** `Router(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:** `Router(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.

	Command or Action	Purpose
Step 8	**end** **Example:** `Router(ca-trustpoint)# end`	Exits ca-trustpoint configuration mode.
Step 9	**crypto pki authenticate** *name* **Example:** `Router(config)# crypto pki authenticate secdsp`	Authenticates the CA. • Accept the trustpoint CA certificate if prompted.
Step 10	**crypto pki enroll** *name* **Example:** `Router(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:** `Router(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 142.

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:** `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-card** *slot* **Example:** `Router(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:** `Router(config-voicecard)# dspfarm`	Adds a specified voice card to those participating in a DSP resource pool.
Step 5	**dsp services dspfarm** **Example:** `Router(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.	--
Step 7	**exit** **Example:** `Router(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 144.

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:** `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* **Example:** `Router(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.

	Command or Action	Purpose
Step 4	**sccp ccm** *ip-address* **identifier** *identifier-number* **version** *version-number* **Example:** `Router(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:** `Router(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:** `Router(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.
Step 7	**associate profile** *profile-identifier* **register** *device-name* **Example:** `Router(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:** `Router(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.

	Command or Action	Purpose
Step 9	**trustpoint** *trustpoint-label* **Example:** `Router(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:** `Router(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:** `Router(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:** `Router(config-dspfarm-profile)# associate application sccp`	Associates SCCP to the DSP farm profile.
Step 14	**no shutdown** **Example:** `Router(config-dspfarm-profile)# no shutdown`	Allocates DSP farm resources and associates them with the application.
Step 15	**exit** **Example:** `Router(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 145.

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:** `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	**telephony-service** **Example:** `Router(config)# telephony-service`	Enters telephony-service configuration mode.

	Command or Action	Purpose
Step 4	**sdspfarm transcode sessions** *number* **Example:** `Router(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:** `Router(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:** `Router(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:** `Router(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.
Step 8	**max-dn** *max-directory-numbers* **Example:** `Router(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:** `Router(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:** `Router(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.

	Command or Action	Purpose
Step 11	**tftp-server-credentials trustpoint** *label* **Example:** `Router(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:** `Router(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:** `Router(config-telephony)# no sccp`	Disables SCCP and its related applications (transcoding and conferencing) and exits telephony-service configuration mode.
Step 14	**sccp** **Example:** `Router(config)# sccp`	Enables SCCP and related applications (transcoding and conferencing).
Step 15	**end** **Example:** `Router(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 148.

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

	Command or Action	Purpose
Step 4	**destination-pattern** *string* **Example:** `Router(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:** `Router(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:** `Router(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.
Step 7	**incoming called-number** *string* **Example:** `Router(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:** `Router(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:** `Router(config-dial-peer)# end`	Exits dial peer voice configuration mode.
Step 10	**dial-peer voice** *tag* **voip** **Example:** `Router(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.

	Command or Action	Purpose
Step 11	Repeat Steps 4, 5, 6, and 7 to configure a second dial peer.	--
Step 12	**srtp** **Example:** `Router(config-dial-peer)# srtp`	Specifies that SRTP is used to enable secure calls for the dial peer.
Step 13	**codec** *codec* **Example:** `Router(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 14	**exit** **Example:** `Router(config-dial-peer)# exit`	Exits dial peer voice configuration mode.

- Troubleshooting Tips, page 154

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 154
- Enabling SRTP on a Dial Peer, page 155
- Troubleshooting Tips, page 156

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:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice service voip** **Example:** `Router(config)# voice service voip`	Enters voice-service configuration mode and specifies VoIP encapsulation as the voice-encapsulation type.
Step 4	**srtp fallback** **Example:** `Router(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:** `Router(conf-voi-serv)# exit`	Exits voice service configuration mode.

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

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:

```
Router> enable
```

Step 2 **show call active voice brief**
Displays call information for voice calls in progress.

Example:

```
Router# 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:

```
Router# 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:

```
Router# 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

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
```

Example: Enabling SRTP on the Cisco UBE

Example: Enabling SRTP Globally

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

Example: Enabling SRTP on a Dial Peer

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

Feature Information for CUBE Support for SRTP-RTP Internetworking

Feature History table for the ISR

Table 33 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	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**.
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.

Configuring RTCP Report Generation

The assisted Real-time Transport Control Protocol (RTCP) feature adds the ability for Cisco Unified Border Element (Cisco UBE) to generate standard RTCP keepalive reports on behalf of endpoints. RTCP reports determine the liveliness of a media session during prolonged periods of silence, such as call hold or mute. Therefore, it is important for the Cisco UBE to generate RTCP reports irrespective of whether the endpoints send or receive media.

Cisco UBE generates RTCP report only when inbound and outbound call legs are SIP, or SIP to H.323, or H.323 to SIP.

Finding Feature Information

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

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

Prerequisites

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 <TBD> or a later release must be installed and running on your Cisco ASR 1000 Series Router.

Restrictions

- RTCP report generation over IPv6 is not supported.
- RTCP report generation is not supported for Secure Real-time Transport Protocol (SRTP) or SRT Control Protocol (SRTCP) pass-through as Cisco UBE is not aware of the media encryption or decryption keys.
- RTCP report generation is not supported for loopback calls, T.38 fax, and modem relay calls.
- RTCP or SRTCP report generation is not supported when Cisco UBE inserts a Digital Signal Processor (DSP) for RTP-SRTP interworking on RTP and SRTP call legs.
- RTCP report generation is not supported when there is a call hold with an invalid media address such as 0.0.0.0 in Session Description Protocol (SDP) or Open Logical Channel (OLC).
- RTCP report generation is not supported for RTCP multiplexed with RTP on the same address and port.
- RTCP report generation is not supported on enterprise aggregation services routers (ASR) Cisco UBE.
- RTCP packet generation is not supported on the SIP leg when the H.323 leg puts the SIP leg on hold in a Slow Start to Delayed-Offer call.

Configuring RTCP Report Generation on Cisco UBE

RTCP keepalive packets indicate session liveliness. When configured on Cisco UBE, RTCP keepalive packets are sent on both inbound and outbound SIP or H.323 call legs.

Perform this task to configure RTCP report generation on Cisco UBE.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **allow-connections** *from-type* **to** *to-type*
5. **rtcp keepalive**
6. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice service voip** **Example:** `Router(config)# voice service voip`	Enters voice service configuration mode.
Step 4	**allow-connections** *from-type* **to** *to-type* **Example:** `Router(conf-voi-serv)# allow-connections sip to sip`	Allows connections between SIP endpoints in a VoIP network.
Step 5	**rtcp keepalive** **Example:** `Router(conf-voi-serv)# rtcp keepalive`	Configures RTCP keepalive report generation.
Step 6	**end** **Example:** `Router(conf-voi-serv)# end`	Exits voice service configuration mode and returns to privileged EXEC mode.

Troubleshooting Tips

Use the following debug commands for debugging related to RTCP keepalive packets:

- **debug voip rtcp packet** --Shows details related to RTCP keepalive packets such as RTCP sending and receiving paths, Call ID, Globally Unique Identifier (GUID), packet header, and so on.

```
Router# debug voip rtcp packet
01:06:27.450: //6/xxxxxxxxxxxx/RTP//Event/voip_rtp_send_rtcp_keepalive: Generate RTCP
Keepalive
*Mar 17 01:06:27.450: rtcp_send_report: Attributes
        (src ip=192.168.30.3, src port=17101, dst ip=192.168.30.4, dst port=18619
         bye=0, initial=1, ssrc=0x07111E02, keepalive=1)
*Mar 17 01:06:27.450: rtcp_construct_keepalive_report: Constructed Report
        (rtcp=0x2E5AF214, ssrc=0x07111E02, source->ssrc=0x00001E03, total_len=36)
2E5AF210:          80C90001 07111E02 81CA0006      .I.......J..
2E5AF220: 07111E02 010F302E 302E3040 392E3435  ......0.0.0@9.45
2E5AF230: 2E33302E 33000000 00                 .30.3....
```

Caution Under moderate traffic loads, the **debug voip rtp packet** command produces a high volume of output and the command should be enabled only when the call volume is very low.

- **debug voip rtp packet** --Shows details about VoIP RTP packet debugging trace.

```
Router# debug voip rtp packet
VOIP RTP All Packets debugging is on
```

- **debug voip rtp session** --Shows all RTP session debug information.

```
Router# debug voip rtp session
VOIP RTP All Events debugging is on
```

- **debug voip rtp error** --Shows details about debugging trace for RTP packet error cases.

```
Router# debug voip rtp error
VOIP RTP Errors debugging is on
```

- **debug ip rtp protocol** --Shows details about RTP protocol debugging trace.

```
Router# debug ip rtp protocol
RTP protocol debugging is on
```

- **debug voip rtcp session** --Shows all RTCP session debug information.

```
Router# debug voip rtcp session
VOIP RTCP Events debugging is on
```

- **debug voip rtcp error** -- Shows details about debugging trace for RTCP packet error cases.

```
Router# debug voip rtcp error
VOIP RTCP Errors debugging is on
```

Feature Information for Configuring RTCP Report 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.

Feature History Table entry for the Cisco Unified Border Element. .

Table 34 Feature Information for Configuring RTCP Report Generation

Feature Name	Releases	Feature Information
Assisted RTCP	15.1(2)T	This feature adds the ability for Cisco UBE to generate standard RTCP keepalive reports on behalf of endpoints and ensures the liveliness of a media session during prolonged periods of silence, such as call hold. The following commands were introduced or modified in this release: **rtcp keepalive**, **debug voip rtcp**, **debug voip rtp**, **debug ip rtp protocol**, and **ip rtcp report interval**.

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

Table 35 Feature Information for Configuring RTCP Report Generation

Feature Name	Releases	Feature Information
Assisted RTCP	TBD	This feature adds the ability for Cisco UBE to generate standard RTCP keepalive reports on behalf of endpoints and ensures the liveliness of a media session during prolonged periods of silence, such as call hold. The following commands were introduced or modified in this release: **rtcp keepalive**, **debug voip rtcp**, **debug voip rtp**, **debug ip rtp protocol**, and **ip rtcp report interval**.

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

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

Prerequisites for SIP 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.

Feature History Table entry for the Cisco Unified Border Element.

Table 36 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 History Table entry for the Cisco Unified Border Element (Enterprise).

Table 37 Feature Information for SIP SRTP Fallback to Nonsecure RTP

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**

Configuring Support for Interworking Between RSVP Capable and RSVP Incapable Networks

The Support for Interworking Between RSVP Capable and RSVP Incapable Networks feature provides precondition-based Resource Reservation Protocol (RSVP) support for basic audio call and supplementary services on Cisco 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 feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

Prerequisites

- 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 task.

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 <TBD> or a later release must be installed and running on your Cisco ASR 1000 Series Router.

Restrictions

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

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

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:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type slot / port* **Example:** `Router(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:** `Router(config-if)# ip rsvp bandwidth 10000 100000`	Enables RSVP for IP on an interface.
Step 5	**end** **Example:** `Router(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:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**dial-peer voice** *tag* **voip** **Example:** `Router(config)# dial-peer 77 voip`	Enters dial peer voice configuration mode.
Step 4	**no acc-qos** {**controlled-load** | **guaranteed-delay**} [**audio** | **video**] **Example:** `Router(config-dial-peer)# no acc-qos controlled-load`	Removes any value configured for the **acc-qos** command. • ◦ **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:** `Router(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:** `Router(config-dial-peer)# end`	Exits dial peer voice configuration mode and returns to privileged EXEC mode.

Configuring EO to EO DO to DO and DO to EO at the Dial Peer

Perform this task to configure support for EO to EO, DO to DO, and DO to EO at the dial peer level.

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. **exit**
7. **interface** *type* **slot/port**
8. **ip rsvp bandwidth** [*reservable-bw* [*max-reservable-bw*] [**sub-pool** *reservable-bw*]]
9. **exit**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**dial-peer voice** *tag* **voip** **Example:** `Router(config)# dial-peer voice 77 voip`	Enters dial peer voice configuration mode.
Step 4	**no acc-qos** {**controlled-load** | **guaranteed-delay**} [**audio** | **video**] **Example:** `Router(config-dial-peer)# no acc-qos controlled-load`	Removes any value configured for the **acc-qos** command. • ◦ **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** {**controlled-load** | **guaranteed-delay**} [**audio** | **video**] [**bandwidth** [**default** *bandwidth-value*] [**max** *bandwidth-value*]] **Example:** `Router(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 the **acc-qos controlled-load** command in the previous step, then use the **req-qos controlled-load** command here.
Step 6	**exit** **Example:** `Router(config-dial-peer)# exit`	Exits dial peer voice configuration mode and returns to global configuration mode.
Step 7	**interface** *type* **slot/port** **Example:** `Router(config)# interface FastEthernet 0/1`	Configures an interface type and enters interface configuration mode.

	Command or Action	Purpose
Step 8	**ip rsvp bandwidth** [*reservable-bw* [*max-reservable-bw*] [**sub-pool** *reservable-bw*]] **Example:** `Router(config-if)# ip rsvp bandwidth 10000 100000`	Enables RSVP for IP on an interface.
Step 9	**exit** **Example:** `Router(config-if)# exit`	Exits interface 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:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**dial-peer voice** *tag* **voip** **Example:** `Router(config)# dial-peer 77 voip`	Enters dial peer voice configuration mode.
Step 4	**acc-qos** {**best-effort** | **controlled-load** | **guaranteed-delay**} [**audio** | **video**] **Example:** `Router(config-dial-peer)# acc-qos best-effort`	Configures mandatory RSVP on the dial-peer. • ◦ **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:** `Router(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:** `Router(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:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**dial-peer voice** *tag* **voip** **Example:** `Router(config)# dial-peer voice 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:** `Router(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. • ◦ **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).
Step 5	**end** **Example:** `Router(config-dial-peer)# end`	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:** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**dial-peer voice** *tag* **voip** **Example:** `Router(config)# dial-peer voice 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:** `Router(config-dial-peer)# ip qos dscp af11 media rsvp-pass`	Configures DSCP values based on RSVP status. • ◦ **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:** `Router(config-dial-peer)# end`	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:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**dial-peer voice** *tag* **voip** **Example:** `Router(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:** `Router(config-dial-peer)# ip qos policy-locator voice`	Configures a QoS policy locator (application ID) used to deploy RSVP policies for specifying bandwidth reservations on Cisco IOS Session Initiation Protocol (SIP) devices.
Step 5	**end** **Example:** `Router(config-dial-peer)# end`	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:** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**dial-peer voice** *tag* **voip** **Example:** `Router(config)# dial-peer voice 66 voip`	Enters dial peer voice configuration mode.
Step 4	**ip qos defending-priority** *defending-pri-value* **Example:** `Router(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:** `Router(config-dial-peer)# ip qos preemption-priority 75`	Configures the RSVP preemption priority value for determining QoS.
Step 6	**end** **Example:** `Router(config-dial-peer)# end`	Exits dial peer configuration mode and returns to privileged EXEC mode.

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

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

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

Verifying Support for Interworking Between RSVP Capable and RSVP Incapable Networks

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

SUMMARY STEPS

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

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**show sip-ua calls** **Example:** `Router# show sip-ua calls`	(Optional) Displays active user agent client (UAC) and user agent server (UAS) information on SIP calls.
Step 3	**show ip rsvp installed** **Example:** `Router# show ip rsvp installed`	(Optional) Displays RSVP-related installed filters and corresponding bandwidth information.
Step 4	**show ip rsvp reservation** **Example:** `Router# 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:** `Router# show ip rsvp interface detail GigabitEthernet 0/0`	(Optional) Displays the interface configuration for hello.
Step 6	**show sccp connections details** **Example:** `Router# show sccp connections details`	(Optional) Displays SCCP connection details, such as call-leg details.
Step 7	**show sccp connections rsvp** **Example:** `Router# show sccp connections rsvp`	(Optional) Displays information about active SCCP connections that are using RSVP.
Step 8	**show sccp connections internal** **Example:** `Router# show sccp connections internal`	(Optional) Displays the internal SCCP details, such as time-stamp values.

Command or Action	Purpose
Step 9 **show sccp** [**all** | **connections** | **statistics**] **Example:** `Router# show sccp statistics`	(Optional) Displays SCCP information, such as administrative and operational status.

Feature Information for Configuring Support 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.

ISR Feature table entry

Table 38 Feature Information for Interworking Between RSVP Capable and RSVP Incapable Networks

Feature Name	Releases	Feature Information
Interworking Between RSVP Capable and RSVP Incapable Networks	15.0(1)XA 15.1(3)T	The Support for Interworking Between RSVP Capable and RSVP Incapable Networks feature provides precondition-based RSVP support for basic audio call and supplementary services on the Cisco UBE. Support for Configuring EO-EO, DO-DO and DO-EO support on dial peer was introduced in 15.1(3)T. 15.1(3)T--Configuring EO-EO, DO-DO and DO-EO support on dial peer.

ASR Feature table entry

Table 39 Feature Information for Interworking Between RSVP Capable and RSVP Incapable Networks

Feature Name	Releases	Feature Information
Interworking Between RSVP Capable and RSVP Incapable Networks	TBD	The Support for Interworking Between RSVP Capable and RSVP Incapable Networks feature provides precondition-based RSVP support for basic audio call and supplementary services on the Cisco UBE.

VoIP for IPv6

VoIPv6 adds IPv6 capability to existing VoIP features. VoIPv6 requires IPv6 and IPv4 dual-stack support on voice gateways and MTP, IPv6 support for SIP trunks, and SCCP-controlled analog voice phones. In addition, 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.

Finding Feature Information

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

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

Prerequisites

Listing the minimum SW release is required. Use the following wording:

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 VoIP for IPv6

To enable this feature, see the " Implementing VoIP for IPv6" section in the *Cisco IOS IPv6 Configuration Guide, Release 15.0*.

Detailed command information for the VoIP for IPv6 commands is located in the *Cisco IOS IPv6 Command Reference*.

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 40 Feature Information for VoIP for IPv6

Feature Name	Releases	Feature Information
VoIP for IPv6	12.4(22)T	VoIPv6 adds IPv6 capability to existing VoIP features. 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.

Table 41 Feature Information for VoIP for IPv6

Feature Name	Releases	Feature Information
VoIP for IPv6	Cisco IOS XE Release 3.3S	VoIPv6 adds IPv6 capability to existing VoIP features. 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.

Support for Software Media Termination Point

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

Finding Feature Information

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

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

Information About Support for Software Media Termination Point

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

How to Configure Support for Software Media Termination Point

Prerequisites

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

Cisco Unified Border Element (Enterprise)

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

Restrictions

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

Configuring Support for Software Media Termination Point

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**sccp local** *interface-type interface-number* [**port** *port-number*] **Example:** `Router(config)# sccp local gigabitethernet0/0/0`	Selects the local interface that SCCP applications (transcoding and conferencing) use to register with Cisco UCM. • *interface type* --Can be an interface address or a virtual-interface address such as Ethernet. • *interface number* --Interface number that the SCCP application uses to register with Cisco UCM. • (Optional) **port** *port-number*--Port number used by the selected interface. Range is 1025 to 65535. Default is 2000.
Step 4	**sccp ccm** {*ipv4-address* | *ipv6-address* | *dns*} **identifier** *identifier-number* [**port** *port-number*] **version** *version-number* **Example:** `Router(config)# sccp ccm 10.1.1.1 identifier 1 version 7.0+`	Adds a Cisco UCM server to the list of available servers and sets the following parameters: • *ipv4-address* --IP version 4 address of the Cisco UCM server. • *ipv6-address* --IP version 6 address of the Cisco UCM server. • *dns* --DNS name. • **identifier** --Specifies the number that identifies the Cisco UCM server. Range is 1 to 65535. • **port** *port-number* (Optional)--Specifies the TCP port number. Range is 1025 to 65535. Default is 2000. • **version** *version-number* --Cisco UCM version. Valid versions are 3.0, 3.1, 3.2, 3.3, 4.0, 4.1, 5.0.1, 6.0, and 7.0+. There is no default value.
Step 5	**sccp** **Example:** `Router(config)# sccp`	Enables the Skinny Client Control Protocol (SCCP) and its related applications (transcoding and conferencing).

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

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

- Examples, page 199
- Troubleshooting Tips, page 199

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 42 Feature Information for Support for Software Media Termination Point

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

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

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

Prerequisites

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 43 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 44 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**.

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

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

Prerequisites for 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 45 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 46 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**.

Additional References

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

Related Documents

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

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

Standards

Standard	Title
ITU-T G.711	--

MIBs

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

RFCs

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

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

Technical Assistance

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

Glossary

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

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

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

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

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

CLI --command-line interface.

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

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

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

dial peer --An addressable call endpoint.

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

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

DSP --Digital Signal Processor.

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

EFXS --IP phone virtual voice ports.

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

FXS --analog telephone voice ports.

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

H.323 --An International Telecommunication Union (ITU-T) standard that describes packet-based video, audio, and data conferencing. H.323 is an umbrella standard that describes the architecture of the

conferencing system and refers to a set of other standards (H.245, H.225.0, and Q.931) to describe its actual protocol.

iLBC --internet Low Bitrate Codec.

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

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

ISDN --Integrated Services Digital Network.

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

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

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

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

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

PER --Packed Encoding Rule.

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

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

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

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

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

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

RFC --Request For Comments.

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

SCCP --Skinny Client Control Protocol.

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

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

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

session interval --The largest amount of time that can occur between INVITE requests in a call before a call is timed out. The session interval is conveyed in the Session-Expires header. The UAS obtains this

value from the Session-Expires header of a 2*xx* INVITE response that it sends. Proxies and UACs determine this value from the Session-Expires header in a 2*xx* INVITE response they receive.

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

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

SPI --service provider interface.

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

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

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

TDM --time-division multiplexing.

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

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

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

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

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

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

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

VFC --Voice Feature Card.

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