H.323-to-SIP Connections on a Cisco Unified Border Element

Revised: October 27, 2009,
First Published: June 19, 2006
Last Updated: October 27, 2009

This chapter describes how to configure and enable features for H.323-to-SIP connections in a Cisco Unified Border Element topology.

Activation

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.

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 "Cisco Unified Border Element Features Roadmap" section on page 1.

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

For more information about Cisco IOS voice features, see the entire Cisco IOS Voice Configuration Library—including feature documents, and troubleshooting information—at http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124tcg/vcl.htm.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Contents

Prerequisites for Configuring H.323-to-SIP Connection on a Cisco Unified Border Element

- Perform the prerequisites listed in the "Prerequisites for Cisco Unified Border Element Configuration" section on page 20 in this guide.
- Perform fundamental gateway configuration listed in the "Prerequisites for Fundamental Cisco Unified Border Element Configuration" section on page 44 in this guide.
- Perform basic H.323 gateway configuration.
- Perform basic H.323 gatekeeper configuration.

Note For configuration instructions, see the "Configuring H.323 Gateways" and "Configuring H.323 Gatekeepers" chapters of the *Cisco IOS Voice, Video, and Fax Configuration Guide*, Release 12.2.

Restrictions for H.323-to-SIP Connections on a Cisco Unified Border Element

- Changing codecs during rotary dial peer selection is not supported.
- Codec preference order in voice class should be the same in all dial peers.
- Configure extended capabilities on dial peers for fast start-to-early media scenarios.
- Delayed Offer to Slow-Start is not supported for SRTP-to-SRTP H.323-to-SIP calls.
- During a triggered INVITE scenario the Cisco UBE always generates a delayed offer INVITE.
- Fast-start to delayed-media signal interworking is not supported.
- Fast Start to Early Offer Supplementary Service will not work without extended capabilities configured under dial-peer.
- GSMFR and GSMEFR codecs are not supported.
- H450.2 & H450.3 are enabled & invisible under dial peers by default. H.450 cannot be enabled at the dial peer level if they are globally disabled.

- Media flow-around is not supported.
- Passing multiple diversion headers or multiple contact header in 302 to the H.323 leg is not supported.
- RSVP for supplementary scenarios is not supported.
- Session refresh is not supported.
- SIP-to-H.323 Supplementary Services based on H.450 is not supported.
- Slow-start to early media signal interworking is not supported.
- Supplementary services are Empty Capability Set (ECS) based supplementary services from the H.323 perspective, not H.450 supplementary services.
- Transcoding for supplementary calls is not supported.
- DTMF Interworking rtp-nte to out of band is not supported when high density transcoder is enabled. Use normal transcoding for rtp-nte to out of band DTMF interworking.

Cisco IOS Release 12.4(15)XY and earlier releases:

- SRTP Passthrough is not supported.

Cisco IOS Release 12.4(11)XJ2 and earlier releases:

- Delayed-media to slow-start signal interworking is not supported.
- H323-SIP Supplementary Services is not supported (ECS based).

Cisco IOS Release 12.4(11)T and earlier releases:

- Codec Transparent is not supported.

Cisco IOS Release 12.4(2)T and earlier releases:

- Extended codec support and codec filtering is not supported.

Cisco IOS Release 12.3(8)T and earlier releases:

- Basic call is not supported.

Information About H.323-to-SIP Connections on a Cisco Unified Border Element

- All codecs using static payload are supported.
- Fast-start to early media signal interworking is supported.
- H.323-to-SIP Supplementary Services are supported in Cisco IOS Release12.4(15)XY and later.
- Supported codecs using dynamic payload are g726r16 and g726r24.
- Slow-start to delayed-media signal interworking is supported.
- One or multiple codes may configured on the incoming and out-going dial-peer.
- SRTP-to-SRTP for SIP-to-H.323 calls is supported:
  - Supported signal interworking include: Fast-Start to Early Offer, Early Offer to Fast-Start, and Slow-Start to Delayed Offer.

How to Configure H.323-to-SIP Connections on a Cisco Unified Border Element

The section contains the following tasks:

H.323-to-SIP Basic Call Interworking for Session Border Controller (SBC)

This feature enables the IP-to-IP gateway to bridge calls between networks that support different VoIP call-signaling protocols (SIP and H.323). The SIP-to-H.323 protocol interworking capabilities of the Cisco Unified Border Element support the following:

- Basic voice calls (G.711 and G.729 codecs)
- UDP and TCP transport
- Interworking between H.323 Fast-Start and SIP early-media signaling
- Interworking between H.323 Slow-Start and SIP delayed-media signaling
- DTMF relay interworking:
  - H.245 alpha/signal <--> SIP RFC 2833
  - H.245 alpha/signal <--> SIP Notify
- Codec transcoding (G.711-G.729)
- Calling/called name and number
- T.38 fax relay and Cisco fax relay
- RADIUS call-accounting records
- RSVP synchronized with call signaling
- TCL IVR 2.0 for SIP, including media playout and digit collection (RFC 2833 DTMF relay)

H.323-to-SIP Supplementary Feature Interworking for Session Border Controller (SBC)

Provides enhanced termination and re-origination of signaling and media between VoIP and Video Networks in conformance with RFC3261. New features offered in this release on the Cisco 28xx, 38xx, 5350XM and 5400XM include:

- Support H.323-to-SIP Supplementary services for Cisco Unified Communications Manager with MTP on the H.323 Trunk.
- ILBC Codec Support
- Interworking between G.711 inband DTMF to RFC2833
- VXML 3.x support
- VXML support with SIP Notify

Restrictions

- H450.2 & H450.3 are enabled & invisible under dial peers by default. H.450 cannot be enabled at the dial peer level if they are globally disabled.
- RSVP for supplementary scenarios is not supported.
- Transcoding for supplementary calls is not supported.

H.323-to-SIP Supplementary Service Enhancements for Session Border Controller (SBC)

H.323-to-SIP features offered in this release include:

- Mapping ECS to ReINVITE and ECS to REFER on the Cisco IOS SBC.

Configuring H.323-to-SIP Connections on a Cisco Unified Border Element

To configure H.323-to-SIP connections on a Cisco Unified Border Element. perform the steps in this section.

Restrictions

Connections are disabled by default in Cisco IOS images that support the Cisco Unified Border Element

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **allow-connections**
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 VoIP voice-service configuration mode.
Step 4	**`allow-connections`** *`from-type`* **`to`** *`to-type`* **Example:** `Router(conf-voi-serv)# allow-connections h323 to sip`	Allows connections between specific types of endpoints in an Cisco Unified Border Element. Arguments are as follows: • *from-type*—Type of connection. Valid values: **h323**, **sip**. • *to-type*—Type of connection. Valid values: **h323**, **sip**. **Note** H.323-to-H.323: By default, H.323-to-H.323 connections are disabled and POTS-to-any and any-to-POTS connections are enabled.
Step 5	**`exit`** **Example:** `Router(conf-voi-serv)# exit`	Exits the current mode.

Configuring DTMF Relay Digit-Drop on a Cisco Unified Border Element

To avoid sending both in-band and out-of band tones to the outgoing leg when sending Cisco Unified Border Element calls in-band (rtp-nte) to out-of band (h245-alphanumeric). Configure the **dtmf-relay rtp-nte digit-drop** command on the incoming SIP dial-peer. On the H.323 side configure either **dtmf-relay h245-alphanumeric** or **dtmf-relay h245-signal**. This may also be used for H.323-to-SIP calls.

To configure DTMF relay digit drop on an Cisco Unified Border Element, perform the steps in this section.

Restrictions

The debug output will show that the H245 out of band messages are sent to the TGW. However, the digits are not heard on the phone.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice tag voip**
4. **dtmf-relay** [**cisco-rtp**] [**h245-alphanumeric**] [**rtp-nte** [**digit-drop**]]
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** *number* **voip** **Example:** `Router(config)# dial-peer voice 2 voip`	Enters dial-peer configuration mode for the specified VoIP dial peer.
Step 4	**dtmf-relay** [**cisco-rtp**] [**h245-alphanumeric**] [**rtp-nte** [**digit-drop**]] **Example:** `Router (config-dial-peer)# dtmf-relay rtp-nte digit-drop h245-alphanumeric`	Forwards DTMF tones. Keywords are as follows: • **cisco-rtp**—Forwards DTMF tones by using RTP with a Cisco-proprietary payload type. • **h245-alphanumeric**—Forwards DTMF tones by using the H.245 alphanumeric method. • **h245-signal**—Forwards DTMF tones by using the H.245 signal UII method. • **rtp-nte**—Forwards DTMF tones by using Real-Time Transport Protocol (RTP) with the Named Telephone Event (NTE) payload type. • **digit-drop**—Passes digits out-of-band, and in-band digits are dropped. **Note** The **digit-drop** keyword is only seen went the **rtp-nte** keyword is configured.
Step 5	**exit** **Example:** `Router(config-dial-peer)# exit`	Exits the current mode.

Examples

The following example shows DTMF-Relay digits configured to avoid sending both in-band and out-of-band tones to the outgoing leg in an Cisco Unified Border Element:

```
.
.
.
dial-peer voice 1 voip
 voice-class codec 2
 dtmf-relay rtp-nte digit-drop h245-alphanumeric
.
.
.
```

Configuring H.323-to-SIP Call Failure Recovery (Rotary) on a Cisco Unified Border Element

Call failure recovery (Rotary) on the Cisco Unified Border Element eliminates the need for identical codec capabilities for all dial peers in the rotary group, and allows the Cisco Unified Border Element to restart the codec negotiation end-to-end. Call failure recovery will continue until “voice hunt stop” is reached.

To configure H.323-to-SIP call failure recovery (rotary) on an Cisco Unified Border Element, perform the steps in this section.

Restrictions

If extended caps (DTMF or T.38) are configured on the outgoing gateway or the trunking gateway, extended caps must be configured in both places.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **h323**
5. **emptycapability**
6. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`configure terminal`
	
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

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

Step 4	`h323`
	
	Example:
	`Router(conf-voi-serv)# h323`
		Enters H.323 voice-service configuration mode.

Step 5	`emptycapability`
	
	Example:
	`Router(conf-serv-h323)# emptycapability`
		Enables call failure recovery (TCS=0).

Step 6	`exit`
	
	Example:
	`Router(conf-serv-h323)# exit`
		Exits the current mode.

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 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.

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" section on page 138.

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.

	Command or Action	Purpose
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.

	Command or Action	Purpose
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.
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** command using 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.
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).
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** `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 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.
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`	(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** 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 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.

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.

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

Managing H.323 IP Group Call Capacities

The Cisco Unified Border Element feature works with the **voice source-group** command to provide matching criteria for incoming calls. The **voice source-group** command assigns a name to a set of source IP group characteristics. The terminating gateway uses these characteristics to identify and translate the incoming VoIP call. If there is no voice source group match, the default carrier ID is used, any source carrier ID on the incoming message is transmitted without change, and no destination carrier is available. Call-capacity information is reported to the gatekeeper, but carrier routing information is not.

If the voice source group matches, the matched source carrier ID is used and the target carrier ID defined in the voice source group is used for the destination carrier ID.

To configure H.323 IP call capabilities, perform the steps in this section.

Restrictions

You can use the commands that follow only when no calls are active. If you try to use these commands with active calls present, the commands are rejected.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **h323**
5. **ip circuit max-calls**
6. **ip circuit carrier-id**
7. **ip circuit default only**
8. **ip circuit default name**
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 VoIP voice-service configuration mode.
Step 4	**h323** **Example:** `Router(config-voice-service)# h323`	Enters H.323 voice-service configuration mode.
Step 5	**ip circuit carrier-id** *carrier-name* [**reserved-calls** *reserved*] **Example:** `Router(config-serv-h323)# ip circuit carrier-id AA reserved-calls 500`	(Optional) Defines an IP circuit using the specified name as the circuit ID. **Note** The **reserved** keyword for this command is optional. Using this keyword creates a specified maximum number of calls for that circuit ID. The default value is 200 call legs.

	Command or Action	Purpose
Step 6	**ip circuit default only** **Example:** `Router(config-serv-h323)# ip circuit default only`	(Optional) Creates a single carrier to use all of the call capacity available to the Cisco Unified Border Element. **Note** If you use the **ip circuit default only** command, you cannot use the **ip circuit carrier-id** command to configure more circuits. Using the **ip circuit default only** command creates a single carrier using the default carrier name.
Step 7	**ip circuit default name** *carrier-name* **Example:** `Router(config-serv-h323)# ip circuit default name AA`	(Optional) Changes the default circuit name.
Step 8	**exit** **Example:** `Router(config-serv-h323)# exit`	Exits the current mode.

Examples

The following examples show a default carrier with no voice source group configured:

Default Carrier with No Voice Source Group

```
voice service voip
 allow-connections h323 to h323
 h323
  ip circuit max-calls 1000
  ip circuit default only
```

If there is no incoming source carrier ID:

- Capacity only is reported to the gatekeeper using the default circuit (two call legs).
- No source or destination carrier information is reported.

If there is an incoming source carrier ID:

- Two call legs are counted against the default circuit and reported to the GK.
- The source carrier ID is passed through the gateway to the terminating leg.

The following examples show a configuration with more reserved calls than the default value for the **max-calls** argument (1000):

Configuration with Default Calls in Excess of 1000

This example assigns 1100 calls to other carriers, leaving 400 calls available to the default carrier:

```
voice service voip
 allow-connections h323 to h323
 h323
  ip circuit max-calls 1000
  ip circuit carrier-id AA reserved-calls 500
  ip circuit carrier-id bb reserved-calls 500
  ip circuit carrier-id cc reserved-calls 100
```

The following examples show the default carrier configured with an incoming source carrier but no voice source group configured.

Note In this example, 800 call legs are implicitly reserved for the default circuit.

Default Carrier and Incoming Source Carrier with No Voice Source Group

Note A gatekeeper is required with carrier-id routing.

```
voice service voip
 allow-connections h323 to h323
 h323
  ip circuit max-calls 1000
  ip circuit carrier-id AA reserved-calls 200
```

If there is no incoming source carrier ID:

- Capacity only is reported to the GK using the default circuit (two call legs).
- No source or destination carrier information is reported.

If there is an incoming source carrier ID called “AA”:

- One call leg is counted against circuit “AA”.
- One call leg (outbound) is counted against the default circuit.
- The source carrier ID is passed through the gateway to the terminating leg.

If there is an incoming source carrier ID called “BB” (for example) or anything other than “AA”:

- Two call legs are counted against the default circuit.
- The source carrier ID “BB” is passed through the gateway to the terminating leg.

The following examples show the first voice source-group match case:

Voice Source-Group Match Case 1

```
voice service voip
 allow-connections h323 to h323
 h323
  ip circuit max-calls 1000
  ip circuit carrier-id AA reserved-calls 200
!
voice source-group 1
 carrier-id source AA
 carrier-id target AA
```

If there is no incoming source carrier ID, the default circuit is used because there is no match in the voice source group.

If there is an incoming source carrier ID called “AA,” the following are in effect:

- The voice source group matches.
- Both call legs are counted against circuit “AA”.
- The source carrier ID is passed through the gateway to the terminating leg.
- The destination carrier ID is “AA”.

The following examples show the second voice source group match case:

Voice Source-Group Match Case 2

```
voice service voip
 allow-connections h323 to h323
 h323
  ip circuit max-calls 1000
  ip circuit carrier-id AA reserved-calls 200
  ip circuit carrier-id BB reserved-calls 200
!
voice source-group 1
 carrier-id source AA
 carrier-id target BB
```

If there is no incoming source carrier ID, the default circuit is used because there is no match in the voice source group.

If there is an incoming source carrier ID called "AA":

- The voice source-group matches.
- One leg is counted against circuit "AA".
- One leg is counted against circuit "BB".
- The source carrier ID is passed through the gateway to the terminating leg.
- The destination carrier ID is "BB".

The following examples show the third voice source-group match case:

Voice Source-Group Match Case 3

```
voice service voip
 allow-connections h323 to h323
 h323
  ip circuit max-calls 1000
  ip circuit carrier-id AA reserved-calls 200
  ip circuit carrier-id BB reserved-calls 200
!
voice source-group 1
 access-list 1
 carrier-id source BB
```

If the access-list matches, the following apply:

- One leg is counted against circuit "BB".
- One leg is counted against the default circuit (for the destination circuit).
- The source carrier ID is synthesized to "BB" and used to report to the gatekeeper. It is also used on the outgoing setup.
- If a source carrier ID is received on the incoming setup, it is overridden with the synthesized carrier ID.

Troubleshooting and Verifying H.323-to-SIP connections on a Cisco Unified Border Element

To troubleshoot or verify connections in an Cisco Unified Border Element, perform the steps in this section. This section contains the following subsections:

- Troubleshooting Tips, page 152
- Verifying Cisco Unified Border Element Configuration and Operation, page 152

Troubleshooting Tips

Caution Under moderate traffic loads, these **debug** commands produce a high volume of output.

- Use the **debug voip ipipgw** command to debug the Cisco Unified Border Element feature.
- Use any of the following additional **debug** commands on the gateway as appropriate:
  - **debug cch323 all**
  - **debug ccsip all**
  - **debug h225 asn1**
  - **debug h225 events**
  - **debug h245 asn1**
  - **debug h245 events**
  - **debug voip ipipgw**
  - **debug voip ccapi inout**

Note For examples of **show** and **debug** command output and details on interpreting the output, see the following resources:

- Cisco IOS Debug Command Reference, Release 12.4T
- *Cisco IOS Voice Troubleshooting and Monitoring Guide*
- *Troubleshooting and Debugging VoIP Call Basics*
- *Voice Gateway Error Decoder for Cisco IOS*
- *VoIP Debug Commands*

Verifying Cisco Unified Border Element Configuration and Operation

To verify Cisco Unified Border Element IP-to-IP feature configuration and operation, perform the following steps (listed alphabetically) as appropriate.

Note The word "calls" refers to call legs in some commands and output.

SUMMARY STEPS

1. **show call active video**
2. **show call active voice**
3. **show call history fax**
4. **show call history video**
5. **show call history voice**
6. **show crm**
7. **show dial-peer voice**

8. **show running-config**
9. **show voip rtp connections**

DETAILED STEPS

Step 1 **show call active video**

Use this command to display the active video H.323 call legs.

Step 2 **show call active voice**

Use this command to display call information for voice calls that are in progress.

Step 3 **show call active fax**

Use this command to display the fax transmissions that are in progress.

Step 4 **show call history video**

Use this command to display the history of video H.323 call legs.

Step 5 **show call history voice**

Use this command to display the history of voice call legs.

Step 6 **show call history fax**

Use this command to display the call history table for fax transmissions that are in progress.

Step 7 **show crm**

Use this command to display the carrier ID list or IP circuit utilization.

Step 8 **show dial-peer voice**

Use this command to display information about voice dial peers.

Step 9 **show running-config**

Use this command to verify which H.323-to-H.323, H.323-to-SIP, or SIP-to-SIP connection types are supported.

Step 10 **show voip rtp connections**

Use this command to display active Real-Time Transport Protocol (RTP) connections.

Where to Go Next

- H.323-to-H.323 Connections on a Cisco Unified Border Element
- SIP-to-SIP Connections on a Cisco Unified Border Element
- Cisco Unified Border Element for H.323 Cisco Unified Communications Manager to H.323 Service Provider Connectivity
- Configuring Cisco Unified Border Element Videoconferencing

Additional References

The following sections provide references related to H.323-to-SIP IP-to-IP Gateway Connections

The following sections provide additional references related to the Cisco UBE Configuration Guide.

Note

- In addition to the references listed below, each chapter provides additional references related to Cisco Unified Border Element.
- Some of the products and services mentioned in this guide may have reached end of life, end of sale, or both. Details are available at http://www.cisco.com/en/US/products/prod_end_of_life.html.
- The preface and glossary for the entire voice-configuration library suite of documents is listed below.

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 12.4	• Cisco IOS Release 12.4 Configuration Guides • Cisco IOS Release 12.4T Configuration Guides
Cisco IOS Release 12.3	• Cisco IOS Release 12.3 documentation • Cisco IOS Voice Troubleshooting and Monitoring Guide • Tcl IVR Version 2.0 Programming Guide
Cisco IOS Release 12.2	*Cisco IOS Voice, Video, and Fax Configuration Guide*, Release 12.2
DSP documentation	High-Density Packet Voice Feature Card for Cisco AS5350XM and AS5400XM Universal Gateways http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/vfc_dsp.html
GKTMP (GK API) Documents	• *GKTMP Command Reference*: http://www.cisco.com/en/US/docs/ios/12_2/gktmp/gktmpv4_2/gk_cli.htm • *GKTMP Messages*: http://www.cisco.com/en/US/docs/ios/12_2/gktmp/gktmpv4_2/gk_tmp.html

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
Cisco Unified Border Element Configuration Examples	• Local-to-remote network using the IPIPGW http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a00801b0803.shtml • Remote-to-local network using the IPIPGW: http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a0080203edc.shtml • Remote-to-remote network using the IPIPGW: http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a0080203edd.shtml • Remote-to-remote network using two IPIPGWs: http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a0080203edb.shtml
Related Application Guides	• Cisco Unified Communications Manager and Cisco IOS Interoperability Guide • Cisco IOS Fax, Modem, and Text Support over IP Configuration Guide • “Configuring T.38 Fax Relay” chapter • Cisco IOS SIP Configuration Guide • Cisco Unified Communications Manager (CallManager) Programming Guides • Quality of Service for Voice over IP
Related Platform Documents	• Cisco 2600 Series Multiservice Platforms • Cisco 2800 Series Integrated Services Routers • Cisco 3600 Series Multiservice Platforms • Cisco 3700 Series Multiservice Access Routers • Cisco 3800 Series Integrated Services Routers • Cisco 7200 Series Routers • Cisco 7301
Related gateway configuration documentation	Media and Signaling Authentication and Encryption Feature for Cisco IOS H.323 Gateways. http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/htsecure.htm

Related Topic	Document Title
Cisco IOS NAT Configuration Guide, Release 12.4T	*Configuring Cisco IOS Hosted NAT Traversal for Session Border Controller* http://www.cisco.com/en/US/docs/ios/12_4t/ip_addr/configuration/guide/htnatsbc.html
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
H.323 Version 4 and earlier	*H.323 (ITU-T VOIP protocols)*
H.323 - H.245 Version 12, Annex R	*H.323 (ITU-T VOIP protocols)*

MIBs

MIB	MIBs Link
• CISCO-DSP-MGMT-MIB • CISCO-VOICE-DIAL-CONTROL-MIB • IP-TAP-MIB • TAP2-MIB • USER-CONNECTION-TAP-MIB	To locate and download MIBs for selected platforms, Cisco IOS 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 2833	*RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*
RFC 3203	*DHCP reconfigure extension*
RFC 3261	*SIP: Session Initiation Protocol*

RFC	Title
RFC 3262	*Reliability of Provisional Responses in Session Initiation Protocol (SIP)*
RFC 3323	*A Privacy Mechanism for the Session Initiation Protocol (SIP)*
RFC 3325	*Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks*
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

Feature Information for H.323-to-SIP Connections on a Cisco Unified Border Element

Table 1lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.3(1) or a later release appear in the table.

For information on a feature in this technology that is not documented here, see the "Cisco Unified Border Element Features Roadmap."

Note Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for H.323-to-SIP Connections on a Cisco Unified Border Element

Feature Name	Releases	Feature Information
Accounting	12.3(11)T	RADIUS call-accounting records, calling/called name and number.
Call Admission Control	12.3(11)T	RSVP synchronized with call signaling.
Cisco Unified Communications Manager Connections	12.4(6)XE	H.323-to-SIP Supplementary services for Cisco Unified Communications Manager with MTP on the H.323 Trunk
Cisco UBE MIB support	15.0(1)XA	This feature was introduced.
Codec Support	12.4(11)T	iLBC Codec Support
Codec Transcoding	12.3(11)T	Codec transcoding (G.711-G.729)—This feature enables the IP-to-IP gateway to bridge calls between networks that support different VoIP call-signaling protocols (SIP and H.323)
DTMF	12.3(11)T 12.4(6)XE	12.3(11)T—DTMF relay • H.245 alpha/signal <--> SIP RFC 2833 • H.245 alpha/signal <--> SIP Notify 12.4(6)XE—G.711 Inband DTMF to RFC 2833
Fax/Modem	12.3(11)T	T.38 fax relay and Cisco fax relay
Interworking Between RSVP Capable and RSVP Incapable Networks	15.0(1)XA	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. The following section provides information about this feature: • Configuring Support for Interworking Between RSVP Capable and RSVP Incapable Networks
Managing H.323 IP Group Call Capacities	12.2(13)T	Creates a maximum capacity for the IP group providing extra control for load and resource balancing.

Table 1 Feature Information for H.323-to-SIP Connections on a Cisco Unified Border Element (continued)

Feature Name	Releases	Feature Information
Mapping ECS to ReINVITE and ECS to REFER on the Cisco IOS SBC.	12.4(20)T	H.323-to-SIP Supplementary Service Enhancements for Session Border Controller (SBC)
Media Modes	12.3(1)	Media flow-around capability on the IP-to-IP gateway by supporting the processing of call set-up and teardown request (VoIP call signaling) and for media streams (flow-through and flow-around)
Rotary Support	12.3(11)T	H.323-to-H.323 Call Failure Recovery (Rotary) on a Cisco Unified Border Element. Eliminates codec restrictions and enables the Cisco UBE to restart codec negotiation with the originating endpoint based on the codec capabilities of the next dial peer in the rotary group for H.323-to-H.323 interconnections.
Signaling Interworking	12.3(11)T 12.4(4)T	12.3(11)T—This feature enables SIP-to-H.323 protocol interworking capabilities of the Cisco Unified Border Element: • Interworking between H.323 Fast-Start and SIP early-media signaling • Interworking between H.323 Slow-Start and SIP delayed-media signaling 12.4(4)T—Extended SIP-to-H.323 Call Interworking for Session Border Controller (SBC)
TCL IVR	12.3(11)T 12.4(11)T	12.3(11)T—TCL IVR 2.0 for SIP, including media playout and digit collection (RFC 2833 DTMF relay) 12.4(11)T —TCL IVR support with SIP NOTIFY DTMF
Transport Protocols	12.3(11)T	UDP and TCP transport
VXML	12.4(6)XE 12.4(11)T	12.4(6)XE— • VXML 3.x support • VXML support with SIP Notify 12.4(11)T—VXML support with SIP NOTIFY DTMF