Fundamental Cisco Unified Border Element Configuration

Revised: March 19, 2010
First Published: June 19, 2006
Last Updated: March 19, 2010

This chapter describes fundamental configuration tasks required for Fundamental Cisco Unified Border Element functionality. A Cisco Unified Border Element, in this guide also called an IP-to-IP gateway (IPIPGW), border element (BE), or session border controller, facilitates connectivity between independent VoIP networks by enabling H.323 VoIP and videoconferencing calls from one IP network to another. This gateway performs most of the same functions of a PSTN-to-IP gateway, but typically joins two IP call legs, rather than a PSTN and an IP call leg.

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/en/US/docs/ios/12_3/vvf_c/cisco_ios_voice_configuration_library_glossary/vcl.htm.

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

Contents

Prerequisites for Fundamental Cisco Unified Border Element Configuration

- Perform the prerequisites listed in the "Prerequisites for Cisco Unified Border Element Configuration" section 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 Fundamental Cisco Unified Border Element Configuration

- Cisco Unified Border Elements that require the Registration, Admission, and Status (RAS) protocol must have a via-zone-enabled gatekeeper or equivalent.
- Cisco Unified Border Elements interoperate with Cisco ATA 186, Cisco ATA 188, Cisco CallManager, Cisco CallManager Express 3.1, Cisco IOS gateways, NetMeeting, and Polycom ViewStation.
- Cisco fax relay is reported as a voice call on an Cisco Unified Border Element.
- Fax calls are reported as a modem plus fax call when modem CLI are present.
- Slow-start to fast-start interworking is supported only for H.32-to-H.323 calls.
- 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.

- The transcoding process on the Cisco Unified Border Element will always drop fast-start calls down to slow-start between H.323 endpoints even when the H.323 terminating endpoints support fast-start calls.
- Cisco Unified Border Element supports T.38 fax relay (H.323 Annex D). However, endpoints configured with Named Signaling Events (NSE) may result in reduced fax transmission quality and are not supported.

Information About Cisco Unified Border Element Features

Gateway feature benefits include the following:

- Codec filtering by restricting codecs advertised on outbound call legs. For example, restriction of high-bandwidth codecs is possible on the reorigination side of the Cisco Unified Border Element outbound dial peer.
- Support for changing codecs during rotary dial peer selection.
- Network privacy by hiding the internal network structure from other administrative domains.
- Ability to create interconnections between different VoIP network types (such as SIP-to-H.323, H.323-to-SIP, and SIP-to-SIP protocol interworking).
- Better voice quality, cost and space savings (including rack density), and feature set compared with back-to-back gateways.
- Support for TDM voice.
- Support for Cisco ATA188 and third-party endpoints.
- More control of calls routed between ITSPs.

How to Configure Fundamental Cisco Unified Border Element

This section contains the following tasks:

- Configuring an Ethernet Interface, page 50
- Configuring a RTP Loopback Interface, page 51
- Configuring Codec Transparency on a Cisco Unified Border Element, page 53
- Configuring iLBC Codec on a Cisco Unified Border Element, page 56
- iSAC Codec Support on TDM-IP Voice Gateways and Cisco UBE Platforms, page 56
- SG3 Fax Support on Cisco TDM-IP Voice Gateways and Cisco UBE Platforms, page 65
- Configuring QoS for a Cisco Unified Border Element, page 74
- Configuring Cisco Unified Border Element for High Utilization, page 76
- Configuring Cisco Unified Border Element with OSP, page 79
- Media Statistics on a Cisco Unified Border Element, page 84
- Voice Quality Enhancements on Cisco Unified Border Element, page 92
- Troubleshooting and Verifying Fundamental Cisco Unified Border Element Configuration and Operation, page 104

Configuring an Ethernet Interface

You can configure the Cisco Unified Border Element feature to operate with either a single Ethernet interface for all incoming, outgoing, and via-zone gatekeeper traffic or two Ethernet interfaces for signaling and media streams (optional but highly recommended for single-interface configurations). To configure an Ethernet interface, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot*/*port*
4. **ip route-cache same-interface**
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	**`interface`** *`type slot/port`* **Example:** `Router(config)# interface fastethernet 0/1`	Selects the Ethernet interface that you want to configure.

Step 4	`ip route-cache same-interface`
	Example:
	`Router(config-if)# ip route-cache same-interface`
		Controls the use of high-speed switching caches for IP routing by enabling fast-switching packets to back out on the same interface on which they arrived.

Step 5	`exit`
	Example:
	`Router(config-if)# exit`
		Exits the current mode.

Examples

The following example shows a configuration that uses a single Ethernet interface for all traffic:

```
interface FastEthernet0/1
 ip address 10.16.8.6 255.255.0.0
 no ip redirects
 ip route-cache same-interface
 speed auto
 full-duplex
 h323-gateway voip interface
 h323-gateway voip id 7206-vgk1 ipaddr 10.16.8.71 1719
 h323-gateway voip h323-id 3660-hud1
 h323-gateway voip tech-prefix 1#
 h323_gateway voip bind srcaddr 10.16.8.6
```

Configuring a RTP Loopback Interface

The Cisco Unified Border Element supports configuration of an RTP loopback dial peer for use in verifying and troubleshooting H.323 networks. When a call encounters an RTP loopback dial peer, the gateway automatically signals call connect and loops all voice data back to the source. In contrast to normal calls through the VoIP-to-VoIP gateway, RTP loopback calls consist of only one call leg.

To configure a RTP loopback interface, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *number* **voip**
4. **incoming called-number** *string*
5. **destination-pattern** *string*
6. **codec** *codec*
7. **session target loopback:rtp**
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.

	Command or Action	Purpose
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	**incoming called-number** *string* **Example:** `Router(config-dial-peer)# incoming called-number 555.+`	Associates a prefix with the dial peer for incoming call legs. This enables a specific codec to be applied to incoming call legs.
Step 5	**destination-pattern** *string* **Example:** `Router(config-dial-peer)# destination-pattern 555.+`	Associates the called number prefix with this dial peer for outgoing call legs.
Step 6	**codec** *codec* **Example:** `Router(config-dial-peer)# codec g711ulaw`	Assigns a codec to the dial peer. **Note** The assigned codec must be supported by the incoming call. A codec preference list can be used in place of the specific codec. The specific codec will cause the IP-to-IP mode to be disabled for these calls. The transparent codec option cannot be used for RTP loopback.
Step 7	**session target loopback:rtp** **Example:** `Router(config-dial-peer)# session target loopback:rtp`	Specifies the RTP loopback option for all calls using this dial peer.
Step 8	**exit** **Example:** `Router(config-dial-peer)# exit`	Exits the current mode.

Examples

Using a Single Dial Peer on a Cisco Unified Border Element

```
Router(config)# dial-peer voice 5550199 voip
 Router(config-dial-peer)# incoming called-number 5550199
 Router(config-dial-peer)# destination-pattern 5550199
 Router(config-dial-peer)# codec g711ulaw
 Router(config-dial-peer)# session target loopback:rtp
```

Using Separate Dial Peers on a Cisco Unified Border Element

```
dial-peer voice 5550188 voip
 incoming called-number 5550188
 session target ras
 codec g711ulaw
!
dial-peer voice 5550182 voip
 destination-pattern 5550188
 session target loopback:rtp
```

Using a Codec Preference List to Support Additional Codecs

```
voice class codec 1
 codec preference 1 g711ulaw
 codec preference 2 g729r8

dial-peer voice 5429999 voip
 incoming called-number 5550199
 destination-pattern 5550199
 voice-class codec 1
 session target loopback:rtp
```

Configuring Codec Transparency on a Cisco Unified Border Element

Codec transparency enables the Cisco Unified Border Element to pass codec capabilities between endpoints. If you configure transparency, the Cisco Unified Border Element uses the codec that was specified by the endpoints for setting up a call.

To configure codec transparency on an Cisco Unified Border Element, perform the steps in this section. This section contains the following subsections:

- Configuring Codec Transparency for All Dial Peers in a Voice Class, page 53
- Configuring Codec Transparency for an Individual Dial Peer, page 54

Restrictions

- Codec transparency is only supported for H.323-to-H.323 calls.
- Codec filtering must be based on codec types; filtering based on byte size is not supported.
- Codec transparency is not supported when call start interwork is configured.
- For video calls, you must configure codec transparency in both incoming and outgoing dial peers. Codec filtering may not be possible for video calls.

Configuring Codec Transparency for All Dial Peers in a Voice Class

To configure codec transparency for all dial peers in a voice class, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice class codec** *tag*
4. **codec preference** *value codec-type*
5. **exit**
6. **dial-peer voice** *number* **voip**
7. **voice class codec** *tag*
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	**voice class codec** *tag* **Example:** `Router(config)# voice class codec 1`	Enters voice-class configuration mode for the specified codec voice class.
Step 4	**codec preference** *value codec-type* **Example:** `Router(config-class)# codec preference 1 transparent`	Specifies a list of preferred codecs to use on a dial peer. In this case, specifies that the transparent codec (1 transparent) is to be used so that codec capabilities are passed transparently between endpoints.
Step 5	**exit** **Example:** `Router(config-class)# exit`	Exits the current mode.
Step 6	**dial-peer voice** *number* **voip** **Example:** `Router(config)# dial-peer voice 1 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 1`	Assigns the previously configured codec-selection preference list (codec voice class) to the specified voice class. The tag number maps to the tag number created by means of the **voice class codec** command.
Step 8	**exit** **Example:** `Router(config-dial-peer)# exit`	Exits the current mode.

Configuring Codec Transparency for an Individual Dial Peer

To configure codec transparency for an individual dial peer, perform the steps in this section.

Restrictions

If you plan to configure both incoming and outgoing dial peers, you must specify the transparent codec on the incoming dial peer.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *number* **voip**
4. **codec** *codec-type*
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**dial-peer voice** *number* **voip** **Example:** `Router(config)# dial-peer voice 2 voip`	Enters dial-peer configuration mode for the specified VoIP dial peer.
Step 4	**codec** *codec-type* **Example:** `Router(config-dial-peer)# codec transparent`	Specifies the transparent codec for this dial peer.
Step 5	**exit** **Example:** `Router(config-dial-peer)# exit`	Exits the current mode.

Examples

The following example shows an inbound and outbound dial peer on the same tag in which the inbound dial peer is configured with the transparent codec, and the outbound dial peer is configured with the filter codec:

```
dial-peer voice 1 voip
   incoming called-number .T
   destination-pattern .T
   session target ras
   codec transparent
```

The following example shows separate tags for the inbound and outbound dial peers:

```
dial-peer voice 1 voip
   destination-pattern .T
   session target ras
   codec transparent
```

```
dial-peer voice 2 voip
   incoming called-number .T
   codec transparent
destination-pattern .T
session target ras
```

The following example shows filtering of high-bandwidth codecs applied to dial peer 1. With this configuration, codecs other than those specified are disallowed.

```
voice class codec 1
codec preference 1 g729br8
codec preference 2 g723r53
codec preference 3 g723r68

dial-peer voice 1 voip
voice-class codec 1
```

The following shows a different filtering configuration. With this configuration, codecs other than g729r8 are disallowed.

```
dial-peer voice 1 voip
   destination-pattern .T
   session target ras
```

Configuring iLBC Codec on a Cisco Unified Border Element

The internet Low Bitrate Codec (iLBC) is a standard, high-complexity speech codec that is suitable for robust voice communication over IP. iLBC has built-in error correction functionality that helps the codec perform in networks with a high-packet loss.

Note H.323-to-SIP calls, the iLBC codec configuration must be the same across all the call legs in the call. i.e. originating gateway, Cisco Unified Border Element(s) and terminating gateway.

Additional information and configuration of the iLBC code on an Cisco Unified Border Element can be found at the following links:

- Codecs section of the Dial Peer Configuration on Voice Gateway Routers Guide

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/int_c/dpeer_c/dp_ovrvw.htm#1035124

- Dial Peer Features and Configuration section of the Dial Peer Configuration on Voice Gateway Routers Guide

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/int_c/dpeer_c/dp_confg.htm

iSAC Codec Support on TDM-IP Voice Gateways and Cisco UBE Platforms

This section provides information about Cisco internet Speech Audio Codec (iSAC) support on Cisco Time Division Multiplexing–Internet Protocol (TDM-IP) Voice Gateways and Cisco Unified Border Element (Cisco UBE) platforms.

Contents

Prerequisites for iSAC Codec Support on TDM-IP Voice Gateways and Cisco UBE Platforms

The following prerequisites apply to this feature:

- Working familiarity with Cisco IOS command-line interface and basic configuration procedures for voice gateway networks. Additional basic information with which you should be familiar is provided in the following chapters of the *Cisco Unified Border Element Configuration Guide*:
  - *Overview of Cisco Unified Border Element*
  - *Fundamental Cisco Unified Border Element Configuration*
  - SIP-to-SIP Connections on a Cisco Unified Border Element
- You should be familiar with the configuration information in the *Universal Voice Transcoding Support for IP-to-IP Gateways* document.
- You should be familiar with the *Cisco IOS Fax, Modem, and Text Support over IP Configuration Guide*.

Restrictions for iSAC Codec Support on Cisco TDM-IP Voice Gateways and Cisco UBE Platforms

The following restrictions apply to this feature:

- Low complexity is not supported for the iSAC codec.

Information About iSAC Codec Support on TDM-IP Voice Gateways and Cisco UBE Platforms

To configure iSAC Codec Support on Cisco TDM-IP Voice Gateways and Cisco UBE Platforms, you should understand the following concept:

- iSAC Codec Support on Cisco TDM-IP Voice Gateways and Cisco UBE Platforms Overview, page 58

iSAC Codec Support on Cisco TDM-IP Voice Gateways and Cisco UBE Platforms Overview

The iSAC codec is an adaptive VoIP codec specially designed to deliver wideband sound quality in both low- and high-bit rate applications. The iSAC codec automatically adjusts the bit-rate for the best quality or a fixed bit rate can be used if the network characteristics are known. This codec is designed for wideband VoIP communications. The iSAC codec offers better quality with reduced bandwidth for sideband applications.

How to Configure iSAC Codec Support on Cisco TDM-IP Voice Gateways and Cisco UBE Platforms

This section contains the following procedures:

- Configuring iSAC Codec Support Under VoIP Dial Peer Configuration Mode, page 58
- Configuring iSAC Codec Support Under Voice-Class Configuration Mode, page 59
- Configuring iSAC Codec Support Under DSP Farm Profile Configuration Mode, page 61

Configuring iSAC Codec Support Under VoIP Dial Peer Configuration Mode

Perform the following tasks to configure the use of the iSAC codec for an individual VoIP dial peer. Note that there are other keywords and arguments for the some of the commands in this procedure, but they are not relevant to the configuration of the iSAC codec, so they have been omitted for brevity and clarity.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *tag* **voip**
4. **codec isac** [**mode** {**independent** | **adaptive**} [**bit rate** *value* **framesize** {**30** | **60**}[**fixed**]]]
5. **rtp payload-type cisco-codec-isac**

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 1 voip`	Enters dial-peer configuration mode and defines a dial peer that directs traffic to or from a packet network. • *tag*—Dial-peer identifier that consists of one or more digits. Range: 1 to 2147483647. • **voip**—Calls from this dial peer use voice encapsulation on the packet network.

	Command or Action	Purpose
Step 4	**codec isac** [**mode** {**independent** | **adaptive**} [**bit rate** *value* **framesize** {**30** | **60**} [**fixed**]]] **Example:** `Router(config-dial-peer)# codec isac mode independent`	Specifies the iSAC codec: • **mode**—(Optional) Determines whether configuration mode (VBR) is independent (value 1) or adaptive (value 0). • **bit rate**—(Optional) Configures the target bit rate that is allowed. The range for the *value* argument is 10 to 32 kbps. • **framesize**—(Optional) Specifies the packetization rate. Acceptable values are 30 or 60 ms speech frames sampled at 16 kHz. • **fixed**—(Optional) Indicates that the framesize will be fixed. Applicable to the framesize for adaptive mode only. Default values can be configured by entering the **codec isac** command. Default values are: • Mode: independent • Target bit-rate: 32000 bps • Framesize: 30ms
Step 5	**rtp payload-type cisco-codec-isac** *value* **Example:** `Router(config-dial-peer)# rtp payload-type cisco-codec-isac`	Specifies the iSAC codec for the RTP payload type: • *value*—Range is 96 to 127. The default value is 124.

Configuring iSAC Codec Support Under Voice-Class Configuration Mode

To configure support for the iSAC codec under voice-class configuration mode, complete the following tasks.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice class codec** *tag*
4. **codec isac** [**mode** {**independent** | **adaptive**} [**bit rate** *value* **framesize** {**30** | **60**}[**fixed**]]]
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`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice class codec** *tag* **Example:** `Router(config)# voice class codec 123`	Assigns a previously configured codec selection preference list (codec voice class) to the VoIP dial peer designated by *tag* argument: • Range for the *tag* value is 1 to 10000. • Maps to the tag number created using the **voice class codec** command.
Step 4	**codec isac** [**mode** {**independent** | **adaptive**} [**bit rate** *value* **framesize** {**30** | **60**} [**fixed**]]] **Example:** `Router(config-voice)# codec isac mode independent`	Specifies the iSAC codec: • **mode**—(Optional) Determines whether configuration mode (VBR) is independent (value 1) or adaptive (value 0). • **bit rate—**(Optional) Configures the target bit rate that is allowed. The range for the *value* argument is 10 to 32 kbps. • **framesize**—(Optional) Specifies the packetization rate. Acceptable values are 30 or 60 ms speech frames sampled at 16 kHz. • **fixed**—(Optional) Indicates that the framesize will be fixed. Applicable to the framesize for adaptive mode only. Default values can be configured by entering the **codec isac** command. Default values are: • Mode: independent • Target bit-rate: 32000 bps • Framesize: 30ms
Step 5	**exit** **Example:** `Router(config-voice)# exit`	Exits the current configuration mode.
Step 6	**dial-peer voice** *tag* **voip** **Example:** `Router(config)# dial-peer voice 123 voip`	Enters dial-peer configuration mode for the VoIP dial peer designated by tag.

	Command or Action	Purpose
Step 7	**voice-class codec** *tag* **Example:** `Router(config-dial-peer)# voice-class codec 123`	Assigns a previously configured codec selection preference list (codec voice class) to the VoIP dial peer designated by tag. Range is 1 to 10000. Maps to the tag number created using the **voice class codec** command.
Step 8	**exit** **Example:** `Router(config-dial-peer)# exit`	Exits the current configuration mode.

Configuring iSAC Codec Support Under DSP Farm Profile Configuration Mode

To configure support for the iSAC codec under DSP farm profile configuration mode, complete the following tasks.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice-card** *slot*
4. **dsp services dspfarm**
5. **exit**
6. **dspfarm profile** *profile-identifier* {**conference** | **mtp** | **transcode**}
7. **description** *text*
8. **codec** *codec-type*
9. **maximum sessions** *number*

   or

   maximum sessions {**hardware** | **software**} *number*
10. **maximum conference-participants** *number*
11. **associate application sccp**

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-card** *slot* **Example:** `Router(config)# voice-card 1`	Enters voice-card configuration mode for the network module on which you want to enable DSP resource services.
Step 4	**dsp services dspfarm** **Example:** `Router(config-voicecard)# dsp services dspfarm`	Enables DSP-farm services for the voice card.
Step 5	**exit** **Example:** `Router(config-voicecard)# exit`	Exits voice-card configuration mode.
Step 6	**dspfarm profile** *profile-identifier* {**conference** | **mtp** | **transcode**} **Example:** `Router(config)# dspfarm profile 20 conference`	Enters DSP farm profile configuration mode to define a profile for DSP farm services. **Note** The *profile-identifier* and service type uniquely identifies a profile. If the service type and *profile-identifier* pair is not unique, you are prompted to choose a different *profile-identifier.* **Note** For transcoding, you can specify just the codec type, and the DSP uses the default codec parameter, such as independent mode, 32 kbps bit-rate, and 30 ms framesize.
Step 7	**description** *text* **Example:** `Router(config-dspfarm-profile)# description art_dept`	(Optional) Includes a specific description about the Cisco DSP farm profile.
Step 8	**codec** *codec-type* **Example:** `Router(config-dspfarm-profile)# codec iSAC`	Specifies the codecs supported by a DSP farm profile. To configure iSAC codec support, enter **isac** for the *codec-type*. The iSAC codec configuration supports both G.711-to-any and universal any-to-any configurations. • Repeat this step for each codec supported by the profile. **Note** Hardware MTPs support only G.711 a-law and G.711 u-law. If you configure a profile as a hardware MTP, and you want to change the codec to other than G.711, you must first remove the hardware MTP by using the **no maximum sessions hardware** command. **Note** Only one codec is supported for each MTP profile. To support multiple codecs, you must define a separate MTP profile for each codec.

	Command or Action	Purpose
Step 9	**maximum sessions** *number* or **maximum sessions** {**hardware** | **software**} *number* **Example:** `Router(config-dspfarm-profile)# maximum sessions 4`	Specifies the maximum number of sessions that are supported by the profile. • *number*—Range is determined by the available registered DSP resources. Default is 0. **Note** The **hardware** and **software** keywords apply only to MTP profiles.
Step 10	**maximum conference-participants** *number* **Example:** `Router(config-dspfarm-profile)# maximum conference-participants 64`	Specifies the maximum number of conference participants supported by the profile. • *number*—Range is determined by the available registered DSP resources. Acceptable values are 8, 16, 32, and 64.
Step 11	**associate application sccp** **Example:** `Router(config-dspfarm-profile)# associate application sccp`	Associates the SCCP protocol to the DSP farm profile.

Configuration Examples for iSAC Codec Support on Cisco TDM-IP Voice Gateways and Cisco UBE Platforms

This section provides the following configuration example:

- Configuring iSAC Codec Support on Cisco TDM-IP Voice Gateways and Cisco UBE Platforms

Configuring iSAC Codec Support on Cisco TDM-IP Voice Gateways and Cisco UBE Platforms

The following example shows a sample configuration for iSAC codec support configured under DSP farm profile on a Cisco 2811:

```
Router# show running-config

Building configuration...
Current configuration : 2108 bytes^M
!
! Last configuration change at 16:00:26 PDT Mon Mar 15 2010
!
version 15.1
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
card type t1 0 0
logging buffered 5120000
no logging console
enable password xxx
!
no aaa new-model
```

```
memory-size iomem 5
clock timezone PDT -7
network-clock-participate wic 0
!
ip source-route
!
!
ip cef
!
!
no ip domain lookup
ip host xxxx 223.255.254.254
no ipv6 cef
multilink bundle-name authenticated
!
!
voice-card 0
 dsp services dspfarm
!
!
!
license udi pid CISCO2811 sn xxxxxxxxxxx
archive
 log config
  hidekeys
!
redundancy
!
!
controller T1 0/0/0
 shutdown
 cablelength long 0db
!
!
interface FastEthernet0/0
 ip address 10.2.107.1 255.255.0.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.20.1 255.255.255.0
 no ip proxy-arp
 duplex auto
 speed auto
!
ip forward-protocol nd
!
!
no ip http server
ip route 10.0.0.0 0.0.0.0 10.2.0.1
ip route 10.0.0.0 255.0.0.0 10.2.0.1
ip route 192.0.0.0 255.0.0.0 FastEthernet0/1
ip route 223.0.0.0 255.0.0.0 10.2.0.1
ip route 223.255.254.254 255.255.255.255 10.2.0.1
!
!
control-plane
!
!
!
mgcp fax t38 ecm
!
sccp local FastEthernet0/0
sccp ccm 10.2.105.100 identifier 1 version 7.0
```

```
sccp
!
sccp ccm group 1
 bind interface FastEthernet0/0
 associate ccm 1 priority 1
 associate profile 102 register xxxxUXCODE
 associate profile 101 register CFBxxxxconf
!
dspfarm profile 102 transcode universal
 codec g711ulaw
 codec g711alaw
 codec g729ar8
 codec g729abr8
 codec g729r8
 codec g722-64
 codec ilbc
 codec isac
 codec g729br8
 maximum sessions 5
 associate application SCCP
!
dspfarm profile 101 conference
 codec g711ulaw
 codec g711alaw
 maximum sessions 2
 associate application SCCP
!
!
!
line con 0
exec-timeout 0 0
line aux 0
line vty 0 4
 session-timeout 300
 exec-timeout 0 0
 password lab
 no login
 transport input all
!
exception data-corruption buffer truncate
scheduler allocate 20000 1000
end
```

SG3 Fax Support on Cisco TDM-IP Voice Gateways and Cisco UBE Platforms

This section provides information about SG3 Fax Support on Cisco Time Division Multiplexing–Internet Protocol (TDM-IP) Voice Gateways and Cisco Unified Border Element (Cisco UBE) platforms. The enhancements described in this section provide T.38 fax relay and fax pass-through on TDM-IP voice gateways and on Cisco UBE platforms.

Contents

- How to Configure SG3 Fax Support on Cisco TDM-IP Voice Gateways and Cisco UBE Platforms, page 68
- incoming called-number 52222, page 104
- Feature Information for Cisco Unified Border Element Configuration Guide, page 119

Prerequisites for SG3 Fax Support on Cisco TDM-IP Voice Gateways and Cisco UBE Platforms

The following prerequisites apply to this feature:

- Working familiarity with Cisco IOS command-line interface and basic configuration procedures for voice gateway networks. Additional basic information with which you should be familiar is provided in the following chapters:
  - *Overview of Cisco Unified Border Element*
  - *Fundamental Cisco Unified Border Element Configuration*
  - *SIP-to-SIP Connections on a Cisco Unified Border Element*
- You should be familiar with the configuration information in the *Universal Voice Transcoding Support for IP-to-IP Gateways* document.
- You should be familiar with the *Cisco IOS Fax, Modem, and Text Support over IP Configuration Guide*.

Restrictions for SG3 Fax Support on Cisco TDM-IP Voice Gateways and Cisco UBE Platforms

The following restrictions apply to this feature:

- SG3 fax capability is not supported for Cisco Fax Relay.
- For T.38 fax sessions to operate at SG3 speeds, all the endpoints involved must support T.38 Version 3 (v3) configuration and have negotiated T.38 v3. If all endpoints are not configured for SG3/V.34 speeds, then the slowest speed in the topology is the one supported by all endpoints.

Information About SG3 Fax Support on Cisco TDM-IP Voice Gateways and Cisco UBE Platforms

To configure SG3 Fax Support on Cisco TDM-IP Voice Gateways and Cisco UBE Platforms, you should understand the following concepts:

- SG3 Fax Support on Cisco TDM-IP Voice Gateways and Cisco UBE Platforms Overview

SG3 Fax Support on Cisco TDM-IP Voice Gateways and Cisco UBE Platforms Overview

This feature provides support for V.34 fax relay based on the ITU Specification T.38 version 3 (04/2007) and for fax pass-through at SG3 speed. Prior to Cisco IOS Release 15.1(1)T, SG3-to-SG3 calls would fail because the V.34 modulation was not supported. A fallback solution allowed SG3-to-SG3 connections to be made, but the transmission speed was set to G3 levels.

For T.38 fax sessions to operate at SG3 speeds, all the endpoints involved must support T.38 Version 3 (v3) configuration and have negotiated T.38 v3. For example:

Originating Gateway(T.38 v3)—IP–(T.38 v3)Cisco UBE(T.38 v3)–IP—Terminating Gateway(T.38 v3)

In this context, all currently supported Cisco UBE T.38 flows (H.323-H.323, H.323-SIP and SIP-SIP) are supported in Release 15.1(1)T. However, in topologies where at least one endpoint has a T.38 v0 configuration, the Cisco UBE configuration must be T.38 v0 (the lowest common version). Any other combination of T.38 v3 or v0 configuration involved in the Cisco UBE topologies is not supported.

When two endpoints are involved in negotiating the T.38 parameter, the mandatory parameter is the "FaxVersion." That is, when one of the endpoints supports Version 0 (v0), the resulting session operates as a v0 session. As long as Cisco UBE is configured for the lowest common version of the traffic expected, calls are completed successfully.

The information for supported calls is summarized in Table 1 and Table 2.

Table 1 Supported Call Flows with Mixed Endpoints at v0 and v3 Speeds

Emitting End	Receiving End	Resulting Session
v0	v0	v0
v0	v3	v0
v3	v0	v0
v3	v3	v3

Table 2 Supported Call Flows with Mixed Endpoints and Cisco UBE

Emitting End	Cisco UBE	Receiving End	Resulting Session
v0	v0	v0	v0
v0	v0	v3	v0
v3	v0	v0	v0
v3	v3	v3	v3

How to Configure SG3 Fax Support on Cisco TDM-IP Voice Gateways and Cisco UBE Platforms

This section contains the following procedures:

- Configuring Fax Pass-Through, page 68 (required)
- Configuring T.38 Fax Relay, page 68 (required)

Configuring Fax Pass-Through

To enable the SG3 Fax Support on Cisco TDM-IP Voice Gateways and Cisco UBE Platforms feature, configure fax pass-through as described in the *Configuring Fax Pass-Through* section of the *Cisco IOS Fax, Modem, and Text Support over IP Configuration Guide.*

Configuring T.38 Fax Relay

Perform one of the following tasks to configure T.38 fax relay at the dial-peer level or the global level under voice service voip:

- Configuring One or More Individual VoIP Dial Peers for T.38 Fax Relay, page 68
- Configuring T.38 Fax Relay on VoIP Dial Peers Globally, page 71

Configuring One or More Individual VoIP Dial Peers for T.38 Fax Relay

Perform this task to configure T.38 fax relay for an individual VoIP dial peer.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *tag* **voip**
4. **dtmf-relay h245-signal**
5. **fax protocol t38** [**nse** [**force**]] **version** {**0** | **3**} [**ls-redundancy** *value* [**hs-redundancy** *value*]] [**fallback** {**cisco** | **none** | **pass-through** {**g711ulaw** | **g711alaw**}}]
6. **fax rate** {**12000** | **14400** | **2400** | **4800** | **7200** | **9600** | **disable** | **voice**} [**bytes** *rate*]
7. **session protocol sipv2**

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 1 voip`	Enters dial-peer configuration mode and defines a dial peer that directs traffic to or from a packet network. • *tag*—Dial-peer identifier that consists of one or more digits. Range: 1 to 2147483647. • **voip**—Calls from this dial peer use voice encapsulation on the packet network.
Step 4	**dtmf-relay h245-signal** **Example:** `Router(config-dial-peer)# dtmf-relay h245-signal`	Specifies how an H.323 or Session Initiation Protocol (SIP) gateway relays dual tone multifrequency (DTMF) tones between telephony interfaces and an IP network. • **h245-signal**—(Optional) Forwards DTMF tones by using the H.245 signal User Input Indication method. Supports tones from 0 to 9, *, #, and from A to D.

<table>
<tr><th></th><th>Command or Action</th><th>Purpose</th></tr>
<tr><td>Step 5</td><td>fax protocol t38 [nse [force]] [version {0 | 3}] [ls-redundancy value [hs-redundancy value]] [fallback {cisco | none | pass-through {g711ulaw | g711alaw}}]

Example:
<code>Router(config-dial-peer)# fax protocol t38 version 3</code></td><td>Specifies the global default ITU-T T.38 standard fax protocol to be used for all VoIP dial peers.
• nse—(Optional) Uses Named Signaling Events (NSEs) to switch to T.38 fax relay.
• force—(Optional) Unconditionally, uses Cisco NSE to switch to T.38 fax relay. This option allows T.38 fax relay to be used between Cisco H.323 or Session Initiation Protocol (SIP) gateways and Media Gateway Control Protocol (MGCP) gateways.
• version—(Optional) Specifies a version for configuring fax speed:
– 0—Configures version 0, which uses T.38 version 0 (1998, G3 faxing)
– 3—Configures version 3, which uses T.38 version 3 (2004, V.34 or SG3 faxing)
• ls-redundancy value—(Optional) Specifies the number of redundant T.38 fax packets to be sent for the low-speed V.21-based T.30 fax machine protocol. Range varies by platform from 0 (no redundancy) to 5 or 7. The default is 0.
• hs-redundancy value—(Optional) Specifies the number of redundant T.38 fax packets to be sent for high-speed V.17, V.27, and V.29 T.4 or T.6 fax machine image data. Range varies by platform from 0 (no redundancy) to 2 or 3. The default is 0.
Note Setting the hs-redundancy parameter to a value greater than 0 causes a significant increase in the network bandwidth consumed by the fax call.
• fallback—(Optional) A fallback mode is used to transfer a fax across a VoIP network if T.38 fax relay could not be successfully negotiated at the time of the fax transfer.
• cisco—(Optional) Cisco-proprietary fax protocol.
Note Do not use the cisco keyword for the fallback option if you specified version 3 for SG3 fax transmission.
• none—(Optional) No fax pass-through or T.38 fax relay is attempted. All special fax handling is disabled, except for modem pass-through if configured with the modem pass-through command.
• pass-through—(Optional) The fax stream uses one of the following high-bandwidth codecs:
– g711ulaw—Uses the G.711 u-law codec.
– g711alaw—Uses the G.711 a-law codec.</td></tr>
</table>

	Command or Action	Purpose
Step 6	**fax rate** {**12000** | **14400** | **2400** | **4800** | **7200** | **9600** | **disable** | **voice**} [**bytes** *rate*] **Example:** `Router(config-dial-peer)# fax rate 14400`	(Optional) Selects the fax transmission speed to be attempted when this dial peer is used. • **12000**, **14400**, **2400**, **4800**, **7200**, **9600**—Maximum bits-per-second speed. **Note** If you specified **version 3** in the **fax protocol t38** command and negotiated T.38 version 3, the fax rate is automatically set to 33600. However, this rate cannot be configured by using the **fax rate** command. • **bytes** *rate*—(Optional) Fax packetization rate, in milliseconds (ms). Range: 20 to 48. Default: 20. For T.38 fax relay, this keyword-argument pair is valid only on Cisco AS5350, Cisco AS5400, and Cisco AS5850 routers. For other routers, the packetization rate for T.38 fax relay is fixed at 40 ms and cannot be changed with this keyword-argument pair. • **disable**—Disables fax relay transmission capability. • **voice**—Highest possible transmission speed allowed by the voice rate. For example, if the voice codec is G.711, fax transmission occurs at up to 14400 bps because 14400 bps is less than the 64-kbps voice rate. If the voice codec is G.729 (8 kbps), the fax transmission speed is 7200 bps. This is the default.
Step 7	**session protocol sipv2** **Example:** `Router(config-dial-peer)# session protocol sipv2`	(Optional) Specifies the IETF SIP session protocol for calls between the local and remote routers using the packet network. **Note** This command is required for SIP calls.

Configuring T.38 Fax Relay on VoIP Dial Peers Globally

Perform this task to configure T.38 fax relay globally for previously defined VoIP dial peers.

Note Fax relay parameters that are set for an individual dial peer under the **dial-peer voice** command take precedence over global settings made under the **voice service voip** command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **fax protocol t38** [**nse** [**force**]] **version** {**0** | **3**} [**ls-redundancy** *value* [**hs-redundancy** *value*]] [**fallback** {**cisco** | **none** | **pass-through** {**g711ulaw** | **g711alaw**}}]

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.

	Command or Action	Purpose
Step 4	**fax protocol t38** [**nse** [**force**]] [**version** {**0** | **3**}] [**ls-redundancy** *value* [**hs-redundancy** *value*]] [**fallback** {**cisco** | **none** | **pass-through** {**g711ulaw** | **g711alaw**}}] **Example:** `Router(config-voi-srv)# fax protocol t38 version 3`	Specifies the global default ITU-T T.38 standard fax protocol to be used for all VoIP dial peers. • **nse**—(Optional) Uses Named Signaling Events (NSEs) to switch to T.38 fax relay. • **force**—(Optional) Unconditionally, uses Cisco NSE to switch to T.38 fax relay. This option allows T.38 fax relay to be used between Cisco H.323 or Session Initiation Protocol (SIP) gateways and Media Gateway Control Protocol (MGCP) gateways. • **version**—(Optional) Specifies a version for configuring fax speed: – **0**—Configures version 0, which uses T.38 version 0 (1998, G3 faxing) – **3**—Configures version 3, which uses T.38 version 3 (2004, V.34 or SG3 faxing) • **ls-redundancy** *value*—(Optional) Specifies the number of redundant T.38 fax packets to be sent for the low-speed V.21-based T.30 fax machine protocol. Range varies by platform from 0 (no redundancy) to 5 or 7. The default is 0. • **hs-redundancy** *value*—(Optional) Specifies the number of redundant T.38 fax packets to be sent for high-speed V.17, V.27, and V.29 T.4 or T.6 fax machine image data. Range varies by platform from 0 (no redundancy) to 2 or 3. The default is 0. **Note** Setting the **hs-redundancy** parameter to a value greater than 0 causes a significant increase in the network bandwidth consumed by the fax call. • **fallback**—(Optional) A fallback mode is used to transfer a fax across a VoIP network if T.38 fax relay could not be successfully negotiated at the time of the fax transfer. • **cisco**—(Optional) Cisco-proprietary fax protocol. **Note** Do not use the **cisco** keyword for the fallback option if you specified **version 3** for SG3 fax transmission. • **none**—(Optional) No fax pass-through or T.38 fax relay is attempted. All special fax handling is disabled, except for modem pass-through if configured with the modem pass-through command. • **pass-through**—(Optional) The fax stream uses one of the following high-bandwidth codecs: – **g711ulaw**—Uses the G.711 u-law codec. – **g711alaw**—Uses the G.711 a-law codec.

Configuration Examples for SG3 Fax Support on Cisco TDM-IP Voice Gateways and Cisco UBE Platforms

This section provides the following configuration example:

- Configuring SG3 Fax Support for T.38 protocol on Cisco TDM-IP Voice Gateways and Cisco UBE Platforms: Example, page 74

Configuring SG3 Fax Support for T.38 protocol on Cisco TDM-IP Voice Gateways and Cisco UBE Platforms: Example

The following example shows how to configure SG3 Fax Support for the T.38 protocol on the Cisco TDM-IP Voice Gateways and Cisco UBE Platforms feature:

```
!
voice service voip
 fax protocol t38 version 3 ls-redundancy 0 hs-redundancy 0 fallback cisco
!
!
interface FastEthernet0/0
 ip address 1.2.103.1 255.255.0.0
!
!
!
dial-peer voice 100 voip
 destination-pattern 1.....
 session target ipv4:1.2.103.3
 dtmf-relay h245-signal
 fax protocol t38 version 3 ls-redundancy 0 hs-redundancy 0 fallback cisco
!
dial-peer voice 200 voip
 destination-pattern 2.....
 session protocol sipv2
 session target ipv4:1.2.103.3
 dtmf-relay rtp-nte
 fax protocol pass-through g711ulaw
!
dial-peer voice 6789 voip
 destination-pattern 6789
 session target ipv4:1.2.102.2
 dtmf-relay rtp-nte
 fax protocol pass-through g711ulaw
!
!
sip-ua
```

Configuring QoS for a Cisco Unified Border Element

To assign QoS differentiated services code points (DSCP) for H.323 calls through the Cisco Unified Border Element, perform the steps in this section.

Note With the exception of RSVP, all VoIP QoS options supported by TDM-to-IP gateways are supported by Cisco Unified Border Elements. See the following documents for details and configuration instructions:

- The "Configuring Quality of Service for Voice" chapter in *Cisco IOS Voice, Video, and Fax Configuration Guide, Release 12.2*
- *Quality of Service for Voice over IP*

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *number* **voip**
4. **ip qos dscp ef media**
5. **ip qos dscp af31 signaling**
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	**ip qos dscp ef media** **Example:** `Router(config-dial-peer)# ip qos dscp ef media`	Configures express forwarding for RTP packets.
Step 5	**ip qos dscp af31 signaling** **Example:** `Router(config-dial-peer)# ip qos dscp af31 signaling`	Configures assured forwarding af31 for H.323 signaling.
Step 6	**exit** **Example:** `Router(config-dial-peer)# exit`	Exits the current mode.

Configuring Cisco Unified Border Element for High Utilization

For high-utilization configurations, the Cisco Unified Border Element may require a higher percentage of memory than that which is made available by default during bootup. Additionally, high-utilization configurations may experience an increase in dropped packets.

To configure Cisco Unified Border Element for high utilization, perform the steps in this section. This section contains the following subsections:

- Increase I/O Memory for High Utilization, page 76
- Manage Ethernet Hold Queue for High Utilization, page 77

Increase I/O Memory for High Utilization

To increase the amount of memory available to the Cisco Unified Border Element, perform the steps in this section.

Prerequisites

Determine if sufficient I/O memory is available by using the **show memory** command:

Note If peak utilization is consistently more than 80 percent of the total I/O memory allocated, use the **memory-size iomem** command to set the I/O memory percentage to use less than 80 percent of the allocation.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **show version**
4. **memory-size iomem**

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	**show version** **Example:** `Router# show version`	Displays memory statistics.
Step 4	**memory-size iomem** *i/o-memory-percentage* **Example:** `Router(config)# memory-size iomem 20`	Reallocates the percentage of DRAM to use for I/O memory and processor memory. The argument is as follows: • *i/o-memory-percentage*—Valid values:10, 15, 20, 25, 30, 40, and 50. A minimum of 15 MB of memory is required for I/O memory.

Manage Ethernet Hold Queue for High Utilization

Some traffic patterns and network environments may produce bursts of packets on the Ethernet interfaces used for Cisco Unified Border Element signaling and media. In some cases, these bursts can result in dropped packets when the Ethernet input queue overflows. Similarly, momentary congestion on the local network could inhibit the Cisco Unified Border Element feature, also resulting in dropped packets when the Ethernet output queue overflows.

Because H.323 uses UDP for media transport and RAS signaling, dropped packets have a negative impact on call signaling integrity and voice quality. Packet drops due to momentary, occasional Ethernet queue overflows in bursty networks can be reduced or eliminated by increasing the Ethernet hold queue sizes.

Caution A consistently overloaded Ethernet hold queue may increase latency. You may be required to upgrade the Cisco Unified Border Element feature to a higher-performance platform or distribute traffic to an additional gateway.

To increase the Ethernet input hold queue, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot*/*port*
4. **hold-queue** *length* **in**
5. **hold-queue** *length* **out**
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	**interface** *type slot*/*port* **Example:** `Router(config)# interface ethernet 0/1`	Selects the Ethernet interface that you want to configure.
Step 4	**hold-queue** *length* **in** **Example:** `Router(config)# hold-queue 1024 in`	Sets the Ethernet interface input queue.
Step 5	**hold-queue** *length* **out** **Example:** `Router(config)# hold-queue 1024 out`	Sets the Ethernet interface output queue.
Step 6	**exit** **Example:** `Router(config)# exit`	Exits the current mode.

Examples

In general, set the queue size to the smallest value that resolves the packet drops. Monitor the network using the **show interfaces ethernet** command to confirm that the queue occupancy and drops are both close to zero. For example:

```
Router(config)# interface f0/1
Router(config)# hold-queue 1024 in
Router(config)# hold-queue 1024 out

Router# show interface f0/1 | include queue
  Input queue: 17/1024/0/0 (size/max/drops/flushes); Total output drops: 0
  Output queue :0/1024 (size/max)

Router# show interface f0/1

FastEthernet0/1 is up, line protocol is up
  Hardware is AmdFE, address is 0002.b950.5181 (bia 0002.b950.5181)
  Description: archived via cfg file p8.cfg on Wed May  1 09:46:33 EDT 2002
  Internet address is 10.3.2.63/16
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 104/255, rxload 97/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
```

```
  Full-duplex, 100Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 7/1024/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/1024 (size/max)
  5 minute input rate 38335000 bits/sec, 24068 packets/sec
  5 minute output rate 40897000 bits/sec, 24019 packets/sec
     112943349 packets input, 1022884421 bytes
     Received 405 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog
     0 input packets with dribble condition detected
     113081187 packets output, 2612108380 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out

Router# show running-config interface f0/1

Building configuration...

Current configuration : 420 bytes
!
interface FastEthernet0/1
 ip address 10.3.2.63 255.255.0.0
 no ip redirects
 ip route-cache same-interface
 speed auto
 full-duplex
 h323-gateway voip interface
 h323-gateway voip id 3640-vgk2 ipaddr 10.3.2.72 1719 priority 1
 h323-gateway voip h323-id 3660-hud3
 h323-gateway voip tech-prefix 1#
 h323-gateway voip bind srcaddr 10.3.2.63
 hold-queue 1024 in
 hold-queue 1024 out
```

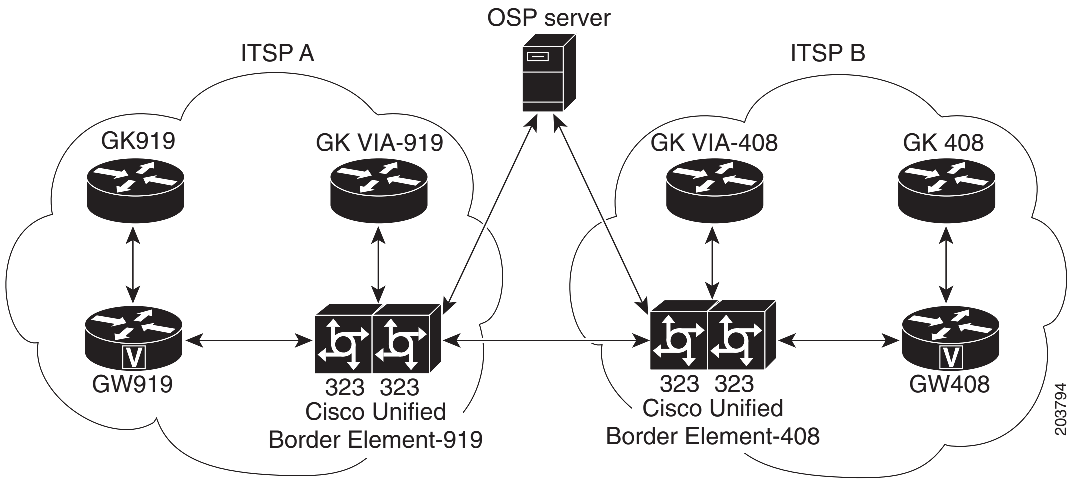
Configuring Cisco Unified Border Element with OSP

The Cisco Unified Border Element with Open Settlement Protocol (OSP) feature enables VoIP service providers to gain the benefits of the Cisco Unified Border Element and to make use of routing, billing, and settlement capabilities offered by OSP-based clearinghouses.

Open Settlement Protocol is a client-server protocol used to establish authenticated connections between gateways. OSP provides for the secure transfer of accounting and routing information between Cisco Unified Border Elements.

Figure 1 shows a sample topology that uses the Cisco Unified Border Element feature with OSP. With the exception of the authentication and accounting messages that are exchanged between the Cisco Unified Border Element and the OSP server, the exchange of messages between the gateways and gatekeepers is similar to the process illustrated in Figure 4 on page 109.

Figure 1 Cisco Unified Border Element with OSP Configuration Topology



Note For details on configuring and using OSP applications, see the "Configuring Settlement Applications" chapter of the *Cisco IOS Voice, Video and Fax Configuration Guide*, Release 12.2.

To configure the Cisco Unified Border Element with OSP, perform the steps in this section.

Prerequisites

- Obtain the required feature license for each platform on which you will configure the Cisco Unified Border Element with OSP feature.
- Install a Cisco IOS image that supports the Cisco Unified Border Element and encryption. See Figure 3 on page 107 for a list of Cisco IOS image requirements.
- Configure OSP on the Cisco Unified Border Element. For detailed instructions on configuring OSP, see the Configuring Settlement Applications chapter of the *Cisco IOS Voice, Video and Fax Configuration Guide*, Release 12.2.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *number* **voip**
4. **application** *application-name*
5. **exit**

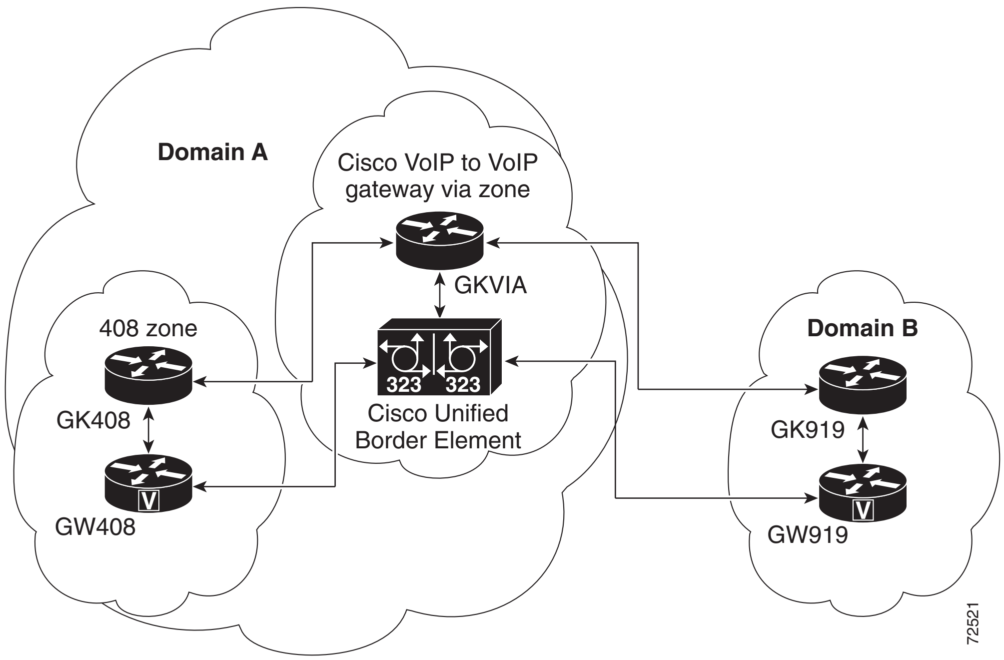
DETAILED STEPS

	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 11 voip`	Enters dial peer configuration mode for the specified VoIP dial peer. **Note** You need to configure only incoming dial peers for OSP.
Step 4	**application** *application-name* **Example:** `Router(config-dial-peer)# application session`	Configure the dial peer to use a Tcl application that supports OSP. **Note** Unless you have configured a Tcl application for OSP, use the default "session" application.
Step 5	**exit** **Example:** `Router(config-dial-peer)# exit`	Exits the current mode.

Examples

Figure 2 shows two ITSPs using Cisco Unified Border Element and OSP to connect calls passing between the two networks. The examples that follow are based on this illustration.

Figure 2 Cisco Unified Border Element with OSP Feature Topology



Sample Configuration for the Cisco Unified Border Element with OSP Feature

The following example shows the dial peer configuration necessary to complete calls using the configuration shown in Figure 3 on page 107:

Cisco Unified Border Element-919 Dial Peers

The following dial peer is used for incoming calls from GW919:

```
dial-peer voice 11 voip
 application session
 incoming called-number 408....
 session target ras
 codec transparent
!
```

The following dial peer is used for outgoing calls to Cisco Unified Border Element-408:

```
dial-peer voice 12 voip
 destination-pattern 408....
 session target settlement
 codec transparent
!
```

The following dial peer is used for incoming calls from Cisco Unified Border Element-408:

```
dial-peer voice 13 voip
 application session
 incoming called-number 919....
 session target settlement
 codec transparent
!
```

The following dial peer is used for outgoing calls to GW919:

```
dial-peer voice 14 voip
 destination-pattern 919....
 session target ras
 codec transparent
!
```

Cisco Unified Border Element-408 Dial Peers

The following dial peer is used for incoming calls from Cisco Unified Border Element-919:

```
dial-peer voice 21 voip
 application session
 incoming called-number 408....
 session target settlement
 codec transparent
!
```

The following dial peer is used for outgoing calls to GW408:

```
dial-peer voice 22 voip
 destination-pattern 408....
 session target ras
 codec transparent
!
```

The following dial peer is used for outgoing calls to Cisco Unified Border Element-919:

```
dial-peer voice 23 voip
 destination-pattern 919....
 session target settlement
 codec transparent
!
```

The following dial peer is used for incoming calls from GW408:

```
dial-peer voice 24 voip
 application session
 incoming called-number 919....
 session target ras
 codec transparent
!
```

Media Statistics on a Cisco Unified Border Element

This chapter describes the media statistics feature. The **media statistics** command allows you to estimate the values of the packet loss, jitter, and the Round Trip Time (RTT) statistics based on RFC-3550.

To enable media statistics on an Cisco Unified Border Element, perform the steps in this section. This section contains the following subsections:

Restrictions

- Integrated TDM-IP and Cisco Unified Border Element is not supported.
- Estimating media statistics feature on Cisco Unified Border Element is available if the **media statistics** command is configured. The feature is disabled by default.
- Cisco Unified Border Element does not initiate RTCP it only passes the received RTCP packet from incoming leg to Outgoing leg.
- Voice quality may be impacted by per-packet touching of an RTP stream for generating the required voice statistics.

Information About Media Statistics in an Cisco Unified Border Element

The Voip RTP library estimates the values based on RTCP packets received on the Cisco Unified Border Element. This feature adds the capability to generate the media statistics in Cisco Unified Border Element and estimate the values of packet loss, jitter, and Round Trip Time (RTT)

Packet Loss

Packet loss is estimated on Cisco Unified Border Element based on RFC 3550. Packet loss calculation is done based on RTP stream and the computation is done in VOIPRTP library by checking the sequence Number.

- The Packet loss value computed is filled in variable cvVoIPCallActiveLostPackets in the CISCO-VOICE-DIAL-CONTROL-MIB
- Packet loss value will be estimated even if the End-End RTCP is not present for the call.

Jitter

Packet jitter is defined as an estimate of the statistical variance of the RTP data packet interarrival time, measured in timestamp units. Jitter is estimated on Cisco Unified Border Elements based on RFC 3550. Jitter is computed in VOIPRTP library.

- The Jitter value computed is filled in variable cvCallActivePlayDelayJitter in CISCO-VOICE-DIAL-CONTROL-MIB.

Round Trip Time

The Round Trip Time (RTT) value computed is filled in variable cvVoIPCallActiveRoundTripDelay in CISCO-VOICE-DIAL-CONTROL-MIB.

- Cisco Unified Border Element handles signaling and Media without DSP and establishes calls with protocols H.323, SIP and also does interworking between H.323 and SIP protocols. As the calls are handled DSP less currently the values populated on Cisco Unified Border Element for voice statistics are displayed as zero.

Note A sub-rtcp message is similar to a rtcp message except the payload type is different. A sub-rtcp message is a cisco proprietary message initiated by the Cisco Unified Border Element.

Configuring Media Statistics in a Cisco Unified Border Element

The media statistics feature can be configured in global, or dial peer configuration mode, perform the steps in this section. This section contains the following subsections:

- Configuring Media Statistics in Voice-Service Configuration Mode, page 85
- Configuring Media Statistics on Dial Peer Configuration Mode, page 86
- Monitoring Media Statistics in a Cisco Unified Border Element, page 87 (optional)
- Verifying Fundamental Cisco Unified Border Element Configurations, page 105

Note
- Before you perform a procedure, familiarize yourself with the following information:
  - "Restrictions" section on page 84
- For help with a procedure, see the monitoring and verifying sections listed above.

Configuring Media Statistics in Voice-Service Configuration Mode

To globally enable media statistics in voice-service configuration mode to estimate the values for packet loss, jitter, and RTT, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **media statistics**
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	**`media statistics`** **Example:** `Router(conf-voi-serv)# media statistics`	Estimates the values of packet loss, jitter, and Round Trip Time (RTT) statistics. • The statistics are displayed using the **show voice history** and **show call active voice** command. • If the media statistics command is disabled the values will be zero.
Step 5	**`exit`** **Example:** `Router(conf-voi-serv)# exit`	Exits the current mode.

Configuring Media Statistics on Dial Peer Configuration Mode

To enable media statistics in on a dial peer voice-service configuration mode to estimate the values for packet loss, jitter, and RTT, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **media statistics**
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	**media statistics** **Example:** `Router(conf-voi-serv)# media statistics`	Estimates the values of packet loss, jitter, and Round Trip Time (RTT) statistics. • The statistics are displayed using the **show voice history** and **show call active voice** command. • If the media statistics command is disabled the values will be zero.
Step 5	**exit** **Example:** `Router(config-voice-service)# exit`	Exits the current mode.

Monitoring Media Statistics in a Cisco Unified Border Element

Monitor the **media statistics** with the **show call active voice** look for following variables:

- LostPackets
- PlayDelayJitter
- RoundTripDelay

SUMMARY STEPS

1. **show call active voice**
2. **show call active voice | i LostPackets**
3. **show call active voice | i RoundTripDelay**
4. **show call active voice | i PlayDelayJitter**
5. **show voip rtp connections**
6. **show call history voice last 2 | i RoundTripDelay**
7. **show call history voice last 2 | i LostPackets**

DETAILED STEPS

Step 1 **show call active voice**

Use this command to display media statistics information and indicate whether the media statistic feature is enabled.

```
c3745-ipipgw#show call active voice
Telephony call-legs: 0
SIP call-legs: 2
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 2
GENERIC:
SetupTime=525050 ms
Index=1
PeerAddress=6662
PeerSubAddress=
PeerId=0
PeerIfIndex=54
LogicalIfIndex=0
ConnectTime=527550 ms
CallDuration=00:00:04 sec
CallState=4
CallOrigin=2
ChargedUnits=0
InfoType=speech
TransmitPackets=112
TransmitBytes=2240
ReceivePackets=318
ReceiveBytes=6360
VOIP:
ConnectionId[0xA6008E71 0xA8FE11D6 0x800B000D 0x2970B190]
IncomingConnectionId[0xA6008E71 0xA8FE11D6 0x800B000D 0x2970B190]
CallID=5
RemoteIPAddress=1.3.7.16
RemoteUDPPort=19512
RemoteSignallingIPAddress=1.3.7.16
RemoteSignallingPort=52111
RemoteMediaIPAddress=1.3.7.16
RemoteMediaPort=19512
RoundTripDelay=0 ms
SelectedQoS=best-effort
tx_DtmfRelay=rtp-nte
FastConnect=FALSE
AnnexE=FALSE
Separate H245 Connection=FALSE
H245 Tunneling=FALSE
SessionProtocol=sipv2
ProtocolCallId=A601C6C1-A8FE11D6-8029B65F-D48EEF95@1.3.7.16
SessionTarget=1.3.7.16
OnTimeRvPlayout=0
GapFillWithSilence=0 ms
GapFillWithPrediction=0 ms
GapFillWithInterpolation=0 ms
GapFillWithRedundancy=0 ms
HiWaterPlayoutDelay=0 ms
LoWaterPlayoutDelay=0 ms
TxPakNumber=0
TxSignalPak=0
```

```
TxComfortNoisePak=0
TxDuration=0
TxVoiceDuration=0
RxPakNumber=0
RxSignalPak=0
RxComfortNoisePak=0
RxDuration=0
RxVoiceDuration=0
RxOutOfSeq=0
RxLatePak=0
RxEarlyPak=0
RxBadProtocol=0
PlayDelayCurrent=0
PlayDelayMin=0
PlayDelayMax=0
PlayDelayClockOffset=0
PlayDelayJitter=0
PlayErrPredictive=0
PlayErrInterpolative=0
PlayErrSilence=0
PlayErrBufferOverFlow=0
PlayErrRetroactive=0
PlayErrTalkspurt=0
OutSignalLevel=0
InSignalLevel=0
LevelTxPowerMean=0
LevelRxPowerMean=0
LevelBgNoise=0
ERLLevel=0
ACOMLevel=0
ErrRxDrop=0
ErrTxDrop=0
ErrTxControl=0
ErrRxControl=0
ReceiveDelay=0 ms
LostPackets=0
EarlyPackets=0
LatePackets=0
SRTP = off
TextRelay = off
VAD = disabled
CoderTypeRate=g729r8
CodecBytes=20
Media Setting=flow-through
CallerName=
CallerIDBlocked=False
OriginalCallingNumber=6662
OriginalCallingOctet=0x0
OriginalCalledNumber=6661
OriginalCalledOctet=0x0
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0x80
TranslatedCallingNumber=6662
TranslatedCallingOctet=0x0
TranslatedCalledNumber=6661
TranslatedCalledOctet=0x0
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0x80
GwReceivedCalledNumber=6661
GwReceivedCalledOctet3=0x0
GwReceivedCallingNumber=6662
GwReceivedCallingOctet3=0x0
GwReceivedCallingOctet3a=0x80
MediaInactiveDetected=no
```

```
MediaInactiveTimestamp=
MediaControlReceived=
LongDurationCallDetected=no
LongDurCallTimestamp=
LongDurcallDuration=
Username=6662
GENERIC:
SetupTime=525050 ms
Index=2
PeerAddress=6661
PeerSubAddress=
PeerId=6661
PeerIfIndex=54
LogicalIfIndex=0
ConnectTime=527550 ms
CallDuration=00:00:06 sec
CallState=4
CallOrigin=1
ChargedUnits=0
InfoType=speech
TransmitPackets=432
TransmitBytes=8640
ReceivePackets=112
ReceiveBytes=2240
VOIP:
ConnectionId[0xA6008E71 0xA8FE11D6 0x800B000D 0x2970B190]
IncomingConnectionId[0xA6008E71 0xA8FE11D6 0x800B000D 0x2970B190]
CallID=6
RemoteIPAddress=1.3.7.112
RemoteUDPPort=18958
RemoteSignallingIPAddress=1.3.7.112
RemoteSignallingPort=5060
RemoteMediaIPAddress=1.3.7.112
RemoteMediaPort=18958
RoundTripDelay=0 ms
SelectedQoS=best-effort
tx_DtmfRelay=rtp-nte
FastConnect=FALSE
AnnexE=FALSE
Separate H245 Connection=FALSE
H245 Tunneling=FALSE
SessionProtocol=sipv2
ProtocolCallId=D0445D00-62B611D6-800DB698-E7A6FDDD@1.3.7.9
SessionTarget=1.3.7.112
OnTimeRvPlayout=0
GapFillWithSilence=0 ms
GapFillWithPrediction=0 ms
GapFillWithInterpolation=0 ms
GapFillWithRedundancy=0 ms
HiWaterPlayoutDelay=0 ms
LoWaterPlayoutDelay=0 ms
TxPakNumber=0
TxSignalPak=0
TxComfortNoisePak=0
TxDuration=0
TxVoiceDuration=0
RxPakNumber=0
RxSignalPak=0
RxComfortNoisePak=0
RxDuration=0
RxVoiceDuration=0
RxOutOfSeq=0
RxLatePak=0
RxEarlyPak=0
```

```
RxBadProtocol=0
PlayDelayCurrent=0
PlayDelayMin=0
PlayDelayMax=0
PlayDelayClockOffset=0
PlayDelayJitter=0
PlayErrPredictive=0
PlayErrInterpolative=0
PlayErrSilence=0
PlayErrBufferOverFlow=0
PlayErrRetroactive=0
PlayErrTalkspurt=0
OutSignalLevel=0
InSignalLevel=0
LevelTxPowerMean=0
LevelRxPowerMean=0
LevelBgNoise=0
ERLLevel=0
ACOMLevel=0
ErrRxDrop=0
ErrTxDrop=0
ErrTxControl=0
ErrRxControl=0
ReceiveDelay=0 ms
LostPackets=0
EarlyPackets=0
LatePackets=0
SRTP = off
TextRelay = off
VAD = disabled
CoderTypeRate=g729r8
CodecBytes=20
Media Setting=flow-through
CallerName=
CallerIDBlocked=False
OriginalCallingNumber=6662
OriginalCallingOctet=0x0
OriginalCalledNumber=6661
OriginalCalledOctet=0x0
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0x80
TranslatedCallingNumber=6662
TranslatedCallingOctet=0x0
TranslatedCalledNumber=6661
TranslatedCalledOctet=0x0
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0x80
GwReceivedCalledNumber=6661
GwReceivedCalledOctet3=0x0
GwOutpulsedCalledNumber=6661
GwOutpulsedCalledOctet3=0x0
GwReceivedCallingNumber=6662
GwReceivedCallingOctet3=0x0
GwReceivedCallingOctet3a=0x80
GwOutpulsedCallingNumber=6662
GwOutpulsedCallingOctet3=0x0
GwOutpulsedCallingOctet3a=0x80
MediaInactiveDetected=no
MediaInactiveTimestamp=
MediaControlReceived=
LongDurationCallDetected=no
LongDurCallTimestamp=
LongDurcallDuration=
Username=6662
```

```
Telephony call-legs: 0
SIP call-legs: 2
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 2
```

Step 2 Router# **show call active voice | i LostPackets**

```
LostPackets=0
LostPackets=126
```

Step 3 Router# **show call active voice | i RoundTripDelay**

```
RoundTripDelay=0 ms
RoundTripDelay=4 ms
```

Step 4 Router# **show call active voice | i PlayDelayJitter**

```
PlayDelayJitter=0
PlayDelayJitter=24
```

Step 5 Router# **show voip rtp connections**

```
VoIP RTP active connections :
No. CallId     dstCallId  LocalRTP RmtRTP LocalIP         RemoteIP
1   5          6          17892    17794  15.5.34.5       15.5.34.158
2   6          5          16990    18744  15.5.34.5       15.5.34.6
Found 2 active RTP connections
```

Voice Quality Enhancements on Cisco Unified Border Element

To configure voice quality enhancements on the Cisco UBE, perform the steps in this section. This section contains the following subsections:

- Configuring Codec Repacketization, page 94
- Configuring IP-to-IP Call Gain/Loss Control, page 97
- Configuring Voice Quality Metrics, page 100
- SRST Support for G.722 Codec, page 103

Codec Repacketization

Codec repacketization is used to connect dissimilar networks that have different packetization time periods. A portion of a network might be set to generate packets on the Real-Time Transport Protocol (RTP) voice stream every 10 ms, while another portion may have a packetization period of 20 ms. When one side can adjust to the other’s packetization, the call is completed successfully. However, if both sides cannot agree on a common packetization, the call may fail. The codec repacketization enhancement prevents this call failure scenario.

By enabling the Cisco UBE gateway to do codec repacketization, one side of the call can be one packetization period, while allowing the other side can be another. Behavior is predictable, and you can always connect different portions of the voice network.

Note Be aware that in most cases, the packet sizes can be negotiated to a size both ends of a network can support. Use of the codec repacketization feature should be limited to extreme cases, and should always be used with caution. The maximum payload-size value for G.729r8 and G.723 codecs is 60 bytes.

Because repacketization uses digital signal processor (DSP) transcoding, there is a potential performance impact on DSP and Cisco IOS software. Therefore, codec repacketization should be used only when necessary. To explain the circumstances of when repacketization is and is not necessary, the following scenarios are provided (using G.711 codec as the example):

- **Scenario 1**—Endpoint-1 (G.711, byte 160, fixed-byte) connects to Endpoint-2 (G.711, byte 240, fixed-byte)

  In this case, repacketization will occur because there are codec byte mismatches between endpoints and both endpoints are configured with the **fixed-bytes** option of the **codec** command.
- **Scenario 2**—Endpoint-1 (G.711, byte 160) connects to Endpoint-2 (G.711, byte 240)

  In this case, repacketization does not occur because neither endpoint is configured with the **fixed-bytes** option of the **codec** command. The current CLI codec byte negotiation is used.
- **Scenario 3**—Endpoint-1 (G.711, byte 160, fixed-byte) connects to Endpoint-2 (G.711, byte 160, fixed-byte)

  In this case, the **fixed-bytes** option of the **codec** command is configured at both endpoints, but Cisco IOS software detects that repacketization is not needed. No repacketization is performed.
- **Scenario 4**—Endpoint-1 (G.711, byte 160, fixed-byte) connects to Endpoint-2 (G.711, byte 240)

  Endpoint 1 uses fixed codec byte size 160 and Endpoint 2 likes to use codec byte size 240. In this case, repacketization occurs because of the **fixed-bytes** option configured on Endpoint-1.

Prerequisites

- You should be familiar with the configuration information in the *Universal Voice Transcoding Support for IP-to-IP Gateways* document.

Restrictions

- The codec repacketization feature described in this document applies to SIP-to-SIP voice network connections.
- For the codec repacketization feature, the G.729r8 and G.723 codecs do not support a voice payload-size greater than 60 bytes.
- The IP-IP Call Gain/Loss Control and Voice Quality Measurements features apply to Cisco UBE voice connections. That is, the H.323 protocol can also be used.
- Secure Real-Time Transport Protocol (SRTP) is not supported in this feature.

Configuring Codec Repacketization

To configure codec repacketization on a voice gateway, you must configure codec byte size with different values for the incoming and outgoing Voice over IP (VoIP) dial peers.

- Configuring Codec Repacketization the Incoming VoIP Dial Peer, page 94
- Configuring Codec Repacketization the Outgoing VoIP Dial Peer, page 95
- Verifying Codec Repacketization, page 96

Configuring Codec Repacketization the Incoming VoIP Dial Peer

To configure the incoming VoIP dial peer, complete the following task:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice voip**
4. **incoming called-number** *number*
5. **codec** *codec-type* **bytes** *payload-size* **fixed-bytes**

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 voip`** **Example:** `Router(config)# dial-peer voice voip`	Enters dial-peer configuration mode, and specifies VoIP as the method of voice encapsulation.
Step 4	**`incoming called-number`** *`number`* **Example:** `Router(config-dialpeer)# incoming called-number 12345`	Specifies a digit string that can be matched by an incoming call to associate the call with the dial peer. • *number*—Series of digits that specify a pattern for the E.164 or private dialing plan telephone number. Valid entries are the digits 0 through 9, the letters A through D, and some special characters. (See the *incoming called-number (dial-peer) command* in the *Cisco IOS Voice Command Reference* for more information.)

	Command or Action	Purpose
Step 5	**codec** *codec-type* **bytes** *payload-size* **fixed-bytes** **Example:** `Router(config-dialpeer)# codec g711ulaw bytes 160 fixed-bytes`	Specifies the voice coder rate of speech for a dial peer, the number of bytes in the voice payload of each frame, and indicates that the codec byte size is fixed and non-negotiable.

Configuring Codec Repacketization the Outgoing VoIP Dial Peer

To configure the outgoing VoIP dial peer, complete the following task:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *tag* **voip**
4. **destination-pattern** *number*
5. **session target** *destination-address*
6. **codec** *codec-type*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**dial-peer voice** *tag* **voip** **Example:** `Router(config)# dial-peer voice 123 voip`	Enters dial-peer configuration mode, defines a particular dial peer, and specifies the method of voice encapsulation as VoIP. • *tag*—Digits that define a particular dial peer. Range is from 1 to 2147483647.
Step 4	**destination-pattern** *string* **Example:** `Router(config)# destination-pattern 12345`	Specifies either the prefix or the full E.164 telephone number to be used for a dial peer. • *string*—Series of digits that specify a pattern for the E.164 or private dialing plan telephone number. Valid entries are the digits 0 through 9, the letters A through D, and some special characters. (See the *destination-pattern command* in the *Cisco IOS Voice Command Reference* for more information.)

	Command or Action	Purpose
Step 5	**session target ipv4:***destination-address* **Example:** `Router(config-dialpeer)# session target ipv4:10.1.1.1`	Designates a network-specific address to receive calls from a VoIP dial peer. • **ipv4:***destination-address*—IP address of the dial peer to receive calls.
Step 6	**codec** *codec-type* **Example:** `Router(config-dialpeer)# codec g711ulaw`	Specifies the voice coder rate of speech for a dial peer.

Table 3 shows some commonly used mappings from codec bytes to codec ms packets.

Table 3 Packet Bytes and Packet Time Conversion for Codecs Supported in Repacketization (Transrating) Function

Codec	Packet Bytes for 10 ms Packet	Packet Bytes for 20 ms Packet	Packet Bytes for 30 ms Packet	Codec Bit Rate (bps), Packet Time in ms (PT), and Packet Byte Conversion Formula
g711ulaw, g711alaw	80 bytes	160 bytes	240 bytes	64,000 bps; PB = PT x 8
g729abr8, g729ar8, g729br8, g729r8[1]	10 bytes	20 bytes	30 bytes	8,000 bps; PB = PT
g722-64	80 bytes	160 bytes	240 bytes	64,000 bps; PB = PT x 8
g723r63[2]	–	–	24 bytes	6,300 bps; PB = PT/30 x 24 Note: For PT = 60 ms, PB = 48 bytes
g723r53[3]	–	–	20 bytes	5,300 bps; PB = PT/30 x 20 Note: For PT = 60 ms, PB = 40 bytes

1. The supported packetization period for G.729r8 is limited to a maximum of 60 ms or payload size of 60 bytes.
2. The supported packetization period for G.723r63 is limited to a maximum of 60 ms or payload size of 48 bytes.
3. The supported packetization period for G.723r53 is limited to a maximum of 60 ms or payload size of 40 bytes.

Verifying Codec Repacketization

To verify that codec repacketization is turned on and working properly, use the following **show** commands:

Step 1 Use the **show voip rtp connections** command to display the active RTP connections. The following sample output shows four active RTP connections:

```
Router# show voip rtp connections

        VoIP RTP active connections :
        No. CallId     dstCallId  LocalRTP RmtRTP  LocalIP        RemoteIP
        1   37         38          16582    18236  10.1.1.2       10.1.1.7
        2   38         37          16524    19542  10.1.1.2       10.1.1.1
        3   39         40          17644    2000   10.1.1.2       10.1.1.2
        4   41         40          16622    2000   10.1.1.2       10.1.1.2
```

Step 2 Use the **show sccp connections** command to display information about the connections controlled by the Skinny Client Control Protocol (SCCP) transcoding and conferencing applications:

```
Router# show sccp connections
        sess_id     conn_id     stype mode      codec    ripaddr          rport sport

           3           4        xcode sendrecv g711u    100.1.1.2        2000  16622
           3           3        xcode sendrecv g711u    100.1.1.2        2000  17644

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

Configuring IP-to-IP Call Gain/Loss Control

This feature enables the adjustment of the audio volume within a Cisco UBE call. As with codec repacketization, dissimilar networks that have different built-in loss/gain characteristics may experience connectivity problems. By adding the ability to control the loss/gain within the Cisco UBE, you can more easily connect your networks.

Caution For gain/loss control, be aware that adding gain in a network with echo can generate feedback loud enough to cause hearing damage. Always exercise extreme caution when configuring gain into your network.

To configure IP-IP Call Gain/Loss Control on a voice gateway, you must configure the incoming and outgoing VoIP dial peers, perform the steps in this section. This section contains the following subsections:

- Configuring IP-to-IP Call Gain/Loss Control on the Incoming VoIP Dial Peer, page 97
- Configuring IP-to-IP Call Gain/Loss Control on the Outgoing VoIP Dial Peer, page 99
- Verifying IP-IP Call Gain/Loss, page 100

Configuring IP-to-IP Call Gain/Loss Control on the Incoming VoIP Dial Peer

To configure the incoming VoIP dial peer, complete the following task:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *tag* **voip**
4. **codec**-*type*
5. **incoming called-number** *number*
6. **audio incoming level-adjustment** *value*
7. **audio outgoing level-adjustment** *value*

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 123 voip`	Enters dial-peer configuration mode, defines a particular dial peer, and specifies the method of voice encapsulation as VoIP. • *tag*—Digits that define a particular dial peer. Range is from 1 to 2147483647.
Step 4	**`incoming called-number`** *`number`* **Example:** `Router(config-dialpeer)# incoming called-number 12345`	Specifies a digit string that can be matched by an incoming call to associate the call with the dial peer. • *number*—Series of digits that specify a pattern for the E.164 or private dialing plan telephone number. Valid entries are the digits 0 through 9, the letters A through D, and some special characters. (See the *incoming called-number (dial-peer) command* in the *Cisco IOS Voice Command Reference* for more information.)
Step 5	**`codec`** *`codec-type`* **Example:** `Router(config-dialpeer)# codec g711ulaw`	Specifies the voice coder rate of speech for a dial peer. • *value*—Specifies the voice coder rate for speech.
Step 6	**`audio incoming level-adjustment`** *`value`* **Example:** `Router(config-dialpeer)# audio incoming level-adjustment`	Enables the incoming IP-IP call gain/loss feature on either the incoming dial peer or the outgoing dial peer. • *value*—Range is -27 to 16.
Step 7	**`audio outgoing level-adjustment`** *`value`* **Example:** `Router(config-dialpeer)# audio outgoing level-adjustment`	Enables the outgoing IP-IP call gain/loss feature on either the incoming dial peer or the outgoing dial peer. • *value*—Range is -27 to 16.

Configuring IP-to-IP Call Gain/Loss Control on the Outgoing VoIP Dial Peer

To configure the outgoing VoIP dial peer, complete the following task:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dial-peer voice** *tag* **voip**
4. **destination-pattern** *number*
5. **session target** *destination-address*
6. **codec** *codec-type*
7. **audio incoming level-adjustment** *value*
8. **audio outgoing level-adjustment** *value*

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 123 voip`	Enters dial-peer configuration mode, defines a particular dial peer, and specifies the method of voice encapsulation as VoIP. • *tag*—Digits that define a particular dial peer. Range is from 1 to 2147483647.
Step 4	**`destination-pattern`** *`string`* **Example:** `Router(config-dialpeer)# destination-pattern 12345`	Specifies either the prefix or the full E.164 telephone number to be used for a dial peer. • *string*—Series of digits that specify a pattern for the E.164 or private dialing plan telephone number. Valid entries are the digits 0 through 9, the letters A through D, and some special characters. (See the *destination-pattern command* in the *Cisco IOS Voice Command Reference* for more information.)
Step 5	**`session target ipv4:`***`destination-address`* **Example:** `Router(config-dialpeer)# session target ipv4:10.1.1.1`	Designates a network-specific address to receive calls from a VoIP dial peer. • **ipv4:***destination-address*—IP address of the dial peer to receive calls.

	Command or Action	Purpose
Step 6	**codec** *codec-type* **Example:** `Router(config-dialpeer)# codec g711ulaw`	Specifies the voice coder rate of speech for a dial peer.
Step 7	**audio incoming level-adjustment** *value* **Example:** `Router(config-dialpeer)# audio incoming level-adjustment 5`	Enables the incoming IP-IP call gain/loss feature on either the incoming dial peer or the outgoing dial peer. • *value*—Range is -27 to 16.
Step 8	**audio outgoing level-adjustment** *value* **Example:** `Router(config-dialpeer)# audio outgoing level-adjustment -5`	Enables the outgoing IP-IP call gain/loss feature on either the incoming dial peer or the outgoing dial peer. • *value*—Range is -27 to 16.

Note The DSP requires one level for each stream, so the *value* for audio incoming level-adjustment and the *value* for audio outgoing level-adjustment will be added together. If the combined values are outside of the limit the DSP can perform, the value sent to the DSP will be either the minimum (-27) or maximum (+16) supported by the DSP.

Verifying IP-IP Call Gain/Loss

To verify that IP-IP call gain/loss is turned on and working properly, use the following **show** commands:

Step 1 Use the **show call active** command to display the gain/loss statistics for active calls on the dial peer:

```
Router# show call active
```

Step 2 Use the **show call history** command to display the gain/loss statistics history on the dial peer:

```
Router# show call history
```

Configuring Voice Quality Metrics

This feature adds voice quality measurements for the Cisco UBE voice call. Prior to this feature, the ability to gather statistics within the gateway required a TDM-to-IP call because the DSP performed statistics gathering. The Voice Quality Metrics feature enables statistics gathering on packet arrival (late/lost/early). From these statistics, a voice quality measurement is developed to give the quality of the call. The output is in a simple format, using a system of good, poor, and bad types of ratings.

The Voice Quality Metrics feature is enabled by the addition of the **media monitoring** [*max-calls*] command:

- Under **voice service voip**, enter the **media monitoring** [*max-calls*] command to define the maximum number of monitoring calls. This creates a monitoring pool with a maximum number of elements.
- For Cisco IAD 2400sSeries, under **voip service voip**, enter the **allow-connections sip to sip** command.

- You must also enter the **media monitoring** command at the dial-peer level to enable monitoring for the calls landing on the dial peer.

Note Because each monitoring call uses a table of 500 entries to hold RTP packet header information, time stamp, etc. for the background statistics process, about 12150 bytes of extra memory are needed for a call using the Voice Quality Metrics function. The **media monitoring** command allows you to use different voice quality metrics to experiment with the memory impact on the gateway. When the **media monitoring** command is not configured, no data structure collects voice quality metrics, so no voice quality monitoring occurs.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **mode border-element**
5. **media monitoring** [*max-calls*]
6. **end**
7. **dial-peer voice** *tag* **voip**
8. **media monitoring**

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 Voice over IP as the voice-encapsulation type.

Step 4	`mode border-element`
	
	Example:
	`Router(conf-voi-serv)# mode border-element`
		Enables the audio call-scoring of the **media monitoring** command. If you do not enter the **mode border-element** command, the **media monitoring** command is not available for Cisco UBE voice connections.
		Note The **mode border-element** command is for configuration on the Cisco 2900 and Cisco 3900 series platforms only. Do not use this command on the Cisco 2800 or Cisco 3800 series platforms. For Cisco IAD 2400 series platforms, use the **allow-connections sip to sip** command.

	Command or Action	Purpose
Step 5	**media monitoring** [*max-calls*] **Example:** `Router(conf-voi-serv)# media monitoring 300`	Enables media monitoring and specifies the maximum number of calls to be monitored. • *max-calls*—Range for this value is 1 to 302.
Step 6	**end** **Example:** `Router(conf-voi-serv)# end`	• Exits voice service configuration mode and returns to global configuration mode.
Step 7	**dial-peer voice** *tag* **voip** **Example:** `Router(config)# dial-peer voice 123 voip`	Enters dial-peer configuration mode, defines a particular dial peer, and specifies the method of voice encapsulation as VoIP. • *tag*—Digits that define a particular dial peer. Range is from 1 to 2147483647.
Step 8	**media monitoring** **Example:** `Router(config-dialpeer)# media monitoring`	Enables media monitoring for calls landing on the dial peer specified in Step 7.

Verifying Voice Quality Metrics

To verify that the voice quality metrics feature is turned on and working properly, use the following **show** commands:

- **show voice monitoring-channels**
- **show call active voice**
- show call active voice stats

Step 1 Use the **show voice monitoring-channels** command to display monitoring statistics:

```
Router# show voice monitoring-channels

  max vq mon channels =  10 vq mon channels in use =  2 vq mon channels left =8
```

Step 2 Use the **show call active voice** command to display statistics on the Cisco UBE if the Voice Quality Metrics feature is configured. An abbreviated sample of output follows:

```
Router# show call active voice

  RxPakNumber=5496
  RxSignalPak=0
  RxComfortNoisePak=0
  RxDuration=109900
  RxVoiceDuration=109920
  RxOutOfSeq=0
  RxLatePak=0
  RxEarlyPak=0
  RxBadProtocol=0
  LevelRxPowerMean=0
  ErrRxDrop=0
  ErrRxControl=0
```

Step 3 Use the **show call active voice stats** command to display Concealment Statistics and R-Factor Statistics (G.107 MOS) on the Cisco UBE if the Voice Quality Metrics feature is configured. A sample of output follows for a voice call using G.711ulaw, VAD on, and at 5 percent packet loss rate:

```
Router# show call active voice stats

DSP/CS: CR=0.0527, AV=0.0502, MX=0.0527, CT=1220, TT=24270, OK=50, CS=44, SC=0, TS=50,
DC=0

SP/RF: ML=3.9855, MC=0.0000, R1=79, R2=0, IF=15, ID=0, IE=0, BL=25, R0=94, VR=1.1
```

In the sample output, the following can be noted:

- The average conceal ratio (AV) is about 5 percent
- The ratio of total conceal time and total speech time is about 5 percent (1220/24270)
- BL for codec G.711 is 25 (based on G.113)
- IE for codec G.711 is 0 (G.113)
- R0 is 94 (G.107)

Table 4 defines the abbreviations used in the sample output.

Table 4 Router output definations for the show call active command

Type	Abbreviation	Definition
DSP/CS: Concealment Statistics	CR	concealRatioCurrent
	AV	ConcealRatioAverage
	MX	ConcealRatioMaximum
	CT	ConcealDuration
	TT	SpeechDuration
	OK	OkSeconds
	CS	ConcealSeconds
	SC	SevereConcealSeconds
	TS	SevereConcealThreshold
DSP/RF: R-Factor Statistics (G.107 MOS)	ML	MOSLQE
	R1	RFactorProfile1
	IF	IeEff
	BL	CodecBaselineBPL
	R0	R0Default
	VR	R-Factor version

SRST Support for G.722 Codec

SRST provides fail-over support for IP phones at remote branch offices that are supported by a central Cisco Unified Communications Manager system with the phones running the SCCP/SIP protocol across WAN links.

Phones are provisioned by Cisco Unified Communications Manager. This information is stored in the phones and then made available to the SRST router when the WAN link fails. SRST extracts the stored information from the phones when they register for service with SRST. SRST uses this information to automatically build the needed configuration.

Prior to Cisco IOS Release 15.0(1)M, G.711 ulaw has been the default narrowband codec for LAN. As the use of wideband codecs expands, G.722 is expected to be the default wideband codec. This increased use of the G.722 codec in LANs has created a need for SRST support with this codec.

This feature provides support for the G.722 codec in SRST mode. To enable G.722-64K codec support as the default codec in SRST mode, enter the **codec g722-64k** command in call-manager-fallback configuration mode:

```
Router(config)# call-manager-fallback
Router(config-cm-fallback)# codec g722-64k
```

The following shows a sample configuration of call-manager-fallback with the G.722 codec configured:

```
Router# call-manager-fallback
max-conferences 8 gain -6
transfer-system full-consult
codec g722-64

incoming called-number 52222
```

Troubleshooting and Verifying Fundamental Cisco Unified Border Element Configuration and Operation

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

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
- The Sub-RTCP sender report (SR) and receiver report (RR) packets are feedback packets of RTP Senders and RTP Receivers respectively.
- The SR includes a 20-byte sender information section for use by active senders.
- Both the SR and RR forms include zero or more reception report blocks and each reception report block provides statistics about the data received from the particular source.
- Use the **debug voip rtcp sub-rtcp** command to debug for LostPackets in the Media Statistics feature.

```
Router# debug voip rtcp sub-rtcp

VOIP RTCP Subrtcp debugging is on
Oct 16 19:35:26.870: SUBRTCP:tx SR (15.5.34.5-17893)->(15.5.34.158,17795)
rtcp-intv(5002 ms)
Oct 16 19:35:26.870: SUBRTCP Sender Report dump Length - 32:
```

```
80 FA 00 07 0F 25 22 05 80 C8 00 05 C8 DE 5D 7E DE C6 2A 6D 00 00 00 00  00 00 00 00
00 00 00 00
Oct 16 19:35:26.878: SUBRTCP:tx SR (15.5.34.5-16991)->(15.5.34.6,18745) rtcp-intv(5005
ms)
Oct 16 19:35:26.878: SUBRTCP Sender Report dump Length - 32:
80 FA 00 07 05 CD 22 05 80 C8 00 05 C8 DE 5D 7E E0 D2 59 C1 00 00 00 00  00 00 00 00
00 00 00 00
```

- Use the **debug voip statistics** command to debug the Media Statistics feature in the Cisco Unified Border Element.

```
Router# debug voip rtp statistics

VOIP RTP Statistics debugging is on
Oct 16 19:38:20.000: RTP[15.5.34.6-0x1B5B2298]: loss(0) jitter(5 ms, 5992 us)
Oct 16 19:38:22.556: RTP[15.5.34.6-0x1B5B2298]: loss(0) jitter(8 ms, 8054 us)
```

For additional 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*
- *VoIP Debug Commands*

Verifying Fundamental Cisco Unified Border Element Configurations

To verify Cisco Unified Border Element 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.

Configuration Examples for Fundamental Cisco Unified Border Element

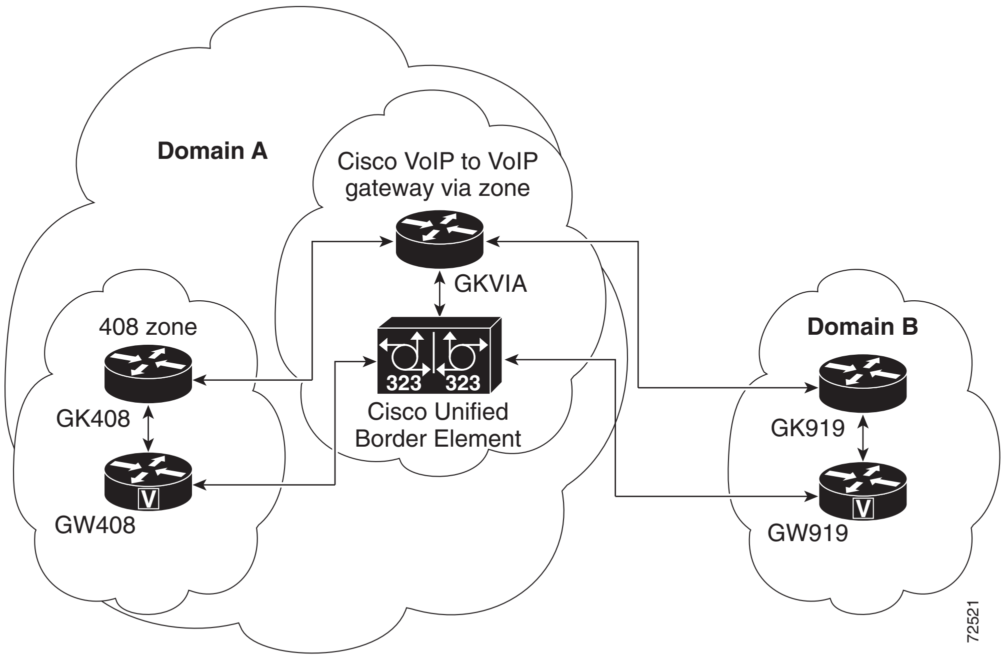
This chapter includes the following configuration examples:

- Cisco Unified Border Element: Example, page 107
- Local-to-Remote Network Using the Cisco Unified Border Element: Example, page 109
- Remote-to-Local Network Using the Cisco Unified Border Element: Example, page 110
- Remote-to-Remote Network Using a Cisco Unified Border Element: Example, page 111
- Remote-to-Remote Network Using Two Cisco Unified Border Elements: Example, page 112
- Codec Repacketization: Example, page 113
- Voice Quality Metrics: Example, page 114

Cisco Unified Border Element: Example

Figure 3 shows an example configuration of the Cisco Unified Border Element feature.

Figure 3 Cisco Unified Border Element Feature Topology



For a detailed description of the actions that occur during a call, see Figure 1 on page 80 The following examples show gateway and gatekeeper configuration.

Originating Gateway Configuration: Example

```
interface Ethernet0/0
 ip address 10.16.8.132 255.255.255.0
 half-duplex
 h323-gateway voip interface
 h323-gateway voip id GK408 ipaddr 10.16.8.123 1718
 h323-gateway voip h323-id GW408
!
dial-peer voice 919 voip
 destination-pattern 919.......
 session target ras
!
gateway
```

Originating Gatekeeper Configuration: Example

```
gatekeeper
 zone local GK408 usa 10.16.8.123
 zone remote GKVIA usa 10.16.8.24 1719
 zone prefix GKVIA 919*
 gw-type-prefix 1#*
 no shutdown
```

Cisco Unified Border Element Configuration: Example

```
!
voice service voip
 no allow-connections any to pots
 no allow-connections pots to any
 allow-connections h323 to h323
 h323
  ip circuit max-calls 1000
  ip circuit default only
!
!
interface FastEthernet0/0
 ip address 10.16.8.145 255.255.255.0
 ip route-cache same-interface
 duplex auto
 speed auto
 h323-gateway voip interface
 h323-gateway voip id GKVIA ipaddr 10.16.8.24 1718
 h323-gateway voip h323-id IPIPGW
 h323-gateway voip tech-prefix 1#
!
!
dial-peer voice 919 voip
 incoming called-number 919.......
 destination-pattern 919.......
 session target ras
 codec transparent
!
gateway
```

Via Zone Gatekeeper Configuration: Example

```
gatekeeper
 zone local GKVIA usa 10.16.8.24
 zone remote GK919 usa 10.16.8.146 1719 invia GKVIA outvia GKVIA
 zone prefix GK919 919*
 no shutdown
```

Terminating Gateway: Example

```
interface Ethernet0/0
 ip address 10.16.8.134 255.255.255.0
 half-duplex
 h323-gateway voip interface
 h323-gateway voip id GK919 ipaddr 10.16.8.146 1718
 h323-gateway voip h323-id GW919
 h323-gateway voip tech-prefix 919
!
dial-peer voice 919 pots
 destination-pattern 919.......
 port 1/0:1
!
gateway
```

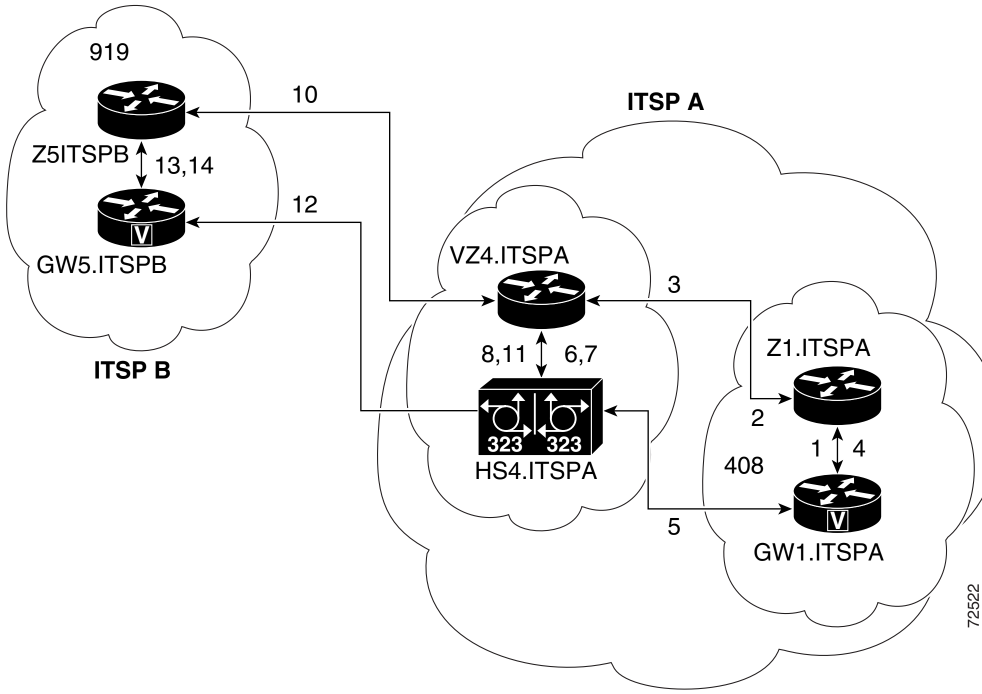
Terminating Gatekeeper Configuration: Example

```
gatekeeper
 zone local GK919 usa 10.16.8.146
 gw-type-prefix 1#* default-technology
 no shutdown
```

Local-to-Remote Network Using the Cisco Unified Border Element: Example

Figure 4 shows a local-to-remote network using the Cisco Unified Border Element feature.

Figure 4 Local-to-Remote Network Using the Cisco Unified Border Element Feature Topology

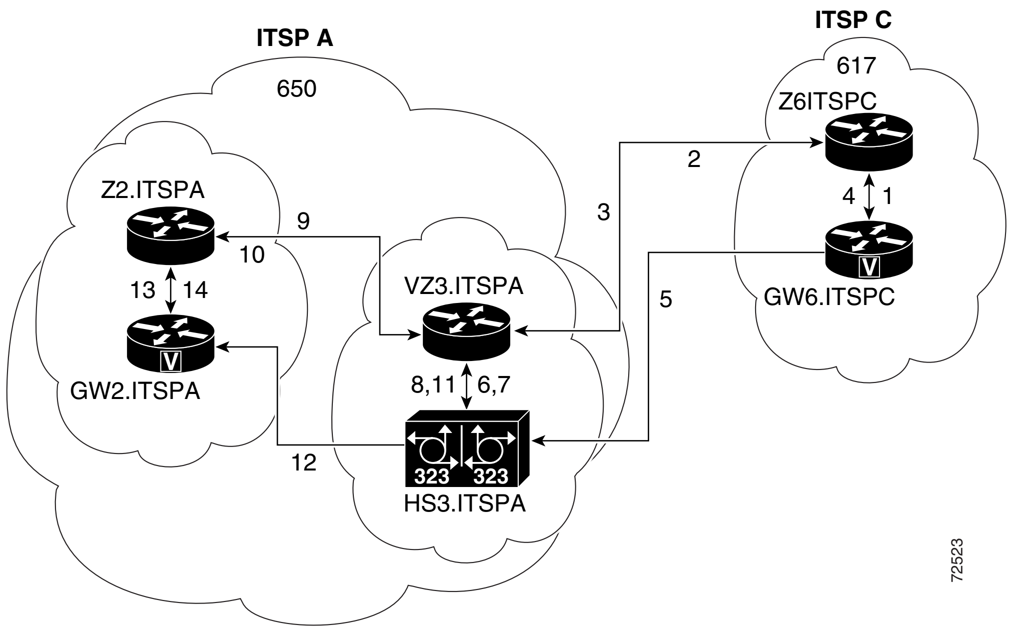


Note For a detailed configuration example of a local-to-remote network using the Cisco Unified Border Element, see the following URL: :http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example09186a00801b0803.shtml

Remote-to-Local Network Using the Cisco Unified Border Element: Example

Figure 5 shows a remote-to-local network using the Cisco Unified Border Element feature.

Figure 5 Remote-to-Local Network Using the Cisco Unified Border Element Feature Topology

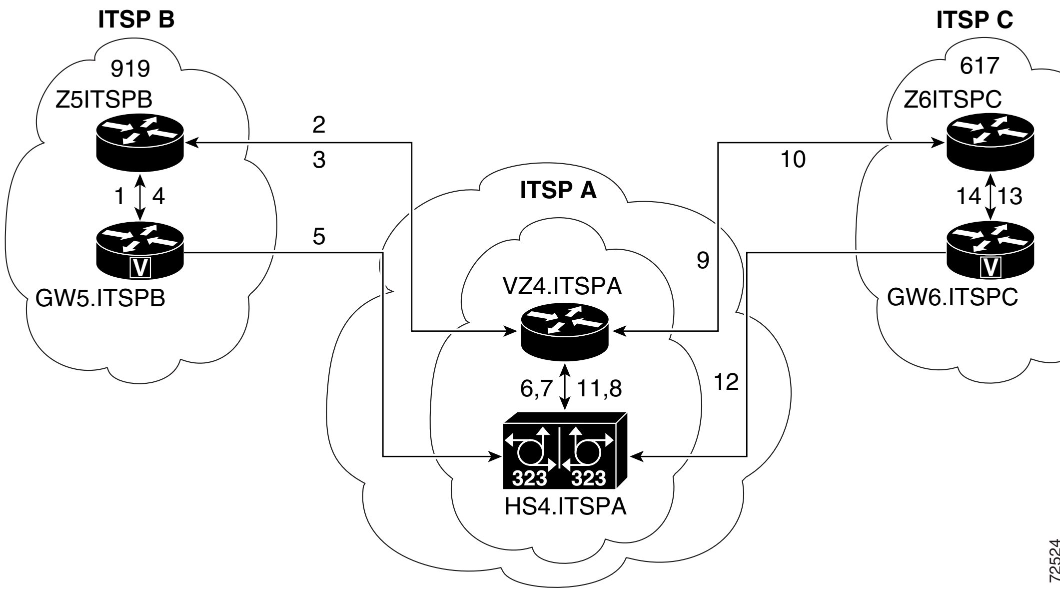


Note For a detailed configuration example of a remote-to-local network using the Cisco Unified Border Element, see the following URL:
http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example
09186a0080203edc.shtml.

Remote-to-Remote Network Using a Cisco Unified Border Element: Example

Figure 6 shows a remote-to-remote network using an Cisco Unified Border Element.

Figure 6 Remote-to-Remote Network Using a Cisco Unified Border Element Topology

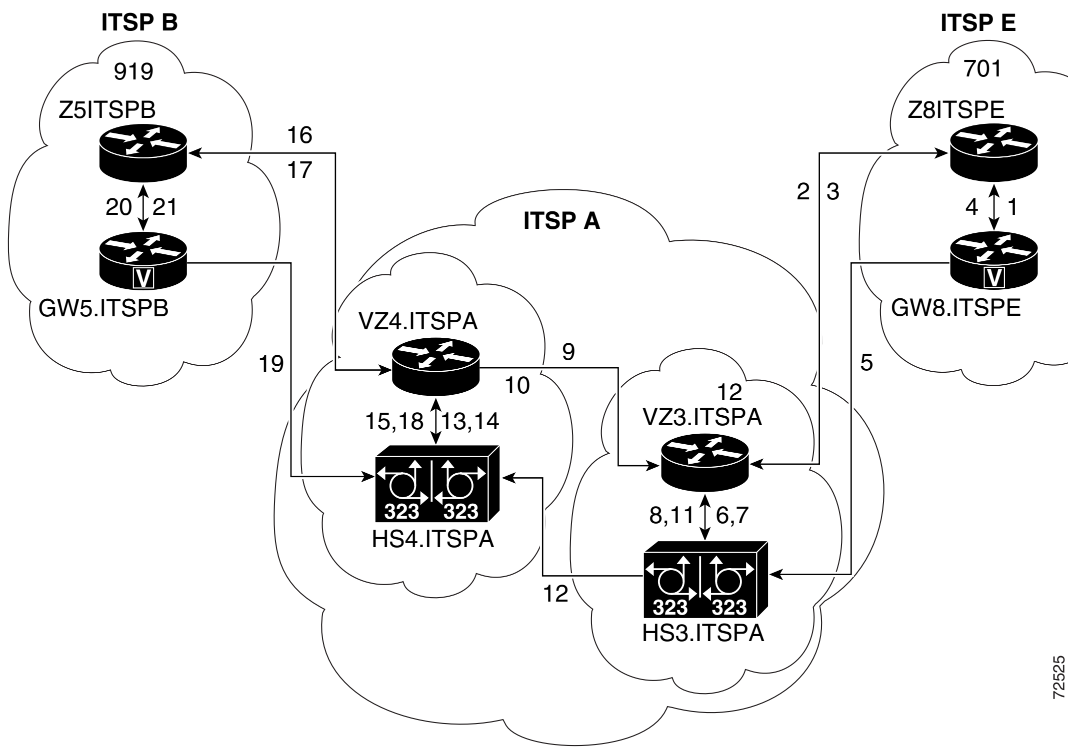


Note For a detailed configuration example of a remote-to-remote network using the Cisco Unified Border Element, see the following URL:
http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example
09186a0080203edd.shtml.

Remote-to-Remote Network Using Two Cisco Unified Border Elements: Example

Figure 7 shows a remote-to-remote network using two Cisco Unified Border Elements.

Figure 7 Remote-to-Remote Network Using Two Cisco Unified Border Elements Topology



Note For a detailed configuration example of a remote-to-remote network using two Cisco Unified Border Elements, see the following URL:
http://www.cisco.com/en/US/tech/tk1077/technologies_configuration_example
09186a0080203edb.shtml.

Using the Cisco Unified Border Element to Assign DSCP Code Points to Gateway Traffic

The following example configures the Cisco Unified Border Element to assign DSCP code points to traffic that passes through the gateway:

```
dial-peer voice 1 voip
 incoming called-number .T
 destination-pattern .T
 ip qos dscp ef media
 ip cos dscp af31 signaling
 session target ras
 codec transparent
```

Using Class and Policy Maps to Control Bandwidth Allocation

The following example uses class and policy maps to control bandwidth allocation based on matching received DSCP code points:

```
class-map match-all Silver-Data
 match ip dscp af11
 match ip dscp af12
 match ip dscp af13
class-map match-all Voice-Control
 match ip dscp af31
class-map match-all Gold-Data
 match ip dscp af21
 match ip dscp af22
 match ip dscp af23
class-map match-all Voice
 match ip dscp ef
!
!
policy-map LLQ
 class Voice
  priority percent 40
 class Voice-Control
  bandwidth remaining percent 5
 class Gold-Data
  bandwidth remaining percent 45
 class Silver-Data
  bandwidth remaining percent 35
 class class-default
bandwidth remaining percent 5
  random-detect dscp-based
  random-detect dscp 2   70    128   10
  random-detect dscp 4   58    128   10
  random-detect dscp 6   44    128   10
policy-map FairQueue
 class class-default
```

Codec Repacketization: Example

The following is a sample configuration of codec repacketization for a destinated callee number 52222:

```
dial-peer voice 416 voip
destination-pattern 52222
session protocol sipv2
session target ipv4:1.7.92.99
codec g711ulaw bytes 160 fixed-bytes
!
dial-peer voice 4161 voip
incoming called-number 52222
session protocol sipv2
codec g711ulaw bytes 80 fixed-bytes
```

Voice Quality Metrics: Example

The following is a sample configuration of the voice quality metrics feature on a gateway that allows a maximum of 100 calls to be monitored, and calls under voip dial-peer 4161 to be monitored:

```
voice service voip
media monitor 100
allow-connections h323 to h323
allow-connections h323 to sip
allow-connections sip to h323
allow-connections sip to sip
dial-peer voice 4161 voip
media monitoring
```

Where to Go Next

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

Table 5 lists 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 5 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 5 Feature Information for fundamental Cisco Unified Border Element Configuration

Feature Name	Releases	Feature Information
Cisco Unified Border Element with OSP	12.2(13)T3	Enables VoIP service providers to gain the benefits of the Cisco Unified Border Element and to make use of routing, billing, and settlement capabilities offered by OSP-based clearinghouses.
Codec support	12.2(13)T3 12.4(11)T	12.2(13)T3—Codec Transparency on an Cisco Unified Border Element. Enables the Cisco Unified Border Element to pass codec capabilities between endpoints. 12.4(11)T—iLBC Codec on an Cisco Unified Border Element. Supports robust voice communication over IP using the iLBC codec in Cisco Unified Border Element networks.
Ethernet Interface	12.2(13)T3	Configures Cisco Unified Border Element feature to operate with either a single Ethernet interface for all incoming, outgoing, and via-zone gatekeeper traffic or two Ethernet interfaces for signaling and media streams.
Hosted NAT Traversal Enhancements	12.4(11)XJ2	This feature was introduced.
Identify Alternate endpoint Call Attempts in RADIUS Call Accounting Records	12.4(4)T	This feature was introduced.
Interoperability Enhancements to the Cisco Unified Border Element	12.4(4)T	This feature was introduced.
IP Call Leg Statistics (Delay, Jitter and Return Trip Time)	12.4(11)XJ2	This feature was introduced.
iSAC Codec Support on Cisco TDM-IP Voice Gateways and Cisco UBE Platforms	15.1(1)T	This feature provides support for the iSAC wideband codec on TDM-IP voice gateways and on Cisco UBE platforms.
Media Modes	12.3(1)	Cisco Unified Border Element with Media Flow-Around
Microsoft NetMeeting Interoperability	12.3(7)T	This feature was introduced.
QoS for an Cisco Unified Border Element	12.2(13)T3	Assigns differentiated services code points (DSCP) for H.323 calls through the Cisco Unified Border Element,

Table 5 Feature Information for fundamental Cisco Unified Border Element Configuration (continued)

Feature Name	Releases	Feature Information
Rotary Support	12.3(11)T	12.3(11)T—Call-Failure Recovery (rotary)
RTP Loopback Interface	12.2(13)T3	The Cisco Unified Border Element supports configuration of an RTP loopback dial peer for use in verifying and troubleshooting H.323 networks.
Signaling Interworking	12.3(11)T	Slow-Start to Fast-Start Interworking
SG3 Fax Support on Cisco TDM-IP Voice Gateways and Cisco UBE Platforms	15.1(1)T	This feature provides T.38 fax relay and fax pass-through on TDM-IP voice gateways and on Cisco UBE platforms.
Tcl+IVR in an IP-Only Environment	12.3(7)T	This feature was introduced.
Transcoding and Interworking:	12.3(11)T 12.4(11)XJ2	12.3(11)T—Voice-Codec Transcoding 12.4(11)XJ2—DTMF Transcoding and Interworking: • H245 <--> KPML • T.38 Fax using NSE • Transcoding with AS5x platforms
Voice Quality Enhancements on Cisco Unified Border Element Platforms	15.0(1)M	This feature provides the following enhancements to voice quality on Cisco Unified Border Element (Cisco UBE) platforms: • Codec Repacketization—Connects dissimilar networks that may have different packetization time periods. • IP-IP Call Gain/Loss Control—Enables the adjustment of the audio volume within a Cisco UBE voice call. • Voice Quality Measurements—Adds voice quality measurements for the Cisco UBE voice call.

Glossary

DSP—Digital Signal Processor

ETSI—European Telecommunications Standards Institute

GSM—Groupe Speciale Mobile

RTP—Real-Time Transport Protocol

SCCP—Skinny Client Control Protocol

SIP—Session Initiation Protocol

SRTP—Secure Real-Time Transport Protocol

VoIP—Voice over Internet Protocol

TDM—Time Division Multiplexing

3GPP—Third Generation Partnership Project

3G—Third generation

Note See *Internetworking Terms and Acronyms* for terms not included in this glossary.