Configuring H.323 Gateways

This chapter describes the configuration of H.323 gateways.

Feature History for Basic Service Relationships (H.225 Annex-G)

Release	Modification
12.2(11)T	This feature was introduced.

Feature History for Cisco H.323 Scalability and Interoperability Enhancements for Gatekeepers

Release	Modification
12.2(2)XA	This feature was introduced.
12.2(4)T	This feature was integrated into this release.
12.2(2)XB1	This feature was implemented on the Cisco AS5850.
12.2(11)T	This feature was integrated into this release.

Feature History for Gateway Codec Order Preservation and Shutdown Control

Release	Modification
12.3(1)	This feature was introduced.

Feature History for H.323 Dual Tone Multifrequency Relay Using Named Telephone Events

Release	Modification
12.2(2)XB	The Dual Tone Multifrequency Relay for SIP Calls Using Named Telephone Events feature was introduced. The Media Gateway Control Protocol-Based Fax (T.38) and Dual Tone Multifrequency (IETF RFC 2833) Relay feature was also introduced.
12.2(11)T	H.323 support for DTMF relay was added.

Feature History for H.323 Version 2 Enhancements

Release	Modification
12.0(5)T	This feature was introduced.

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

12.1(5)XM2	Support was added for the Cisco AS5350 and Cisco AS5400.
12.2(2)XA	The **call rscmon update-timer** command was added.
12.2(4)T	The **call rscmon update-timer** command was integrated into this release. Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 is not included.
12.2(2)XB1	This feature was implemented on the Cisco AS5850.
12.2(11)T	This feature was integrated into this release.

Feature History for H.323v4 Gateway Zone Prefix Registration Enhancements

Release	Modification
12.2(15)T	This feature was introduced.
12.3(3)	The **ras rrq dynamic prefixes** and the **rrq dynamic-prefixes-accept** commands were modified to be disabled by default.
12.3(4)T	This feature was integrated into this release.
12.4(9)T	The **terminal-alias-pattern** command was introduced to send the gateway priority along with dynamic zone prefixes from the gateway.

Feature History for Signal ISDN B-Channel ID to Enable Application Control of Voice Gateway Trunks

Release	Modification
12.3(7)T	This feature was introduced.

Feature History for H.323 VoIP Call Preservation Enhancements for WAN Link Failures

Release	Modification
12.4(4)XC	This feature was introduced.
12.4(9)T	This feature was integrated into this release.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Note For more information about these and other related Cisco IOS voice features, see the following:

- "H.323 Overview" section on page 9
- For information about the full set of Cisco IOS voice features, see the entire Cisco IOS Voice Configuration Library—including library preface, glossary, and other documents—at http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/cisco_ios_voice_configuration_library_glossary/vcl.htm

Contents

Note For complete descriptions of the commands used in this chapter, see the command references listed in the "Additional References" section on page 119.

Prerequisites for Configuring H.323 Gateways

- Perform the prerequisites that are listed in the "Prerequisites for Configuring an H.323 Network" section on page 9.
- Develop a network plan that details the requirements and characteristics of your VoIP network. For more information, see the documents in the "Additional References" section on page 21
- Ensure that the routers you intend to configure as H.323 gateways are running a Cisco IOS software image that contains gateway functionality.
- To use H.323 security and accounting features, do the following:
  - These features use the H.235 standard. Because the standard is broad, ensure that the gatekeeper provides H.235 functionality that specifically complements the gateway implementation described in this document.
  - The H.323 gateway sends accounting information using a nonstandard field in the ClearToken field. Ensure that the gatekeeper can retrieve this information from the ClearToken field.

Restrictions for Configuring H.323 Gateways

Restrictions are described in the Restrictions for Configuring an H.323 Network, page 10

Note The gatekeeper authenticates the endpoint based on the general ID. It does not relate the H.323 ID and general ID. Both the gateway H323_ID and the generalID in ClearTokens should be same.

How to Configure H.323 Gateways

This section contains the following information:

- Configuring a Router Interface as a Gateway, page 28
- Shutting Down and Enabling VoIP Services on a Gateway, page 30
- Configuring Gateway RAS, page 33

- Configuring E.164-Address Registration, page 39
- Configuring In-Band Tones and Announcements, page 39
- Configuring Gateway AAA, page 41
- Configuring H.235 Gateway Security, page 41
- Configuring Alternate-Gatekeeper Support, page 48
- Configuring DTMF Relay, page 51
- Configuring FXS Hookflash Relay, page 56
- Configuring Multiple Codecs, page 58
- Configuring Rotary Calling Pattern, page 60
- Configuring H.323 Support for Virtual Interfaces, page 60
- Configuring Annex G, page 62
- Configuring H.225, page 72
- Configuring the VoIP Transport Method, page 78
- Configuring Zone Bandwidth Management, page 78
- Configuring H.323 Version 4 Zone Prefix Registration, page 85
- Configuring Call Admission Control, page 92
- Configuring Trunk-Based and Carrier-Based Routing, page 92
- Configuring Signal ISDN B-Channel ID to Enable Application Control of Voice Gateway Trunks, page 92
- Configuring H.323 VoIP Call Preservation Enhancements for WAN Link Failures, page 95

Configuring a Router Interface as a Gateway

To configure a Cisco device as an H.323 gateway in a service provider environment, configure at least one of its interfaces as a gateway interface. Use either an interface that is connected to the gatekeeper or a loopback interface for the gateway interface. The interface that is connected to the gatekeeper is usually a LAN interface: Fast Ethernet, Ethernet, FDDI, or Token Ring.

Configuring a Router Interface

To configure a gateway interface, use the following commands beginning in global configuration mode.

SUMMARY STEPS

1. **gateway**
2. **exit**
3. **ip cef**
4. **interface** *type number* [*nametag*]
5. **h323-gateway voip interface**
6. **h323-gateway voip id** *gatekeeper-id* {**ipaddr** *ip-address* [*port*] | **multicast**} [**priority** *priority*]
7. **h323-gateway voip h323-id** *interface-id*

8. **h323-gateway voip tech-prefix** *prefix*
9. **exit**

DETAILED STEPS

	Command	Purpose

Step 1	**`gateway`**
	Example:
	`Router(config)# gateway`
		Enters gateway configuration mode and enables the gateway.

Step 2	**`exit`**
	Example:
	`Router(config-gateway)# exit`
		Exits the current mode.

Step 3	**`ip cef`**
	Example:
	`Router(config)# ip cef`
		(Optional) Enables Cisco Express Forwarding routing.

Step 4	**`interface`** *`type number`* **`[`***`nametag`***`]`**
	Example:
	`Router(config)# interface serial 0`
		Enters interface configuration mode for the interface that is connected to the gatekeeper. Keywords and arguments are as follow:
		• *type*—Type of interface to be configured.
		• *number*—Port, connector, or interface card number. The number is assigned at the factory at the time of installation or when added to a system and can be displayed with the **show interfaces** command.
		• *nametag*—Logic name to identify the server configuration so that multiple entries of server configuration can be entered.

Step 5	**`h323-gateway voip interface`**
	Example:
	`Router(config-if)# h323-gateway voip interface`
		Identifies this as a VoIP gateway interface.

	Command	Purpose
Step 6	**h323-gateway voip id** *gatekeeper-id* {**ipaddr** *ip-address* [*port*]| **multicast**} [**priority** *priority*] **Example:** `Router(config-if)# h323-gateway voip id gk3.gg-dn1 ipaddr 172.18.0.0 1719`	(Optional) Defines the name and location of the gatekeeper for this gateway. Keywords and arguments are as follows: • *gatekeeper-id*—H.323 identification of the gatekeeper. Must exactly match the gatekeeper ID in the gatekeeper configuration. Recommended format: name.domainname. • **ipaddr** *ip-address*—IP address to be used to identify the gatekeeper. • *port*—Port number used. • **multicast**—Gateway uses multicast to locate the gatekeeper. • **priority** *priority*—Priority of this gatekeeper. Range: 1 to 127. Default: 127.
Step 7	**h323-gateway voip h323-id** *interface-id* **Example:** `Router(config-if)# h323-gateway voip h323-id name@domainname`	(Optional) Defines the H.323 name of the gateway, identifying this gateway to its associated gatekeeper. Usually this ID is the name of the gateway, with the gatekeeper domain name appended: name@domainname.
Step 8	**h323-gateway voip tech-prefix** *prefix* **Example:** `Router(config-if)# h323-gateway voip tech-prefix 1#`	(Optional) Defines the numbers used as the technology prefix that the gateway registers with the gatekeeper. Can contain up to 11 characters. Although not strictly necessary, a pound symbol (#) is frequently used as the last digit in a prefix. Valid characters: 0 to 9, #, and *.
Step 9	**exit** **Example:** `Router(config-if)# exit`	Exits the current mode.

Verifying a Router Interface

To verify the router interface, perform the following step.

Step 1 **show gateway**

Use this command to verify gateway configuration by displaying the current registration information and gateway status.

```
Router# show gateway
```

Shutting Down and Enabling VoIP Services on a Gateway

This section contains the following procedures:

- Shutting Down and Enabling VoIP Service, page 31 (optional)
- Shutting Down and Enabling VoIP Submodes, page 31 (optional)

- Verifying Gateway Status, page 32

Shutting Down and Enabling VoIP Service

To shut down or enable all VoIP services on a Cisco gateway, use the following commands beginning in global configuration mode.

SUMMARY STEPS

1. **voice service voip**
2. **no shutdown forced**
3. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`voice service voip`**
	Example:
	`Router(config)# voice service voip`
		Enters voice-service-VoIP configuration mode.

Step 2	**`no shutdown forced`**
	Example:
	`Router(conf-voi-serv)# shutdown forced`
		Shuts down or enables VoIP call services.

Step 3	**`exit`**
	Example:
	`Router(conf-voi-serv)# exit`
		Exits the current mode.

Shutting Down and Enabling VoIP Submodes

To shut down and enable VoIP submodes, use the following commands beginning in global configuration mode.

SUMMARY STEPS

1. **voice service voip**
2. **h323**
3. **no call service stop maintain-registration**
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**voice service voip** **Example:** `Router(config)# voice service voip`	Enters voice-service-VoIP configuration mode.
Step 2	**h323** **Example:** `Router(conf-voi-serv)# h323`	Selects H.323-call-processing submode.
Step 3	**no call service stop forced maintain-registration** **Example:** `Router(conf-voi-serv)# call service stop maintain-registration`	Shuts down or enables VoIP call services for the selected submode.
Step 4	**exit** **Example:** `Router(conf-voi-serv)# exit`	Exits the current mode.

Verifying Gateway Status

To verify gateway status, perform the following step.

Step 1 **show gateway**

Use this command to display gateway status.

The following example displays output after the gateway has been shut down:

```
Router# show gateway

H.323 ITU-T Version: 4.0   H323 Stack Version: 0.1
 H.323 service is shutdown
 Gateway  Router is not registered to any gatekeeper
```

The following example displays output after a graceful shutdown with calls in progress:

```
Router# show gateway

H.323 ITU-T Version: 4.0   H323 Stack Version: 0.1
 H.323 service is shutting down
 Gateway  Router is registered to Gatekeeper GK1
```

The following example displays output when H.323 call service has been shut down with the **call service stop maintain-registration** command:

```
Router# show gateway

H.323 ITU-T Version: 4.0   H323 Stack Version: 0.1
 H.323 service is shutdown
 Gateway  Router is registered to Gatekeeper GK1
```

Configuring Gateway RAS

This section contains the following information:

- Configuring Basic RAS, page 33
- Configuring RAS Retries and Timers, page 36
- Configuring Gateway-Resource-Availability Reporting, page 39

Registration, Admission, and Status (RAS) signaling performs registration, admissions, status, and disengage procedures between the H.323 VoIP gateway and the H.323 VoIP gatekeeper. RAS tells the gatekeeper to translate a E.164 phone number of the session target into an IP address.

In the RAS exchange between a gateway and a gatekeeper, a technology prefix is used to identify the specific gateway when the selected zone contains multiple gateways. The **tech-prefix** command is used to define technology prefixes.

In most cases there is a dynamic protocol exchange between the gateway and the gatekeeper that enables the gateway to inform the gatekeeper about technology prefixes and where to forward calls. If, for some reason, that dynamic registry feature is not in effect, statically configure the gatekeeper to query the gateway for this information.

Note To configure the gatekeeper to query for prefix and forwarding information, see "Configuring H.323 Gatekeepers and Proxies" section on page 121.

To configure RAS, define specific parameters for the applicable POTS and VoIP dial peers. The POTS dial peer informs the system of which voice port to direct incoming VoIP calls to and (optionally) determines that RAS-initiated calls have a technology prefix prepended to the destination telephone number. The VoIP dial peer determines how to direct calls that originate from a local voice port into the VoIP cloud to the session target. The session target indicates the address of the remote gateway where the call is terminated. There are several different ways to define the destination gateway address:

- By statically configuring the IP address of the gateway.
- By defining the Domain Name System (DNS) name of the gateway.
- By using RAS. If RAS is used, the gateway determines the destination target by querying the RAS gatekeeper.

Configuring Basic RAS

To configure basic RAS, use the following commands beginning in global configuration mode.

SUMMARY STEPS

1. **dial-peer voice** *tag* **pots**
2. **destination-pattern** *string*[**T**]
3. **port** *controller***:D**
4. **exit**
5. **dial-peer voice** *tag* **voip**
6. **destination-pattern** *string*[**T**]
7. **tech-prefix** *number*

8. **session target ras**
9. **exit**

DETAILED STEPS

	Command	Purpose

Step 1	**`dial-peer voice`** *`tag`* **`pots`**
	Example:
	`Router(config)# dial-peer voice 456 pots`
		Enters dial-peer configuration mode for the POTS dial peer designated by *tag*.

Step 2	**`destination-pattern`** *`string`*`[`**`T`**`]`
	Example:
	`Router(config-dial-peer)# destination-pattern 1513200....`
		Specifies the E.164 address associated with this dial peer. Keywords and arguments are as follows:
		• *string*—E.164 or private dialing plan telephone number. Valid entries: digits 0 to 9, letters A to D, and the following special characters:
		– Asterisk (*) and pound sign (#)—Keys that appear on standard touchtone dial pads.
		– Comma (,)—Pause between digits.
		– Period (.)—Match to any entered digit (used as a wildcard).
		– Percent sign (%)—The previous digit or pattern zero or multiple times, similar to wildcard usage in the regular expression.
		– Circumflex (^)—Match to the beginning of the string.
		– Dollar sign ($)—Match to the null string at the end of the input string.
		– Backslash (\)—Is followed by a single character matching that character or used with a single character having no other significance (matching that character).
		– Question mark (?)—The previous digit occurred zero or one time.
		– Brackets ([ ])—Range of digits. Digits (0 to 9) are enclosed in brackets. Similar to a regular expression rule.
		– Parentheses (( ))—A pattern. Same as the regular expression rule—for example, 408(555). Use parentheses in conjunction with symbols ? or %.
		For more information on applying wildcard symbols to destination patterns and the dial strings that result, see Dial Peer Configuration on Voice Gateway Routers.
		• **T**—Control character indicating that the **destination-pattern** value is a variable-length dial string.

	Command	Purpose
Step 3	**port** *controller*:**D** **Example:** `Router(config-dial-peer)# port 0:D`	(Cisco AS5300 only) Associates this POTS dial peer with a specific voice port. Keywords and arguments are platform dependent.
Step 4	**exit** **Example:** `Router(config-dial-peer)# exit`	Exits the current mode.
Step 5	**dial-peer voice** *tag* **voip** **Example:** `Router(config)# dial-peer voice 123 voip`	Enters dial-peer configuration mode for the VoIP peer designated by *tag*.
Step 6	**destination-pattern** *string*[**T**] **Example:** `Router(config-dial-peer)# destination-pattern 1513200....`	See Step 2 above.
Step 7	**tech-prefix** *number* **Example:** `Router (config-dial-peer)# tech-prefix 9#`	Defines the numbers used as the technology prefix that the gateway registers with the gatekeeper. Can contain up to 11 characters. Although not strictly necessary, a pound symbol (#) is frequently used as the last digit in a prefix. Valid characters: 0 to 9, #, and *.
Step 8	**session target ras** **Example:** `Router (config-dial-peer)# session target ras`	Specifies that the RAS protocol is being used to determine the IP address of the session target—meaning that a gatekeeper translates the E.164 address to an IP address.
Step 9	**exit** **Example:** `Router (config-dial-peer)# exit`	Exits the current mode.

Verifying RAS Configuration

To verify RAS configuration, perform the following step.

Step 1 **show dial-peer voice**

Use this command to verify the POTS and VoIP dial-peer configuration.

The following example shows output for a VoIP dial peer using RAS on a Cisco AS5300:

```
Router# show dial-peer voice 1234

VoiceOverIpPeer1234
tag = 1234, destination-pattern = 1234',
answer-address = ',
group = 1234, Admin state is up, Operation state is up,
incoming called-number = ', connections/maximum = 0/unlimited,
application associated:
type = voip, session-target = ras',
technology prefix: 8#
ip precedence = 0, UDP checksum = disabled,
session-protocol = cisco, req-qos = controlled-load,
acc-qos = best-effort,
fax-rate = voice, codec = g729r8,
Expect factor = 10, Icpif = 30,
VAD = enabled, Poor QOV Trap = disabled,
```

Troubleshooting Tips

- To display the types and addressing of RAS messages sent and received, use the **debug ras** command. The debug output lists the message type using mnemonics defined in ITU-T specification H.225.
- To display additional information about the actual contents of the H.225 RAS messages, use the **debug h225 asn1** command.

Configuring RAS Retries and Timers

You can configure RAS message timeout values, message retry counter values, and registration request (RRQ) message time-to-live and early transmit time margins on Cisco gateways. This provides greater flexibility in configuring gateways in different network environments.

The **ras timeout** command configures the number of seconds for the gateway to wait before resending a RAS message to a gatekeeper. The **ras retry** command configures the number of times to resend the RAS message after the timeout period expires. The default values for timeouts and retries are acceptable in most networks. You can use these commands if you are experiencing problems in RAS message transmission between gateways and gatekeepers. For example, if you have gatekeepers that are slow to respond to a type of RAS request, increasing the timeout value and the number of retries increases the call success rate, preventing lost billing information and unnecessary switchover to an alternate gatekeeper.

The **ras rrq ttl** command configures the number of seconds that the gateway should be considered active by the gatekeeper. The gateway transmits this value in the RRQ message to the gatekeeper. The **margin** *time* keyword and argument allow the gateway to transmit an early RRQ to the gatekeeper before the time-to-live value advertised to the gatekeeper.

Configuring RAS Timeout and Retry Counters

To configure RAS message timeout values and retry counters, use the following commands beginning in global configuration mode.

SUMMARY STEPS

1. **voice service voip**
2. **h323**
3. **ras timeout** {**all** | **arq** | **brq** | **drq** | **grq** | **rai** | **rrq**} *value*
4. **ras retry** {**all** | **arq** | **brq** | **drq** | **grq** | **rai** | **rrq**} *value*
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**voice service voip** **Example:** `Router(config)# voice service voip`	Enters voice-service configuration mode for VoIP.
Step 2	**h323** **Example:** `Router(conf-voi-serv)# h323`	Enters voice-service-h323 configuration mode.
Step 3	**ras timeout** {**all** | **arq** | **brq** | **drq** | **grq** | **rai** | **rrq**} *value* **Example:** `Router(conf-serv-h323)# ras timeout all 10`	Sets RAS timeout conditions. Keywords and argument are as follows: • **all**—All RAS message counters that do not have explicit values configured individually. If the **no ras timeout all** command is entered, all values are set to the default except the individual values that were configured separately. • **arq**—Admission request (ARQ) message counter. • **brq**—Bandwidth request (BRQ) message counter. • **drq**—Disengage request (DRQ) message counter. • **grq**—Gatekeeper request (GRQ) message counter. • **rai**—Resource availability indication (RAI) message counter. • **rrq**—Registration request (RRQ) message counter. • *value*—How long the gateway waits for a message from the gatekeeper before timing out, in seconds. Range: 1 to 45.
Step 4	**ras retry** {**all** | **arq** | **brq** | **drq** | **grq** | **rai** | **rrq**} *value* **Example:** `Router(conf-serv-h323)# ras retry grq 5`	Sets RAS retry conditions. Keywords are as in step 3. The argument is as follows: • *value*—Number of times that the gateway resends messages to the gatekeeper after timeout. Range: 1 to 30.
Step 5	**exit** **Example:** `Router(conf-serv-h323)# exit`	Exits the current mode.

Configuring RRQ Time-to-Live Value

To configure the RRQ time-to-live value, use the following commands beginning in global configuration mode.

SUMMARY STEPS

1. **voice service voip**

2. **h323**
3. **ras rrq ttl** *time-to-live* [**margin** *time*]
4. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`voice service voip`**
	Example:
	`Router(config)# voice service voip`
		Enters voice-service configuration mode for VoIP.

Step 2	**`h323`**
	Example:
	`Router(conf-voi-serv)# h323`
		Enters voice-service-h323 configuration mode.

Step 3	**`ras rrq ttl`** *`time-to-live`* `[`**`margin`** *`time`*`]`
	Example:
	`Router(conf-serv-h323)# ras rrq ttl 90 margin 30`
		Sets time-to-live parameters. Argument and keyword are as follows:
		• *time-to-live*—How long, in seconds, the gatekeeper considers the gateway active. Range: 15 to 4000 (must be greater than the **margin** *time* value).
		• **margin** *time*—How long, in seconds, an RRQ message can be transmitted from the gateway before the time-to-live value advertised to the gatekeeper. Range: 1 to 60 (this value times two must be less than or equal to the *time-to-live* value).

Step 4	**`exit`**
	Example:
	`Router(conf-serv-h323)# exit`
		Exits the current mode.

Verifying RAS Retries and Timers

To verify RAS retries and timers, perform the following step.

Step 1 **show running config**

Use this command to verify RAS message retry counters, timeout values, and time-to-live values.

```
Router# show running-config

Current configuration : 925 bytes
!
version 12.3
.
.
.
voice service voip
 h323
  ras rrq ttl 90 margin 30
  ras timeout all 7
  ras timeout grq 10
  ras timeout drq 30
  ras retry all 10
  ras retry grq 5
.
.
.
```

Examples

The following example shows the GRQ message timeout value set to 10 seconds and all other RAS message timeout values set to 7 seconds:

```
Router(conf-serv-h323)# ras timeout grq 10
Router(conf-serv-h323)# ras timeout all 7
```

The following example shows the GRQ message counter set to 5 and all other RAS message counters set to 10:

```
Router(conf-serv-h323)# ras retry all 10
Router(conf-serv-h323)# ras retry grq 5
```

The following example shows the time-to-live value configured to 90 seconds and the **margin** *time* value configured to 30 seconds:

```
Router(conf-serv-h323)# ras rrq ttl 90 margin 30
```

Configuring Gateway-Resource-Availability Reporting

To allow gatekeepers to make intelligent call-routing decisions, the gateway reports the status of its resource availability to its gatekeeper. Resources that are monitored are digital-signal-level 0 (DS0) channels and digital-signal-processor (DSP) channels.

The gateway reports its resource status to the gatekeeper using the RAS Resource Availability Indication (RAI). When a monitored resource falls below a configurable threshold, the gateway sends a RAI to the gatekeeper indicating that the gateway is almost out of resources. When the available resources then cross over another configurable threshold, the gateway sends an RAI indicating that the resource depletion condition no longer exists.

You can configure resource-reporting thresholds by using the **resource threshold** command. Upper and lower thresholds are separately configurable to prevent the gateway from operating sporadically because of the availability or lack of resources.

Configuring E.164-Address Registration

If phones are connected directly to the gateway, the Cisco H.323 Version 2 gateway allows fully qualified E.164 numbers to be registered with the gatekeeper. When configuring the gateway, use the **register e164** command to register these E.164 numbers.

Configuring In-Band Tones and Announcements

In-band progress tones and announcements are required for PSTN services and for ISDN speech and 3.1-kHz voice services, per Bellcore and ANSI specifications. To guarantee that in-band tones and announcements are generated when required and at the appropriate switch, Cisco H.323 signaling software ensures that the progress indicator (PI) is carried end to end in call-signaling messages between the called party and the calling party. The PI in outbound dial peers can also be configured at the H.323 VoIP gateway, if necessary.

The PI is an IE that signals when in-band tones and announcements are available. The PI controls whether the local switch generates the appropriate tone or announcement or whether the remote switch is responsible for the generation. For example, if the terminating switch generates the ringback tone, it sends a PI of 1 or 8 in the alerting message. If the originating switch receives an alerting message without a PI, it generates the ringback tone.

The specific PI that a switch sends in call messages, if any, depends on the model of the switch. To ensure that in-band communication is generated appropriately, it may be necessary in some instances to override the default behavior of the switch by manually configuring the PI at the Cisco H.323 gateway.

The PI is configurable in setup messages from the outbound VoIP dial peer, typically at the originating gateway, and in alert, progress, and connect messages from the outbound POTS dial peer, typically at the terminating gateway. The PI is configured by the **progress_ind** command. Table 1 shows the PI values that can be configured on the H.323 gateway.

Table 1 Configurable Progress Indicator Values for H.323 Gateways

PI	Description	Message Type
0	No progress indicator is included.	Setup
1	Call is not end-to-end ISDN; further call progress information may be available in-band.	Alert, setup, progress, connect
2	Destination address is non-ISDN.	Alert, progress, connect
3	Origination address is non-ISDN.	Setup
8	In-band information or appropriate pattern is now available.	Alert, progress, connect

When interworking is between ISDN and non-ISDN networks, the originating gateway reacts as follows:

- If the originating switch does not include a PI in setup messages, the originating gateway assumes that the originating switch is ISDN and expects the switch to generate the ringback tone. Determine which device generates the ringback tone by using the **progress_ind** command in dial-peer configuration mode:
  - To enable the terminating switch to generate the ringback tone, set the PI to 8 in the alert messages on the terminating gateway. The progress indicator is configured in the POTS dial peer.
  - To enable the originating gateway to generate the ringback tone, set the PI to 3 in setup messages on the originating gateway. The PI is configured in the VoIP dial peer.

  Note If the terminating gateway sends an alert message with no PI value, the originating gateway generates the ringback tone. But if the terminating gateway sends an alert message that has a PI of 1, 2, or 8, the originating gateway does not generate ringback tone.

- The originating gateway cuts through the voice path in the backward direction when it receives a progress or alert message that has a PI of 1, 2, or 8.

Note Pure ISDN calls may use different protocols at the originating and terminating ends. For example, a call may originate on ETSI and terminate on NI2. If the two protocols are not compatible end to end, the gateway drops all IEs from messages, including the progress indicator. Because a progress indicator is required in all progress messages, the originating gateway inserts a PI of 1 in the progress message. To avoid dropping IEs, use the **isdn gateway-max-internetworking** command to prevent the gateway from checking protocol compatibility.

Configuring Gateway AAA

For the gateway to provide authentication and accounting services, enable and configure your gateway to support authentication, authorization, and accounting (AAA) services. AAA enables the gateway to interact with a RADIUS security server to authenticate users (typically incoming calls) and to perform accounting services.

Note

- For information about AAA configuration on a gateway, see *Configuring AAA for Cisco Voice Gateways* at http://www.cisco.com/en/US/docs/ios/voice/aaa/configuration/guide/15_0/va_15_0_book.html
- For information about RADIUS and AAA security services, see the *Cisco IOS Security Configuration Guide* at http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/15_0/sec_user_services_15_0_book.html.

Configuring H.235 Gateway Security

This section contains the following information:

Information About H.235 Gateway Security

The Cisco H.235-based security and accounting features described in this section can be used by a gatekeeper, which is considered a known and trusted entity, to authenticate, authorize, and route H.323 calls.

The Cisco H.323 gateway supports the use of CryptoH323Tokens for authentication. The CryptoH323Token is defined in the ITU-T H.225 Version 2 standard and is used in a "password-with-hashing" security scheme as described in section 10.3.3 of the H.235 specification.

A cryptoToken can be included in any RAS message to authenticate the sender of the message. A separate database can be used for user ID and password verification.

Cisco H.323 gateways support three levels of authentication:

- Endpoint—The RAS channel used for gateway-to-gatekeeper signaling is not a secure channel. To ensure secure communication, H.235 allows gateways to include an authentication key in their RAS messages. This key is used by the gatekeeper to authenticate the source of the messages. At the endpoint level, validation is performed on all messages from the gateway. The cryptoTokens are validated using the password configured for the gateway.

  Note To secure the RAS messages and calls, it is essential that the gatekeeper provides authentication based on the secure key. The gatekeeper must support H.235 security using the same security scheme as the Cisco gateway.

- Per-Call—When the gateway receives a call over the telephony leg, it prompts the user for an account number and PIN. These two numbers are included in certain RAS messages sent from the endpoint to authenticate the originator of the call.
- All—This option is a combination of the other two. With this option, the validation of cryptoTokens in ARQ messages is based on an the account number and PIN of the user making a call. The validation of cryptoTokens sent in all the other RAS messages is based on the password configured for the gateway.

CryptoTokens for RRQs, unregistration requests (URQs), DRQs, and the terminating side of ARQs contain information about the gateway that generated the token. The cryptoTokens include the gateway identification (ID)—which is the H.323 ID configured on the gateway—and the gateway password. The cryptoTokens for the originating-side ARQ messages contain information about the user that is placing the call, including the user ID and PIN.

Although the scenarios in this document describe how to use the security and accounting features in a prepaid call environment, these features may also be used to authorize IP calls that originate in another domain (interservice provider or intercompany calls).

H.235-based security and accounting features can be used with AAA. The gateway can be configured to use the gatekeeper for call authentication or authorization, and AAA can be used for call accounting.

In addition, H.235-based security and accounting features include support for the following:

- Settlement with the gatekeeper, which allows the gateway to obtain, track, and return accounting information
- Call metering, which allows the gateway to terminate a call if it exceeds the allotted time (in the case of prepaid calls)

Note The H.235 security and accounting features described in this document are separate from, and should not be confused with, the standard interactive-voice-response (IVR) and AAA features used to authenticate inbound calls or with the settlement functions provided by the Open Settlement Protocol (OSP).

Settlement with the Gatekeeper

The H.235 security and accounting features are designed to support a variety of situations in which some form of authentication or tracking is required. The security features control access through a userID-password database. The accounting enhancements allow call usage to be tracked at the origin and at the destination.

Fields in the RAS messages allow the gateway to report call-usage information to the gatekeeper. The call-usage information is included in the DRQ message that is sent when the call is terminated.

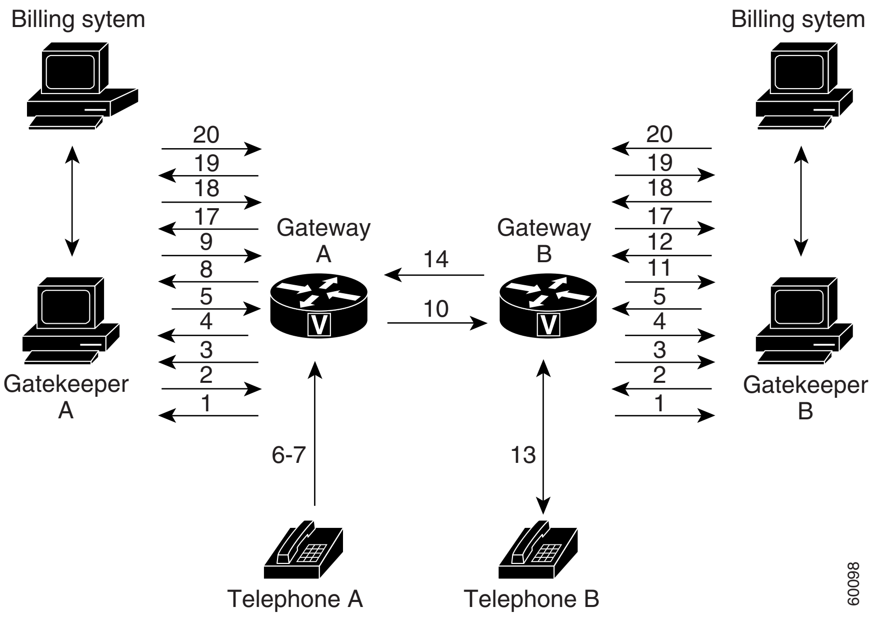
Call Tracking

With prepaid calling services, an account number and PIN must be entered and the duration of the call must be tracked against the remaining credit of the customer. The Cisco H.323 gateway monitors prepaid account balances and terminates a call if the account is exceeded.

Note Because authentication information includes a time stamp, it is important that all Cisco H.323 gateways and gatekeepers (or other entities that perform authentication) be synchronized. Cisco H.323 gateways must be synchronized using the Network Time Protocol (NTP).

Figure 1 illustrates the flow of a possible call for which H.323 security and accounting features are used.

Figure 1 Flow for a Call That Requires H.323 Security and Accounting Features



In this example, Telephone A is attempting to establish a phone call to Telephone B. The following numbered explanations correspond to the action taking place at each numbered reference in Figure 1.

Gateways Establish Secure Communication with the Gatekeepers

1. Gateways A and B send GRQ messages to their respective gatekeepers. The GRQ message includes the authentication capability and the algorithm object ID.
2. Gatekeepers A and B respond to their respective gateways with gatekeeper confirmation (GCF) messages. The GCF message includes the authentication capability and the algorithm object ID.
3. If the values for the H.323 security parameters do not match what is expected, the gatekeeper responds with a gatekeeper rejection (GRJ) message that contains a reject reason of securityDenial. This prompts the gateway to resend the GRQ.
4. Gateways A and B send RRQ messages to their respective gatekeepers. The RRQ message includes authentication information in the cryptoToken field.
5. Gatekeepers A and B respond to their respective gateways with registration confirmation (RCF) messages.

If an authentication failure occurs, the gatekeeper responds with a registration rejection (RRJ) message.

Secure Telephone Communications Initiated

6. Telephone A establishes a connection with Gateway A.
7. Gateway A initiates the IVR script to obtain the account number and PIN of the user and the desired destination telephone number.
8. Gateway A sends an ARQ message to Gatekeeper A. The gateway must include additional information in the ARQ message to enable the gatekeeper to authenticate the call. The information included in the ARQ message varies depending on whether the ARQ message is being sent by the source or the destination gateway. At this point in the scenario, it is the source gateway that is requesting admission. Therefore, the ARQ message includes the account number and PIN of the user. This information is encrypted using MD5 hashing and is included in the cryptoTokens field.
9. Gatekeeper A validates the authentication information, resolves the destination telephone number, and determines the appropriate destination gateway (which is Gateway B in this case). Then Gatekeeper A sends an admission confirmation (ACF) message to Gateway A. The ACF message includes the billing information of the user (such as a reference ID and current account balance for prepaid call services) and an access token.
10. Gateway A sends a setup message to Gateway B. The setup message also includes the access token.
11. Gateway B sends an ARQ message to Gatekeeper B. The ARQ message includes the access token received from Gateway A.
12. Gatekeeper B validates the authentication information in the access token and responds to Gateway B with an ACF message.

    If the authentication information is in error, Gatekeeper B sends an admission rejection (ARJ) message to Gateway B with a reject reason of securityDenial.
13. Gateway B initiates a call to the destination telephone.
14. When the destination telephone is answered, Gateway B sends a connect message to Gateway A.
15. Gateways A and B start their timers to meter the call. If the caller is using prepaid call services, the meter is constantly compared to the account balance of the user, which was included in the ACF message sent in Step 9.

Telephone Communications Terminated

16. The call is terminated when one of the parties hangs up or, in the case of prepaid call services, when either of the gateways determines that the account balance of the user has been exceeded.
17. Gateways A and B send DRQ messages to the their respective gatekeepers. The DRQ message contains the resulting billing information.
18. Gatekeepers A and B send disengage confirmation (DCF) messages to their respective gateways.

Communication Between the Gateways and the Gatekeepers Terminated

19. Gateways A and B send URQ messages to their respective gatekeepers.
20. Gatekeepers A and B send unregistration confirmation (UCF) messages to their respective gateways.

Downloading IVR Scripts

Tool Command Language (TCL) IVR scripts are the default scripts for all Cisco voice features that use IVR.

The H.323 security and accounting enhancements described in this document require the use of one of the following IVR scripts:

- voip_auth_acct_pin_dest.tcl
- voip_auth_acct_pin_dest_2.tcl

Note For more information on TCL IVR applications, see the *Cisco IOS TCL and VoiceXML Application Guide* at http://www.cisco.com/en/US/docs/ios/voice/ivr/configuration/guide/tcl_c.html.

voip_auth_acct_pin_dest.tcl Script

The voip_auth_acct_pin_dest.tcl script does the following:

- Prompts the caller to enter an account number, PIN, and destination number. This information is provided to an H.323 gatekeeper, which authenticates and authorizes the call.

  If the caller is using a debit card account number, the following occurs:

  - The gatekeeper returns the remaining credit time amount.
  - The TCL script monitors the time remaining and, based on a configured value, plays a "time running out" message to the caller. The message (such as, "You have only 3 minutes remaining on your credit.") is played only to the calling party. The called party hears silence during this time. For example, if the configured timeout value is 3 minutes, the message is played when the caller has only 3 minutes of credit left.
  - The TCL script plays a warning message when the credit of the user has been exhausted. The message (such as, "Sorry, you have run out of credit.") is played only to the calling party. The called party hears silence during this time.
- Allows the caller to make subsequent calls to different destinations without disconnecting from the call leg. Thus, the caller is required to enter the account ID and PIN only once (during initial authorization). For making subsequent calls, the caller needs to enter only the destination number. After completing a call to one destination, the caller can disconnect the call by pressing the pound (#) key on the keypad and holding it down from 1 to 2 seconds. If the # key is pressed down for more than 1 second, it is treated as a long pound (#). The called party is disconnected, and the caller is prompted to enter a new destination number. Once a new destination number is entered, the call is authenticated and authorized using this number and the previously provided account number and PIN.

  This feature also allows the caller to continue making additional calls if the called party hangs up.
- Reauthenticates and authorizes each new call. Each time a caller enters a new destination number, the TCL script reauthenticates or authorizes the call with the gatekeeper and, if the caller is using a debit card account, obtains the remaining credit time information.
- Allows the caller to enter the necessary information without having to hear all or any of the prompts. The TCL script stops playing (or does not begin playing) the prompt if it detects that the caller wants to enter the information without listening to the prompt.

Note The normal terminating character for the account number, PIN, and destination number is the pound (#) key.

- Allows the caller to interrupt announcements by pressing the touchtone key. This TCL script stops playing announcements when the system detects that the caller has pressed any touchtone key.
- Allows the caller to interrupt partially entered numbers and restart from the beginning by pressing a designated key on the keypad. The asterisk (*) key is configured as the interrupt key in the TCL script. The caller can use the asterisk key to cancel an entry and then reenter the account number, PIN, or destination number. The caller is allowed to re-enter a field only a certain number of times. The number of retries may be configured. The default is three times.
- Can terminate a field by size instead of the terminating character (#). The TCL script allows a specified number of digits to be entered in the account number and PIN fields. This means that the caller can type all the digits (without the terminating character) and the script determines how to extract different fields from the number strings. If the caller uses the terminating character, the terminating character takes precedence and the fields are extracted accordingly.
- Supports two languages. The IVR script supports two languages, which must be similar in syntax. The languages must be similar in the manner in which numbers are constructed—especially for currency, amount, and time. All the prompts are recorded and stored in both languages. The language selection is made when the caller presses a predefined key in response to a prompt (such as, “For English, press 1. For Spanish, press 2.”). The TCL script uses the selected language until the caller disconnects.

voip_auth_acct_pin_dest_2.tcl Script

The voip_auth_acct_pin_dest_2.tcl script is a simplified version of the voip_auth_acct_pin_dest.tcl script. It prompts the caller for an account number followed by a PIN. The caller is then prompted for a destination number. This information is provided to the H.323 gatekeeper that authenticates and authorizes the call. This script provides prompts only in English.

If the caller is using a debit account number, it plays a “time running out” message when the caller has 10 seconds of credit time remaining. It also plays a “time has expired” message when the credit of the caller has been exhausted.

Configuring H.235 Gateway Security

To use the H.235 security features for routing H.323 calls as illustrated above, do the following:

- Enable H.323 security on the gateway.
- Download the appropriate TCL IVR scripts from the Cisco Connection Online Software Support Center. The URL to this site is as follows:

  http://www.cisco.com/cgi-bin/tablebuild.pl/tclware
- Configure the IVR inbound dial peer on the gateway router.

To enable security on the gateway, use the following commands beginning in global configuration mode.

SUMMARY STEPS

1. **gateway**
2. **security password** *password* **level** {**endpoint** | **per-call** | **all**}

3. **exit**
4. **dial-peer voice** *tag* **pots**
5. **call application voice** *application-name location word*
6. **destination-pattern** *string*[**T**]
7. **port** *controller-number*:**D**
8. **exit**

DETAILED STEPS

	Command	Purpose
Step 1	**gateway** **Example:** `Router(config)# gateway`	Enters gateway configuration mode.

Step 2	**security password** *password* **level** {**endpoint** | **per-call** | **all**}
	Example:
	`Router(config-gateway)# security password password level all`
		Enables security and specifies the level of validation to be performed.
		• *password*—Gateway password.
		• **endpoint**—Validation is performed on all RAS messages sent by the gateway using the cryptoTokens that are generated based on the security password configured for the gateway.
		• **per-call**—Validation is performed only on the admission messages from the H.323 endpoints to the gateway ARQ messages). The gateway prompts the user for an account number and PIN. These two numbers are sent from the endpoint and are used to authenticate the originator of the call.
		• **all**—Combination of the **endpoint** and **per-call** options. Specifies that validation be performed on all RAS messages sent by the gateway. The validation of cryptoTokens in ARQ messages is based on the account number and PIN of the user making the call, and the validation of cryptoTokens sent in all other RAS messages is based on the password configured for the gateway.

Step 3	**exit** **Example:** `Router(config-gateway)# exit`	Exits the current mode.
Step 4	**dial-peer voice** *tag* **pots** **Example:** `Router(config)# dial-peer voice 1 pots`	Enters dial-peer configuration mode for the POTS dial peer designated by the *tag* value.

	Command	Purpose

Step 5	**`call application voice`** *`application-name location word`*
	Example:
	`Router(config-dial-peer)# call application voice xyz tftp://172.18.16.2/samp/xyz.tcl`
		Initiates the IVR application and the selected TCL application name.
		• *application-name*—Character string that defines the name of the application.
		• *location*—Location of the TCL file in URL format. Valid values: TFTP, FTP, or flash.
		• *word*—Text string that defines an attribute-value (AV) pair specified by the TCL script and understood by the RADIUS server.

Step 6	**`destination-pattern`** *`string`*`[`**`T`**`]`
	Example:
	`Router(config-dial-peer)# destination-pattern 1513200....`
		Specifies the E.164 address associated with this dial peer. For an explanation of the keywords and arguments, see the "Configuring Gateway RAS" section on page 33, Step 2.

Step 7	**`port`** *`controller-number`***`:D`**
	Example:
	`Router(config-dial-peer)# port 0:D`
		(Cisco AS5300 only) Configures the voice port associated with this dial peer. Keywords and arguments are as follows:
		• *controller-number*—The T1 or E1 controller.
		• **:D**—D channel associated with the ISDN PRI.
		Note Command syntax varies by platform.

Step 8	**`exit`**
	Example:
	`Router(config-dial-peer)# exit`
		Exits the current mode.

Verifying H.235 Gateway Security

To verify H.235 gateway security, perform the following step.

Step 1 **show running-config**

Use this command to display the security password and level when it is enabled. By default, security is disabled.

```
Router# show running-config

security password 151E0A0E level all
```

Configuring Alternate-Gatekeeper Support

This section contains the following information:

- Restrictions for Alternate-Gatekeeper Support, page 49
- Information About Alternate-Gatekeeper Support, page 49
- Configuring Alternate-Gatekeeper Support, page 50

- Verifying Configuration of Alternate-Gatekeeper Support, page 51

Restrictions for Alternate-Gatekeeper Support

- You can use this feature only with a gatekeeper that supports the alternate gatekeeper functionality.
- The timer/retry number of RAS messages remains internal to the gateway as currently implemented. This feature does not include commands to allow tuning of these parameters.
- The alternate gatekeeper list is volatile—when the gateway loses power or is reset or reloaded, the alternate gatekeeper list that has been acquired from the gatekeeper is lost.

Information About Alternate-Gatekeeper Support

A gatekeeper manages H.323 endpoints in a consistent manner, allowing them to register with the gatekeeper and to locate another gatekeeper. The gatekeeper provides logic variables for proxies or gateways in a call path to provide connectivity with the Public Switched Telephone Network (PSTN), to improve quality of service (QoS), and to enforce security policies. Multiple gatekeepers may be configured to communicate with one another, either by integrating their addressing into the DNS or by using Cisco IOS configuration options.

An alternate gatekeeper provides redundancy for a gateway in a system in which gatekeepers are used. Redundant H.323 zone support in the gateway allows a user to configure two gatekeepers in the gateway (one as the primary and the other as the alternate). All gatekeepers are active. Each alternate gatekeeper, or gatekeeper node, shares its local zone information so that the cluster can effectively manage all local zones within the cluster. Each alternate gatekeeper has a unique local zone. Clusters provide a mechanism for distributing call processing seamlessly across a converged IP network infrastructure to support IP telephony, facilitate redundancy, and provide feature transparency and scalability.

An endpoint that detects the failure of its gatekeeper can safely recover from that failure by utilizing an alternate gatekeeper for future requests, including requests for existing calls. A gateway can only be registered to a single gatekeeper at a time. Only one gatekeeper is allowed to manage a single zone. The cluster manages up to five similarly configured zones and shares resources between the alternate gatekeepers in the cluster for each zone. You can define up to 100 zones in a single gatekeeper.

With gatekeeper clustering there is the potential that bandwidth may be overcommitted in a cluster. For example, suppose that there are five gatekeepers in a cluster and that they share 10 Mbps of bandwidth. Suppose that the endpoints registered to those alternates start placing calls quickly. It is possible that within a few seconds, each gatekeeper could be allocating 3 Mbps of bandwidth if the endpoints on each of the gatekeepers request that much bandwidth. The net result is that the bandwidth consumed in the cluster is 15 Mbps.

The alternate gatekeeper was purposely designed to restrict bandwidth because there is no clear way to sync bandwidth information quickly and efficiently. To work around this problem, “announcement” messages were restricted to intervals as small as 10 seconds. If the gatekeepers get into a situation in which endpoints request bandwidth rapidly, the problem is discovered and corrective action takes place within 10 seconds. Assuming that the gatekeepers are not synchronized on their timers, the announcement messages from the various gatekeepers are likely to be heard more quickly. Therefore, the problem is less severe. The potential exists, however, for overcommitment of the bandwidth between announcement messages if the call volume increases substantially in a short amount of time (as small as 10 seconds).

Note If you monitor your bandwidth, it is recommended that you consider lowering the maximum bandwidth so that if “spikes” such as those described above do occur, some bandwidth is still available.

Configuring Alternate-Gatekeeper Support

To configure alternate gatekeeper support on a gateway, use the following commands beginning in global configuration mode.

SUMMARY STEPS

1. **interface Ethernet 0/1**
2. **h323-gateway voip interface**
3. **h323-gateway voip id** *gatekeeper-id* {**ipaddr** *ip-address* [*port*]| **multicast**} [**priority** *priority*]
4. **h323-gateway voip id** *gatekeeper-id* {**ipaddr** *ip-address* [*port*] | **multicast**} [**priority** *priority*]
5. **h323-gateway voip h323-id** *interface-id*
6. **exit**

DETAILED STEPS

	Command	Purpose

Step 1	**`interface Ethernet 0/1`**
	Example:
	`Router(config)# interface Ethernet 0/1`
		Enters interface configuration mode for the selected Ethernet interface.

Step 2	**`h323-gateway voip interface`**
	Example:
	`Router(config-if)# h323-gateway voip interface`
		Identifies this as a VoIP gateway interface.

Step 3	**h323-gateway voip id** *gatekeeper-id* {**ipaddr** *ip-address* [*port*]| **multicast**} [**priority** *priority*] **Example:** `Router(config-if)# h323-gateway voip id gk3.gg-dn1 ipaddr 172.18.0.0 1719`	Identifies the gatekeeper for this gateway interface and sets its attributes. For an explanation of the keywords and arguments, see the "How to Configure H.323 Gateways" section on page 27, step 6.
Step 4	**h323-gateway voip id** *gatekeeper-id* **{ipaddr** *ip-address* **[***port***] | multicast} [priority** *priority***]** **Example:** `Router(config-if)# h323-gateway voip id gk3.gg-dn1 ipaddr 172.18.0.0 1721`	Identifies the alternate gatekeeper and sets its attributes.

	Command	Purpose
Step 5	**h323-gateway voip h323-id** *interface-id* **Example:** `Router(config-if)$ h323-gateway voip id gk4.gg-dn1 ipaddr 209.165.202.132 1719`	Defines the H.323 name of the gateway, identifying this gateway to its associated gatekeeper. Usually this ID is the name of the gateway, with the gatekeeper domain name appended to the end: name@domainname.
Step 6	**exit** **Example:** `Router(config-if)# exit`	Exits the current mode.

Verifying Configuration of Alternate-Gatekeeper Support

To verify configuration of alternate-gatekeeper support, perform the following step.

Step 1 **show gateway**

Use this command to verify that an alternate gatekeeper is configured.

```
Router# show gateway

Permanent Alternate Gatekeeper List
priority 127 id bmx1 ipaddr 10.77.241.103 1719 register needed
priority 127 id bmx2 ipaddr 10.77.241.117 1719 register needed
Primary gatekeeper ID bmx1 ipaddr 10.77.241.103 1719
```

Configuring DTMF Relay

This section contains the following information:

- Restrictions for DTMF Relay, page 51
- Information About DTMF Relay, page 51
- Configuring DTMF Relay, page 54
- Monitoring and Maintaining DTMF Relay, page 56

Restrictions for DTMF Relay

- Asynchronous dtmf-relay signaling configuration is not supported.
- DTMF-relay signaling must have the same configuration on both the outbound gateway and the trunking gateway.

Information About DTMF Relay

Dual-tone multifrequency (DTMF) is the tone generated on a touchtone phone when the keypad digits are pressed. During a call, DTMF may be entered to access interactive voice response (IVR) systems, such as voice mail and automated banking services.

Although DTMF is usually transported accurately when using high-bit-rate voice codecs such as G.711, low-bit-rate codecs such as G.729 and G.723.1 are highly optimized for voice patterns and tend to distort DTMF tones. As a result, IVR systems may not correctly recognize the tones.

DTMF relay solves the problem of DTMF distortion by transporting DTMF tones “out of band,” or separate from the encoded voice stream.

Relay Types

Cisco gateways currently support the following methods of DTMF relay:

- Cisco-proprietary Real-Time Transport Protocol (RTP)—DTMF tones are sent in the same RTP channel as voice data. However, the DTMF tones are encoded differently from the voice samples and are identified by a different RTP payload type code. Use of this method accurately transports DTMF tones, but because it is proprietary, it requires the use of Cisco gateways at both the originating and terminating endpoints of the H.323 call.
- H.245 signal or alphanumeric—These methods separate DTMF digits from the voice stream and send them through the H.245 signaling channel instead of through the RTP channel. The tones are transported in H.245 User Input Indication messages. The H.245 signaling channel is a reliable channel, so the packets that transport the DTMF tones are guaranteed to be delivered. However, because of the overhead of using a reliable protocol, and depending on network congestion conditions, the DTMF tones may be slightly delayed. All H.323 version 2 compliant systems are required to support the “h245-alphanumeric” method, while support of the “h245-signal” method is optional.
- Named Telephone Events (NTEs). Using NTE to relay DTMF tones provides a standardized means of transporting DTMF tones in RTP packets according to section 3 of RFC 2833, RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals, developed by the Internet Engineering Task Force (IETF) Audio/Video Transport (AVT) working group. RFC 2833 defines formats of NTE RTP packets used to transport DTMF digits, hookflash, and other telephony events between two peer endpoints. With the NTE method, the endpoints perform per-call negotiation of the DTMF relay method. They also negotiate to determine the payload type value for the NTE RTP packets. User preference for DTMF relay types is not supported, and DTMF relay forking is not supported.

The ability of a gateway to receive DTMF digits in a particular format and the ability to send digits in that format are independent functions. No configuration is necessary to receive DTMF digits from another H.323 endpoint using any of the methods described. The Cisco gateway is capable of receiving DTMF tones transported by any of these methods at all times.

Capabilities and Priorities

Cisco H.323 gateways advertise capabilities using H.245 capabilities messages. By default, they advertise that they can receive all DTMF relay modes. If the capabilities of the remote gateway do not match, the Cisco H.323 gateway transmits DTMF tones as in-band voice.

Configuring DTMF relay on the Cisco H.323 gateway sets preferences for how the gateway handles DTMF transmission. You can enable more than one DTMF relay option for a particular dial peer. If more than one option is enabled and if the peer indicates that it is capable of receiving DTMF in more than one of these formats, the gateway sends DTMF using the method among the supported formats that it considers to be the most preferred. If the remote device supports multiple formats, the gateway chooses the format according to the following priority:

1. cisco-rtp (highest priority)
2. h245-signal
3. h245-alphanumeric
4. rtp-nte
5. None—DTMF sent in-band

Payload Types

In addition, Cisco gateways provide support for asymmetrical payload types. Payload types can differ between local and remote endpoints. Therefore, the Cisco gateway can transmit one payload type value and receive a different payload type value.

The **dtmf-relay h245-signal** command relays a more accurate representation of a DTMF digit than does the **dtmf-relay h245-alphanumeric** command because tone duration information is included along with the digit value. This information is important for applications requiring that a key be pressed for a particular length of time. For example, one popular calling card feature allows the caller to terminate an existing call by pressing the # key for more than 2 seconds and then making a second call without having to hang up in between. This feature is beneficial because the access number and personal identification number (PIN) code do not need to be dialed again. Outside-line access charges, which are common at hotels, may also be avoided.

The **dtmf-relay h245-alphanumeric** command simply relays DTMF tones as ASCII characters. For instance, the DTMF digit 1 is transported as the ASCII character 1. There is no duration information associated with tones in this mode. When the Cisco H.323 gateway receives a DTMF tone using this method, the gateway generates the tone on the PSTN interface of the call using a fixed duration of 500 ms. All systems that are H.323 Version 2-compliant are required to support the **dtmf-relay h245-alphanumeric** command, but support of the **dtmf-relay h245-signal** command is optional.

H.245 Tunneling of DTMF Relay in Conjunction with Fast Connect

Through H.245 tunneling, H.245 messages are encapsulated within H.225 messages without using a separate H.245 TCP connection. When tunneling is enabled, one or more H.245 messages can be encapsulated in any H.225 message. H.245 tunneling is not supported as a stand-alone feature; initiation of H.245 tunneling procedures can be initiated only by using the **dtmf-relay** command and only from an active fast connect call. Furthermore, if **dtmf-relay** is configured on a Version 2 VoIP dial peer and the active call has been established by using fast connect, tunneling procedures initiated by the opposite endpoint are accepted and supported.

H.245 tunneling is backward compatible with H.323 Version 1 configurations.

Configuring DTMF Relay

To configure DTMF relay on a gateway, use the following commands beginning in global configuration mode.

SUMMARY STEPS

1. **dial-peer voice tag voip**
2. **dtmf-relay [cisco-rtp] [h245-alphanumeric] [h245-signal] [rtp-nte]**
3. **rtp payload-type nte** *number*
4. **codec** {**clear-channel** | **g711alaw** | **g711ulaw** | **g723ar53** | **g723ar63** | **g723r53** | **g723r63** | **g726r16** | **g726r24** | **g726r32** | **g726r53** | **g726r63** | **g728** | **g729abr8** | **g729ar8** | **g729br8** | **g729r8** | **gsmefr** | **gsmfr**} [**bytes** *payload_size*]
5. **destination-pattern** *string*[**T**]
6. **session target** {**ipv4:***destination-address* | **dns:[s. | d. | e. | u.]** *hostname* | **loopback:rtp** | **loopback:compressed** | **loopback:uncompressed**}

   or

session target {**ipv4:***destination-address* | **dns:**[**$s$.** | **$d$.** | **$e$.** | **$u$.**] *hostname* | **loopback:rtp** | **loopback:compressed** | **loopback:uncompressed** | **mailto:**{*name* | **$d$.**}@*domainname*}

7. **exit**

DETAILED STEPS

	Command	Purpose

Step 1	`dial-peer voice tag voip`
	Example:
	`Router(config)# dial-peer voice tag voip`
		Enters dial-peer configuration mode for the VoIP dial peer designated by *tag*.

Step 2	`dtmf-relay [cisco-rtp] [h245-alphanumeric] [h245-signal] [rtp-nte]`
	Example:
	`Router(config-dial-peer)# dtmf-relay cisco-rtp h245-alphanumeric h245-signal rtp-nte`
		Forwards DTMF tones. Keywords are as follows:
		• **cisco-rtp**—Forwards DTMF tones by using RTP with a Cisco-proprietary payload type.
		• **h245-alphanumeric**—Forwards DTMF tones by using the H.245 “alphanumeric” User Input Indication (UII) method. Range: tones 0 to 9, *, #, and A to D. Use this keyword to configure DTMF relay.
		• **h245-signal**—Forwards DTMF tones by using the H.245 “signal” UII method. Range: tones 0 to 9, *, #, and A to D.
		• **rtp-nte**—Forwards DTMF tones by using Real-Time Transport Protocol (RTP) with the Named Telephone Event (NTE) payload type.

Step 3	`rtp payload-type nte number`
	Example:
	`Router(config-dial-peer)# rtp payload-type nte 100`
		Identifies the payload type of a Real-Time Transport Protocol (RTP) packet. Keyword and argument are as follows:
		• **nte** *number*—Payload type is a Named Telephone Event (NTE). Range: 96 to 127. Default: 101.
		Do not use the following numbers, because they have preassigned values: 96, 97, 100, 121 to 123, and 125 to 127.
		Use of these values causes the command to fail. You must first reassign the value in use to a different unassigned number, for example:
		`rtp payload-type nse 105`
		`rtp payload-type nte 100`

Step 4	`codec {clear-channel | g711alaw | g711ulaw | g723ar53 | g723ar63 | g723r53 | g723r63 | g726r16 | g726r24 | g726r32 | g726r53 | g726r63 | g728 | g729abr8 | g729ar8 | g729br8 | g729r8 | gsmefr | gsmfr} [bytes payload_size]`
	Example:
	`Router(config-dial-peer)# codec g711alaw`
		Specifies the voice coder rate of speech for a dial peer.

	Command	Purpose
Step 5	**destination-pattern** *string*[**T**] **Example:** `Router(config-dial-peer)# destination-pattern 1513200....`	Specifies the prefix, the full E.164 telephone number, or an ISDN directory number to be used for a dial peer (depending on the dial plan). For an explanation of the keywords and arguments, see the "Configuring Gateway RAS" section on page 33, Step 2.

Step 6	**Cisco 2600 Series and Cisco 3600 Series**
	session target {**ipv4:***destination-address* | **dns:**[**$s$.** | **$d$.** | **$e$.** | **$u$.**] *hostname* | **loopback:rtp** | **loopback:compressed** | **loopback:uncompressed**}
	Cisco AS5300
	session target {**ipv4:***destination-address* | **dns:**[**$s$.** | **$d$.** | **$e$.** | **$u$.**] *hostname* | **loopback:rtp** | **loopback:compressed** | **loopback:uncompressed** | **mailto:**{*name* | **$d$.**}**@***domainname*}
	Example:
	`Router(config-dial-peer)# session target ipv4:192.168.0.0`
		Specifies a network-specific address for a specified dial peer or destination gatekeeper.

Step 7	**exit** **Example:** `Router(config-dial-peer)# exit`	Exits the current mode.

Monitoring and Maintaining DTMF Relay

To monitor and maintain H.323 DTMF relay using NTE, use the following commands.

Step 1 **debug voip rtp session named-event**

Use this command to turn on debugging for RTP NTEs.

Step 2 **show voip rtp connections**

Use this command to display local and remote calling ID and IP address and port information.

Configuring FXS Hookflash Relay

A hookflash indication is a brief on-hook condition that occurs during a call. It is not long enough in duration to be interpreted as a signal to disconnect the call. Create a hookflash indication by quickly depressing and then releasing the hook on your telephone.

PBXs and telephone switches are frequently programmed to intercept hookflash indications and use them as a way to allow a user to invoke supplemental services. For example, your local service provider may allow you to enter a hookflash as a means of switching between calls if you subscribe to a call waiting service.

In the traditional telephone network, a hookflash results in a voltage change on the telephone line. Because there is no equivalent of this voltage change in an IP network, the ITU H.245 standard defines a message representing a hookflash. To send a hookflash indication using this message, an H.323 endpoint sends an H.245 user input indication message containing a "signal" structure with a value of "!". This value represents a hookflash indication.

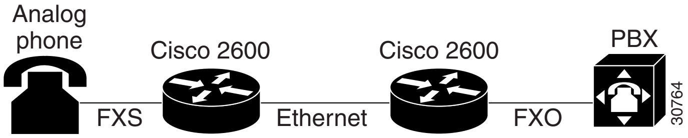
Cisco H.323 Version 2 software includes limited support for relaying hookflash indications using the H.245 protocol. H.245 user input indication messages containing hookflash indications that are received on the IP call leg are forwarded to the plain old telephone service (POTS) call leg if the POTS interface is Foreign Exchange Office (FXO). If the interface is not FXO, any H.245 hookflash indication that is received is ignored. This support allows IP telephony applications to send hookflash indications to a PBX through the Cisco gateway and thereby invoke the IOS supplementary services of the PBX if the PBX supports access to those features using hookflash.

The gateway does not originate H.245 hookflash indications in this release. For example, it does not forward hookflash indications from foreign-exchange-station (FXS) interfaces to the IP network over H.245.

The acceptable duration of a hookflash indication varies by equipment vendor and by country. Although one PBX may consider a 250-ms on-hook condition to be a hookflash, another PBX may consider this condition to be a disconnect. Therefore, the **timing hookflash-out** command allows the administrator to define the duration of a hookflash signal generated on an FXO interface.

Figure 2 illustrates an FXS hookflash being translated to an H.245 user input.

Figure 2 Translating an FXS Hookflash to an H.245 User Input



In Cisco H.323 Version 2 software, an FXS hookflash relay is generated only if the following two conditions are met:

- The other endpoint supports the reception of an H.245 hookflash and advertise this using the "Receive User Input Capability" message during H.245 capabilities exchange.
- The call is established with either the **h245-alphanumeric** or **h245-signal** variant of the **dtmf-relay** command.

This implies that the VoIP dial peer is configured for **dtmf-relay h245-alphanumeric** or **dtmf-relay h245-signal**, but not **cisco-rtp**.

Enter the **timing hookflash-input** command on FXS interfaces to specify the maximum length of a hookflash indication. If the hookflash lasts longer than the specified limit, then the FXS interface processes the indication as an onhook.

To configure hookflash relay on a gateway, use the following commands beginning in global configuration mode.

SUMMARY STEPS

1. **voice-port**
2. **timing hookflash-input** *duration*
3. **timing hookflash-out** *duration*

4. **exit**

DETAILED STEPS

	Command	Purpose
Step 1	**Cisco 2600 and 3600 Series** `Router(config)# voice-port {slot/subunit/port}	{slot/port:ds0-group-no}` **Cisco 7200 Series** `Router(config)# voice-port {slot/port:ds0-group-no}	{slot-number/subunit-number/port}` **Example:** `Router(config)# voice-port 1/0/0`	Enters voice-port configuration mode. Keywords and arguments vary by platform. • *slot*—Slot in which the voice interface card or voice port adapter is installed. Range: 0 to 3. • *subunit*—Subunit on the voice interface card in which the voice port is located. Range: 0 to 1. • *port*—Voice port. Range varies by type of router.

Step 2	`timing hookflash-input duration`
	Example:
	`Router(config-voice-port)# timing hookflash-input 200`
		Specifies the maximum duration of a hookflash indication, in ms. If the hookflash lasts longer than the specified limit, the Foreign Exchange Station (FXS) interface processes the indication as an on-hook. Range: 50 to 1550. Default: 600.

Step 3	`timing hookflash-out duration`
	Example:
	`Router(config-voice-port)# timing hookflash-out 200`
		Specifies the duration, in ms, of the hookflash indications that the gateway generates on a Foreign Exchange Office (FXO) interface. Range: 50 to 1550. Default: 400.

Step 4	`exit`
	Example:
	`Router(config-voice-port)# exit`
		Exits the current mode.

Configuring Multiple Codecs

Normally only one codec is specified when a dial peer is configured on a gateway. However, you can configure a prioritized list of codecs to increase the probability of establishing a connection between endpoints during the H.245 exchange phase.

Codec-order preservation enables a gateway to pass codec preferences to the terminating leg of a VoIP call. This feature was developed primarily for Cisco multiservice IP-to-IP gateways (IPIPGWs), which are configured to use a transparent codec. The transparent codec enables an IPIPGW to pass codecs from the originating endpoint to the terminating endpoint; however, previous versions of the IPIPGW did not preserve the preferential order of the codecs.

With codec-order preservation, the IPIPGW passes codecs transparently from the originating device, listed in order of preference, to the terminating device. It also enables gateways to pass user-configured codecs in their preferred order when the endpoints exchange capabilities, enabling endpoints to use the codec that best suits both devices.

Codec-order preservation is enabled by default in Cisco gateways running Cisco IOS Release 12.3(1) and later releases. No further configuration is needed.

To configure multiple codecs for a dial peer, use the following commands beginning in global configuration mode.

SUMMARY STEPS

1. **voice class codec** *tag*
2. **codec preference** *value codec-type* [**bytes** *payload-size*]
3. **exit**
4. **dial-peer voice** *tag* **voip**
5. **voice-class codec** *tag*
6. **exit**

DETAILED STEPS

	Command	Purpose

Step 1	**`voice class codec`** *`tag`*
	Example:
	`Router(config)# voice class codec 123`
		Enters voice-class configuration mode and assigns an identification tag number for a codec voice class. The *tag* argument is the unique number assigned to the voice class. Range: 1 to 10000. Each tag must be unique on the router.

Step 2	**`codec preference`** *`value codec-type`* `[`**`bytes`** *`payload-size`*`]`
	Example:
	`Router(config-class)# codec preference 1 g711alaw`
		Adds codecs to the prioritized list of codecs. Keyword and arguments are as follows:
		• *value*—Order of preference, with 1 being the most preferred and 12 being the least preferred.
		• *codec-type*—Type of codec preferred.
		• **bytes** *payload-size*—Size of the voice frame in bytes. Values depend on the codec type and the packet voice protocol.

Step 3	**`exit`**
	Example:
	`Router(config-class)# exit`
		Exits the current mode.

Step 4	**`dial-peer voice`** *`tag`* **`voip`**
	Example:
	`Router(config)# dial-peer voice 456 voip`
		Enters dial-peer configuration mode for the VoIP dial peer designated by *tag*.

Step 5	**`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: 1 to 10000. Maps to the tag number created using the **voice class codec** command.

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

Verifying Preservation

To verify preservation, perform the following step.

Step 1 **show running-config**

Use this command to verify the codecs defined for a particular prioritized list of codecs.

```
Router(config-dial-peer)# show running config
```

Configuring Rotary Calling Pattern

Rotary calling pattern routes an incoming call that arrives over a telephony interface back out through another telephony interface under certain circumstances. Rotary calling pattern primarily provides reliable service during network failures.

Call establishment using rotary calling pattern is supported by rotary group support of dial peers, where multiple dial peers may match a given destination phone number and be selected in sequence. In addition, if the destinations need to be tried in a certain order, preference may be assigned. Use the **preference** command when configuring the dial peers to reflect the preferred order (0 being the highest preference and 10 the lowest).

If several dial peers match a particular destination pattern, the system attempts to place a call to the dial peer configured with the highest preference. If the call cannot be completed because of a system outage (for example, the gatekeeper or gateway cannot be contacted), the rotary call pattern performs the following tasks:

- Lists all the conditions under which this instance occurs.
- Retries the call to the next highest preference dial peer.
- Continues until no more matching dial peers are found.

If there are equal priority dial peers, the order is determined randomly.

Note You can configure hunting-algorithm precedence. See the **preference** command in the “Dial Peer Features and Configuration” chapter in *Dial Peer Configuration on Voice Gateway Routers at* http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/dial_peer/dpeer_c.html.

Configuring H.323 Support for Virtual Interfaces

H.323 support for virtual interfaces allows the IP address of the gateway to be configured so that the IP address included in the H.323 packet is always the source IP address of the gateway, regardless of the physical interface and protocol used. This single-address feature allows firewall applications to be easily configured to work with H.323 messages.

Configuring the Source IP Address of a Gateway

To configure a source IP address for a gateway, use the following commands beginning in global configuration mode.

SUMMARY STEPS

1. **interface**
2. **h323-gateway voip bind srcaddr** *ip-address*
3. **exit**

DETAILED STEPS

	Command	Purpose
Step 1	**interface** *type slot***/***port* **Example:** `Router(config)# interface serial 0/0`	Enters interface configuration mode for the specified interface. Keywords and arguments vary by platform.
Step 2	**h323-gateway voip bind srcaddr** *ip-address* **Example:** `Router(config-if)# h323-gateway voip bind srcaddr 192.168.0.0`	Sets the source IP address to be used for this gateway. The argument is as follows: • *ip-address*—IP address to be used for outgoing H.323 traffic, which includes H.225, H.245, and RAS messages. Typically, this is the IP address assigned to the Ethernet interface.
Step 3	**exit** **Example:** `Router(config-if)# exit`	Exits the current mode.

Verifying the Source IP Address of the Gateway

To verify the source IP address of the gateway, perform the following step.

Step 1 **show running-config**

Use this command to verify the source IP address of the gateway. The output shows the source IP address that is bound to the interface.

```
router# show running-config

interface Loopback0
 ip address 10.0.0.0 255.255.255.0
 no ip directed-broadcast
 h323-gateway voip bind srcaddr 10.0.0.0
!
interface Ethernet0/0
 ip address 172.18.194.50 255.255.255.0
 no ip directed-broadcast
 h323-gateway voip interface
 h323-gateway voip id j70f_2600_gk2 ipaddr 172.18.194.53 1719
 h323-gateway voip h323-id j70f_3640_gw1
 h323-gateway voip tech-prefix 3#
.
.
.
```

In the following example, Ethernet interface 0/0 is used as the gateway interface. For convenience, the **h323-gateway voip bind srcaddr** command has been specified on the same interface. The designated source IP address is the same as the IP address assigned to the interface.

```
interface Ethernet0/0
 ip address 172.18.194.50 255.255.255.0
 no ip directed-broadcast
 h323-gateway voip interface
 h323-gateway voip id j70f_2600_gk2 ipaddr 172.18.194.53 1719
 h323-gateway voip h323-id j70f_3640_gw1
 h323-gateway voip tech-prefix 3#
 h323-gateway voip bind srcaddr 172.18.194.50
```

Configuring Annex G

This section contains the following information:

- Information About Annex G, page 62
- Configuring and Provisioning an Annex G Border Element, page 63
- Removing an Annex G Border Element ID, page 66
- Configuring Basic Service Relationships, page 67
- Configuring Usage Indication, page 70
- Verifying Annex G Configuration, page 71

Information About Annex G

Annex G of the H.323 standard provides address resolution using border elements (BE). The BE (as described in Annex G) is colocated with the Cisco H.323 gatekeeper and provides additional address resolution capabilities. The BE can cache address information from neighboring BEs. When the gatekeeper receives a call that it cannot resolve, it can contact its local BE. If the address is in the BE’s cache, the BE on the gatekeeper sends an AccessRequest to the BE in the terminating domain. If the address is not in the BE’s cache, then the BE attempts to resolve the address by sending an AccessRequest to each of its neighboring BEs.

Note The Annex G BEs support Hot Standby Routing Protocol (HSRP) for high reliability and availability. You can identically configure multiple gatekeepers and BEs and use HSRP to designate a primary BE and other standby BEs. If the primary BE is down, a standby BE operates in its place. You configure the local address with an HSRP address in BE configuration.

Figure 3 illustrates a call flow for a scenario in which a call has originated in the zone administered by Border Element D, but the address cannot be resolved locally.

Figure 3 ***Address Resolution Using Border Elements***

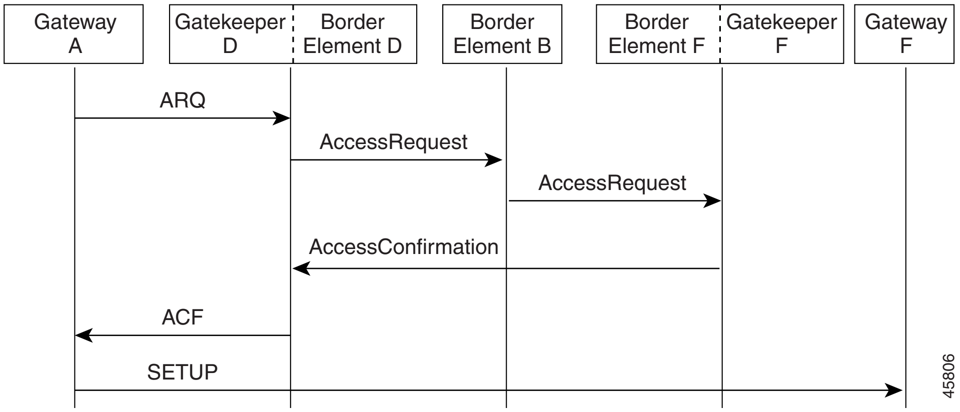


Table 2 describes how address resolution works in the illustration.

Table 2 ***Address Resolution Using Border Elements***

Elements	**Action**
Gateway A to Gatekeeper D/Border Element D	GW A sends an ARQ to GK D/BE D.
Gatekeeper D/Border Element D to Border Element B	GK D/BE D is a noncaching BE and cannot resolve the address internally. Therefore, BE D sends an AccessRequest to BE B.
Border Element B to Border Element F/Gatekeeper F	BE B searches its cache to for the closest match and locates a descriptor that indicates that the access request should be sent to BE F/GK F.
Border element F/gatekeeper F to Border Element D	BE F/GK F returns an access confirmation to BE D. The access confirmation contains a template with a single address indicating where the SETUP message should be sent.
Gatekeeper D/Border Element D to Gateway A	GK D/BE D sends an ACF to GW A.
Gateway A to Gateway F	GW A sends a SETUP message to GW F.

Configuring and Provisioning an Annex G Border Element

To configure and provision an Annex G border element, use the following commands beginning in global configuration mode.

Note Cisco supports one BE per gatekeeper.

SUMMARY STEPS

1. **call-router h323-annexg** *border-element-id*
2. **local ip** *ip-address* [**port** *local-port*]
3. **neighbor** *ip-address*
4. **port** *neighbor-port*

5. **id** *neighbor-id*
6. **cache**
7. **query-interval** *query-interval*
8. **exit**
9. Repeat Steps 3 to 8 for each neighbor BE that you configure.
10. **advertise** [**static** | **dynamic** | **all**]
11. **ttl** *value*
12. **hopcount** *value*
13. **no shutdown**
14. **timer accessrequest sequential delay** *value*
15. **exit**
16. **gatekeeper**
17. **h323-annexg** *border-element-id* **cost** *cost* **priority** *priority*
18. **prefix** *prefix** [**seq** | **blast**]
19. **exit**
20. **exit**

DETAILED STEPS

	Command	Purpose

Step 1	**`call-router h323-annexg`** *`border-element-id`*
	Example:
	`Router(config)# call-router h323-annexg be20`
		Enters Annex G configuration mode for the border element.

Step 2	**`local ip`** *`ip-address`* [**`port`** *`local-port`*] **Example:** `Router(config-annexg)# local ip 192.168.0.0`	Defines the local domain, including the IP address and port that this BE should use for interacting with remote BEs. Specify a port only if you want to use a nonstandard port number; otherwise, use the default standard well-known port 2099.

Step 3	**`neighbor`** *`ip-address`*
	Example:
	`Router(config-annexg)# neighbor 192.168.0.0`
		Enters neighbor configuration mode to configure a neighboring BE that interacts with the local BE for the purpose of obtaining addressing information and aiding in address resolution.

Step 4	**`port`** *`neighbor-port`*
	Example:
	`Router(config-annexg-neigh)# port 2000`
		(Optional) Specifies the neighbor's port number that is used for exchanging Annex G messages. Default: 2099. Do not use this command if you want to use the default value; use it only if you want a value other than 2099.

Step 5	**`id`** *`neighbor-id`*
	Example:
	`Router(config-annexg-neigh)# id be20`
		(Optional) Sets the local ID of the neighboring BE. The ID is used locally to identify the neighbor and has no global significance in the Annex G network.

	Command	Purpose

Step 6	**`cache`**
	Example:
	`Router(config-annexg-neigh)# cache`
		(Optional) Configures the local BE to cache the descriptors received from its neighbors. If caching is enabled, the neighbors are queried at the specified interval for their descriptors.

Step 7	**`query-interval`** *`query-interval`*
	Example:
	`Router(config-annexg-neigh)# query-interval 20`
		(Optional) Sets the interval at which the local BE queries the neighboring BE, in minutes. Default: 30. Do not use this command if you want to use the default query interval; use it only if you want a query interval other than 30 minutes.

Step 8	**`exit`**
	Example:
	`Router(config-annexg-neigh)# exit`
		Exits the current mode.

Step 9	Repeat Steps 3 to 8 for each neighbor BE that you configure.	—

Step 10	**`advertise`** `[`**`static`** `|` **`dynamic`** `|` **`all`**`]`
	Example:
	`Router(config-annexg)# advertise dynamic`
		Specifies the type of descriptors that the BE advertises to its neighbors. Keywords are as follows:
		• **static**—Only the descriptors provisioned on this BE are advertised. This is the default.
		• **dynamic**—Only dynamically learned descriptors are advertised.
		• **all**—Both static and dynamic descriptors are advertised.

Step 11	**`ttl`** *`value`*
	Example:
	`Router(config-annexg)# ttl 2600`
		Sets the time-to-live value for advertisements, in seconds. Default: 3180 (53 minutes).

Step 12	**`hopcount`** *`value`*
	Example:
	`Router(config-annexg)# hopcount 5`
		Specify the maximum number of BE hops through which an address resolution request can be forwarded. Default: 7.

Step 13	**`no shutdown`**
	Example:
	`Router(config-annexg)# no shutdown`
		Starts the BE. By default, when a BE is first configured, it is shut down, so you must use this command after you configure each BE.

Step 14	**`timer accessrequest sequential delay`** *`value`*
	Example:
	`Router(config-annexg)# timer accessrequest sequential delay 3`
		Specifies the intermessage delay (in increments of 100 ms). Range: 0 to 10. Default: 1 (100 ms). Setting this to 0 causes AccessRequest messages to be blasted to applicable neighboring BEs.

Step 15	**`exit`**
	Example:
	`Router(config-annexg)# exit`
		Exits the current mode.

	Command	Purpose
Step 16	**gatekeeper** **Example:** `Router(config)# gatekeeper`	Enters H.323-gatekeeper configuration mode.
Step 17	**h323-annexg** *border-element-id* **cost** *cost* **priority** *priority* **Example:** `Router(config-gk)# h323-annexg be20 cost 35 priority 20`	Enters BE configuration mode and enables the BE on the GK. Keywords and arguments are as follows: • *border-element-id*—Identifier of the border element that you are provisioning. Associates the gatekeeper with the BE identifier that is configured on the BE. Valid values: any International Alphabet 5 (IA5) string, without spaces and up to 20 characters in length. • **cost** *cost*—Cost associated with this border element. When a gatekeeper sends requests to remote zones and to the BE in its attempt to resolve an address, the remote zone or BE that resolves the address and has the lowest cost and highest priority is given preference. Range: 1 to 99. Default: 50. • **priority** *priority*—Priority associated with this border element. When a gatekeeper sends requests to remote zones and to the BE in its attempt to resolve an address, the remote zone or BE that resolves the address and has the lowest cost and highest priority is given preference. Range: 1 to 99. Default: 50.
Step 18	**prefix** prefix* * [**seq** | **blast**] **Example:** `Router(config-gk-annexg)# 419*`	(Optional) Specifies the prefixes for which a BE should be queried for address resolution. Default: the GK forwards all remote zone queries to the BE. Do not use this command unless you want to restrict queries sent to the BE to a specific prefix or set of prefixes.
Step 19	**exit** **Example:** `Router(config-gk-annexg)# exit`	Exits the current mode.
Step 20	**exit** **Example:** `Router(config-gk)# exit`	Exits the current mode.

Removing an Annex G Border Element ID

To remove an Annex G border element ID, use the following commands beginning in global configuration mode.

SUMMARY STEPS

1. **call-router h323-annexg** *border-element-id*
2. **neighbor** *ip-address*

3. **no id** *neighbor-id*
4. **exit**
5. Repeat Steps 3 to 8 for each neighbor BE that you configure.
6. **no shutdown**
7. **exit**

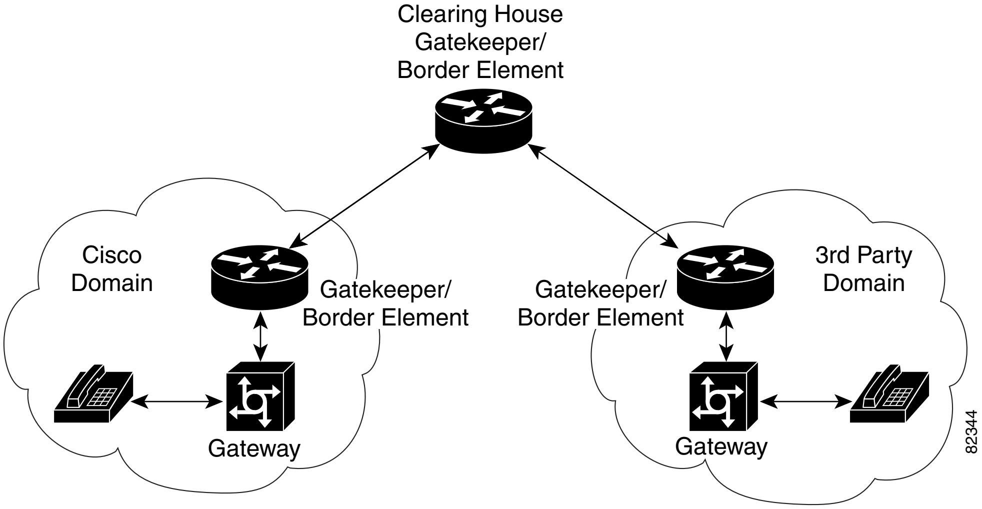
DETAILED STEPS

	Command	Purpose
Step 1	**call-router h323-annexg** *border-element-id* **Example:** `Router(config)# call-router h323-annexg be20`	Enters Annex G configuration mode for the border element.
Step 2	**neighbor** *ip-address* **Example:** `Router(config-annexg)# neighbor 192.168.0.0`	Enters neighbor configuration mode to configure a neighboring BE that interacts with the local BE for the purpose of obtaining addressing information and aiding in address resolution.
Step 3	**no id** *neighbor-id* **Example:** `Router(config-annexg-neigh)# no id be20`	Removes a neighbor ID from the list of configured neighbor BEs. **Note** If a undefined neighbor ID is entered a error message stating “Entry not valid, id not configured”.
Step 4	**exit** **Example:** `Router(config-annexg-neigh)# exit`	Exits the current mode.
Step 5	Repeat Steps 3 to 8 for each neighbor BE that you configure.	—
Step 6	**shutdown** **Example:** `Router(config-annexg)# no shutdown`	Starts the BE. By default, when a BE is first configured, it is shut down, so you must use this command after you configure each BE.
Step 7	**exit** **Example:** `Router(config-annexg-neigh)# exit`	Exits the current mode.

Configuring Basic Service Relationships

Cisco H.225 Annex G implementation supports the minimal set of Annex G features that are needed to allow Cisco border elements (BE) to interoperate with other BEs per the iNow profile for IP telephony interoperability. The implementation also allows Cisco BEs to interoperate with ClearingHouse and other third-party elements. Figure 4 depicts a basic network configuration of BEs, gatekeepers, and Clearing Houses. This feature addresses the link between the gatekeeper/border element (GK/BE) in a Cisco domain and the ClearingHouse border element that complies with the Annex G specification and the iNow profile.

Figure 4 Basic Network Configuration


Clearing House Gatekeeper/ Border Element
Cisco Domain
Gatekeeper/ Border Element
Gatekeeper/ Border Element
3rd Party Domain
Gateway
Gateway
82344

Restrictions for Basic Service Relationships

- Authentication is not supported
- Packet-level integrity checking is not supported.
- ClearingHouse CryptoTokens are not supported.
- Clustered gatekeeper and border element are not supported.
- Interoperation with LRQ-based gatekeeper networks is not supported.
- Layered Annex G networks are not supported.
- Usage indications are supported only within the context of active Service Relationships.

Prerequisites for Basic Service Relationships

- Provision Annex G border elements before configuring Annex G service relationships.

SUMMARY STEPS

1. **call-router h323-annexg** *border-element-id*
2. **access-policy neighbors-only**
3. **domain-name** *id*
4. **neighbor** *ip-address*
5. **service-relationship**
6. **outbound retry-interval** *interval_number*
7. **inbound ttl** *ttl-value*
8. **no shutdown**
9. **exit**
10. **exit**
11. **exit**

DETAILED STEPS

	Command	Purpose
Step 1	**call-router h323-annexg** *border-element-id* **Example:** `Router(config)# call-router h323-annexg be20`	Enters Annex-G configuration mode for the specified border element.
Step 2	**access-policy neighbors-only** **Example:** `Router(config-annexg)# access-policy neighbors-only`	As a prerequisite for configuring service relationships, sets the **access-policy** to accept requests only from known neighbors. Default: **no access-policy** allows request from any border element.
Step 3	**domain-name** *id* **Example:** `Router(config-annexg)# domain-name id`	Sets the domain name reported in service relationships.
Step 4	**neighbor** *ip-address* **Example:** `Router(config-annexg-neigh)# neighbor 192.168.0.0`	Enters neighbor configuration mode to configure a neighboring BE that interacts with the local BE for the purpose of obtaining addressing information and aiding in address resolution.
Step 5	**service-relationship** **Example:** `Router(config-annexg-neigh)# service-relationship`	Enters service-relationship mode.
Step 6	**outbound retry-interval** *interval_number* **Example:** `Router(config-nxg-neigh-svc)# outbound retry-interval 15`	(Optional) Defines the retry period for attempting to establish the outbound relationship between border elements, in seconds. Default: 30.
Step 7	**inbound ttl** *ttl-value* **Example:** `Router(config-nxg-neigh-svc)# inbound 100`	(Optional) Sets the duration of the inbound service relationship and interval in which the remote peer must reestablish the service relationship, in seconds. Default: 120.
Step 8	**no shutdown** **Example:** `Router(config-nxg-neigh-svc)# no shutdown`	Enables the service relationship.
Step 9	**exit** **Example:** `Router(config-nxg-neigh-svc)# exit`	Exits the current mode.

	Command	Purpose
Step 10	**exit** **Example:** `Router(config-annexg-neigh)# exit`	Exits the current mode.
Step 11	**exit** **Example:** `Router(config-annexg)# exit`	Exits the current mode.

Configuring Usage Indication

To enter usage indication submode and configure usage-indicators after service relationships are established, use the following commands beginning in global configuration mode.

SUMMARY STEPS

1. **call-router h323-annexg** *border-element-id*
2. **neighbor** *ip-address*
3. **usage-indication**
4. **retry interval** *seconds*
5. **retry window** *minutes*
6. **exit**
7. **exit**
8. **exit**

DETAILED STEPS

	Command	Purpose
Step 1	**call-router h323-annexg** *border-element-id* **Example:** `Router(config)# call-router h323-annexg be20`	Enters Annex-G configuration mode for the specified border element.
Step 2	**neighbor** *ip-address* **Example:** `Router(config-annexg)# neighbor 192.168.0.0`	Enters neighbor configuration mode to configure a neighboring BE that interacts with the local BE for the purpose of obtaining addressing information and aiding in address resolution.
Step 3	**usage-indication** **Example:** `Router(config-annexg-neigh)# usage-indication`	Enters config-nxg-neigh-usg mode.

Step 4	**`retry interval`** *`seconds`*
	Example:
	`Router(config-nxg-neigh-usg)# retry interval 600`
		(Optional) Defines the time, in seconds, between delivery attempts. Default: 900.

Step 5	**`retry window`** *`minutes`*
	Example:
	`Router(config-nxg-neigh-usg)# retry window 1200`
		(Optional) Defines the total time, in minutes, that a border element attempts delivery. Default: 1440 (24 hours).

Step 6	**`exit`**
	Example:
	`Router(config-nxg-neigh-usg)# exit`
		Exits the current mode.

Step 7	**`exit`**
	Example:
	`Router(config-annexg-neigh)# exit`
		Exits the current mode.

Step 8	`Router(config-annexg)#` **`exit`**
	Example:
	`Router(config-annexg)# exit`
		Exits the current mode.

Verifying Annex G Configuration

To verify Annex G configuration, perform the following step.

Step 1 **show call-router status**

Use this command to display Annex G border-element status.

```
Router# show call-router status neighbors

ANNEX-G CALL ROUTER STATUS:
  ===========================
    Border Element ID Tag    : Celine
    Domain Name              : Celine-Domain
    Border Element State     : UP
    Border Element Local IP : 172.18.193.31:2099
    Advertise Policy         : STATIC descriptors
    Hopcount Value           : 7
    Descriptor TTL           : 3180
    Access Policy            : Neighbors only
    Current Active Calls     : 0
    Current Calls in Cache   : 0
    Cumulative Active Calls : 0
    Usage Ind Messages Sent : 0
    Usage Ind Cfm Rcvd       : 0
    IRRs Received            : 0
    DRQs Received            : 0
    Usage Ind Send Retrys    : 0

  NEIGHBOR INFORMATION:
  =====================
    Local Neighbor ID : (none)
    Remote Element ID : (unknown)
    Remote Domain ID  : (unknown)
    IP Addr           : 1.2.3.4:2099
    Status            : DOWN
    Caching           : OFF
    Query Interval    : 30 MIN (querying disabled)
    Usage Indications :
      Current Active Calls : 0
      Retry Period         : 600 SEC
      Retry Window         : 3600 MIN
    Service Relationship Status: ACTIVE
      Inbound Service Relationship  : DOWN
        Service ID     : (none)
        TTL            : 1200 SEC
      Outbound Service Relationship : DOWN
        Service ID     : (none)
        TTL            : (none)
        Retry interval : 120 SEC (0 until next attempt)
```

Configuring H.225

This section contains the following information:

- Associating the H.323 Voice Class with Each VoIP Dial Peer, page 72
- Configuring the SETUP Response Timeout Value, page 73
- Configuring the Number of Concurrent Calls Per Connection, page 74
- Changing the Idle Timer for Concurrent Calls, page 74
- Configuring Overlap Signaling on H.323 Terminating Gateways, page 75
- Configuring No Retry on User Busy in an H.323 Gateway, page 76
- Configuring the VoIP Transport Method, page 78

Associating the H.323 Voice Class with Each VoIP Dial Peer

To associate the H.323 voice class with a dial peer, use the following commands beginning in global configuration mode.

SUMMARY STEPS

1. **dial-peer voice** *tag* **voip**
2. **voice-class h323** *number*
3. **exit**

DETAILED STEPS

	Command	Purpose
Step 1	**dial-peer voice** *tag* **voip** **Example:** `Router(config)# dial-peer voice 123 voip`	Enters dial-peer configuration mode for the remote VoIP dial peer designated by *tag*.
Step 2	**voice-class h323** *number* **Example:** `Router(config-dial-peer)# voice-class h323 456`	Associates the specified H.323 voice class (and all of its related attributes) with the dial peer.
Step 3	**exit** **Example:** `Router(config-dial-peer)# exit`	Exits the current mode.

Configuring the SETUP Response Timeout Value

To configure the timeout value for the response of the outgoing SETUP message, use the following commands in global configuration mode.

SUMMARY STEPS

1. **voice class h323** *number*
2. **h225 timeout setup** *value*
3. **exit**

DETAILED STEPS

	Command	Purpose
Step 1	**voice class h323** *number* **Example:** `Router(config)# voice class h323 123`	Enters voice-class mode to create or modify the specified H.323 voice class.
Step 2	**h225 timeout setup** *value* **Example:** `Router(config-class)# h225 timeout setup 10`	Sets the timeout value, in seconds, for the response of the outgoing SETUP message. If the timer expires, the GK tries an alternate endpoint (if configured and specified in the ACF); otherwise, it terminates the call. Range: 0 to 30. Default: 15.
Step 3	**exit** **Example:** `Router(config-class)# exit`	Exits the current mode.

Configuring the Number of Concurrent Calls Per Connection

To limit the number of concurrent calls on an H.225 TCP connection, use the following commands in global configuration mode.

SUMMARY STEPS

1. **voice service voip**
2. **h323**
3. **session transport tcp** [**calls-per-connection** *value*]
4. **exit**

DETAILED STEPS

	Command	Purpose

Step 1	`voice service voip`
	Example:
	`Router(config)# voice service voip`
		Enters voice-service configuration mode.

Step 2	`h323`
	Example:
	`Router(conf-voi-serv)# h323`
		Enters H.323-voice-service configuration mode.

Step 3	`session transport tcp [calls-per-connection value]`
	Example:
	`Router(conf-serv-h323)# session transport tcp`
		Sets the number of concurrent calls for a single TCP connection. Range: 1 to 9999. Default: 5.

Step 4	`exit`
	Example:
	`Router(conf-serv-h323)# exit`
		Exits the current mode.

Changing the Idle Timer for Concurrent Calls

To change the H.225 idle timer for concurrent calls, use the following commands in global configuration mode.

SUMMARY STEPS

1. **voice service voip**
2. **h323**
3. **h225 timeout tcp call-idle** {**value** *value* | **never**}
4. **exit**

DETAILED STEPS

	Command	Purpose

Step 1	**`voice service voip`**
	Example:
	`Router(config)# voice service voip`
		Enters voice-service configuration mode.

Step 2	**`h323`**
	Example:
	`Router(conf-voi-serv)# h323`
		Enter s H.323-voice-service configuration mode.

Step 3	**`h225 timeout tcp call-idle`** `{`**`value`** *`value`* `|` **`never`**`}`
	Example:
	`Router(conf-serv-h323)# h225 timeout tcp call-idle never`
		Sets a timer to maintain a connection when no calls are active.

Step 4	**`exit`**
	Example:
	`Router(conf-serv-h323)# exit`
		Exits the current mode.

Configuring Overlap Signaling on H.323 Terminating Gateways

The terminating gateway is responsible for collecting all the called number digits. Overlap signaling is implemented by matching destination patterns on the dial peers. When H.225 signal overlap is configured on the originating gateway, it sends the SETUP to the terminating gateway once a dial-peer match is found. The originating gateway sends all further digits received from the user to the terminating gateway using INFO messages until it receives a sending complete message from the user. The terminating gateway receives the digits in SETUP and subsequent INFO messages and does a dial-peer match. If a match is found, it sends a SETUP with the collected digits to the PSTN. All subsequent digits are sent to the PSTN using INFO messages to complete the call.

To configure overlap signaling on H.323 terminating gateways, perform the following steps.

SUMMARY STEPS

1. **voice service voip**
2. **h323**
3. **h225 signal overlap**
4. **h225 timeout t302**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`voice service voip`**
	Example:
	`Router(config)# voice service voip`
		Enters VoIP voice-service configuration mode.

Step 2	**`h323`**
	Example:
	`Router(conf-voi-serv)# h323`
		Enters H.323 voice-service configuration mode.

Step 3	**`h225 signal overlap`**
	Example:
	`Router(conf-serv-h323)# h225 signal overlap`
		Activates overlap signaling to the destination gateway.

Step 4	**`h225 timeout t302`** *`seconds`*
	Example:
	`Router(conf-serv-h323)# h225 timeout t302 15`
		Sets the t302 timer timeout value. The argument is as follows:
		• *seconds*— Number of seconds for timeouts. Range: 1 to 30.

Step 5	**`exit`**
	Example:
	`Router(conf-serv-h323)# exit`
		Exits the current mode.

Configuring No Retry on User Busy in an H.323 Gateway

This section describes how to configure the alternate endpoint hunt for failed calls in an IP-to-IP Gateway (IPIPGW) based on Q.850 disconnect cause codes.

The default behavior of the gateway is to retry all alternate endpoints received from the gatekeeper regardless of the ReasonComplete reason. Perform this task if you want to stop the alternate endpoint hunt retry attempts when the ReasonComplete is User-busy or Invalid-number.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **h323**
5. **no h225 alt-ep hunt** [**all** | *cause-code*]

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 a voice encapsulation type.

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

Step 5	**`no h225 alt-ep hunt user-busy`**
	Example:
	`Router(conf-serv-h323)# no h225 alt-ep hunt user-busy`
		Disables alternate endpoint hunts.
		• all—Continue hunt for all disconnect cause codes.
		• cause-code—May be entered as standard Q.850 number or as text.
		Note Alternate endpoint hunt is enabled for all cause codes by default. Command will be visible only for the negated hunt cause codes (with **no** prefixed).
		Note This functionality, requires a Cisco Gatekeeper. See the "Configuring H.323 Gatekeepers and Proxies" chapter of this guide.

Examples

The following example shows a configuration that disables the alternate endpoint hunt for user busy and no answer:

```
!
voice service voip
h323
no h225 alt-ep hunt user-busy
no h225 alt-ep hunt no-answer
!
```

Configuring the VoIP Transport Method

To configure the VoIP transport method, use the following commands beginning in global configuration mode.

SUMMARY STEPS

1. **voice service voip**
2. **h323**
3. **session transport** {**udp** | **tcp**}
4. **exit**

DETAILED STEPS

	Command	Purpose

Step 1	`voice service voip`
	Example:
	`Router(config)# voice service voip`
		Enters voice-service configuration mode.

Step 2	`h323`
	Example:
	`Router(conf-voi-serv)# h323`
		Enters H.323-voice-service configuration mode.

Step 3	`session transport {udp | tcp}`
	Example:
	`Router(conf-serv-h323)# session transport tcp`
		Sets the underlying transport layer protocol for H.323 messages to be used across all VoIP dial peers. If you specify **udp**, Annex E is used. For concurrent calls, you must specify **tcp**.

Step 4	`exit`
	Example:
	`Router(conf-serv-h323)# exit`
		Exits the current mode.

Configuring Zone Bandwidth Management

In the current version of the Cisco H.323 gateway (which conforms with H.323 version 3), the reported bandwidth is bidirectional. Initially, 128 kb is reserved. If the endpoints in the call select a more efficient codec, the gatekeeper is notified of the bandwidth change.

If you prefer to use the behavior of previous Cisco H.323 gateway versions for zone bandwidth management, configure the gateway accordingly.

To configure the Cisco H.323 gateway to use its previous behavior, use the following commands beginning in global configuration mode.

SUMMARY STEPS

1. **gateway**
2. **emulate cisco h323 bandwidth**
3. **exit**

DETAILED STEPS

	Command	Purpose

Step 1	**`gateway`**
	Example:
	`Router(config)# gateway`
		Enters gateway configuration mode.

Step 2	**`emulate cisco h323 bandwidth`**
	Example:
	`Router(config-gateway)# emulate cisco h323 bandwidth`
		Sets the gateway to use its previous behavior for bandwidth management.

Step 3	**`exit`**
	Example:
	`Router(config-gateway)# exit`
		Exits the current mode.

Configuring Generic Transparency Descriptor for GKTMP Using SS7 Interconnect for Voice Gateways Version 2.0

This section contains the following information:

- Information About GTD for GKTMP Using SS7 Interconnect for Voice Gateways, page 79
- Prerequisites for GTD for GKTMP Using SS7 Interconnect for Voice Gateways, page 81
- Configuring GTD System-Wide, page 81
- Configuring GTD for a Dial Peer, page 82
- Verifying GTD, page 83

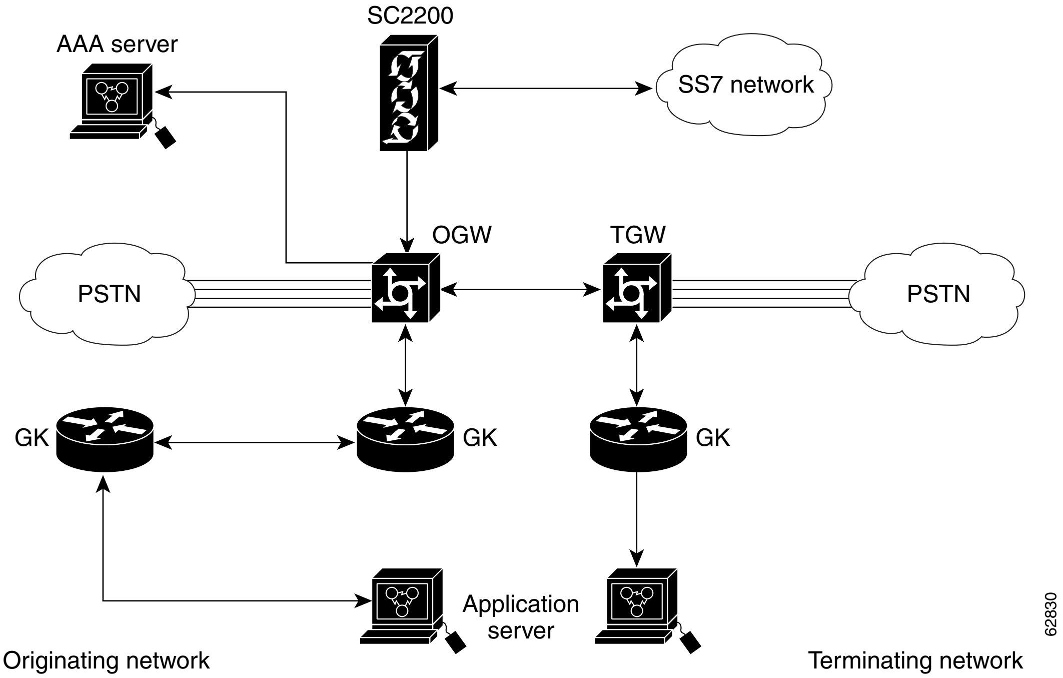
Information About GTD for GKTMP Using SS7 Interconnect for Voice Gateways

The GTD for GKTMP Using SS7 Interconnect for Voice Gateways feature provides additional functionality to Cisco gateways and gatekeepers in a Cisco SS7 Interconnect for Voice Gateways Solution. The generic transparency descriptor or generic telephony descriptor (GTD) format is defined in the a Cisco-proprietary draft. GTD format defines parameters and messages of existing SS7 ISUP protocols in text format and allows SS7 messages to be carried as a payload in the H.225 RAS messages between gateway and gatekeeper. With the GTD feature, the gatekeeper extracts the GTD message and the external route server derives routing and accounting information based upon the GTD information provided from the Cisco Gatekeeper Transaction Message Protocol (GKTMP).

Currently routing on Cisco gateways is based on generic parameters such as originating number, destination number, and port source. Adding support for SS7 ISUP messages allows the VoIP network to use additional routing enhancements found in traditional TDM switches.

Figure 5 shows an example of a Cisco SS7 Interconnect for Voice Gateways solution using the GTD feature.

Figure 5 Cisco SS7 Interconnect for Voice Gateways Solution With the GTD Feature



In the originating network, the following events occur:

- The Cisco SC2200 receives SS7 messages from the SS7 network and encapsulates them into GTD format. The messages are then passed to the Cisco originating gateway (OGW).
- Using the GTD feature, the OGW transmits the GTD payload in the Admission Request (ARQ) message to GK1.
- GK1 transmits the GTD payload in a Location Request (LRQ) message to GK2.
- GK 2 uses GKTMP with the GTD feature to decode the GTD payload and transmits it to the route server with the REQUEST LRQ message.
- The route server returns a RESPONSE LCF (Location Confirmation) message that includes the GTD payload to GK2. The route server also returns a service descriptor code (SC) field to GK2. (The SC field is transmitted to the AAA server for billing purposes. The SC field conveys the Carrier ID and trunk number information that is determined by and passed from the Route Server.)
- GK2 passes the LCF that includes the GTD payload and the SC field to GK1.
- GK1 sends an Admission Confirmation (ACF) message that includes the GTD payload to the OGW, along with the SC field.
- The OGW sends the SC field and call detail records (CDRs) to the AAA server.
- When the call ends, the Cisco SC2200 receives the SS7 messages, encodes them into GTD format, and passes them to the OGW.

- The OGW sends a Disengage Request (DRQ) with the GTD payload to GK1.
- GK1 sends the DRQ with the GTD payload to the route server.

In the terminating network, the following events occur:

- The OGW sends the GTD in H.225 the SETUP message to the terminating gateway (TGW).
- The TGW sends regular RAS messages to the gatekeeper.

Prerequisites for GTD for GKTMP Using SS7 Interconnect for Voice Gateways

- Configure your VoIP network and the Cisco SS7 Interconnect for Voice Gateways Solution, including the following components:
  - Cisco SC2200—Cisco MGC Software Release 9.1(5) or higher
  - Cisco IOS gateways—Cisco IOS Release 12.2(2)XU or higher
  - Cisco IOS gatekeepers—Cisco IOS Release 12.2(2)XU or higher
  - Route servers
  - AAA servers

Note For more information on software and components of the Cisco SS7 Interconnect for Voice Gateways Solution, see the release notes and other documentation at http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel7/soln/das/index.htm

Configuring GTD System-Wide

To configure the GTD feature system-wide for a VoIP network, enter the commands shown below. If you want to configure the feature on individual dial peers rather than system-wide, use the commands in the "Configuring GTD for a Dial Peer" section on page 82.

SUMMARY STEPS

1. **voice service voip**
2. **signaling forward** {**none** | **unconditional**}
3. **exit**

DETAILED STEPS

	Command	Purpose

Step 1	**`voice service voip`**
	Example:
	`Router(config)# voice service voip`
		Enters voice-service configuration mode.

Step 2	**`signaling forward`** {**`unconditional`** | **`none`**}
	Example:
	`Router(conf-voi-serv)# signaling forward unconditional`
		Chooses whether or not the gateway forwards signaling payload to another gateway. Keywords are as follows:
		• **unconditional**—Forward payload to the remote end, even if the attached external route server has modified the payload.
		• **none**—Do not forward payload.

Step 3	**`exit`**
	Example:
	`Router(conf-voi-serv)# exit`
		Exits the current mode.

Configuring GTD for a Dial Peer

To configure the GTD feature on an individual dial peer, follow the steps below.

SUMMARY STEPS

1. **dial-peer voice** *tag* **voip**
2. **signaling forward** {**conditional** | **unconditional** | **none**}
3. **exit**

DETAILED STEPS

	Command	Purpose

Step 1	**`dial-peer voice`** *`tag`* **`voip`**
	Example:
	`Router(config)# dial-peer voice 4 voip`
		Enters dial-peer configuration mode for the VoIP dial peer designated by *tag*.

Step 2	**`signaling forward`** `{`**`conditional`** `|` **`unconditional`** `|` **`none`**`}`
	Example:
	`Router(config-dial-peer)# signaling forward conditional`
		Chooses whether or not the gateway forwards signaling payload to another gateway. Keywords are as follows:
		• **conditional**—Forward payload as defined in the **session target** command.
		– If the target is a non-RAS target, forward to the H.323 endpoint using H.225 messages.
		– If the target is a RAS target, for a non-GTD payload, forward. For a GTD payload, encapsulate the payload in an ARQ/DRQ message and send it to the originating gateway. The gateway conveys the payload to the GKTMP and external route server for a flexible route decision based up the ISUP GTD parameters. The gateway then conditionally forwards the payload based upon the route server's instruction.
		• **unconditional**—Forward the payload to the remote end, even if the attached external route server has modified the payload.
		• **none**—Do not forward payload.

Step 3	**`exit`**
	Example:
	`Router(config-dial-peer)# exit`
		Exits the current mode.

Verifying GTD

To verify GTD, perform the following step.

Step 1 **show running-config**

Use this command to verify that the GTD feature is configured.

The following shows sample output for system-wide employment.

```
Router# show running-config

Building configuration...

Current configuration : 4192 bytes
!
version 12.2
service config
no service single-slot-reload-enable
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service internal
service udp-small-servers
!
hostname as5300-2
!
voice service voip
 signaling forward unconditional
 h323
.
.
.
```

The following shows sample output for employment on select dial peers.

```
Router# show running-config

Building configuration...

Current configuration : 4192 bytes
!
version 12.2
service config
no service single-slot-reload-enable
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service internal
service udp-small-servers
!
hostname as5300-2
!
.
.
.
!
dial-peer voice 1 pots
 application session
 incoming called-number 25164
 port 0:D
!
dial-peer voice 1513 voip
 destination-pattern 1513.......
 session target ipv4:1.8.156.3
!
dial-peer voice 1408525 voip
 destination-pattern 1408525....
!
dial-peer voice 1800877 voip
 destination-pattern 1800877....
 session target ipv4:1.8.156.3
!
dial-peer voice 2 pots
 destination-pattern 51550
 no digit-strip
 direct-inward-dial
 port 3:D
!
dial-peer voice 51557 voip
 destination-pattern 51557
 signaling forward unconditional
 session target ras
!
```

```
dial-peer voice 52557 voip
 destination-pattern 52557
 signaling forward unconditional
 session target ipv4:1.8.156.3
!
.
.
.
```

Configuring H.323 Version 4 Zone Prefix Registration

The H.323v4 Gateway Zone Prefix Registration Enhancements feature provides support for two capabilities included in H.323 Version 4: additive registration and dynamic zone prefix registration. Additive registration allows a gateway to add to or modify a list of aliases contained in a previous registration without first unregistering from the gatekeeper. Dynamic zone prefix registration allows a gateway to register actual public switched telephone network (PSTN) destinations served by the gateway with its gatekeeper.

Information About H.323v4 Gateway Zone Prefix Registration Enhancements

To configure the H.323v4 Gateway Zone Prefix Registration Enhancements feature, you must understand the following concepts:

- Additive Registration, page 85
- Dynamic Zone Prefix Registration, page 85

Additive Registration

Prior to H.323 version 4, there was no way for a large device, such as a gateway, to register hundreds or thousands of E.164 alias addresses with a gatekeeper. The limiting factor was the size of a User Datagram Protocol (UDP) packet, which does not allow an unlimited number of aliases in a single heavyweight **registration request** (RRQ) RAS message.

To allow an endpoint to register an unlimited number of aliases with the gatekeeper, H.323v4 introduces the concept of *additive registration*. When the gateway registers with a gatekeeper, it provides an initial list of aliases. Additive registration allows the gateway to send subsequent RRQ messages with more lists of aliases until the gatekeeper has the complete list of the gateway’s aliases.

When the gatekeeper wants to acknowledge only a subset of the aliases proposed in an additive RRQ, the gatekeeper returns a registration confirm (RCF) RAS message specifying the accepted aliases. The gateway assumes that the aliases not listed in the RCF were rejected.

Dynamic Zone Prefix Registration

H.323v4 allows a gateway to register actual zone prefixes that it can terminate to the PSTN with a gatekeeper. A gateway can register multiple zone prefixes with the gatekeeper via the RRQ message and subsequently remove one or more zone prefixes using an unregistration request (URQ) RAS message indicating the specific prefixes to be removed. When the gatekeeper receives the URQ, it leaves the gateway registered and removes the specified zone prefixes.

When the H.323v4 Gateway Zone Prefix Registration Enhancements feature is enabled on a trunking gateway, all addresses specified by the destination patterns in the plain old telephone service (POTS) dial peers that are operational are advertised to the gatekeeper.

The gatekeeper treats these addresses similarly to configured zone prefixes. The dynamically registered zone prefixes are used in routing decisions just as if they had been entered using the **zone prefix** command. Dynamically registered zone prefixes have a default gateway priority of 5.

Table 3 shows destination patterns on gateway GW1 and how the gatekeeper GK1 views the dynamically registered prefixes.

Table 3 Gateway Prefixes Dynamically Registered on the Gatekeeper

GW1 Configuration	GK1 Corresponding Pseudo Configuration

`dial-peer voice 919 pots`
`destination-pattern 919.......`
`port 0:D`
	`gatekeeper`
	`zone local GK1 cisco.com 172.18.197.132`
	`zone prefix GK1 919....... gw-priority 5 GW1`

`dial-peer voice 5551001pots`
`destination-pattern 5551001`
`port 0:D`
	`gatekeeper`
	`zone local GK1 cisco.com 172.18.197.132`
	`zone prefix GK1 5551001* gw-priority 5 GW1`

`dial-peer voice 408 pots`
`destination-pattern 408T`
`port 0:D`
	`gatekeeper`
	`zone local GK1 cisco.com 172.18.197.132`
	`zone prefix GK1 408* gw-priority 5 GW1`

Configuring H.323v4 Gateway Zone Prefix Registration Enhancements

This section contains the following tasks:

- Enabling the Dynamic Zone Prefix Registration, page 86 (required)
- Enabling the Dynamic Zone Prefix Registration Along with the Gateway Priority, page 88
- Verifying Gateway Advertisement of Dynamic Zone Prefixes, page 89
- Verifying Gatekeeper Processing of Additive RRQ Messages, page 90
- Troubleshooting H.323v4 Gateway Zone Prefix Registration Enhancements, page 90

Enabling the Dynamic Zone Prefix Registration

This task shows you how to enable the gateway to send an advertisement of dynamic prefixes in additive RRQ RAS messages automatically to the gatekeeper.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **h323**
5. **ras rrq dynamic prefixes**
6. **exit**
7. **gatekeeper**
8. **rrq dynamic-prefixes-accept**
9. **exit**

DETAILED STEPS

	Command or Action	Purpose

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

Step 1	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 2	**`voice service voip`**
	Example:
	`Router(config)# voice service voip`
		Enters voice service configuration mode.

Step 3	**`h323`**
	Example:
	`Router(config-voice-service)# h323`
		Enters the H.323 voice service configuration mode.

Step 4	**`ras rrq dynamic prefixes`**
	Example:
	`Router(conf-serv-h323)# ras rrq dynamic prefixes`
		Enables the gateway to send an advertisement of dynamic prefixes in additive RRQ RAS messages.
		Note In Cisco IOS Release 12.2(15)T, this command was enabled by default. Beginning in Cisco IOS Release 12.3(3), this command is disabled by default.

Step 5	**`exit`**
	Example:
	`Router(conf-serv-h323)# exit`
		Exits voice service voip h323 configuration mode and enters global configuration mode.

Step 6	**`gatekeeper`**
	Example:
	`Router(config)# gatekeeper`
		Enters gatekeeper configuration mode.

Step 7	**`rrq dynamic-prefixes-accept`**
	Example:
	`Router(config-gk)# rrq dynamic-prefixes-accept`
		Enables the gatekeeper to receive the RRQ RAS messages from the gateway.
		Note In Cisco IOS Release 12.2(15)T, this command was enabled by default. Beginning in Cisco IOS Release 12.3(3), this command is disabled by default.

Step 8	**`exit`**
	Example:
	`Router(config-gk)# exit`
		Exits gatekeeper configuration mode.

Enabling the Dynamic Zone Prefix Registration Along with the Gateway Priority

This task shows you how to configure the priority to the dynamic prefixes on the gateway. Allowing you to configure a different priority to each of the dynamic prefix. When configured, the gateway sends the priority along with the prefixes in additive RRQ and the gatekeeper assigns the received priority to the gateway for a given dynamic prefix.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **h323**
5. **terminal-alias-pattern 22... priority 8**
6. **terminal-alias-pattern 23* priority 7**
7. Repeat Step 5 for each prefix on the gateway.
8. **ras rrq dynamic prefixes**
9. **exit**

DETAILED STEPS

	Command or Action	Purpose

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

Step 1	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 2	**`voice service voip`**
	Example:
	`Router(config)# voice service voip`
		Enters voice-service configuration mode.

Step 3	**`h323`**
	Example:
	`Router(config-voice-service)# h323`
		Enters H.323 voice-service configuration mode.

Step 4	**`terminal-alias-pattern 22... priority 8`**
	Example:
	`Router(conf-serv-h323)# terminal-alias-pattern 23 priority 8`
		Assigns priority to a dynamic prefix. The prefixes mentioned in this command should exactly match the prefixes configured in the **destination-pattern** command of POTS dial-peer.
		Note Dynamic zone prefix does not support destination patterns with regular expression. It accepts the patterns ending with dot "." and asterisk "*" only.

	Command or Action	Purpose

Step 5	`terminal-alias-pattern 23* priority 7`
	Example:
	`Router(conf-serv-h323)# terminal-alias-pattern 23* priority 7`
		Assigns priority to a dynamic prefix. The prefixes mentioned in this command should exactly match the prefixes configured in the **destination-pattern** command of POTS dial-peer.
		Note Dynamic zone prefix does not support destination patterns with regular expression. It accepts the patterns ending with dot "." and asterisk "*" only.

Step 6	Repeat Step 5 for each priority you configure.	—

Step 7	**`ras rrq dynamic prefixes`**
	Example:
	`Router(conf-serv-h323)# ras rrq dynamic prefixes`
		Enables the gateway to send an advertisement of dynamic prefixes in additive RRQ RAS messages.
		Note In Cisco IOS Release 12.2(15)T, this command was enabled by default. Beginning in Cisco IOS Release 12.3(3), this command is disabled by default.

Step 8	**`exit`**
	Example:
	`Router(conf-serv-h323)# exit`
		Exits gatekeeper configuration mode.

Verifying Gateway Advertisement of Dynamic Zone Prefixes

Perform this task to verify that the gateway is advertising dynamic zone prefixes**.**

SUMMARY STEPS

1. **enable**
2. **show gateway**
3. **show h323 gateway prefixes**

DETAILED STEPS

	Command or Action	Purpose

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

Step 2	**`show gateway`**
	Example:
	`Router# show gateway`
		Displays the current status of the gateway.

Step 3	**`show h323 gateway prefixes`**
	Example:
	`Router# show h323 gateway prefixes`
		Displays the status of the gateway destination pattern database and the status of the individual destination patterns along with it's configured priority.
		• Verify that gateway additive RRQ support is enabled, that the pattern database is active, and that destination patterns have been acknowledged by the gatekeeper.

Verifying Gatekeeper Processing of Additive RRQ Messages

Perform this task to verify that the gatekeeper is processing additive RRQ messages.

SUMMARY STEPS

1. **enable**
2. **show gatekeeper zone prefix** [**all**]
3. **show gatekeeper gw-type-prefix**
4. **show gatekeeper endpoints**

DETAILED STEPS

	Command or Action	Purpose

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

Step 2	`show gatekeeper zone prefix [all]`
	Example:
	`Router# show gatekeeper zone prefix all`
		Displays the gatekeeper zone prefix table.
		• Use the **all** keyword to display the dynamic zone prefixes registered by each gateway.
		• Use the **include** filter with the **all** keyword to display the prefixes associated with a particular gateway.

Step 3	`show gatekeeper gw-type-prefix`
	Example:
	`Router# show gatekeeper gw-type-prefix`
		Displays the gateway technology prefix table.

Step 4	`show gatekeeper endpoints`
	Example:
	`Router# show gatekeeper endpoints`
		Displays the status of all registered endpoints for a gatekeeper.

Troubleshooting H.323v4 Gateway Zone Prefix Registration Enhancements

Use the **debug h225 asn1** command to observe the dynamic registration process. The **debug h225 asn1** command is intended only for troubleshooting purposes because the volume of output generated by the software can result in severe performance degradation on the router.

Prerequisites

Attach a console directly to a router running Cisco IOS Release 12.2(15)T or a later release.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **logging buffered** [*buffer-size* | *level*]

4. **no logging console**
5. **end**
6. **debug h225 asn1**
7. **show logging** [**history** | **slot** *slot-number* | **summary** | **count**]
8. **no debug h225 asn1**

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	**logging buffered** [*buffer-size* | *level*] **Example:** Router(config)# logging buffered 65536	Limits messages logged to an internal buffer based on severity.
Step 4	**no logging console** **Example:** Router(config)# no logging console	Disables all logging to the console terminal. • To reenable logging to the console, use the **logging console** command in global configuration mode.
Step 5	**end** **Example:** Router(config)# end	Exits to privileged EXEC mode.
Step 6	**debug h225 asn1** **Example:** Router# debug h225 asn1	Displays ASN1 contents of RAS and Q.931 messages. **Caution** This command slows down the system considerably. Connections may time out.
Step 7	**show logging** [**history** | **slot** *slot-number* | **summary** | **count**] **Example:** Router# show logging	Displays the state of logging (syslog).
Step 8	**no debug h225 asn1** **Example:** Router# no debug h225 asn1	Disables display of ASN1 contents of RAS and Q.931 messages.

Configuring Call Admission Control

Cisco H.323 gateways provide the ability to support resource-based call admission control (CAC) processes. These resources include system resources such as CPU, memory, and call volume, and interface resources such as call volume.

If system resources are not available to admit the call, two kinds of actions are provided: system denial which busyouts all of T1 or E1 or per call denial, which disconnects, hairpins, or plays a message or tone. If the interface-based resource is not available to admit the call, the call is dropped from the session protocol.

Note For information on CAC, see *Trunk Connections and Conditioning Features* at http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/cisco_ios_voice_configuration_library_glossary/vcltrunk.html.

Configuring Trunk-Based and Carrier-Based Routing

Voice wholesalers use multiple ingress and egress carriers to route traffic. A call coming into a gateway on a particular ingress carrier must be routed to an appropriate egress carrier. As networks grow and become more complicated, the dial plans needed to route the carrier traffic efficiently become more complex and the need for carrier-sensitive routing (CSR) increases.

Note For information on routing, see *VoIP Gateway Trunk and Carrier Based Routing Enhancements* at the following URL: http://www.cisco.com/en/US/docs/ios/12_2t/12_2t11/feature/guide/ftgwrepg.html

Configuring Signal ISDN B-Channel ID to Enable Application Control of Voice Gateway Trunks

This section contains the following information:

- Information About Signal ISDN B-Channel ID, page 92
- Configuring Signal ISDN B-Channel ID, page 93
- Troubleshooting Signal ISDN B-Channel ID, page 93

Information About Signal ISDN B-Channel ID

The Signal ISDN B-Channel ID to Enable Application Control of Voice Gateway Trunks feature enables call-management applications to identify specific ISDN bearer (B) channels used during a voice-gateway call for billing purposes. With identification of the B channel, H.323 gateways can enable port-specific features such as voice recording and call transfer.

In Cisco IOS releases prior to 12.3(7)T, fields used to store call leg information regarding the telephony port do not include B channel information. B-channel information is used to describe incoming ISDN call legs. The Signal ISDN B-Channel ID to Enable Application Control of Voice Gateway Trunks feature allows H.323 and SIP gateways to receive B-channel information from incoming ISDN calls. The acquired B-channel information can be used during call transfer or to route a call.

SIP and H.323 gateways use two different commands to enable receiving the B channel of a telephony call leg. Using a different command for each protocol allows users to run the two protocols on one gateway simultaneously.

Note For information on using this feature on SIP gateways, see the information on SIP ISDN support features in the *Cisco IOS SIP Configuration Guide* at http://www.cisco.com/en/US/docs/ios/voice/sip/configuration/guide/15_0/sip_15_0_book.html

For H.323, if the **billing b-channel** command is configured, the H.323 gateway accesses B-channel information on all calls in the ARQ, LRQ, and GKTMP messages.

Configuring Signal ISDN B-Channel ID

To provide H.323 users with B-channel information, use the following commands beginning in global configuration mode.

SUMMARY STEPS

1. **voice service voip**
2. **h323**
3. **billing b-channel**
4. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`voice service voip`**
	Example:
	`Router(config)# voice service voip`
		Enters voice-service configuration mode and specifies a voice-encapsulation type.

Step 2	**`h323`**
	Example:
	`Router(conf-voi-serv)# h323`
		Enters H.323-voice-service configuration mode.

Step 3	**`billing b-channel`**
	Example:
	`Router(conf-serv-h323)# billing b-channel`
		Enables the H.323 gateway to access B-channel information on all H.323 calls.

Step 4	**`exit`**
	Example:
	`Router(conf-serv-h323)# end`
		Exits the current mode.

Troubleshooting Signal ISDN B-Channel ID

To troubleshoot signal ISDN B-channel ID problems, perform the following steps.

Step 1 **debug h245 asn1**

Use this command to display ASN1 contents of H.245 messages.

The following sample command output shows an H.323 ARQ nonstandard message. The format of the B-channel billing information is: 1 is the D-channel ID, 1 is the T1 controller, and 10 is the B-channel.

```
Router# debug h245 asn1

.
.
.
value ARQnonStandardInfo ::=
 {
   sourceAlias
   {
   }
   sourceExtAlias
   {
   }
   interfaceSpecificBillingId 1:D 1:DS1 10:DS0
   gtd '49414D2C0D0A50524E2C6973646E2A2C2...'H
 }
.
.
.
```

Step 2 **debug gatekeeper servers**

Use this command on gatekeeper to trace all the message exchanges between a gatekeeper and an external application. It also displays any errors that occur in sending messages to the external application or in parsing messages from the external application.

The following sample command output also shows B-channel information. The format of the B-channel billing information is as follows: 1 is the D-channel ID, 1 is the T1 controller, and 10 is the B-channel.

```
Router# debug gatekeeper servers

"REQUEST ARQ
Version-id:402
From:voip6-2600-1
To:GKTMP_SERVER
Transaction-Id:81A3EB4000000001
Content-Length:258
i=I:1.3.26.21:1720
s=E:9190001 H:voip6-5300-1
d=E:4080001
b=1280
A=F
C=C13CB8DE-C47F-11D3-80A9-FC0BFCA7B068
c=C13D5506-C47F-11D3-80AB-FC0BFCA7B068
B= 1:D 1:DS1 10:DS0
```

Configuring H.323 VoIP Call Preservation Enhancements for WAN Link Failures

H.323 VoIP call preservation enhancements for WAN link failures sustains connectivity for H.323 topologies where signaling is handled by an entity that is different from the other endpoint, such as a gatekeeper that provides routed signaling or a call agent, such as the Cisco BTS 10200 Softswitch, Cisco PGW 2200, or Cisco CallManager, that brokers signaling between the two connected parties.

Call preservation is useful when a gateway and the other endpoint (typically an Cisco Unified IP phone) are collocated at the same site and the call agent is remote and therefore more likely to experience connectivity failures.

Note If a preserved H.323 call is torn down at a IP PBX, a call-stop record will be generated while Real-time Transport Protocol (RTP) is still flowing. Such an event can be misused to generate a signaling error and allow toll bypass, thus affecting per-call billing integrity.

H.323 call preservation covers the following types of failures and connections:

Failure Types

- WAN failures that include WAN links flapping or degraded WAN links
- Cisco Unified CallManager software failure, such as when the ccm.exe service crashes on a Cisco Unified CallManager server.
- LAN connectivity failure, except when a failure occurs at the local branch

Connection Types

- Calls between two Cisco Unified CallManager controlled endpoints
  - During Cisco Unified CallManager reloads
  - When a Transmission Control Protocol (TCP) connection between one or both endpoints and Cisco Unified CallManager used for signaling H.225.0 or H.245 messages is lost or flapping
  - Between endpoints that are registered to different Cisco Unified CallManagers in a cluster and the TCP connection between the two Cisco Unified CallManagers is lost
  - Between IP phones and the PSTN at the same site
- Calls between Cisco IOS gateway and an endpoint controlled by a softswitch where the signaling (H.225.0, H.245 or both) flows between the gateway and the softswitch and media flows between the gateway and the endpoint.
  - When the softswitch reloads.
  - When the H.225.0 or H.245 TCP connection between the gateway and the softswitch is lost, and the softswitch does not clear the call on the endpoint
  - When the H.225.0 or H.245 TCP connection between softswitch and the endpoint is lost, and the soft-switch does not clear the call on the gateway
- Call flows that involve a Cisco IP in IP (IPIP) gateway running in media flow-around mode that reload or lose connection with the rest of the network

Note that after the media is preserved, the call is torn down later when either one of the parties hangs up or media inactivity is detected. In cases where there is a machine-generated media stream, such as music streaming from a media server, the media inactivity detection will not work and the call may hang. Cisco Unified CallManager addresses such conditions by indicating to the gateway that such calls should not be preserved, but third-party devices or IPIP gateways would not do this.

Flapping is defined for this feature as the repeated and temporary loss of IP connectivity that can be caused by WAN or LAN failures. H.323 VoIP calls between a Cisco IOS gateway and Cisco Unified CallManager may be torn down when flapping occurs. When Cisco Unified CallManager detects that the TCP connection is lost, it clears the call and closes the TCP sockets used for the call by sending a TCP FIN, without sending an "H.225.0 Release Complete" or "H.245 End Session" message. This is called quiet clearing. The TCP FIN sent from the Cisco Unified CallManager could reach the gateway if the network comes up for a short duration, and the gateway will tear the call down. Even if the TCP FIN does not reach the gateway, the TCP keepalives sent from the gateway could reach Cisco Unified CallManager when the network comes up. Cisco Unified CallManager will send TCP RST messages in response to the keepalives as it has already closed the TCP connection. The gateway will tear down H.323 calls if it receives the RST message.

Configuration of H.323 VoIP call preservation enhancements for WAN link failures involves configuring the **call preserve** command. If you are using Cisco Unified CallManager you must enable the "Allow Peer to Preserve H.323 Calls" parameter from Cisco Unified CallManager's Service Parameters window.

The **call preserve** command causes the gateway to ignore socket closure or socket errors on H.225.0 or H.245 connections for active calls, allowing the socket to be closed without tearing down calls using those connections.

Call preservation may be reported through Syslog, which optionally can be obtained through a simple network management protocol (SNMP) trap. New syslog messages are printed when call preservation is applied. An SNMP trap can be configured on this syslog message, so you can be notified when call preservation occurs on a gateway.

Preservation information is displayed through the **show h323 calls preserved** command. The following is an example of the command's output:

```
CallID = 11EC , Calling Number = , Called Number = 3210000 ,
RemoteSignallingIPAddress=9.13.0.26 , RemoteSignallingPort=49760 ,
RemoteMediaIPAddress=9.13.0.11 , RemoteMediaPort=17910 , Preserved Duration = 262 , Total
Duration = 562 , H225 FD = -1 , H245 FD = -1
```

The previous example represents one preserved call. One such display is provided per preserved call. The **show h323 calls preserved** displays active calls only. No history is output.

To obtain additional information about a call, you can also use the **show call active voice** command. Calls can be cleared with the **clear call voice causecode** command.

Prerequisites

- This feature may be used on all Cisco Unified CallManager system hardware configurations. If you are not using Cisco Unified CallManager, this feature can only be configured on the Cisco AS5000 Series.
- For bidirectional silence detection, Cisco IOS gateways with 5510 digital signal processors (DSPs) are needed.
- It is recommended that media inactivity detection be configured so that preserved calls are torn down after conversations are over. Two available media inactivity detection features are discussed in the "Configuring Signal ISDN B-Channel ID" section on page 93. They are RTP and RTP Control Protocol (RTCP) inactivity detection and bidirectional silence detection. For more information about media inactivity detection, see the "Configuring Media Inactive Call Detection" chapter in the *Cisco IOS Tcl IVR and VoiceXML Application Guide—12.3(14)T and Later*.

Restrictions

H.323 VoIP Call preservation enhancements for WAN link failures does not support the following:

- Calls in transient call states
- Calls in for which a H.225.0 connection has not occurred
- Calls on which supplementary services are in progress, such as when one of the parties is on hold.
- Calls that involve a media resource located across a WAN, such as conference resources
- Calls where the two parties are registered to different Cisco Unified CallManager clusters
- The "Do Not Preserve" function (using an H.225 Notify message) on networks without Cisco CallManager.

Configuring H.323 Call Preservation Enhancements for WAN Link Failures

The tasks for configuring H.323 VoIP call preservation enhancements for WAN link failures include the following:

- Configuring the Gateway, page 97
- Configuring Cisco Unified CallManager, page 102 (Cisco CallManager Only)

Configuring the Gateway

The **call preserve** command activates H.323 VoIP call preservation. RTP and RTCP inactivity detection and bidirectional silence detection can be used with this feature. Note that voice activity detection (VAD) must be set to off if you are using RTP and RTCP inactivity detection. VAD may be set to on, for bidirectional silence detection. For configuration examples, see the "RTP and RTCP Inactivity Detection Configuration Example" section on page 118 and "Bidirectional Silence Detection Enable Example" section on page 118.

When bidirectional silence and RTP and RTCP inactivity detection are configured, they are enabled for all calls by default. To enable them for H.323 VoIP preserved calls only, you must use the **call preserve** command's **limit-media-detection** keyword.

H.323 VoIP call preservation can be applied to all calls and to dial peers. The required steps are described in the following sections:

- Configuring H.323 VoIP Call Preservation for All Calls, page 97
- Configuring H.323 VoIP Call Preservation for a Dial Peer, page 98

Configuring H.323 VoIP Call Preservation for All Calls

The following describes how to configure H.323 VoIP call preservation for all calls.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **h323**
5. **call preserve** [**limit-media-detection**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**voice service voip** **Example:** `Router (config)# voice service voip`	Enters voice-service configuration mode.
Step 4	**h323** **Example:** `Router (config-voi-serv)# h323`	Enables the H.323 voice service configuration commands.
Step 5	**call preserve** [**limit-media-detection**] **Example:** `Router (config-voi-h323)# call preserve`	Enables the preservation of H.323 VoIP calls. • **limit-media-detection**—Limits RTP and RTCP inactivity detection and bidirectional silence detection (if configured) to H.323 VoIP preserved calls only.
Step 6	**exit** **Example:** `Router# exit`	Exits H.323 configuration mode.
Step 7	**exit** **Example:** `Router# exit`	Exist voice service voip configuration mode.

Examples

The following configuration example enables H.323 VoIP call preservation for all calls.

```
voice service voip
 h323
  call preserve
```

The following configuration example enables H.323 VoIP call preservation and limits RTP and RTCP inactivity detection and bidirectional silence detection (if configured) to preserved calls only:

```
voice service voip
 h323
  call preserve limit-media-detection
```

Configuring H.323 VoIP Call Preservation for a Dial Peer

The following describes how to configure H.323 VoIP call preservation for a dial peer.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **voice-class h323** *tag*
4. **call preserve** [**limit-media-detection**]
5. **exit**
6. **dial-peer voice** *tag* **voip**
7. **voice-class h323** *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 h323`** *`tag`*
	Example:
	`Router (config)# voice-class h323 4`
		Assigns an H.323 voice class to a VoIP dial peer.
		• tag—Unique number to identify the voice class. Range is from 1 to 10000.

Step 4	**`call preserve`** `[`**`limit-media-detection`**`]`
	Example:
	`Router (config-class)# call preserve`
		Enables the preservation of H.323 VoIP calls.
		• **limit-media-detection**—Limits RTP and RTCP inactivity detection and bidirectional silence detection (if configured) to H.323 VoIP preserved calls only.

Step 5	**`exit`**
	Example:
	`Router (config)# exit`
		Exits H.323 voice class configuration mode.

Step 6	**`dial-peer voice`** *`tag`* **`voip`**
	Example:
	`Router (config)# dial-peer voice 1 voip`
		Defines a particular dial peer.

	Command or Action	Purpose
Step 7	**voice-class h323** *tag* **Example:** `Router (config-dial-peer)# voice-class h323 4`	Assigns an H.323 voice class to a VoIP dial peer. • tag—Unique number to identify the voice class. Range is from 1 to 10000.
Step 8	**exit** **Example:** `Router# exit`	Exits dial-peer voice configuration mode.

Examples

The following configuration example enables H.323 VoIP call preservation for dial peer 1.

```
voice-class h323 4
 call preserve
dial-peer voice 1 voip
 voice-class h323 4
```

Troubleshooting Tips

- Enable the **voice iec syslog** command in global configuration mode to display the reason that a call has disconnected after call preservation. The following is an example of the **voice iec syslog** command output line that display this information:

```
Nov 29 12:39:55.167: %VOICE_IEC-3-GW: H323: Internal Error (Socket error):
```

- Calls on hold are not preserved and a non-standard message with “callPreserveIE FALSE” is sent in the notify message. Use the **debug h225 asn** command for debug. The following is example output:

```
Router# debug h225 asn
H.225 ASN1 Messages debugging is on
3725-GW1#
*May 3 15:57:27.920: H225.0 INCOMING ENCODE BUFFER::=
28501900060008914A00040000D2D6D6D87EB11D02000000090D194410A00100110140B50000120A80A480
04000101000100
*May 3 15:57:27.920:
*May 3 15:57:27.920: H225.0 INCOMING PDU ::=
value H323_UserInformation ::=
{
h323-uu-pdu
{
h323-message-body notify :
{
protocolIdentifier { 0 0 8 2250 0 4 }
callIdentifier
{
guid '00D2D6D6D87EB11D02000000090D1944'H
}
}
h245Tunneling FALSE
nonStandardControl
{
{
nonStandardIdentifier h221NonStandard :
{
t35CountryCode 181
t35Extension 0
manufacturerCode 18
}
data '80A48004000101000100'H
}
}
}
}
*May 3 15:57:27.924: H225 NONSTD INCOMING ENCODE BUFFER::= 80A48004000101000100
*May 3 15:57:27.924:
*May 3 15:57:27.924: H225 NONSTD INCOMING PDU ::=
value H323_UU_NonStdInfo ::=
{
callMgrParam
{
interclusterVersion 1
enterpriseID {}
}
callPreserveParam
{
callPreserveIE FALSE
}
}
```

When the call is resumed, “callPreserve” is again set to True as shown in the following output example:

```
Router# debug h225 asn
*May 3 15:57:32.676: H225.0 INCOMING ENCODE BUFFER::=
28501900060008914A00040000D2D6D6D87EB11D02000000090D194410A001001B0140B50000121480A680
04000101000943004C0580323030300140
*May 3 15:57:32.676:
*May 3 15:57:32.676: H225.0 INCOMING PDU ::=
value H323_UserInformation ::=
{
h323-uu-pdu
{
h323-message-body notify :
{
protocolIdentifier { 0 0 8 2250 0 4 }
callIdentifier
{
guid '00D2D6D6D87EB11D02000000090D1944'H
}
}
h245Tunneling FALSE
nonStandardControl
{
{
nonStandardIdentifier h221NonStandard :
{
t35CountryCode 181
t35Extension 0
manufacturerCode 18
}
data '80A680040001010009430 04C0580323030300140'H
}
}
}
}
*May 3 15:57:32.680: H225 NONSTD INCOMING ENCODE BUFFER::=
80A6800400010100094300 4C0580323030300140
*May 3 15:57:32.680:
*May 3 15:57:32.680: H225 NONSTD INCOMING PDU ::=
value H323_UU_NonStdInfo ::=
{
```

```
callMgrParam
{
interclusterVersion 1
enterpriseID {}
}
callSignallingParam
{
connectedNumber '4C058032303030'H
}
callPreserveParam
{
callPreserveIE TRUE
}
}
```

- Use the **debug cch323 all** command after call setup to see if call is going into preserved state. Note that this command generates verbose output, and a console message is printed for every preserved call. In the following output, the relevant information appears in boldface:

```
Router# debug cch323 all
(CCH323-6-CALL_PRESERVED).
Nov 29 12:39:55.167: //-1/xxxxxxxxxxxx/H323/cch323_ct_main: SOCK 3 Event 0x1
Nov 29 12:39:55.167: //31/A9E0FB268017/H323/cch323_h225_handle_conn_loss:
cch323_h225_handle_conn_loss Call not torn down despite H.225.0 socket error: socket
error status = 1, ccb status = 403760899, fd = 3, pre-V3 = 0
Nov 29 12:39:55.167: %CCH323-6-CALL_PRESERVED: cch323_h225_handle_conn_loss: H.323
call preserved due to socket closure or error, Call Id = 4593, fd = 3
Nov 29 12:39:55.167: %VOICE_IEC-3-GW: H323: Internal Error (Socket error):
IEC=1.1.186.5.7.6 on callID 31 GUID=A9E0FB26600B11DA8017000653455072
Nov 29 12:39:55.167: //-1/xxxxxxxxxxxx/H323/h323_set_release_source_for_peer:
ownCallId[31], src[6]
Nov 29 12:39:55.167: //-1/xxxxxxxxxxxx/H323/h323_gw_clean_send_blocked_watch: fd 3
Nov 29 12:39:55.167: //-1/xxxxxxxxxxxx/H323/cch323_cleanup_xport: hashDestroy for
TcpFDTbl
```

- The following are additional debug commands can be used to troubleshoot the problems associated with H.323 VoIP call preservation:
  - **debug h225 asn1**
  - **debug h225 q931**
  - **debug h245 asn1**

Configuring Cisco Unified CallManager

If you are using Cisco Unified CallManager, you must activate H.323 call preservation through the “Allow Peer to Preserve H.323 Calls” parameter, which preserves the following:

- Active H323 calls with quiet clear triggered by the other half of the call
- Active H323 calls with TCP socket closed on the H.323 end before the H.225 or H.245 release signal is received
- Active H323 calls with a signal distribution layer (SDL) link that is out of service and detected on the H323 end

Procedure

Step 1 Choose **Service** > **Service Parameters**.

Step 2 From the Service menu select Cisco Unified CallManager.

Step 3 Click **Advanced**.

Step 4 Scroll to the Clusterwide Parameter (Device — H.323) section.

Step 5 Set the “Allow Peer to Preserve H.323 Calls” parameter to True.

Step 6 At the top of the screen click **Update**.

Configuration Examples for H.323 Gateways

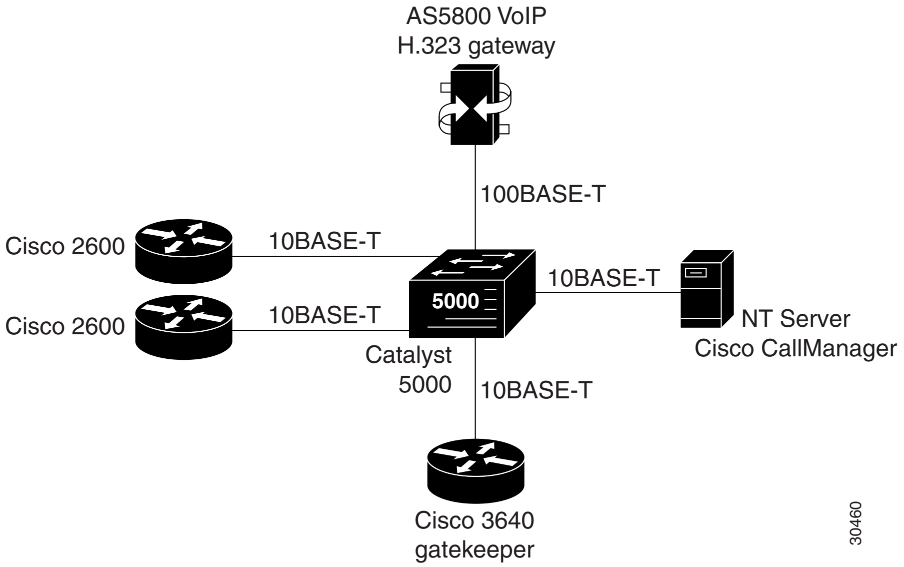
This section provides the following configuration examples:

- RAS: Example, page 103
- Gateway Security: Example, page 105
- Alternate Gatekeeper Support: Example, page 107
- DTMF Relay: Example, page 108
- Multiple Codecs: Example, page 108
- Rotary Calling Pattern: Example, page 108
- H.323 Support for Virtual Interfaces: Example, page 109
- H.225 Annex-G: Example, page 109
- GTD Payload: Examples, page 110
- H.323v4 Gateway Zone Prefix Registration Enhancements: Examples, page 111
- Signal ISDN B-Channel ID: Example, page 115
- H.323 VoIP Call Preservation Enhancements for WAN Link Failures Examples, page 117

RAS: Example

Figure 6 shows a Cisco 2600 and a Cisco AS5800 as gateways and a Cisco 3640 as a gatekeeper.

Figure 6 VoIP for the Cisco AS5800



The following example shows a Cisco AS5800 as a gateway using RAS:

```
! Configure the T1 controller. (This configuration is for a T3 card.)
controller T1 1/0/0:1
 framing esf
 linecode b8zs
 pri-group timeslots 1-24
!
! Configure POTS and VoIP dial peers.
dial-peer voice 11111 pots
 incoming called-number 12345
 destination-pattern 9#11111
 direct-inward-dial
 port 1/0/0:1:D
 prefix 11111
!
dial-peer voice 12345 voip
 destination-pattern 12345
 tech-prefix 6#
 session target ras
!
! Enable gateway functionality.
gateway
!
! Enable Cisco Express Forwarding.
ip cef
!
! Configure and enable the gateway interface.
interface FastEthernet0/3/0
 ip address 172.16.0.0.255.255.255.0
 no ip directed-broadcast
 no keepalive
 full-duplex
 no cdp enable
h323-gateway voip interface
 h323-gateway voip id gk3.gg-dn1 ipaddr 172.18.0.0 1719
 h323-gateway voip h323-id gw3@gg-dn1
 h323-gateway voip tech-prefix 9#
!
! Configure the serial interface.(This configuration is for a T3 serial interface.)
```

```
interface Serial1/0/0:1:23
 no ip address
 no ip directed-broadcast
 ip mroute-cache
 isdn switch-type primary-5ess
 isdn incoming-voice modem
 no cdp enable
```

Gateway Security: Example

H.323 Gateway Security

The following example illustrates H.323 security configuration on a Cisco AS5300 gateway.

```
hostname um5300
!
enable password xyz
!
resource-pool disable
!
clock timezone EST -5
clock summer-time EDT recurring
ip subnet-zero
no ip domain-lookup
!
isdn switch-type primary-5ess
isdn voice-call-failure 0
call application voice xyz tftp://172.18.16.2/samp/xyz.tcl
call application voice load xys
mta receive maximum-recipients 1024
!
xgcp snmp sgcp
!
controller T1 0
 framing esf
 clock source line primary
 linecode b8zs
 pri-group timeslots 1-24
!
controller T1 1
 framing esf
 clock source line secondary 1
 linecode b8zs
 pri-group timeslots 1-24
!
controller T1 2
!
controller T1 3
!
voice-port 0:D
!
voice-port 1:D
!
dial-peer voice 4001 pots
 application xyz
 destination-pattern 4003
 port 0:D
 prefix 4001
!
dial-peer voice 513 voip
 destination-pattern 1513200....
 session target ras
```

```
!
dial-peer voice 9002 voip
 destination-pattern 9002
 session target ras
!
dial-peer voice 4191024 pots
 destination-pattern 4192001024
 port 0:D
 prefix 4001
!
dial-peer voice 1513 voip
 destination-pattern 1513.......
 session target ras
!
dial-peer voice 1001 pots
 destination-pattern 14192001001
 port 0:D
!
gateway
 security password 151E0A0E level all
!
 interface Ethernet0
 ip address 10.99.99.7 255.255.255.0
 no ip directed-broadcast
 shutdown
!
interface Serial0:23
 no ip address
 no ip directed-broadcast
 isdn switch-type primary-5ess
 isdn protocol-emulate user
 isdn incoming-voice modem
 fair-queue 64 256 0
 no cdp enable
!
interface Serial1:23
 no ip address
 no ip directed-broadcast
 isdn switch-type primary-5ess
 isdn protocol-emulate user
 isdn incoming-voice modem
 isdn guard-timer 3000
 isdn T203 10000
 fair-queue 64 256 0
 no cdp enable
!
interface FastEthernet0
 ip address 172.18.72.121 255.255.255.192
 no ip directed-broadcast
 duplex auto
 speed auto
 h323-gateway voip interface
 h323-gateway voip id um5300@vgkcisco3 ipaddr 172.18.72.58 1719
 h323-gateway voip h323-id um5300
 h323-gateway voip tech-prefix 1#
!
no ip http server
ip classless
ip route 10.0.0.0 172.18.72.65
!
!
line con 0
 exec-timeout 0 0
 length 0
 transport input none
line aux 0
line vty 0 4
 password xyz
 login
!
ntp clock-period 17179974
ntp server 172.18.72.124
```

H.235 Gateway Security

The following example shows output from configuring secure registrations from the gatekeeper and identifying which RAS messages the gatekeeper checks to find authentication tokens:

```
dial-peer voice 10 voip
 destination-pattern 4088000
 session target ras
 dtmf-relay h245-alphanumeric
!
gateway
 security password 09404F0B level endpoint
```

The following example shows output from configuring which RAS messages contain gateway-generated tokens:

```
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
radius-server host 10.25.0.0 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server deadtime 5
radius-server key lab
radius-server vsa send accounting
!
gatekeeper
 zone local GK1 test.com 10.0.0.3
 zone remote GK2 test2.com 10.0.2.2 1719
 accounting
 security token required-for registration
 no use-proxy GK1 remote-zone GK2 inbound-to terminal
 no use-proxy GK1 remote-zone GK2 inbound-to gateway
 no shutdown
```

Alternate Gatekeeper Support: Example

In the following example, the gateway is configured to have alternate gatekeepers. The primary and secondary gatekeepers are configured with the priority option. The priority range is 1 to 127. The first alternate gatekeeper is configured as priority 120; the second alternate gatekeeper is not configured, so remains at the default setting of 127.

```
interface Ethernet 0/1
 ip address 172.18.193.59 255.255.255.0
 h323-gateway voip interface
 h323-gateway voip id GK1 ipaddr 172.18.193.65 1719 priority 120
 h323-gateway voip id GK2 ipaddr 172.18.193.66 1719
 h323-gateway voip h323-id cisco2
```

DTMF Relay: Example

The following example configures DTMF relay with the **cisco-rtp** keyword when sending DTMF tones to dial peer 103:

```
dial-peer voice 103 voip
 dtmf-relay cisco-rtp
```

The following example configures DTMF relay with the **cisco-rtp** or **h245-signal** keywords when DTMF tones are sent to dial peer 103:

```
dial-peer voice 103 voip
 dtmf-relay cisco-rtp h245-signal
```

The following example configures the gateway to send DTMF in-band (the default) when DTMF tones to are sent dial peer 103:

```
dial-peer voice 103 voip
 no dtmf-relay
```

The following example shows that DTMF relay is configured on an H.323 gateway using NTE RTP and H.245 signaling. In this example, the Named Signaling Event (NSE) value in use is reassigned to a different, unassigned number (110). NTE payload is then assigned to the previously used value (100).

```
dial-peer voice 400 voip
 destination-pattern 400
 dtmf-relay rtp-nte h245-signal
 rtp payload nse 110
 rtp payload-type nte 100
 session target ipv4:172.18.193.181
```

Multiple Codecs: Example

The following configuration shows how to create a list of prioritized codecs and apply that list to a specific VoIP dial peer:

```
 voice class codec 99
  codec preference 1 g711alaw
  codec preference 2 g711ulaw bytes 80
  codec preference 3 g723ar53
  codec preference 4 g723ar63 bytes 144
  codec preference 5 g723r53
  codec preference 6 g723r63 bytes 120
  codec preference 7 g726r16
  codec preference 8 g726r24
  codec preference 9 g726r32 bytes 80
  codec preference 10 g728
  codec preference 11 g729br8
  codec preference 12 g729r8 bytes 50
!
dial-peer voice 1919 voip
  voice-class codec 99
```

Rotary Calling Pattern: Example

The following example configures POTS dial peer 10 for a preference of 1, POTS dial peer 20 for a preference of 2, and Voice over Frame Relay dial peer 30 for a preference of 3:

```
dial-peer voice 10 pots
```

```
destination pattern 5552150
preference 1

dial-peer voice 20 pots
destination pattern 5552150
preference 2

dial-peer voice 30 vofr
destination pattern 5552150
preference 3
```

H.323 Support for Virtual Interfaces: Example

In the following example, Ethernet interface 0/0 is used as the gateway interface. For convenience, the **h323-gateway voip bind srcaddr** command is specified on the same interface. The designated source IP address is the same as the IP address assigned to the interface.

```
interface Ethernet0/0
 ip address 172.18.194.50 255.255.255.0
 no ip directed-broadcast
 h323-gateway voip interface
 h323-gateway voip id j70f_2600_gk2 ipaddr 172.18.194.53 1719
 h323-gateway voip h323-id j70f_3640_gw1
 h323-gateway voip tech-prefix 3#
 h323-gateway voip bind srcaddr 172.18.194.50
```

H.225 Annex-G: Example

The following example shows the gatekeeper border element router with service relationship and usage-reporting functionality turned on:

```
Router# show running config

Building configuration...
.
.
.
call-router h323-annexg boston1
 neighbor 1.2.3.4
  service-relationship
   outbound retry interval 120
   inbound ttl 1200
   no shutdown
  usage-indication
   retry interval 600
   retry window 3600
 domain-name Celine-Domain
 access-policy neighbors-only
 local ip 172.18.193.31
 no shutdown
.
.
.
```

GTD Payload: Examples

GTD Payload System-Wide

The following example shows the GTD feature configured on the system:

```
Router# show running-config

Building configuration...

Current configuration : 4192 bytes
!
version 12.2
service config
no service single-slot-reload-enable
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service internal
service udp-small-servers
!
hostname as5300-2
!
voice service voip
 signaling forward unconditional
 h323
!
.
.
.
```

GTD Payload on a Dial Peer

The following example shows GTD configured with unconditional forwarding on two dial peers:

```
Router# show running-config

Building configuration...

Current configuration : 4192 bytes
!
version 12.2
service config
no service single-slot-reload-enable
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service internal
service udp-small-servers
!
hostname as5300-2
!
.
.
.
!
dial-peer voice 1 pots
 application session
 incoming called-number 25164
 port 0:D
!
dial-peer voice 1513 voip
```

```
 destination-pattern 1513.......
 session target ipv4:1.8.156.3
!
dial-peer voice 1408525 voip
 destination-pattern 1408525....
!
dial-peer voice 1800877 voip
 destination-pattern 1800877....
 session target ipv4:1.8.156.3
!
dial-peer voice 2 pots
 destination-pattern 51550
 no digit-strip
 direct-inward-dial
 port 3:D
!
dial-peer voice 51557 voip
 destination-pattern 51557
 signaling forward unconditional
 session target ras
!
dial-peer voice 52557 voip
 destination-pattern 52557
 signaling forward unconditional
 session target ipv4:1.8.156.3
!
gateway
!
.
.
```

H.323v4 Gateway Zone Prefix Registration Enhancements: Examples

Verifying Gateway Advertisement of Dynamic Zone Prefixes

The following example displays the status of the destination pattern database and the status of the individual destination patterns for Gatekeeper1:

```
Gateway1# show h323 gateway prefixes

GK Supports Additive RRQ         : True
GW Additive RRQ Support Enabled  : True
Pattern Database Status          : Active


Destination                                          Active
Pattern                          Status              Dial-Peers
================================================================
1110509*                         ADD ACKNOWLEDGED        2
1110511*                         ADD ACKNOWLEDGED        2
23*                              ADD ACKNOWLEDGED        2
```

Verifying Gatekeeper Processing of Additive RRQs Example

The following example displays the zone prefix table, including the dynamic zone prefixes, for Gatekeeper1:

```
Gatekeeper1# show gatekeeper zone prefix all

                    ZONE PREFIX TABLE
      ===============================================
GK-NAME               E164-PREFIX      Dynamic GW-priority
-------               -----------      -------------------
gatekeeper1           1110507*         gateway2 /5
gatekeeper2           1110508*
gatekeeper1           1110509*         gateway1 /5
gatekeeper1           1110511*         gateway1 /5
gatekeeper1           23*              gateway1 /5
gatekeeper1           4666002*
gatekeeper3           55530..
gatekeeper1           7779...
```

Verifying Dynamic Zone Prefix Registration based on Gateway Priority Lists Example

The following example displays the gateway destination-pattern database status:

```
Router# show h323 gateway prefixes

GK Supports Additive RRQ  :True
GW Additive RRQ Support   :True
Pattern Database          :Active

Destination Active
Pattern                    Status         Dial-Peers    Priority
=================================================================
1110509*                   ADD ACKNOWLEDGED    2           8
1110511*                   ADD ACKNOWLEDGED    2
23*                        ADD ACKNOWLEDGED    2           4
```

Troubleshooting H.323v4 Gateway Zone Prefix Registration Enhancements Example

The following example displays the ASN1 contents of RAS messages sent during the registration process:

```
Gatekeeper1# debug h225 asn1

U.S. Eastern time (GMT -5/-4)
voice:(919) 392-6007.Feb 5 16:27:05.894:RAS INCOMING ENCODE BUFFER::= 00 A0004306 0008914A
00040001 07072ACC 3D2800B5 00001240 0238500A 00320036 00300030 002D0031 02400500 33003600
34003000 2D003101 00C4C0
.Feb 5 16:27:05.906:
.Feb 5 16:27:05.906:RAS INCOMING PDU ::=

value RasMessage ::= gatekeeperRequest :
    {
      requestSeqNum 68
      protocolIdentifier { 0 0 8 2250 0 4 }
      rasAddress ipAddress :
      {
        ip '0107072A'H
        port 52285
      }
      endpointType
      {
        vendor
        {
          vendor
          {
            t35CountryCode 181
            t35Extension 0
            manufacturerCode 18
          }
        }
        gateway
        {
          protocol
          {
            voice :
            {
            },            h323 :
            {
            }
          }
        }
        mc FALSE
        undefinedNode FALSE
      }
      gatekeeperIdentifier {“2600-1”}
      endpointAlias
      {
        h323-ID :{“3640-1”},
        dialedDigits :”919”
      }
    }

.Feb 5 16:27:05.926:RAS OUTGOING PDU ::=

value RasMessage ::= gatekeeperConfirm :
    {
      requestSeqNum 68
      protocolIdentifier { 0 0 8 2250 0 4 }
      gatekeeperIdentifier {“2600-1”}
      rasAddress ipAddress :
      {
        ip '01070721'H
        port 1719
      }
    }

.Feb 5 16:27:05.934:RAS OUTGOING ENCODE BUFFER::= 04 80004306 0008914A 00040A00 32003600
30003000 2D003100 01070721 06B7
.Feb 5 16:27:05.938:
.Feb 5 16:27:05.946:RAS INCOMING ENCODE BUFFER::= 0E C0004406 0008914A 00048001 00010707
2A06B801 00010707 2ACC3D28 00B50000 12400238 50024005 00330036 00340030 002D0031 0100C4C0
A0003200 36003000 30002D00 3100B500 0012288B 08000200 3B010001 00018002 7000
.Feb 5 16:27:05.958:
.Feb 5 16:27:05.958:RAS INCOMING PDU ::=

value RasMessage ::= registrationRequest :
    {
      requestSeqNum 69
      protocolIdentifier { 0 0 8 2250 0 4 }
      discoveryComplete TRUE
      callSignalAddress
      {
        ipAddress :
        {
          ip '0107072A'H
          port 1720
        }
      }
      rasAddress
      {
        ipAddress :
        {
          ip '0107072A'H
          port 52285
        }
      }
      terminalType
      {
        vendor
        {
          vendor
          {
            t35CountryCode 181
            t35Extension 0
            manufacturerCode 18
          }
        }
        gateway
        {
          protocol
          {
            voice :
            {
            },            h323 :
            {
            }
          }
        }
        mc FALSE
        undefinedNode FALSE
      }
      terminalAlias
      {
        h323-ID :{“3640-1”},
        dialedDigits :”919”
      }
      gatekeeperIdentifier {“2600-1”}
      endpointVendor
      {
        vendor
        {
          t35CountryCode 181
          t35Extension 0
          manufacturerCode 18
        }
      }
      timeToLive 60
      keepAlive FALSE
      willSupplyUUIEs FALSE
      maintainConnection TRUE
      usageReportingCapability
      {
        nonStandardUsageTypes
        {
        }
        startTime NULL
        endTime NULL
        terminationCause NULL
      }
    }

.Feb 5 16:27:05.998:RAS OUTGOING PDU ::=

value RasMessage ::= registrationConfirm :
    {
      requestSeqNum 69
      protocolIdentifier { 0 0 8 2250 0 4 }
      callSignalAddress
      {
      }
      terminalAlias
      {
        h323-ID :{“3640-1”},
        dialedDigits :”919”
      }
      gatekeeperIdentifier {“2600-1”}
      endpointIdentifier {“816F7A1000000001”}
      alternateGatekeeper
      {
      }
      timeToLive 60
      willRespondToIRR FALSE
      maintainConnection TRUE
      supportsAdditiveRegistration NULL
      usageSpec
      {

        {
          when
          {
            end NULL
            inIrr NULL
          }
          callStartingPoint
          {
            connect NULL
          }
          required
          {
            nonStandardUsageTypes
            {
            }
            startTime NULL
            endTime NULL
            terminationCause NULL
          }
        }
      }
```

Signal ISDN B-Channel ID: Example

The following example shows an H.323 and SIP ISDN B-channel configuration example.

```
Current configuration : 3394 bytes
!
version 12.3
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service internal
!
memory-size iomem 15
ip subnet-zero
!
!
no ip domain lookup
!
voice service voip
 h323
  billing b-channel
 sip
```

```
  ds0-num

ip dhcp pool vespa
 network 192.168.0.0 255.255.255.0
 option 150 ip 192.168.0.1
 default-router 192.168.0.1
!
!
voice call carrier capacity active
!
voice class codec 1
 codec preference 2 g711ulaw
!
!
no voice hpi capture buffer
no voice hpi capture destination
!
!
fax interface-type fax-mail
mta receive maximum-recipients 0
!
!
interface Ethernet0/0
 ip address 10.8.17.22 255.255.0.0
 half-duplex
!
interface FastEthernet0/0
 ip address 192.168.0.1 255.255.255.0
 speed auto
 no cdp enable
 h323-gateway voip interface
 h323-gateway voip id vespa2 ipaddr 10.8.15.4 1718
!
router rip
 network 10.0.0.0
 network 192.168.0.0
!
ip default-gateway 10.8.0.1
ip classless
ip route 0.0.0.0 0.0.0.0 10.8.0.1
no ip http server
ip pim bidir-enable
!
!
tftp-server flash:SEPDEFAULT.cnf
tftp-server flash:P005B302.bin
call fallback active
!
!
call application global default.new
call rsvp-sync
!
voice-port 1/0
!
voice-port 1/
!
mgcp profile default
!
!
dial-peer voice 1 pots
 destination-pattern 5100
 port 1/0
!
dial-peer voice 2 pots
```

```
 destination-pattern 9998
 port 1/1
!
dial-peer voice 123 voip
 destination-pattern [12]...
 session protocol sipv2
 session target ipv4:10.8.17.42
 dtmf-relay sip-notify
!
gateway
!
sip-ua
 retry invite 3
 retry register 3
 timers register 150
 registrar dns:myhost3.cisco.com expires 3600
 registrar ipv4:10.8.17.40 expires 3600 secondary
!
!
telephony-service
 max-dn 10
 max-conferences 4
!
ephone-dn 1
number 4001
!
ephone-dn 2
number 4002
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
login
line vty 5 15
 login
!
no scheduler allocate
end
```

H.323 VoIP Call Preservation Enhancements for WAN Link Failures Examples

This section includes the following configuration examples:

H.323 VoIP Call Preservation for All Calls Example

The following configuration example enables H.323 VoIP call preservation for all calls:

```
voice service voip
 h323
  call preserve
```

H.323 VoIP Call Preservation for a Dial Peer Example

The following configuration example enables H.323 VoIP call preservation for one dial peer:

```
voice class h323 4
 call preserve

dial-peer voice 1
 voice class h323 4
```

H.323 Call Preservation for RTP and RTCP and Silence Detection Example

The following configuration example enables H.323 VoIP call preservation and limits RTP and RTCP inactivity detection and bidirectional silence detection (if configured) to H.323 VoIP preserved calls only:

```
voice service voip
 h323
  call preserve limit-media-detection
```

RTP and RTCP Inactivity Detection Configuration Example

The following configuration example can be used to enable RTP and RTCP inactivity detection for dial peers. Note that for call preservation VAD must be set to off (**no vad** command):

```
dial-peer voice 10 voip
 no vad
gateway
 timer receive-rtcp 4
ip rtcp report-interval 60
```

Bidirectional Silence Detection Enable Example

The following configuration example enables bidirectional silence detection:

```
gateway
 timer media-inactive 5
ip rtcp report interval
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS Release 12.4	• Cisco IOS Release 12.4 Configuration Guides • Cisco IOS Release 12.4T Configuration Guides • Cisco IOS Release 12.4 Command References • Cisco IOS Voice Configuration Library http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/cisco_ios_voice_configuration_library_glossary/vcl.htm **Note** This website contains the library preface and glossary.
Cisco IOS Release 12.3	• Cisco IOS Release 12.3 documentation • Cisco IOS voice commands • 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 at http://www.cisco.com/en/US/docs/ios/12_2/voice/configuration/guide/fvvfax_c.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

Related Topic	Document Title
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 at: http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_programming_reference_guides_list.html • *Quality of Service for Voice over IP* at http://www.cisco.com/en/US/docs/ios/qos/configuration/guide/15_0/qos_15_0_book.html

Standards

Standards	Title
ITU-T E.164	Overall network operation, telephone service, service operation and human factors
ITU-T H.225 Version 2	Call signalling protocols and media stream packetization for packet-based multimedia communication systems
ITU-T H.235	Security and encryption for H-Series (H.323 and other H.245-based) multimedia terminals
ITU-T H.323	Packet-based multimedia communications systems
ITU-T H.450	Supplementary services for multimedia

MIBs

MIBs	MIBs Link
• CISCO-GATEKEEPER-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

RFCs	Title
RFC 2833	*RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

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