



Cisco H.323 Version 2 Phase 2

Feature History

Release	Modification
12.1(1)T	This feature was integrated into Cisco IOS Release 12.1(1)T.

This document describes the enhancements to Cisco H.323 Version 2 for Phase 2 feature in Cisco IOS Release 12.1(1)T. It includes the following sections.

- [Feature Overview, page 1](#)
- [Supported Platforms, page 8](#)
- [Supported Standard MIBs and RFCs, page 9](#)
- [Prerequisites, page 10](#)
- [Configuration Tasks, page 10](#)
- [Verifying, page 19](#)
- [Command Reference, page 22](#)
- [Glossary, page 38](#)

Feature Overview

Cisco H.323 Version 2 Phase 2 upgrades Cisco IOS software by adding the following optional features and facilitates customized extensions to the Cisco Gatekeeper.

- [H.323v2 Fast Connect, page 2](#)
- [H.245 Tunneling of DTMF Relay in conjunction with Fast Connect, page 3](#)
- [H.450.2 Call Transfer, page 3](#)
- [H.450.3 Call Deflection, page 3](#)
- [Translation of FXS Hookflash Relay, page 4](#)
- [H.235 Security, page 4](#)
- [Gatekeeper Transaction Message Protocol \(GKTMP\) and RAS Messages, page 5](#)
- [Gatekeeper and Alternate Endpoints, page 6](#)
- [Gatekeeper C Code Generic API for GKTMP in a Unix Environment, page 6](#)
- [Gateway Support for Network-Based Billing Number, page 6](#)

H.323v2 Fast Connect

The Fast Connect feature allows endpoints to establish media channels without waiting for a separate H.245 connection to be opened. This streamlines the number of messages that are exchanged and the amount of processing that must be done before endpoint connections can be established. A high-level view of the Fast Connect procedures within the H.323 protocol follows:

- The calling endpoint transmits a SETUP message containing the fastStart element that contains a sequence of encoded logical channel structures, each representing a different capability media type for both “send” and “receive” directions.
- The called endpoint selects one or more of the media types offered by the calling endpoint for the send and receive directions and returns its selections as logically encoded Q.931 messages up to and including CONNECT. At this point, the called endpoint must be prepared to receive media along any of the channels it selected.
- If H.245 procedures are needed and one or both of the endpoints do not support tunneling, then a separate H.245 connection is used.

This feature is not explicitly configurable. All version 2 VoIP endpoints will be capable on initiating or accepting Fast Connect calls. It is assumed that the gateway is capable of sending and receiving Fast Connect procedures unless its corresponding dial peer has been configured for RSVP (in other words, the req-qos is set to a value other than the default of best-effort). If the dial peer has been configured for RSVP, then traditional “slow” connect procedures will be followed, and the endpoint will neither attempt to initiate Fast Connect nor respond to a Fast Connect request from its peer.

A terminating endpoint can reject Fast Connect by simply omitting the fastStart element from all Q.931 messages up to and including CONNECT. In this case, normal H.245 procedures are followed and a separate H.245 TCP connection is established. So, if an endpoint does not support the Fast Connect procedures, normal H.245 procedures are followed. In addition, certain conditions can cause a Fast Connect call to fall back to normal H.245 procedures to complete the call.

Once a media connection has been opened (an audio path has been established), either endpoint has the option of switching to H.245 procedures (if they are needed) by using H.245 tunneling, whereby H.245 messages are encapsulated within the h245Control element of Q.931 messages.

The **dtmf-relay** command is the only H.245 cognizant command that can initiate H.245 tunneling procedures from a Fast Connect call. If H.245 tunneling is active on the call, switching to a separate TCP H.245 connection is not supported.

A Cisco terminating endpoint accepts a Fast Connect request only if a pair of symmetric codecs (codecs in both directions are the equivalent or identical) can be selected from a list that has been offered. The originating endpoint is constrained only by what it can send through the codec (or voice class codec list) associated with the dial peer.

If the Cisco originating endpoint has offered multiple codecs and the terminating endpoint selects a pair of asymmetric (mismatched) codecs, then, the originating endpoint initiates separate H.245 procedures to correct the asymmetric codec situation.

Fast Connect is backward compatible with H.323 Version 1 configurations.

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

Through H.245 tunneling, H.245 messages are encapsulated within Q.931 messages without using a separate H.245 TCP connection. When tunneling is enabled, one or more H.245 messages can be encapsulated in any Q.931 message. H.245 tunneling is not supported as a standalone 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.

H.450.2 Call Transfer

Call Transfer allows an H.323 endpoint to redirect an answered call to another H.323 endpoint. Cisco Gateways support H.450.2 Call Transfer as the transferred and transferred-to party. The transferring endpoint must be an H.450-capable terminal; the Cisco Gateway cannot act as the transferring endpoint. gatekeeper-controlled or gatekeeper-initiated Call Transfer is not supported.

**Note**

Certain devices are limited in their support of H.450. The Cisco 1700 and ubr820 platforms do not support Interactive Voice Response (IVR). Therefore, these platforms are not able to act as H.450 Transferring endpoints.

H.450.2 specifies two variants of Call Transfer:

1. Transfer without consultation—The transferring endpoint supplies the number of the transferred-to endpoint as part of the transfer request, and the two remote endpoints are transferred together. As mentioned above, a Cisco Gateway cannot be the transferring endpoint.
2. Transfer with consultation—This feature is not currently supported.

H.450.3 Call Deflection

Call Deflection is a feature under H.450.3 Call Diversion (Call Forwarding) that allows a called H.323 endpoint to redirect the unanswered call to another H.323 endpoint. Cisco gateways support H.450.3 Call Deflection as the originating, deflecting, and deflected-to gateway. The Cisco gateway as the deflecting gateway will support invocation of Call Deflection only by using an incoming PRI QSIG message (a Call Deflection cannot be invoked by using any other trunk type).

If the deflecting endpoint is a Cisco gateway, the telephony endpoint on the deflecting gateway's PRI invokes Call Deflection by sending an equivalent QSIG Reroute Invoke within a FACILITY message to the gateway. The deflecting gateway then uses the procedures outlined in H.450.3 Call Deflection to transfer the call to another endpoint. Note that the initiation of Deflection using QSIG Reroute Invoke is valid only on calls that arrived as H.323 calls at the deflecting Gateway. In other words, for calls that arrived at the Gateway through a telephony interface (such as a hairpin call) or using a non-H.323 IP protocol, QSIG Reroute Invoke will be ignored.

H.323 Version 2 Phase 2 does not support gatekeeper-controlled or initiated Call Deflection.

**Note**

Certain devices are limited in their support of H.450. The Cisco AS5800 is not able to convert QSIG to H.450. The Cisco 1700 and ubr820 platforms do not support IVR. Therefore, these devices are not able to act as H.450 Deflecting endpoints.

H.235 Security

Security for Registration, Admission, and Status protocol (RAS) signaling between H.323 endpoints and Gatekeepers is enhanced in H.323 Version 2 Phase 2 by including secure endpoint registration of the Cisco gateway to the Cisco Gatekeeper and secure per-call authentication. In addition it will provide for the protection of specific messages related to OSP (Open Settlement Protocol) and other messages as required via encryption tokens. The authentication type is “password with hashing” as described in ITU H.235. Specifically, the encryption method is MD5 with password hashing. This functionality is provided by the **security token required-for** command on the gatekeeper and the **security password** command on the gateway.

The gatekeeper can interact with a RADIUS security server to perform the authentications. The gateway can also authenticate an external application by using the Gatekeeper Transaction Message Protocol (GKTMP) API.

Per-call authentication is accomplished by validating account and pin numbers that are entered by the user connected to the calling gateway by using an interactive voice response (IVR) prompt.

The security mechanisms described above require the gateway and gatekeeper clocks to be synchronized within 30 seconds of each other by using a Network Time Protocol (NTP) server.

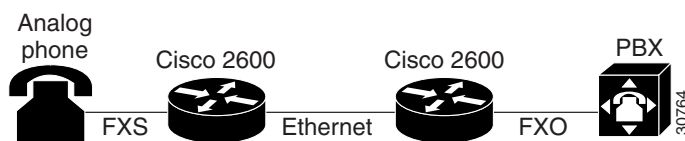
Translation of FXS Hookflash Relay

A “hookflash” indication is a brief on-hook condition during a call. The indication is not long enough in duration to be interpreted as a signal to disconnect the call. You can create a hookflash indication by quickly depressing and 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 might 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 “H.245-signal” or “H.245-alpha” structure with a value of “!”. This value represents a hookflash indication.

Figure 1 Translating an FXS hookflash to an H.245 User Input



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

1. The other endpoint must support the reception of an H.245 hookflash and advertise this using the “Receive User Input Capability” message during H.245 capabilities exchange;
2. The call must be established with either the “H245-alpha” or “h245-signal” variant of dtmf-relay.

This implies that the VoIP dial peer must be configured for dtmf-relay h245-alpha or h245-signal, but not cisco-rtp.

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

The acceptable duration of a hookflash indication varies by equipment vendor and by country. One PBX can consider a 250 ms on-hook condition to be a hookflash; another PBX can consider this condition to be a disconnect.

Gatekeeper Transaction Message Protocol (GKTMP) and RAS Messages

The Gatekeeper Transaction Message Protocol (GKTMP) for the Cisco Gatekeeper provides a transaction-oriented application protocol that allows an external application to modify gatekeeper behavior by processing specified RAS messages.

You can specify a set of triggers that use RAS messages that the gatekeeper recognizes. Triggers are specified filter conditions that must match each type of RAS message. These triggers can be dynamically registered by using the external application, or you can configure this information by using the command on the gatekeeper.

When the gatekeeper receives a RAS message that meets the specified trigger conditions, it forwards the message to the external application in a GKTMP message format. This message is text encoded and sent over TCP. The external application can then modify fields in the message before returning it to the gatekeeper for further processing, or it may return a RAS response to the gatekeeper to be forwarded to the RAS client.

The following messages can be sent in GKTMP:

- ACF—Admission Confirm
- ARJ—Admission Reject
- ARQ—Admission Request
- LCF—Location Confirm
- LRJ—Location Reject
- LRQ—Location Request
- RCF—Registration Confirm
- RRQ—Registration Request
- RRJ—Registration Reject
- URQ—Unregistration Request

The application server interprets RAS messages in the following ways:

- For RRQ, URQ, the application server performs gatekeeper authorization, storing endpoint RAS Gatekeeper IP addresses, and maintaining gatekeeper resource control.

- For ARQ, LRQ, the application server performs authorization and digit translation functions and returns terminating IP addresses or a new E.164 address to the gatekeeper for reorigination by the originating gateway.
- For LCF, LRJ the application server intercepts location responses from a distant gatekeeper and modifies the message fields before responding to the originating gateway.

**Note**

Cisco has developed an API that you can use to provide an interface to the Cisco Gatekeeper. See the *Cisco Gatekeeper External Interface Reference*.

To configure the gatekeeper to receive trigger registrations from the external applications, specify the server's registration port using the **server registration-port** command where the gatekeeper listens for server connections.

You can also configure the gatekeeper to initiate the connection to a specified external application by using the **server trigger** command to specify a set of static trigger conditions for a specified server. You can specify only one application server for each server trigger command. All RAS messages that don't match the selection criteria for any external application are processed normally by the gatekeeper. You can enter the **show gatekeeper servers** and **debug gatekeeper servers** commands to assist in the configuration.

Gatekeeper and Alternate Endpoints

The Alternate Endpoint feature allows a gatekeeper to specify alternative destinations for a call when queried with an Admission Request (ARQ) by an originating gateway. If the first destination gateway fails to connect, the gatekeeper tries all the alternate destinations before going to the next dial peer rotary (if a rotary is configured).

**Note**

This feature is not supported by the Cisco Gatekeeper; it is intended for use with third-party Gatekeepers that implement the Alternate Endpoint field in the ACF message. No support is provided for the gateway to send a list of alternate endpoints in RRQ messages.

Gatekeeper C Code Generic API for GKTMP in a Unix Environment

This API allows 3rd party applications running in a Unix host to send and receive GKTMP messages to a Cisco Gatekeeper. This API may be used to develop back-end services such as authentication, billing and address translation.

Gateway Support for Network-Based Billing Number

This feature informs the gatekeeper of the specific voice port or T1/E1 span from which an incoming call entered the ingress gateway. This is done using a Cisco proprietary, nonstandard field that has been added to the Admission Request (ARQ) message sent by the ingress gateway. No configuration is necessary for this feature.

Benefits

Cisco H.323 Version 2 Phase 2 adds the following benefits to Cisco H.323 Gatekeepers, gateways, and proxies:

- H.323v2 Fast Connect allows endpoints to establish media channels for audio exchange without waiting for a separate H.245 connection to be opened.
- H.245 tunneling allows H.245 messages to be encapsulated within Q.931 messages using H.225 (using Fast Connect) without the use of a separate H.245 TCP connection.
- H.450.2 Call Transfer without consultation and H450.3 Call Deflection provide a limited subset of features to support Internet call waiting
- H.235 security allows only duly authorized and authenticated gateways to access gatekeeper resources.
- Translation of FXS hookflash to H.245 user input along with the previously suggested translation of H.245 user input to FXO hookflash provides end-to-end hookflash relay in FXS-to-FXO configurations.
- Gatekeeper Transaction Message Protocol (GKTMP) for the Cisco Gatekeeper with a corresponding user API for the UNIX environment, which allows a third party to develop elements to control and utilize a gatekeeper for applications beyond what is directly supported in Cisco IOS Release 12.1(1)T.
- Cisco Gatekeeper supports the Gatekeeper MIB, which allows SNMP management.
- Gateway support for the Alternate Endpoint field in ACF allows third-party Gatekeepers to provide more robust call establishment.
- Gateway support for network-based billing number on a per-interface basis allows third-party Gatekeepers to obtain per-call interface usage information for billing or other purposes.
- Gateway support for the voice-port description allows third-party gatekeepers to obtain customer-specific, per-call interface usage information for billing or other purposes.

Restrictions

Cisco IOS releases earlier than Cisco IOS Release 11.3(9)NA and Cisco IOS Release 12.0(3)T contain H.323 Version 1 software that does not support protocol messages with an H.323 Version 2 protocol identifier and will not interoperate with Cisco H.323 Version 2 Phase 2.

**Note**

All systems must be running either Cisco IOS Release 11.3(9)NA and later releases or Cisco IOS Release 12.0(3)T and later releases to interoperate with H.323 Version 2.

To use H.450 services (Call Transfer or Call Deflection), you must use Release 12.1(1)T of the Gatekeeper; H.450 on the gateways is incompatible with previous releases of the Cisco Gatekeeper.

If you are planning to use a Cisco AS5300 universal access server, your software requires VCWare Version 4.04.

Related Features and Technologies

Cisco H.323 Version 2 technologies are typically configured by using a number of available compression and decompression (CODECs) and the high-density DSP/voice modules found in the Cisco IOS Release 12.1 of the *Multiservice Applications Configuration Guide*.

Related Documents

- *Multiservice Applications Configuration Guide*
- *Multiservice Applications Command Reference*
- *Voice over IP Quick Start Guide*
- Voice over IP for the Cisco 3600 Series documentation
- Voice over IP for the Cisco AS5300 documentation
- *Cisco Gatekeeper External Interface Reference*

The following table lists the documentation available for configuring and using Cisco IOS H.323 Gatekeepers, gateways, and proxies:

Document	Release	Cisco 2500 Series	Cisco 2600 Series	Cisco 3600 Series	Cisco AS5300
<i>Multimedia Conference Manager (Configuration)</i>	11.3NA	x		x	
<i>Multimedia Conference Manager (Command Reference)</i>	11.3NA	x		x	
<i>Configuring H.323 VoIP Gateway for Cisco Access Platforms</i>	11.3(7)NA	x		x	x
<i>Using Cisco 3600 and Cisco 2600 Series Routers as H.323 VoIP Gateways</i>	12.0(2)XD		x	x	x

Supported Platforms

The gatekeeper and proxy features apply to the following platforms:

- Cisco 2500 Series
- Cisco 2600 Series
- Cisco 3600 Series
- Cisco 7200 Series
- Cisco MC3810 MultiService Concentrator

The gateway features apply to the following platforms:

- Ciscoubr920
- Cisco 1700 Series
- Cisco 2600 Series
- Cisco 3600 Series

- Cisco 7200 Series
- Cisco 7500 Series
- Cisco AS5300
- Cisco AS5800

Supported Standard MIBs and RFCs

No new MIBs are supported by this feature. No RFCs are supported by this feature.

This feature provides support for the following ITU-T Recommendations:

- ITU-T Recommendation H.225.0, *Cell Signaling Protocols and Media Stream Packetization for Packet Based Multimedia Communications Systems*, version 2, March 1997.
- ITU-T Recommendation H.245, *Control Protocol for Multimedia Communication*, version 3, February 1998.
- ITU-T Recommendation H.323, *Packet-Based Multimedia Communications Systems*, version 2, February 1998.
- ITU-T Recommendation H. 235, *Security and Encryption for H-Series (H.323 and other H.245-based) multimedia terminals*, February 1998.
- ITU-T Recommendation H.450.1, *Generic Functional Protocol for the Support of Supplementary Services in H.323*, February 1998.
- ITU-T Recommendation H.450.2, *Call Transfer Supplementary Service for H.323*, September, 1997.
- ITU-T Recommendation H.450.3, *Call Diversion Supplementary Service for H.323*, September, 1997.

Prerequisites

Before you can use H.323 Version 2 Phase 2 features, you must:

- Establish a working IP network. For more information about configuring IP, see the “IP Overview,” “Configuring IP Addressing,” and “Configuring IP Services” chapters in the Cisco IOS Release 12.1 *Network Protocols Configuration Guide, Part 1*.
- Install the appropriate voice network module and voice interface card for your Cisco router. For more information about the physical characteristics of the voice network module, or how to install it, see the *Voice Network Module and Voice Interface Card Configuration Note* that came with your voice network module.
- Configure Voice over IP. For more information about configuring Voice over IP, see “Related Documents” on page 8.
- Configure H.323 Gatekeepers, gateways, and proxies as needed. For more information about configuring these H.323 components, see “Related Documents” on page 8.
- Configure a RADIUS AAA server to handle security for your network.

In addition to the configuration, make sure that the following information is configured in your CiscoSecure AAA server:

In the `/etc/raddb/clients` file, ensure that the following information is provided:

```
#Client Name      Key
#-----      -----
gk215.cisco.com   testing123
```

Where:

`gk215.cisco.com` is resolved to the IP address of the gatekeeper requesting authentication and

`taeduk@cisco.com` is the h323-id of the gateway authenticating to gatekeeper `gk215.cisco.com`.

In the `/etc/raddb/users` file, ensure that the following information is provided:

```
taeduk@cisco.com Password = "thiswouldbethespassword"
User-Service-Type = Framed-User,
Login-Service = Telnet
```

- Configure an NTP Server for your network.

Configuration Tasks

The H.323 Version 2 Phase 2 configuration options allow you to configure the H.323 components discussed in the following sections:

- [Configuring H.323v2 Fast Connect, page 11](#)
- [Configuring H.245 Tunneling of DTMF Relay in Conjunction with Fast Connect, page 11](#)
- [Configuring H.450, page 11](#)
 - [Configuring Call Deflection, page 14](#)
 - [Configuring Call Transfer Without Consultation, page 12](#)

- [Configuring FXS Hookflash Relay](#), page 16
- [Configuring H.235 Security](#), page 16
- [Configuring the Gatekeeper Transaction Message Protocol \(GKTMP\) and RAS Messages](#), page 17
 - [Configuring a Dialing Prefix for each Gateway](#), page 17
 - [Configuring a Gatekeeper for Interaction with External Applications](#), page 18
 - [Configuring Triggers for External Applications](#), page 18
- [Configuring Gateway Support for Alternate Endpoints.](#), page 19
- [Configuring Gatekeeper C Code Generic API for GKTMP in a Unix Environment](#), page 19
- [Configuring Support for Network-Based Billing Number](#), page 19

Configuring H.323v2 Fast Connect

None

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

None

Configuring H.450

Configuring H.450 will vary, depending on whether you configure the gateway for:

- [Configuring Call Transfer Without Consultation](#)
- [Configuring Call Deflection](#)

Although there are no new commands for configuring H.450 services, the services are enabled only when a TCL/IVR Session Application is configured. Therefore, to use H.450 services, you must configure a TCL/IVR-based “application” on each applicable incoming dial peer for each Cisco Gateway that will be involved in Call Transfer or Call Deflection. If no special TCL/IVR behavior is required, you can use the standard TCL/IVR application “session.” This is not to be confused with application “SESSION,” which is not TCL/IVR-based and does not support H.450 services.

In addition, if Call Deflection is to be initiated from a QSIG PRI, you must configure the PRI for “isdn switch-type primary-qsig”. See the examples that follow.



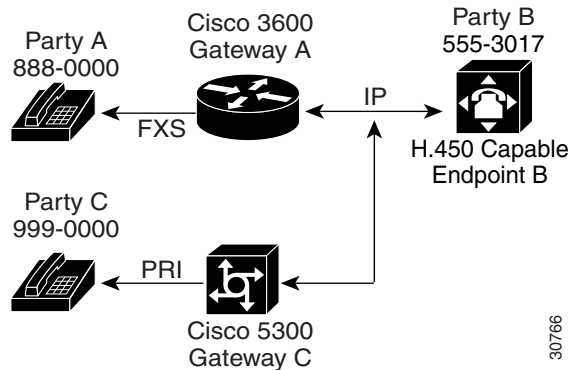
Note

For general information on configuring dial peer application and the meaning of incoming dial peer, please refer to *Voice over IP for the Cisco AS5300*.

Configuring Call Transfer Without Consultation

An example configuration is shown in [Figure 2](#).

Figure 2 H.450 Configuration for Call Transfer Without Consultation



In this example, two gateways are configured to handle call transfers without consultation, so that when Party A calls Party B at 555-3017 at Endpoint B, Endpoint B answers and then invokes Call Transfer to Party C. To do this, you must configure the application session or another TCL/IVR-based application on each applicable incoming dial peer as follows:

1. On Gateway A, the POTS dial peer for destination-pattern 8880000.
2. On Gateway C, the VoIP dial peer for destination-pattern 8880000.

To configure Gateway A POTS dial peer, follow these steps:

	Command	Purpose
Step 1	Router(config)# configure terminal	Enter the global configuration mode.
Step 2	Router(config)# dial-peer voice number pots	Enters dial-peer configuration mode to configure a POTS dial peer. The <i>number</i> value of the dial-peer voice pots command is a tag that uniquely identifies the dial peer.
Step 3	Router(config-dial-peer)# application application-name	Configures the application attribute and identifies the desired TCL script using the <i>application-name</i> argument.
Step 4	Router(config-dial-peer)# destination-pattern [+]string[T]	Configures the destination pattern of the dial peer. Enter the number or pattern of the outbound called number. The <i>string</i> argument is a series of digits that specify an E.164 or private dialing plan telephone number. Valid entries are the digits 0–9 and the letters A–D. The following special characters can be entered in the string: <ul style="list-style-type: none"> • The plus symbol (+) indicates an E.164 standard number. • The star character (*) and the pound sign (#) that appear on standard touch-tone dial pads can be used in any dial string. • The period (.) can be used as a trailing character, and is used as a wildcard character. Multiple periods as trailing characters indicate multiple wildcard digits, such as for the 789... wildcard. The timer (T) keyword can be used to configure variable length dial plans.

	Command	Purpose
Step 5	<code>Router(config-dial-peer)# port slot/port</code>	Specifies the voice slot number and port through which incoming VoIP calls will be received.
Step 6	<code>Router(config)# exit</code>	Exit the dial-peer configuration mode.

To configure VoIP dial peer Gateway B, follow these steps:

	Command	Purpose
Step 1	<code>Router(config)# configure terminal</code>	Enter the global configuration mode.
Step 2	<code>Router(config)# dial-peer voice number voip</code>	Enters dial-peer configuration mode to configure a VoIP dial peer. The <i>number</i> value of the dial-peer voice voip command is a tag that uniquely identifies the dial peer.
Step 3	<code>Router(config-dial-peer)# application application-name</code>	Configures the application attribute and identifies the desired TCL script using the <i>application-name</i> argument.
Step 4	<code>Router(config-dial-peer)# destination-pattern [+]string[T]</code>	Configures the destination pattern of the dial peer. Enter the number or pattern of the outbound called number. The <i>string</i> argument is a series of digits that specify an E.164 or private dialing plan telephone number. Valid entries are the digits 0–9 and the letters A–D. The following special characters can be entered in the string: <ul style="list-style-type: none"> • The plus symbol (+) indicates an E.164 standard number. • The star character (*) and the pound sign (#) that appear on standard touch-tone dial pads can be used in any dial string. • The period (.) can be used as a trailing character, and is used as a wildcard character. Multiple periods as trailing characters indicate multiple wildcard digits, such as for the 789... wildcard. The timer (T) keyword can be used to configure variable length dial plans.
Step 5	<code>Router (config-dial-peer)# session target ipv4:x.x.x.x</code>	Specifies the IP address of the destination gateway for outbound dial peers.
Step 6	<code>Router(config)# exit</code>	Exit the dial-peer configuration mode.

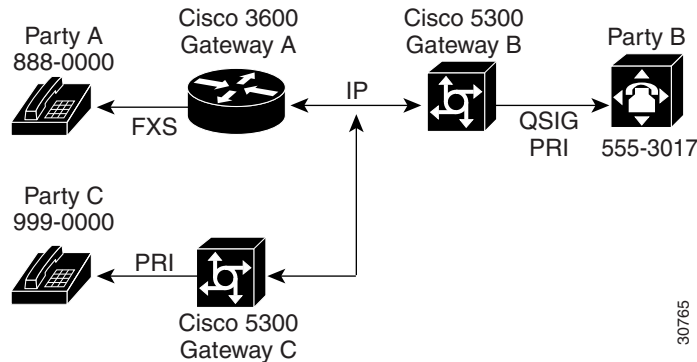
For more information about POTS dial peers, see Cisco IOS Release 12.0 *Voice, Video, and Home Applications Configuration Guide*.

For more information about any of the commands used to configure VoIP dial peers, see Cisco IOS Release 12.0 *Voice, Video, and Home Applications Command Reference*.

Configuring Call Deflection

An example configuration of call deflection is shown in [Figure 3](#).

Figure 3 H.450 Configuration to Redirect Unanswered Calls



In this example, three gateways are configured to redirect unanswered calls, so that when Party A calls Party C, Gateway B can invoke deflection to pass the call to Party C. For this to work, you must to configure “application session” or another TCL/IVR-based application on each applicable incoming dial peer as follows:

1. On Gateway A, the POTS dial peer for destination-pattern 8880000.
2. On Gateway B, the VoIP dial peer and QSIG PRI for destination-pattern 9990000.
3. On Gateway C, the VoIP dial peer for destination-pattern 8880000.

To configure Gateway A POTS dial peer, follow these steps:

Command	Purpose
Step 1 Router(config)# configure terminal	Enter the global configuration mode.
Step 2 Router(config)# dial-peer voice <i>number</i> pots	Enters dial-peer configuration mode to configure a POTS dial peer. The <i>number</i> value of the dial-peer voice pots command is a tag that uniquely identifies the dial peer.
Step 3 Router(config-dial-peer)# application <i>application-name</i>	Configures the application attribute and identifies the desired TCL script using the <i>application-name</i> argument. Note The <i>application-name</i> must be the name of the TCL IVR script. If the application attribute is not configured, or if the POTS dial peer is not created, the default session application will process the call.

	Command	Purpose
Step 4	Router(config-dial-peer)# destination-pattern [+] <i>string</i> [T]	Configures the destination pattern of the dial peer. Enter the number or pattern of the outbound called number. The <i>string</i> argument is a series of digits that specify an E.164 or private dialing plan telephone number. Valid entries are the digits 0–9 and the letters A–D. The following special characters can be entered in the string: <ul style="list-style-type: none"> • The plus symbol (+) indicates an E.164 standard number. • The star character (*) and the pound sign (#) that appear on standard touch-tone dial pads can be used in any dial string. • The period (.) can be used as a trailing character, and is used as a wildcard character. Multiple periods as trailing characters indicate multiple wildcard digits, such as for the 789... wildcard. The timer (T) keyword can be used to configure variable length dial plans.
Step 5	Router (config-dial-peer) # port <i>slot/port</i>	Specifies the voice slot number and port through which incoming VoIP calls will be received.
Step 6	Router(config)# exit	Exit the dial-peer configuration mode.

To configure VoIP dial peer Gateway B and Gateway C, follow these steps for each VoIP Gateway:

	Command	Purpose
Step 1	Router(config)# configure terminal	Enter the global configuration mode.
Step 2	Router(config)# dial-peer voice <i>number</i> voip	Enters dial-peer configuration mode to configure a VoIP dial peer. The <i>number</i> value of the dial-peer voice voip command is a tag that uniquely identifies the dial peer.
Step 3	Router(config-dial-peer)# application <i>application-name</i>	Configures the application attribute and identifies the desired TCL script using the <i>application-name</i> argument.
Step 4	Router(config-dial-peer)# destination-pattern [+] <i>string</i> [T]	Configures the destination pattern of the dial peer. Enter the number or pattern of the outbound called number. The <i>string</i> argument is a series of digits that specify an E.164 or private dialing plan telephone number. Valid entries are the digits 0–9 and the letters A–D. The following special characters can be entered in the string: <ul style="list-style-type: none"> • The plus symbol (+) indicates an E.164 standard number. • The star character (*) and the pound sign (#) that appear on standard touch-tone dial pads can be used in any dial string. • The period (.) can be used as a trailing character, and is used as a wildcard character. Multiple periods as trailing characters indicate multiple wildcard digits, such as for the 789... wildcard. The timer (T) keyword can be used to configure variable length dial plans.
Step 5	Router (config-dial-peer) # session target <i>ipv4:x.x.x.x</i>	Specifies the IP address of the destination gateway for outbound dial peers.
Step 6	Router(config)# exit	Exit the dial-peer configuration mode.

To configure Gateway B PRI, follow these steps:

	Command	Purpose
Step 1	Router(config)# configure terminal	Enter the global configuration mode.
Step 2	Router(config)# interface serial <i>number</i>	Configure the serial interface.
Step 3	Router(config)# isdn switch-type <i>switch-type</i>	Configure the ISDN interface to the central office or ISDN service provider.
Step 4	Router(config)# exit	Exit the dial-peer configuration mode.

Configuring FXS Hookflash Relay

The duration of the hookflash indication can be configured once the VoIP dial peer has been configured for dtmf-relay h245-alpha or 245-signal. To specify the duration of the **hookflash-input** follow these steps on a Cisco AS5800:

	Command	Purpose
Step 1	Router# configure terminal	Enter the global configuration mode.
Step 2	router(config)# voice-port <i>[shelf/slot/port]</i>	Opens voice-port configuration mode and specified the shelf/slot and port number being configured.
Step 3	router(config-voiceport)# timing hookflash-input <i>number</i>	Specifies the duration of the hookflash in milliseconds.

Follow the above steps table to configure the **timing hookflash-output**. Substitute **timing hookflash-output** in place of the **timing hookflash-input**.

Configuring H.235 Security

To enable secure registrations from gatekeeper, and configure which RAS messages the gatekeeper with check to find authentication tokens perform the following steps:

	Command	Purpose
Step 1	Router# configure terminal	Enter the global configuration mode.
Step 2	Router(config)# gatekeeper	Enters the global gatekeeper configuration mode.
Step 3	Router(config-gk)# security token require-for <i>all</i>	Specifies that registration requests will go to aaa for each call.

To configure the which RAS messages will contain gateway generated tokens perform the following steps:

	Command	Purpose
Step 1	Router# configure terminal	Enter the global configuration mode.
Step 2	Router(config)# gateway	Enters the global gatekeeper configuration mode.
Step 3	Router(config-gk)# security password password level {endpoint percall all}	Enables token-based security on the gateway.

Configuring the Gatekeeper Transaction Message Protocol (GKTMP) and RAS Messages

With this version of the gatekeeper software, you can configure the gatekeeper for interaction with external applications. Make sure that you include a priority value for selecting between multiple gateways when you configure the gatekeeper. To configure the gatekeeper, perform the tasks discussed in the following sections:

- [Configuring a Dialing Prefix for each Gateway, page 17](#)
- [Configuring a Gatekeeper for Interaction with External Applications, page 18](#)
- [Configuring Triggers for External Applications, page 18](#)

Configuring a Dialing Prefix for each Gateway

Perform the following steps to put all your gateways in the same zone, use the *gw-priority* argument and specify which gateways are used for calling different area codes:

	Command	Purpose
Step 1	router(config-gk)# zone local localgk xyz.com	Domain xyz.com is assigned to gatekeeper localgk
Step 2	router(config-gk)# zone prefix localgk 408.....	Prefix 408 is assigned to gatekeeper localgk, and no gateway priorities are defined for it; therefore, all gateways registering to localgk can be used equally for calls to the 408 area code. No special gateway lists are built for the 408. prefix; a selection is made from the master list for the zone
Step 3	router(config-gk)# zone prefix localgk 415..... gw-pri 10 gw1 gw2	The prefix 415 is added to gatekeeper localgk, and priority 10 is assigned to gateways gw1 and gw2
Step 4	router(config-gk)# zone prefix localgk 650..... gw-pri 0 gw1	Prefix 650 is added to gatekeeper localgk, and priority 0 is assigned to gateway gw1. A priority 0 is assigned to gateway gw1 to exclude it from the gateway pool for prefix 650. When gw2 registers with gatekeeper localgk, it is added to the gateway pool for each prefix as follows: <ul style="list-style-type: none"> • For gateway pool for 415, gateway gw2 is set to priority 10. • For gateway pool for 650, gateway gw2 is set to priority 5.

Configuring a Gatekeeper for Interaction with External Applications

There are two ways of configuring the gatekeeper for interaction with an external application. You can configure a port number where the gatekeeper listens for dynamic registrations from applications. Using this method, the application connects to the gatekeeper and specifies the trigger conditions in which it is interested.

The second method involves using the command to statically configure the information about the application and its trigger conditions, in which case the gatekeeper initiates a connection to the external application.

Perform the following steps to configuration a gatekeeper specific connection with an external server:

	Command	Purpose
Step 1	Router(config)# gatekeeper	Enters the gatekeeper configuration mode.
Step 2	Router(config-gk)# server registration-port <i>port-number</i>	Establish the server registration port that is used for communication between and specified the port number used.

Configuring Triggers for External Applications

To establish statically configured triggers on a router, follow these steps:

	Command	Purpose
Step 1	Router# configure terminal	Enters global configuration mode.
Step 2	Router(config)# gatekeeper	Enters the gatekeeper configuration mode.
Step 3	Router(config)# server trigger {arq lcf lrj lrq rrq urq} <i>gkid priority server-id server-ip_address server-port</i>	Configures triggers for external applications.
Step 4	Router(config)# info-only	Indicates that messages should be sent as notifications only and not wait for a response from the external application.
Step 5	Router(config)# destination-info {e164 email-id h323-id} <i>value</i>	Configures a trigger that is based on a particular destination. Repeat this command for more destination.
Step 6	Router(config)# redirect-reason <i>value</i>	Limits the qualifying messages based upon the redirect reason. Repeat this command for more destinations.
Step 7	Router(config)# remote-ext-address <i>value</i>	Limits the qualifying messages based upon the remote extension address. Repeat this command for more destinations.
Step 8	Router(config)# endpoint-type <i>value</i>	Configures a trigger that is based on a specific endpoint Repeat this command for more destinations.
Step 9	Router(config)# supported-prefix <i>value</i>	Configures a trigger that is based on a specific supported prefix Repeat this command for more destinations.
Step 10	Router(config)# exit	Exit the <i>config-gk</i> configuration mode

To remove a trigger, use the **no** form of this command. To temporarily suspend a trigger, enter the trigger configuration mode, as described in step 2, and enter the **shutdown** subcommand.

Configuring Gateway Support for Alternate Endpoints.

None

Configuring Gatekeeper C Code Generic API for GKTMP in a Unix Environment

None

Configuring Support for Network-Based Billing Number

None

Verifying

To verify that the Cisco H.323 version 2 phase 2 is configured correctly, use the **show running-config** command in the privileged EXEC mode to display the command settings for the router as shown in the [Configuration Examples](#) section.

Configuration Examples

The following examples display the screen output using the **show running-config** command:

- [H.323v2 Fast Connect Example, page 19](#)
- [H.245 Tunneling of DTMF Relay in conjunction with Fast Connect, page 19](#)
- [Call Transfer Example, page 20](#)
- [Call Deflection Example, page 20](#)
- [FXS Hookflash Relay Example, page 20](#)
- [H.235 Security Example, page 20](#)
- [Gatekeeper Transaction Message Protocol \(GKTMP\) and RAS Messages Example, page 21](#)
- [Gatekeeper and Alternate Endpoints Example, page 21](#)
- [Gatekeeper C Code Generic API for GKTMP in a Unix Environment Example, page 21](#)
- [Gateway Support for Network-Based Billing Number Example, page 21](#)

H.323v2 Fast Connect Example

None

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

None

Call Transfer Example

The following example shows output from configuring a POTS dial peer:

```
dial-peer voice 10 pots
!
dial-peer voice 22 pots
  application session
  destination-pattern 408
```

Call Deflection Example

The following example shows output from configuring a ISDN PRI:

```
!
ipx routing 0010.7be6.47a6
vty-async
isdn switch-type primary-qsig
isdn voice-call-failure 0
isdn alert-end-to-end
```

FXS Hookflash Relay Example

None

H.235 Security Example

The following example shows output from configuring secure registrations from the gatekeeper, and identifying which RAS messages the gatekeeper with check 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 will contain gateway generated tokens:

```
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
radius-server host 25.0.0.1 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
```

Gatekeeper Transaction Message Protocol (GKTMP) and RAS Messages Example

The following is an example of a gatekeeper for interaction with external applications that shows the registration message from Server-123 establishing a connection with Gatekeeper sj.xyz.com on port 20000 and sends a REGISTER RRQ message to Gatekeeper sj.xyz.com to express interest in all RRQs from voice gateways that support a technology prefix of 1# or 2#.

```
REGISTER RRQ
Version-id:1
From:Server-123
To:sj.xyz.com
Priority:2
Notification-Only:
Content-Length:29

t=voice-gateway
p=1#
p=2#
```

Gatekeeper and Alternate Endpoints Example

None

Gatekeeper C Code Generic API for GKTMP in a Unix Environment Example

None

Gateway Support for Network-Based Billing Number Example

None

Command Reference

This section documents new or modified commands for the gatekeeper. All other commands used with this feature are documented in the Cisco IOS Release 12.0 command references.

- [security password](#)
- [security token required-for](#)
- [server registration-port](#)
- [server trigger](#)
- [timing hookflash-input](#)
- [timing hookflash-output](#)
- [show gatekeeper servers](#)
- [debug gatekeeper server](#)

security password

To enable H.323 token-based security and configure the lever of security, use the **security password** command. To stop the gateway from generating tokens for RAS messages, use the **no** for of this command.

security password *password level* { **endpoint** | **per-call** | **all** }

no security password *password level* { **endpoint** | **per-call** | **all** }

Syntax Description		
	password	The gateway password
	endpoint	Validation will be performed on all RAS messages sent by the Gateway. The validation will be performed using the cryptoTokens that are generated based on the security password configured for the Gateway.
	per-call	Validation will be performed only on the admission messages from the H.323 endpoints to the Gateway (ARQ messages)
	all	Validation will be performed on all RAS messages sent by the Gateway. All RAS messages (except ARQ messages) include cryptoTokens that are based on the security password configured for the Gateway. The cryptoToken in ARQ messages is based on a user-supplied account number and PIN.

Defaults none

Command Modes Gatekeeper configuration

Command History	Release	Modification
	12.1(1)T	This command was introduced.

Usage Guidelines

Use the security command to enable identification of registered aliases by RADIUS/TACACS+. If the alias does not exist in RADIUS/TACACS+, the endpoint will not be allowed to register.

A RADIUS/TACACS+ server and encryption key must have been configured in Cisco IOS software for security to work.

Only the first alias of the proper type will be identified. If no alias of the proper type is found, the registration will be rejected.

This command does not allow you to define the password mechanism unless the security type (**h323-id** or **e164** or **any**) has been defined. While the **no security password** command undefines the password mechanism, it leaves the security type unchanged, so security is still enabled. However, the **no security {h323-id | e164 | any}** command disables security entirely, including removing any existing password definitions.

Examples

The following example shows how to enable the identification of registrations using the first H.323 ID found in any registration:

```
security h323id
```

The following example shows how to enable security, authenticating all users by using their H.323-IDs and a password of qwerty2x:

```
security h323-id
security password qwerty2x
```

The following example shows how to enable security, authenticating all users by using their H.323-IDs and the password entered by the user in the H.323-ID alias:

```
security h323-id
security password separator !
```

If a user registers with an H.323-ID of joe!024aqx, the gatekeeper authenticates user joe with password 024aqx, and if that is successful, registers the user with the H.323-ID of joe. If the exclamation mark is not found, the user is authenticated with the default password or a null password if no default has been configured.

The following example shows how to enable security, authenticating all users by using their E.164 IDs and the password entered by the user registered in the H.323-ID alias:

```
security e164
security password separator !
```

Related Commands

Command	Description
accounting (gatekeeper)	Enables the accounting security feature on the gatekeeper.
radius-server host	Specifies a RADIUS server host
radius-server key	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.

security token required-for

To configure the RAS messages so that the gatekeeper checks for access tokens, use the **security token required-for** command. To disable the gatekeeper from checking for tokens in RAS messages, use the **no** form of this command.

```
security token required-for {registration | all}
```

```
no security token required-for {registration | all}
```

Syntax Description

registration	requests will go to aaa for registration only (RRQ)
all	requests will go to aaa for each call (ARQ)

Defaults

No access token is required for authentication if the gatekeeper is configured.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.1(1)T	This command was first introduced.

Usage Guidelines

Use this command to configure the gatekeeper to search for access tokens in RAS messages. These tokens are verified by an AAA server before the gatekeeper responds. If you use the **registration** option, the gatekeeper checks for tokens in all heavyweight RRQ messages. If you use the **all** option, the gatekeeper also checks all ARQ messages—in addition to the RRQ messages.

By using the **no** option of the command the gatekeeper stops checking for authentication tokens in RAS messages.



Note

When you use this command to configure the gatekeeper to check for tokens in RAS messages, heavyweight ARQ and RRQ messages are *not* forwarded to an external application even if ARQ or RRQ trigger conditions are met.

Examples

The following example shows how configure a gatekeeper to require a security token for AAA authentication for all calls:

```
Router(config-gk) # security token re
Router(config-gk) # security token required-for
Router(config-gk) # security token required-for all
```

Related Commands	Command	Description
	debug h225 ans1	Shows additional information about contents of H.225 RAS messages.
	debug aaa auth	Shows information on AAA/TACACS+ authorization.
	debug ras	Shows the types of addressing for RAS messages sent and received.

server registration-port

To define a listener port to be used by the external applications to establish connections to the gatekeeper on this router, use the **server registration-port** command. To close the listener port and no longer receive additional registrations, use the **no** form of this command. Note that existing connections between the gatekeeper and external application are left open.

server registration-port *port number*

no server registration-port *port number*

Syntax Description	<i>port number</i>	Specifies a single range of values from 1 through 65535 for the port number on which the gatekeeper listens for external server connections
---------------------------	--------------------	---

Defaults	The registration port of the gatekeeper is not configured, so no external server can register with this gatekeeper.
-----------------	---

Command Modes	Gatekeeper configuration
----------------------	--------------------------

Command History	Release	Modification
	12.1(1)T	This command was first introduced.

Usage Guidelines	Use this command to configure a server registration port to poll for servers that want to establish connections with the gatekeeper on this router.
-------------------------	---



Note

The **no** form of this command forces the gatekeeper on this router to close the listen socket, so it cannot accept more registrations. However, existing connections between the gatekeeper and servers are left open.

Examples	The following example shows how a listener port for a server is established for connection with a gatekeeper:
-----------------	---

```
Router# server registration-port 20000
```

Related Commands	Command	Description
	server trigger	Configure static server triggers for specific RAS messages to be forwarded to a specified server.

server trigger

To configure a static server trigger for external applications, use the **server trigger** command. To remove a single statically configured trigger entry, use the **no** form of the command. To remove every static trigger you configured, use the **all** form of the command.

```
server trigger {arq | lcf | lrj | lrq | rrq | urq} gkid priority server-id server-ipaddress server-port
```

```
no server trigger {arq | lcf | lrj | lrq | rrq | urq} gkid priority
```

```
no server trigger all
```

Syntax Description

<i>all</i>	Specified to delete all command configured triggers.
arq, lcf, lrj, lrq, rrq, urq	RAS message types. Use these message types to specify a submode in the gatekeeper configuration mode where you configure a trigger for the gatekeeper to act upon. Specify only one message type per server trigger command. There is a different trigger submode for each message type. Each trigger submode has its own set of applicable commands.
<i>gkid</i>	The local gatekeeper identifier.
<i>priority</i>	The priority for each trigger. The range is from 1 through 20, with 1 being the highest priority.
<i>server-id</i>	The external application's ID number.
<i>server-ipaddress</i>	The server's IP address.
<i>server-port</i>	The port on which the Cisco IOS Gatekeeper listens for messages from the external server connection.

Defaults

No server triggers are set.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.1(1)T	This command was first introduced.

Usage Guidelines

Use this command to configure a static server trigger. There are six different server triggers—one for each of the RAS messages. To configure a trigger, go to its submode where a set of subcommands are used to trigger a condition.

Examples

The following examples show each of the six submodes and describe the set of subcommands that are applicable for each submode.

In ARQ submode, enter the following syntax:

```
Router(config-gk)#server trigger arq gkid priority
                    server-id server-ipaddress
                    server-port
Router(config-gk-arqtrigg)#
```

In LCF submode, enter the following syntax:

```
Router(config-gk)#server trigger lcf gkid priority
                    server-id server-ipaddress
                    server-port
Router(config-gk-lcftrigg)#
```

In LRJ submode, enter the following syntax:

```
Router(config-gk)#server trigger lrj gkid priority
                    server-id server-ipaddress
                    server-port
Router(config-gk-lrjtrigg)#
```

In LRQ submode, enter the following syntax:

```
Router(config-gk)#server trigger lrq <gkid> <priority>
                    <server-id> <server-ipaddress>
                    <server-port>
Router(config-gk-lrqtrigg)#
```

In RRQ submode, enter the following syntax:

```
Router(config-gk)#server trigger rrq gkid priority
                    server-id server-ipaddress
                    server-port
Router(config-gk-rrqtrigg)#
```

In URQ submode, enter the following syntax:

```
Router(config-gk)#server trigger urq gkid priority
                    server-id server-ipaddress
                    server-port
Router(config-gk-urqtrigg)#
```

The following options are available in all submodes:

<i>info-only</i>	Information only—no need to wait for acknowledgement.
<i>shutdown</i>	Enter this subcommand to temporarily disable a trigger. The gatekeeper does not consult triggers in a shutdown state when determining what message to forward.

The *destination-info* command is under the ARQ, LRQ, LCF, and LRJ submode and has the following options:

<i>destination-info</i>	Configure <i>destination-info</i> to trigger one of the following conditions:
e164	Configure an E.164 pattern.
email-id	Configure an email ID.

h323-id	Configure an H.323 ID.
word	When configuring the e164 address option, the email-id option, or the h323-id option above, the E.164 address can end in a trailing '.', 's', or '*'.

The *redirect-reason* command is under the ARQ and LRQ submodes and has the following options:

<i>redirect-reason</i>	Configure a <i>redirect-reason</i> to trigger on (range of 0 through 65535) with the following reserved values:
0	Unknown reason.
1	Call forwarding busy or called DTE busy.
2	Call forwarded no reply.
4	Call deflection.
9	Called DTE out of order.
10	Call forwarding by the call DTE.
15	Call forwarding unconditionally.

The *remote-ext-address* command is under the LCF trigger submode and has the following options:

<i>remote-ext-address</i>	Configure remote extension addresses, with the following options:
e164	Configure an E.164 pattern.
word	When configuring the e164 address option, the email-id option, or the h323-id option above, the E.164 address can end in a trailing '.', 's', or '*'.

The *endpoint-type* command is under the RRQ and URQ trigger submodes and has the following options:

<i>endpoint-type</i>	Configure the type of endpoint to trigger, with the following options:
gatekeeper	The endpoint is an H.323 gatekeeper.
h320-gateway	The endpoint is an H.320 gateway.
mcu	The endpoint is a multipoint control unit (MCU).
other-gateway	The endpoint is another type of gateway not specified on this list.
proxy	The endpoint is an H.323 proxy.
terminal	The endpoint is an H.323 proxy.
voice-gateway	The endpoint is a voice gateway.

The **supported-prefix** command is under the RRQ and URQ submodes and has the following options:

supported-prefix	Configure the gateway technology prefix to trigger on.
word	Enter a word within the set of "0123456789#*" when configuring the E.164 pattern for a gateway technology prefix.

Entering the **no** form of the server trigger command removes the trigger definition from the Cisco IOS Gatekeeper with all statically configured conditions under that trigger.

The following example shows how to configure a server trigger on gatekeeper sj.xyz.com to notify external server “Server-123” of any call to an E.164 number that starts with 1800 followed by any 7 digits (1800551212, for example):

```
Router# gatekeeper
Router(config-gk)# server trigger arq sj.xyz.com 1 Server-123 1.14.93.130 1751
Router(config-gk-arqtrigg)# destination-info e164 1800.....
Router(config-gk-arqtrigg)# exit
```

Related Commands

Command	Description
server registration port	Configure a gatekeeper listening port to listen for external server connections.
show gatekeeper servers	Show a list of currently registered and statically configured triggers on this gatekeeper router.

timing hookflash-input

To specify the duration of hookflash indications that the gateway generates on an FXS interface, use the **timing hookflash-input**. To restore the default duration, use the **no** form of this command.

timing hookflash-input *milliseconds*

no timing hookflash-input

Syntax Description.	<i>milliseconds</i>	Specifies the duration of the hookflash. Possible values are 50 through 1550.
----------------------------	---------------------	---

Defaults	Default value is 600 milliseconds.
-----------------	------------------------------------

Command Modes	Voice-port configuration
----------------------	--------------------------

Command History	Release	Modification
	12.1(1)T	This command was introduced.

Usage Guidelines	This command does not affect whether hookflash relay is enabled; hookflash relay is only enabled when dtmf-relay h245-signal is configured on the applicable VoIP dial peers. Hookflash is relayed by using an h245-signal indication and can be sent only when h245-signal is available.
-------------------------	--

Enter the **timing hookflash-input** command on FXS interfaces to specify the maximum duration (in milliseconds) of a hookflash indication. If the hookflash lasts longer than the specified limit, then the FXS interface processes the indication as an on-hook. To set hookflash timing parameters for analog voice interfaces, use the voice-port **timing** subcommand.

Examples	The following example shows how to set the timing hookflash-input indications to a duration of 200 milliseconds, after you have configured voice-port 1/0/0
-----------------	--

```
Router# configure terminal
Router(config)# voice-port 1/0/0
Router(config-voiceport)# timing hookflash-input 200
```

Related Commands	Command	Description
	voice-port	Switch to the voice-port configuration mode from the global configuration mode.

timing hookflash-output

To specify the duration of hookflash indications that the gateway generates on an FXO interface, use the **timing hookflash-output**. To restore the default duration, use the **no** form of this command.

timing hookflash-output *duration*

no timing hookflash-output

Syntax	Description
<i>milliseconds</i>	Specifies the duration of the hookflash. Possible values are 50 through 1550.

Defaults Default value is 400 milliseconds.

Command Modes Voice-port configuration

Command History	Release	Modification
	12.0(6)T	This command was introduced.
	12.1(1)T	The default value was changed.

Usage Guidelines This command does *not* affect whether hookflash relay is enabled; hookflash relay is only enabled when **dtmf-relay h245-signal** is configured on the applicable VoIP dial peers. Hookflash is relayed by using an h245-signal indication and can be sent only when h245-signal is available

Enter the **timing hookflash-output** command on FXO interfaces to specify the duration (in milliseconds) of a hookflash indication. To set hookflash timing parameters for analog voice interfaces, use the voice-port **timing** subcommand.

Examples The following example shows how to set the **timing hookflash-output** indications to a duration of 200 milliseconds, after you have configured voice-port 1/0/0:

```
Router# configure terminal
Router(config)# voice-port 1/0/0
Router(config-voiceport)# timing hookflash-output 200
```

Related Commands	Command	Description
	voice-port	Switch to the voice-port configuration mode from the global configuration mode.

show gatekeeper servers

Enter the **show gatekeeper servers** command to see a list of currently registered and statically configured triggers on this gatekeeper router.

```
show gatekeeper servers [ gkid ]
```

Syntax Description	<i>gkid</i>	(Optional) The local gatekeeper name to which this trigger applies.
Command Modes	EXEC	
Command History	Release	Modification
	12.0(6)T	This command was introduced.

Usage Guidelines

Enter this command to show all server triggers (whether dynamically registered from the external servers or statically configured from the command line interface) on this gatekeeper. If *gkid* is specified, only triggers applied to the specified gatekeeper zone appear. If *gkid* is not specified, server triggers for all local gatekeeper zones on this router appear.

Examples

The following example shows sample operating information output from the gk102 server:

```
Router# show gatekeeper servers gk102

GATEKEEPER SERVERS STATUS
=====

Gatekeeper Server listening port:20000

Gatekeeper-ID:gk102
-----
RRQ Priority:1
  Server-ID:sj-server
  Server IP address:1.14.93.28:42387
  Server type:dynamically registered
  Connection Status:active
  Trigger Information:
    Supported Prefix:10#
    Supported Prefix:3#
RRQ Priority:2
  Server-ID:sf-server
  Server IP address:1.14.93.43:3820
  Server type:CLI-configured
  Connection Status:inactive
  Trigger Information:
    Endpoint-type:MCU
    Endpoint-type:VOIP-GW
    Supported Prefix:99#
ARQ Priority:1
  Server-ID:sj-server
  Server IP address:1.14.93.28:42387
```

```

Server type:dynamically registered
Connection Status:active
Trigger Information:
  Destination Info:M:nilkant@zone14.com
  Destination Info:E:1800.....
  Redirect Reason:Call forwarded no reply
  Redirect Reason:Call deflection

```

Table 1 describes the fields shown in the display.

Table 1 Gatekeeper Server Configuration field Descriptions

Field	Description
Server-ID	Shows the server ID name.
Server IP	Shows the server IP address
Server type	Indicates the type of the server
Connection Status	Indicates if the connection is active or inactive
Trigger Information	To determine which RAS messages the Cisco IOS Gatekeeper forwards to the external application

Related Commands

Command	Description
debug gatekeeper server	Trace all the message exchanges between the Cisco IOS Gatekeeper and the external applications. Show any errors that occur in sending messages to the external applications or in parsing messages from the external applications.

debug gatekeeper server

To trace message exchanges between the Cisco IOS gatekeeper and the external application, use the **debug gatekeeper server** command. To disable this command, use the **no** form of this command.

debug gatekeeper server

no debug gatekeeper server

Syntax Description There are no arguments or keywords.

Defaults Disabled.

Command Modes EXEC

Command History	Release	Modification
	12.1(1)T	This command was introduced.

Usage Guidelines The **debug gatekeeper server** command will show any errors that occur in sending messages to the external applications or in parsing messages from the external applications.

Examples The following example shows how to enable the **debug gatekeeper server** and trace all message exchanges between the Cisco IOS Gatekeeper and the external application:

```
Router# debug gatekeeper servers

Router# show debug
Gatekeeper:
  Gatekeeper Server Messages debugging is on
```

The following example shows how to disable the **debug gatekeeper server**:

```
Router# no debug gatekeeper servers
```

The following example shows sample output from the **debug gatekeeper server**:

```
*Mar 1 00:15:09.812:GK:processing server msg:
REGISTER ARQ
Version-id:300
From:serv
To:dilbert
Priority:5

*Mar 1 00:15:09.812:GK TMSG encoded to write buffer:
"REGISTER ARQ
Version-id:300
```

```

From:dilbert
To:serv
Priority:5
Status:success

"
*Mar 1 00:15:21.992:GK TMSG encoded to write buffer:
"REQUEST ARQ
Version-id:300
From:dilbert
To:serv
Transaction-Id:815F6F940000000A
Content-Length:171

i=I:172.18.193.37:1720
s=E:9194444000 H:daffy
d=E:5553002
b=1280
A=F
C=EC3789D8-CBB9-0077-0000-00000A262988
c=EC3789D8-CBB9-0078-0000-00000A262988
m=T
I=CarrierA

*Mar 1 00:15:22.063:GK:processing server msg:
RESPONSE ACF
Version-id:300
From:serv
To:dilbert
Transaction-Id:815F6F940000000A
Content-Length:47

D=I:172.18.193.25:1720
b=69000
t=gatekeeper

```

Related Commands	Command	Description
	show gatekeeper server	Show information about the gatekeeper servers configured on your network by ID.

Glossary

AAA—Authentication, authorization, and accounting. AAA is a suite of network security services that provides the primary framework through which access control can be set up on your Cisco router or access server.

CODEC—Compression/decompression software.

DTMF—Dual tone multi-frequency.

E1—European digital carrier facility used for transmitting data through the telephone hierarchy. The transmission rate for E1 is 2.048 megabits per second (Mbps).

E.164—International Telecommunication Union (ITU-T) recommendation for international telecommunication numbering. This recommendation provides the number structure and functionality for the three categories of numbers used for international public telecommunication; geographic areas, global services, and networks.

endpoint—An H.323 terminal or gateway. An endpoint can call and be called. It generates or terminates the information stream.

ESF—Extended Superframe. Framing type used on T1 circuits that consists of 24 frames of 192 bits each, with the 193rd bit providing timing and other functions. ESF is an enhanced version of SF format.

FXO—Foreign Exchange Office. A voice interface emulating a PBX trunk line to a switch or telephone equipment to a PBX extension interface.

FXS—Foreign Exchange Station. A voice interface for connecting telephone equipment, which emulates the extension interface of a PBX or the subscriber interface for a switch.

Gatekeeper—An H.323 entity on the LAN that provides address translation and control access to the LAN for H.323 terminals and gateways. The gatekeeper can provide other services to the H.323 terminals and gateways, such as bandwidth management and locating gateways. A gatekeeper maintains a registry of devices in the multimedia network. The devices register with the gatekeeper at startup and request admission to a call from the gatekeeper.

gateway—An H.323 endpoint on the LAN that provides real-time, two-way communication between H.323 terminals on the LAN, other ITU-T terminals in the WAN, or to another H.323 gateway. A gateway allows H.323 terminals to communicate with non-H.323 terminals by converting protocols. A gateway is the point where a circuit-switched call is encoded and repackaged into IP packets.

H.245—An ITU-T standard that describes H.245 endpoint control.

H.323—An ITU-T standard that describes packet-based video, audio, and data conferencing. H.323 is an umbrella standard that describes the architecture of the conferencing system and refers to a set of other standards (H.245, H.225.0, and Q.931) to describe its actual protocol.

H.450.2—Call transfer supplementary service for H.323.

H.450.3—Call diversion supplementary service for H.323.

hookflash—A brief on-hook condition that occurs during a call. The on-hook condition is not long enough to be interpreted as a signal to disconnect the call. You can create a hookflash indication by quickly depressing and then releasing the hook on your telephone.

IVR—Interactive voice response. Term used to describe systems that provide information in the form of recorded messages over telephone lines in response to user input in the form of spoken words or more commonly DTMF signaling.

ITU-T—International Telecommunications Union-Telecommunication Standardization Sector.

packet—Logical grouping of information that includes a header containing control information and (usually) user data. Packets are most often used to refer to network layer units of data.

POTS—Plain old telephone service. Basic telephone service supplying standard single line telephones, telephone lines, and access to the Public Switched Telephone Network.

Q.931—ITU-T specification for signaling to establish, maintain, and clear ISDN network connections.

QSIG—Q (point of the ISDN model) signaling. A common channel signaling protocol based upon ISDN Q.931 standards for digital PBXs.

RRQ—Registration Request RAS message. This message type is sent from an H.323 endpoint to an H.323 gateway.

RTP—Real Time Transport protocol. See RFC 1889.

SF—Super Frame. Common framing type used on T1 circuits. SF consists of 12 frames of 192 bits each with the 193rd bit providing error checking and other functions. SF is superseded by ESF, but is still widely used. Also called D4 framing.

T1—Digital WAN carrier facility. T1 transmits DS 1-formatted data at 1.544 Mbps through the telephone switching network by using alternate mark inversion or B8ZS coding.

T1 trunk—Digital WAN carrier facility. See T1.

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

zone—A collection of all terminals, gateways, and multipoint control units (MCUs) managed by a single gatekeeper. A zone has only one gatekeeper, can be independent of LAN topology, and can comprise multiple LAN segments that are connected by using routers or other devices.

For a list of other internetworking terms, see *Internetworking Terms and Acronyms* that accompanied your access server and is available on the Documentation CD-ROM and Cisco.com at the following URL: <http://www.cisco.com/univercd/cc/td/doc/cisintwk/ita/index.htm>.