Cisco H.323 Version 2 Phase 2

Feature History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1(1)T</td>
<td>This feature was introduced.</td>
</tr>
<tr>
<td>12.1(5)XM2</td>
<td>Support was added for the Cisco AS5350 and Cisco AS5400 universal gateways.</td>
</tr>
</tbody>
</table>

This feature module describes enhancements to Cisco H.323 Version 2 for Phase 2, which is described in the following sections:

- Feature Overview, page 1
- Supported Platforms, page 8
- Supported Standards, MIBs, and RFCs, page 8
- Prerequisites, page 9
- Configuration Examples, page 19
- Command Reference, page 20
- Glossary, page 35

Feature Overview

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

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:

1. 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.
2. 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.

3. 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. 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

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.
Cisco H.323 Version 2 Phase 2

Feature Overview

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 5800 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.

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.

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 hook flash; another PBX can consider this condition to be a disconnect.

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. 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 CLI on the Gatekeeper and the security password CLI 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.
GKTMP

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 CLI 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.

**Gateway Support for 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.

**Gateway Support for a 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.

**Gateway Support for Voice-Port Description**

This feature provides the Gatekeeper with a configurable string that identifies the 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 ARQ message sent by the ingress gateway. The string in the ARQ corresponds to the setting of the `voice-port description` command.

This feature is similar to network-based billing number feature, but differs in two important respects:

- The voice-port description field is only included in the ARQ if the voice-port description is configured through the CLI for the applicable voice-port.
- Because the voice-port description is configurable, the user can provide customer-specific information to the Gatekeeper. For example, the voice-port description can be configured to correspond to the Carrier Identification Code (CIC) for calls received on a particular T1/E1 Span.

**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

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

Note

All systems must be running either Cisco IOS release 11.3(9)NA and later releases or Cisco IOS version 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 following high-density DSP/voice modules.

Related Documents

• Multiservice Applications Configuration Guide
• Multiservice Applications Command Reference
• Voice over IP Quick Start Guide
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:

- Cisco uBR920
- Cisco 1700 Series
- Cisco 2600 Series
- Cisco 3600 Series
- Cisco 7200 Series
- Cisco 7500 Series
- Cisco AS5300
- Cisco AS5400
- Cisco AS5800

Supported Standards, MIBs, and RFCs

**Standards**

This feature adds support for the following ITU-T standards: H.323 Annex E and H.323 Annex G.
**MIBs**

No new or modified MIBs are supported by this feature.

To obtain lists of MIBs supported by platform and Cisco IOS release and to download MIB modules, go to the Cisco MIB web site on Cisco Connection Online (CCO) at 

**RFCs**

No new or modified RFCs are supported by this feature.

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


**Prerequisites**

The Cisco AS5350 and Cisco AS5400 do not support the Mica Modem Card, Microcom Modem Card, or VoIP Feature Card. Voice and modem functions are provided by the Universal Port Dial Feature card running SPE firmware. See the Cisco AS5350 Universal Gateway Card Installation Guide and the Cisco AS5400 Universal Gateway Card Installation Guide for more information. All references to the Cisco AS5300 in this document apply to the Cisco AS5350 and Cisco AS5400 platforms with the following exceptions:

- Use the Universal Port Dial Feature Card instead of the Mica or Microcom modem cards.
- Use SPE firmware instead of portware version 6.7.7.
- Run Cisco IOS Release 12.1(5)XM2 software for VoIP functionality.

**Other Prerequisites**

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

- 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 7.
- Configure H.323 Gatekeepers, gateways, and proxies as needed. For more information about configuring these H.323 components, see “Related Documents” on page 7.
- Configure a RADIUS AAA server to handle security for your network.
- 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.323 Fast Connect, page 10
- Configuring H.245 Tunneling, page 10
- Configuring H.450, page 10
- Configuring a RADIUS/AAA Server, page 15
- Configuring the Gatekeeper, page 16

Note

When configuring a voice port, use the following configuration designations:
For the Cisco AS5300 access server, port designation is port.
For the Cisco AS5400 gateway, port designation is slot/port.
For the Cisco AS5800 access server, port designation is shelf/slot/port.

Configuring H.323 Fast Connect

Because Fast Connect is a H.323 Version 2 compliant feature and the majority of endpoints prefer to establish a call by using Fast Connect procedures, this feature is not configurable. H.323 Fast Connect does not require any additional configuration beyond a working voice configuration.

For more information about configuring voice ports, see “Configuring Voice Ports” in the Cisco IOS Release 12.0 Voice, Video, and Home Applications Configuration Guide.

Configuring H.245 Tunneling

The dtmf-relay command configured on the outgoing VoIP dial peer initiates H.245 tunneling procedures from a Fast Connect call. Note that H.245 tunneling will be activated only if dtmf-relay “h245-alpha” or “h245-signal” (but not “cisco-rtp”) are configured on the VoIP dial peer.

Configuring H.450

How you configure a Cisco gateway for H.450 depends upon whether you want your gateway to:
- Redirect an unanswered call (Call Deflection).
- Transfer an answered call to a new DN (Call Transfer without consultation)
Although there are no new CLI 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” and “isdn alert end-to-end.” 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 Deflection

An example configuration is shown in Figure 2.

*Figure 2  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 B, Party B can invoke deflection to pass the call to Party C. For this to work, you must 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 for destination-pattern 8880000.
3. On Gateway C, the VoIP dial peer for destination-pattern 8880000.

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Router# configure terminal</td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> Router(config)# dial-peer voice 1 pots</td>
<td>Enters the dial-peer configuration mode to configure parameters for the specified Gateway A POTS dial peer. The specific dial peer is identified by tag number 1.</td>
</tr>
</tbody>
</table>
Configuration Tasks

Cisco H.323 Version 2 Phase 2

Cisco IOS Release 12.1(5)XM1

To configure Gateway A global ISDN alert-end-to-end parameter, follow these steps:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 3</td>
<td>Router(config-dial-peer)# application session</td>
</tr>
<tr>
<td>Step 4</td>
<td>Router(config-dial-peer)# destination-pattern 8880000</td>
</tr>
<tr>
<td>Step 5</td>
<td>Router(config-dial-peer)# port 1/1/0</td>
</tr>
<tr>
<td>Step 6</td>
<td>Router(config-dial-peer)# exit</td>
</tr>
</tbody>
</table>

To configure Gateway B VoIP peer, follow these steps:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>Router(config)# isdn alert-end-to-end</td>
</tr>
<tr>
<td>Step 3</td>
<td>Router(config)# exit</td>
</tr>
</tbody>
</table>

To configure Gateway B PRI, follow these steps:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>Router(config)# dial-peer voice 888 voip</td>
</tr>
<tr>
<td>Step 3</td>
<td>Router(config-dial-peer)# application session</td>
</tr>
<tr>
<td>Step 4</td>
<td>Router(config-dial-peer)# destination-pattern 8880000</td>
</tr>
<tr>
<td>Step 5</td>
<td>Router(config-dial-peer)# session target ipv4:1.1.1.1</td>
</tr>
<tr>
<td>Step 6</td>
<td>Router(config-dial-peer)# exit</td>
</tr>
</tbody>
</table>
To configure Gateway C VoIP dial peers, follow these steps:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Router(config)# interface serial0:23</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Router(config)# isdn switch-type primary-qsig</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Router(config)# exit</td>
</tr>
</tbody>
</table>

An example configuration is shown in Figure 3.

**Configuring Call Transfer Without Consultation**

An example configuration is shown in Figure 3.

**Figure 3**  
*H.450 Configuration for Calls 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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 Router# configure terminal</td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td>Step 2 Router(config)# dial-peer voice 1 pots</td>
<td>Enters the dial-peer configuration mode to configure parameters for the specified Gateway A POTS dial peer. The specific dial peer is identified by tag number 1.</td>
</tr>
<tr>
<td>Step 3 Router(config-dial-peer)# application session</td>
<td>Specifies the application that will be invoked for this dial peer. Only TCL-based applications are able to support H.450 services. In this example, the standard TCL/IVR application session is indicated.</td>
</tr>
<tr>
<td>Step 4 Router(config-dial-peer)# destination-pattern 8880000</td>
<td>Specifies the telephone number (E.164 or otherwise) associated with dial peer 1.</td>
</tr>
<tr>
<td>Step 5 Router(config-dial-peer)# port 1/1/0</td>
<td>Specifies the voice slot number, subunit number, and port through which incoming VoIP calls will be received.</td>
</tr>
<tr>
<td>Step 6 Router(config-dial-peer)# exit</td>
<td>Exits the dial-peer configuration mode.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 Router# configure terminal</td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td>Step 2 Router(config)# dial-peer voice 888 voip</td>
<td>Enters the dial-peer configuration mode to configure parameters for the specified Gateway C VoIP dial peer, which is identified by tag number 888.</td>
</tr>
<tr>
<td>Step 3 Router(config-dial-peer)# application session</td>
<td>Specifies the application that will be invoked for this dial peer. Only TCL-based applications are able to support H.450 services. In this example, the standard TCL/IVR application session is indicated.</td>
</tr>
<tr>
<td>Step 4 Router(config-dial-peer)# destination-pattern 8880000</td>
<td>Specifies the telephone number (E.164 or otherwise) associated with dial peer 888.</td>
</tr>
<tr>
<td>Step 5 Router(config-dial-peer)# session target ipv4:1.1.1.1</td>
<td>Specifies the IP address of the destination gateway for “outbound” dial peers. Because this is an “incoming” dial peer, the session target is not applicable, so the IP address is ignored.</td>
</tr>
<tr>
<td>Step 6 Router(config-dial-peer)# exit</td>
<td>Exits the dial-peer configuration mode.</td>
</tr>
</tbody>
</table>
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 Voice-Port Descriptions

The voice-port description feature uses the existing `description` subcommand for the voice port. When you configure the voice-port description, the exact contents of the description field are included in the ARQ message sent from the ingress gateway.

*Note* Configuring the voice-port description has no effect for calls that are not configured to use RAS.

To configure the description on a voice-port, follow these steps:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Router# <code>config terminal</code> Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Router(config)# <code>voice-port voice_port_ID</code> Enter voice-port configuration mode for the specified voice port.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Router(config-voiceport)# <code>description string</code> Defines the description associated with the voice-port.</td>
</tr>
</tbody>
</table>

### Configuring a RADIUS/AAA Server

To configure the RADIUS/AAA server with information about the Gatekeeper for your network installation, follow these steps:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Router(config)# <code>aaa new-model</code> Initiates the AAA script.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Router(config)# <code>aaa authentication login h323 group radius</code> Configures the router to use the H.323 method list for authentication purposes.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Router(config)# <code>radius-server deadtime seconds</code> Defines a threshold time in seconds until the router assumes the RADIUS server is dead. After 120 seconds, the router sends messages alerting an administrator about a security problem.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Router(config)# <code>radius-server host ip-address auth-port port-num acct-port port-num</code> Sets the server host IP address and the ports for both the authentication service and the accounting service.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Router(config)# <code>radius-server key testing123</code> Configure the radius key secret.</td>
</tr>
</tbody>
</table>

In addition to the above 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 = "thiswouldbethepassword"
User-Service-Type = Framed-User,
Login-Service = Telnet
```

### Configuring the Gatekeeper

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 16
- Configuring a Gatekeeper for Interaction with External Applications, page 17
- Configuring Triggers for External Applications, page 18

### Configuring a Dialing Prefix for each Gateway

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. For example:

```
router(config-gk)# zone local localgk xyz.com
router(config-gk)# zone prefix localgk 408........
router(config-gk)# zone prefix localgk 415........ gw-pri 10 gw1 gw2
router(config-gk)# zone prefix localgk 650........ gw-pri 0 gw1
```

In the above commands the following is accomplished:

- Domain `xyz.com` is assigned to Gatekeeper `localgk`.
- 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.
- The prefix `415` is added to Gatekeeper `localgk`, and priority `10` is assigned to gateways `gw1` and `gw2`.
- 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:

- 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 CLI to statically configure the information about the application and its trigger conditions, in which case the Gatekeeper initiates a connection to the external application.

This configuration is for a Gatekeeper (sj.xyz.com) that uses port 20000 for a specific connection with an external server (Server-123). Server-123 has a number of triggers that are used to maintain a database of active gateways, which are used for active call resolution. The configuration is as follows:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Router(config)# Gatekeeper</td>
</tr>
<tr>
<td></td>
<td>Accesses the Cisco IOS Gatekeeper configuration mode by entering the Gatekeeper command.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Router(config-gk)# server registration-port port-num</td>
</tr>
<tr>
<td></td>
<td>Establishes the server registration port that is used for communication between sj.xyz.com and Server-123 by entering the server registration-port command.</td>
</tr>
</tbody>
</table>

Server-123 establishes 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#.

The following is an example of a registration message:

```
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#
```

When Gatekeeper sj.xyz.com receives this message, the information supplied in the message is added to the trigger list. Then, when an endpoint registers with this Gatekeeper by using an RRQ that matches the specified trigger condition in the message, the Gatekeeper sends a notification to Server-123.
See the following example of an RRQ notification sent from the Gatekeeper to the server when the above trigger condition matches:

```plaintext
REQUEST RRQ
Version-id:1
From:sj.xyz.com
To:Server-123
Notification-Only:
Content-Length:89

c=I:171.69.136.205:1720
r=I:171.69.136.205:16523
a=H:gw3-sj
t=voice-gateway
p=1# 2#
```

## Configuring Triggers for External Applications

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Router(config)# Gatekeeper</td>
<td>Accesses the Cisco IOS Gatekeeper configuration mode by entering the <code>Gatekeeper</code> command.</td>
</tr>
<tr>
<td><strong>Step 2</strong> Router(config-gk)# server trigger {arq</td>
<td>lcf</td>
</tr>
<tr>
<td><strong>Step 3</strong> Router(config-gk)# info-only</td>
<td>If the trigger is to end qualifying messages on a notification-only basis, enter the <code>info-only</code> command.</td>
</tr>
<tr>
<td><strong>Step 4</strong> Router(config-gk)# destination-info {e164</td>
<td>email-id</td>
</tr>
<tr>
<td><strong>Step 5</strong> Router(config-gk)# redirect-reason value</td>
<td>If you want to limit the qualifying messages based upon the redirect reason, enter the <code>redirect-reason</code> command. Repeat this command for more destinations.</td>
</tr>
<tr>
<td><strong>Step 6</strong> Router(config-gk)# remote-ext-address value</td>
<td>If you want to limit the qualifying messages based upon the remote extension address, enter the <code>remote-ext-address</code> command. Repeat this command for more destinations.</td>
</tr>
<tr>
<td><strong>Step 7</strong> Router(config-gk)# endpoint-type value</td>
<td>If you want to limit the qualifying messages based upon the endpoint type, enter the <code>endpoint-type</code> command. Repeat this command for more destinations.</td>
</tr>
</tbody>
</table>
To remove a trigger, enter the `no server trigger` command. To temporarily suspend a trigger, enter the trigger configuration mode, as described in step 2, and enter the `shutdown` subcommand.

## Configuration Examples

The configuration examples for H.450 and the GKTMP Gatekeeper are described in the following sections:

- Configuring H.450, page 10
- Configuring the Gatekeeper, page 16
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 12.1 command reference publications.

- security token required-for
- server registration-port
- server trigger
- Debug Commands
- timing hookflash-input
- timing hookflash-output
security token required-for

To configure the RAS messages so that the Gatekeeper checks for access tokens, enter the `security token required-for` command from the `config-gk` mode. To disable the Gatekeeper from checking for tokens in RAS messages, enter the `no` form of this command.

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

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

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>registration</td>
<td>Requires the registering gateway to send an access token in the registration request to the Gatekeeper.</td>
</tr>
<tr>
<td>all</td>
<td>Requires the gateway to send an access token in registration and call setup messages to the Gatekeeper.</td>
</tr>
</tbody>
</table>

**Defaults**

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

**Command Modes**

Gatekeeper configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1(1)T</td>
<td>This command was first introduced.</td>
</tr>
<tr>
<td>12.1(5)XM1</td>
<td>The command was introduced for the Cisco AS5400.</td>
</tr>
</tbody>
</table>

**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.
See the following example to configure a Gatekeeper to utilize an AAA server, enter the gateways that will be registering on the AAA security server, by entering the following commands:

```
Router# aaa new-model
Router(config)# aaa authentication login h323 group radius
Router(config)# radius-server deadtime 120
Router(config)# radius-server host 172.18.192.59 auth-port 1645 acct-port 1646 key lab
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug h225 ans1</td>
<td>Shows additional information about contents of H.225 RAS messages.</td>
</tr>
<tr>
<td>debug aaa auth</td>
<td>Shows information on AAA/TACACS+ authorization.</td>
</tr>
<tr>
<td>debug ras</td>
<td>Shows the types of addressing for RAS messages sent and received.</td>
</tr>
</tbody>
</table>
server registration-port

To configure the listener port for the server to establish a connection with the Gatekeeper, enter the `server registration-port` command from Gatekeeper mode. Enter the `no` form of this command to force the Gatekeeper to close the listening socket so that no more new registration takes place. However, existing connections between the Gatekeeper and the external applications are left open.

```
server registration-port port number

no server registration-port port number
```

### Syntax Description

- **port number**
  - 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 mode

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1(1)T</td>
<td>This command was first introduced.</td>
</tr>
<tr>
<td>12.1(5)XM1</td>
<td>The command was introduced for the Cisco AS5400.</td>
</tr>
</tbody>
</table>

### 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 listening socket, so it cannot accept more registrations. However, existing connections between the Gatekeeper and servers are left open.

### Examples

See the following example of how a listener port for a server is established for connection with a Gatekeeper:

```
Router# server registration-port 20000
```
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>server trigger</td>
<td>Configure static server triggers for specific RAS messages to be forwarded to a specified server.</td>
</tr>
</tbody>
</table>
server trigger

To configure a static server trigger for external applications, enter the server trigger command from Gatekeeper mode. Enter the no form of this command to remove a single statically configured trigger entry. Enter the “all” form of the command to remove every static trigger you configured if you want to delete them all.

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

<table>
<thead>
<tr>
<th>Syntax Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specified to delete all CLI configured triggers.</td>
</tr>
<tr>
<td>arq, lcf, lrj, lrq, rrq, urq</td>
<td>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.</td>
</tr>
<tr>
<td>gkid</td>
<td>The local Gatekeeper identifier.</td>
</tr>
<tr>
<td>priority</td>
<td>The priority for each trigger. The range is from 1 through 20, with 1 being the highest priority.</td>
</tr>
<tr>
<td>server-id</td>
<td>The external application’s ID number.</td>
</tr>
<tr>
<td>server-ipaddress</td>
<td>The server’s IP address.</td>
</tr>
<tr>
<td>server-port</td>
<td>The port on which the Cisco IOS Gatekeeper listens for messages from the external server connection.</td>
</tr>
</tbody>
</table>

Defaults

No server triggers are set.

Command Modes

Configure from Gatekeeper mode.

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1(1)T</td>
<td>This command was first introduced.</td>
</tr>
<tr>
<td>12.1(5)XM1</td>
<td>The command was introduced for the Cisco AS5400.</td>
</tr>
</tbody>
</table>

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. See the following examples.
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-lcfttrigg)#
```

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:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>info-only</td>
<td>Information only—no need to wait for acknowledgement.</td>
</tr>
<tr>
<td>shutdown</td>
<td>Enter this subcommand to temporarily disable a trigger. The Gatekeeper does not consult triggers in a shutdown state when determining what message to forward.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>e164</td>
<td>Configure an E.164 pattern.</td>
</tr>
<tr>
<td>email-id</td>
<td>Configure an email ID.</td>
</tr>
<tr>
<td>h323-id</td>
<td>Configure an H.323 ID.</td>
</tr>
<tr>
<td>word</td>
<td>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 '*'.</td>
</tr>
</tbody>
</table>

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

Configure a redirect-reason to trigger on (range of 0 through 65535) with the following reserved values:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Unknown reason.</td>
</tr>
<tr>
<td>1</td>
<td>Call forwarding busy or called DTE busy.</td>
</tr>
<tr>
<td>2</td>
<td>Call forwarded no reply.</td>
</tr>
<tr>
<td>4</td>
<td>Call deflection.</td>
</tr>
<tr>
<td>9</td>
<td>Called DTE out of order.</td>
</tr>
<tr>
<td>10</td>
<td>Call forwarding by the call DTE.</td>
</tr>
<tr>
<td>15</td>
<td>Call forwarding unconditionally.</td>
</tr>
</tbody>
</table>

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

### remote-ext-address

Configure remote extension addresses, with the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>e164</td>
<td>Configure an E.164 pattern.</td>
</tr>
<tr>
<td>word</td>
<td>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 ‘*’.</td>
</tr>
</tbody>
</table>

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

### endpoint-type

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 a 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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>word</td>
<td>Enter a word within the set of “0123456789**” when configuring the E.164 pattern for a gateway technology prefix.</td>
</tr>
</tbody>
</table>

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.
Examples

See the following example 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server registration port</td>
<td>Configure a Gatekeeper listening port to listen for external server connections.</td>
</tr>
<tr>
<td>show Gatekeeper servers</td>
<td>Show a list of currently registered and statically configured triggers on this Gatekeeper router.</td>
</tr>
</tbody>
</table>
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**

| gkid | (Optional) The local Gatekeeper name to which this trigger applies. |

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(6)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.1(5)XM1</td>
<td>The command was introduced for the Cisco AS5400.</td>
</tr>
</tbody>
</table>

**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

This example shows the operating information of the specified 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
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug Gatekeeper server</td>
<td>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.</td>
</tr>
</tbody>
</table>
timing hookflash-input

Enter the `timing hookflash-input` command from privileged EXEC mode to specify the maximum duration of a hookflash for an FXS interface. Enter the `no` form of this command to restore the default duration for hookflash timing.

```
timing hookflash-input milliseconds
no timing hookflash-input
```

**Syntax Description.**

| milliseconds | Specifies the duration of the hookflash. Possible values are 50 through 1550. |

**Defaults**

Default value is 600 milliseconds.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1(1)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.1(5)XM1</td>
<td>The command was introduced for the Cisco AS5400.</td>
</tr>
</tbody>
</table>

**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**

To implement timing for the hookflash with a duration of 200 milliseconds, see the following example:

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>voice-port</td>
<td>Switch to the voice-port configuration mode from the global configuration mode.</td>
</tr>
</tbody>
</table>
timing hookflash-output

Enter the `timing hookflash-output` command to specify the duration of hookflash indications that the gateway generates on an FXO interface. Enter the `no` form of this command to restore the default duration for hookflash timing.

```
timing hookflash-output duration

no timing hookflash-output
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>milliseconds</td>
<td>Specifies the duration of the hookflash. Possible values are 50 through 1550.</td>
</tr>
</tbody>
</table>

**Defaults**

Default value is 400 milliseconds.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(6)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.1(1)T</td>
<td>The default value was changed.</td>
</tr>
<tr>
<td>12.1(5)XM1</td>
<td>The command was introduced for the Cisco AS5400.</td>
</tr>
</tbody>
</table>

**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**

To implement timing for the hookflash with a duration of 200ms, see the following example 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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>voice-port</td>
<td>Switch to the voice-port configuration mode from the global configuration mode.</td>
</tr>
</tbody>
</table>
Debug Commands

This section documents new or modified `debug` commands. All other commands used with this feature are documented in the Cisco IOS Release 12.1 command reference publications.

`debug Gatekeeper server`
debug Gatekeeper server

Enter the debug Gatekeeper server command from EXEC mode to 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. Enter the no form of this command to disable debugging output.

```
debug Gatekeeper server
no debug Gatekeeper server
```

Syntax Description

There are no arguments or keywords.

Defaults

Disabled.

Command Modes

EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1(1)T</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>12.1(5)XM1</td>
<td>The command was introduced for the Cisco AS5400.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use this command to see information about a Gatekeeper server.

Examples

This example shows debugging information about a Gatekeeper server

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

To turn the Gatekeeper server debugging message off, see the following example:

```
Router# no debug all
```

or

```
Router# no debug Gatekeeper servers
```
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.

DNS—Domain name system used in address translation to convert H.323 IDs, URLs, or e-mail IDs to IP addresses. DNS is also used to locate remote Gatekeepers and to translate names of network nodes into IP addresses or host names of administrative domains.

DNIS—Dialed number identification service (the called number). Feature of trunk lines where the called number is identified; this called number information is used to route the call to the appropriate service.

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.

E&M—Receive and transmit, or Ear and Mouth. Type of signaling originally developed for analog two-state voltage telephony using the ear and mouth leads; in digital telephony, uses two bits.

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.

Glossary

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show Gatekeeper server</td>
<td>Show information about the Gatekeeper servers configured on your network by ID.</td>
</tr>
</tbody>
</table>
GKAPI—Gatekeeper Application Programming Interface.

GKTMP—Gatekeeper Transaction Message Protocol.

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.

ICW—Internet call waiting service.

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.

OSP—Open Settlement Protocol.

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.

PSTN—Public Switched Telephone Network. General term referring to the variety of telephone networks and services in place worldwide.

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 Connection Online (CCO) at the following URL: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ita/index.htm.