

Gatekeeper Trunk and Carrier Based Routing Enhancements

Feature History

Release	Modification
12.2(2)XU	This feature was introduced on the Cisco 3660 and Cisco 7200 platforms for the gatekeeper and on the Cisco 3660, Cisco 5300, Cisco 5350, Cisco 5400, and Cisco 5850 platforms for the gateway.

This feature module describes the Gatekeeper Trunk and Carrier Based Routing Enhancements feature functionality in Cisco IOS Release 12.2(2)XU, and includes the following sections:

- [Feature Overview, page 1](#)
- [Supported Platforms, page 13](#)
- [Supported Standards, MIBs, and RFCs, page 13](#)
- [Prerequisites, page 14](#)
- [Configuration Tasks, page 14](#)
- [Monitoring and Maintaining, page 17](#)
- [Configuration Examples, page 17](#)
- [Command Reference, page 19](#)
- [Glossary, page 89](#)

For information about routing enhancements on the gateway, refer to *Gateway Trunk and Carrier Based Routing Enhancements*.

Feature Overview

Wholesale voice is a service that interconnects two H.323 Voice over IP (VoIP) service providers to complete a call. The Gatekeeper Trunk and Carrier Based Routing Enhancements feature implements the capability to report the PSTN-side interfaces for incoming and outgoing calls to the H.323 gatekeeper and to the peer H.323 gateway and endpoint.

The intent of this feature is to accomplish the following:

- Identify, by means of labeling individual PSTN trunks or trunk groups, the circuit that is sending a call.

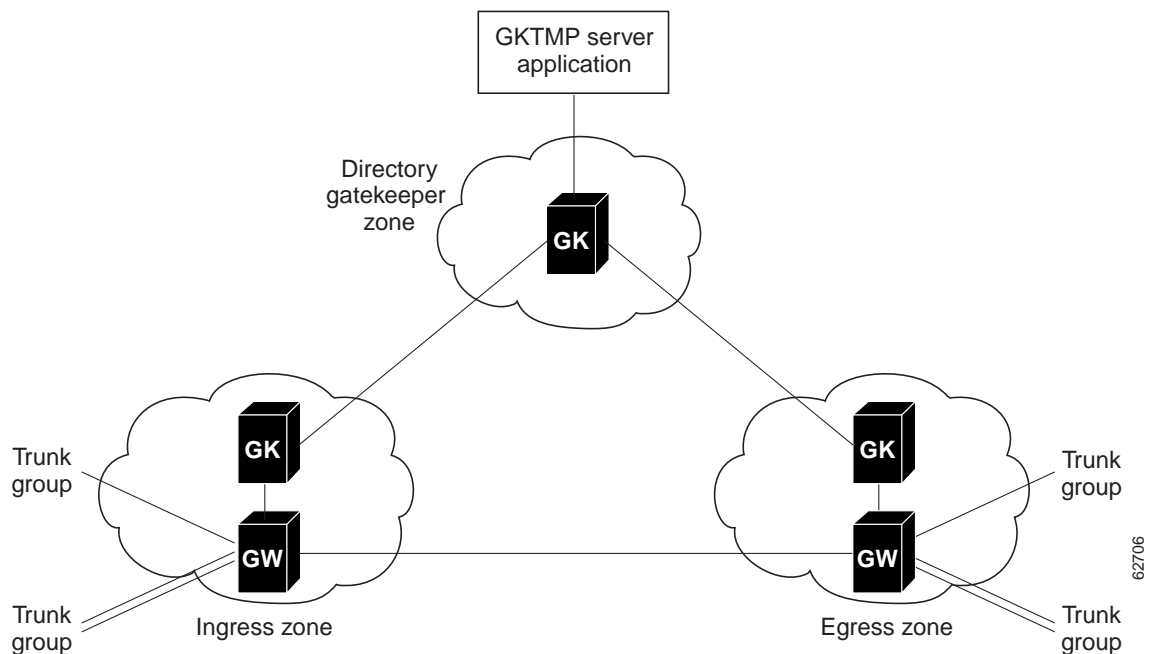


Note This feature refers to *circuits* in the network. Circuits can be DS-0 trunks, trunk groups, or carrier IDs. Call routing is done using either carrier IDs or trunk group labels.

- Route the call to a specific outbound circuit using some criteria, such as inbound circuit, time period, or cost.
- Forward the call to a circuit connected to the specified outbound carrier.

Figure 1 shows the main components of a carrier-sensitive routing network.

Figure 1 General Trunk and Carrier Based Routing Network



As shown in Figure 1, the network has three main components:

- **Gateway** —This component is the first contact that a PSTN call has with the IP network. The calls arriving from the PSTN interconnect come in on a voice port or a *trunk group*, which is a logical group of physical interfaces. The gateway interacts with the gatekeeper to receive routing information. After receiving the call routing information, the gateway routes the call to its destination.

This feature has enhanced the gateway with these software capabilities:

- Enhancements to the gateway and H.323 software for signaling ingress and egress circuit identifiers for a call.
- Trunk group and dial peer enhancements
- Support for H.323 Version 4 call capacities



Note This document provides a high-level overview of the new gateway functionality. The gateway enhancements are described in detail in *Gateway Trunk and Carrier Based Routing Enhancements*.

- Gatekeeper—This component determines the route of the call through the network. For routing calls to a trunk group using the H.323v4 circuit identifier field, the gatekeeper also interacts with the gatekeeper transaction message protocol (GKTMP) server application.

This feature enhances the gatekeeper with the following software capabilities:

- GKTMP message extensions for interaction with the GKTMP server application
 - Interoperability with previous versions of the gatekeeper, existing gateways, and third-party endpoints and gatekeepers
- GKTMP server application—This component, sometimes referred to as the GKTMP router server application, contains the software application responsible for user-specific carrier information, routing parameters, and route detail accounting.

This feature enhances the call detail report (CDR) with these software capabilities:

- GKTMP API library support
- Vendor-specific attributes (VSAs)

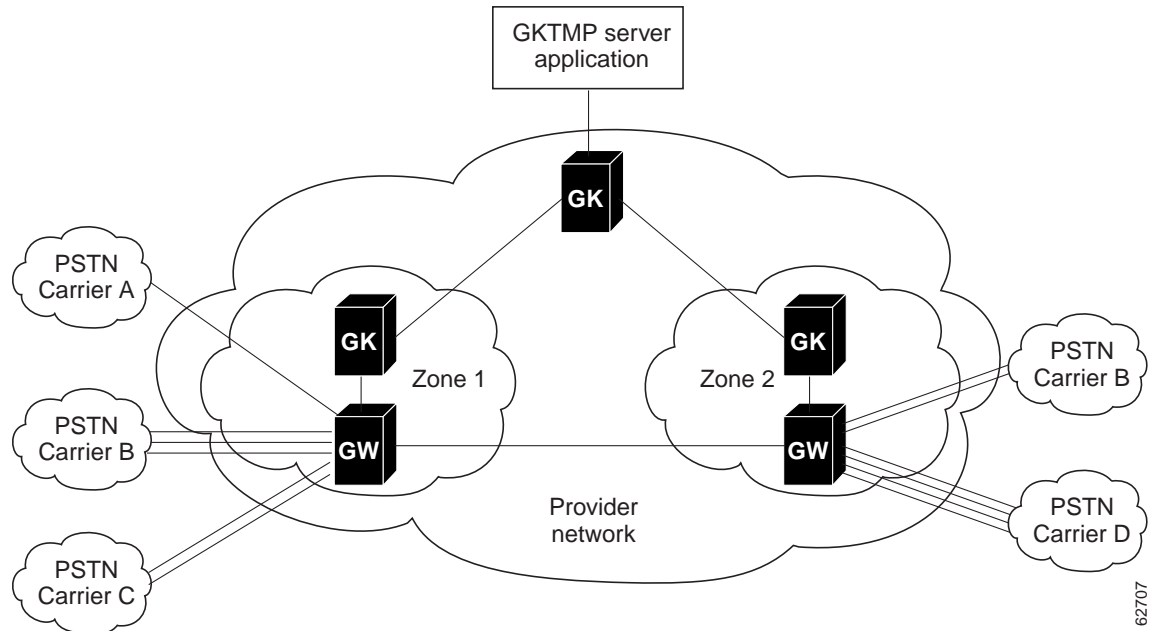
The next section, [Wholesale Voice Network Scenario](#), describes the network configuration that incorporates these features. See [Call Routing, page 4](#) for more detailed descriptions of the new routing functions on the gateways, gatekeepers, and GKTMP server application.

Wholesale Voice Network Scenario

Wholesale voice providers offer call routing services across various types of customer networks. Customers with time-division multiplexing (TDM) transit networks can use gatekeeper trunk and carrier based routing.

In a TDM transit network, customers purchase minutes from the wholesale provider and send the traffic through a set of ingress trunks. Each trunk is assigned to a particular customer. The provider also arranges for a set of carriers or partners to terminate the calls. The wholesale provider's task is to route the calls efficiently and profitably from ingress to egress. Figure 2 illustrates this arrangement.

Figure 2 TDM Transit Network



In this scenario, carriers A, B, and C are ingress carriers with their assigned trunk and carriers B and D are egress carriers with their assigned trunks. Carrier B acts as both a customer and vendor to the wholesale provider.

A PSTN call arrives from an ingress carrier to the provider's gateway. The gateway alerts its gatekeeper that it has a call and needs routing information. The gatekeeper contacts the GKTMP server application gatekeeper, also referred to as a directory gatekeeper, with this request. The directory gatekeeper requests the GKTMP server application for the appropriate routing path and sends that data back to the ingress gatekeeper, who forwards the routing data to the ingress gateway. The gateway sends the call to the egress gateway, which routes the call across the designated PSTN circuit.

Call Routing

A typical GKTMP server application is hosted over a local zone (leaf) gatekeeper or a directory gatekeeper.

A *zone gatekeeper* host triggers the GKTMP server application after receiving an admission request (ARQ) and requires connection to a local operations support system (OSS) for accurate tracking of current calls. The call routing process is shown in Figure 3. However, most call routing decisions require data that spans across the entire system, such as total minutes used by an ingress carrier across all its points of presence (POPs) in the network. The local system would have to be connected to a network OSS.

A *directory gatekeeper* host connects to a global OSS and triggers the GKTMP server application after receiving an inbound location request (LRQ), as shown in Figure 4. All calls, whether from local or remote zones, pass through the directory gatekeeper, making call routing more efficient.

Figure 3 Call Routing Process for a Zone Gatekeeper

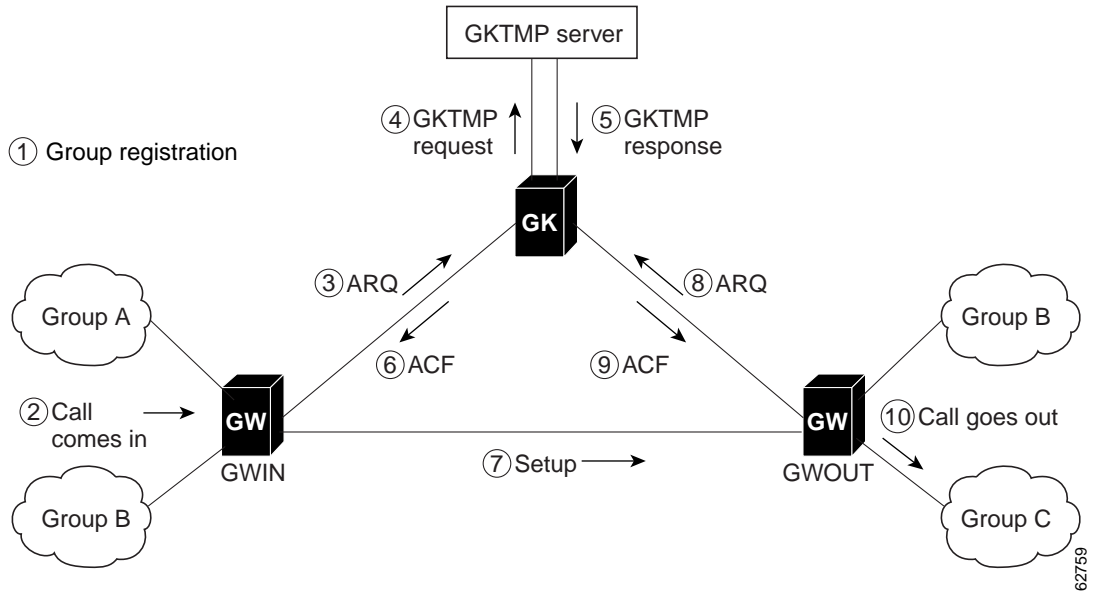


Table 1 explains the steps in the zone gatekeeper call routing process. For clarity, assume the calling party (ANI) is 1234 and the called party (DNIS) is 5678. Groups A, B, and C have circuit identifiers GroupA, GroupB, and GroupC, respectively. (Circuit identifiers represent trunk group labels or carrier IDs.)

Table 1 Call Routing Process for a Zone Gatekeeper

Step	Description
1. The circuit identifiers are registered with the gatekeeper using RRQ messages.	The ingress gateway GWIN registers circuit identifiers GroupA and GroupB and the egress gateway GWOUT registers circuit identifiers GroupB and GroupC.
2. The call comes in to the gateway.	The call arrives at GWIN on GroupA. ANI = 1234 and DNIS = 5678. <div style="border: 1px solid black; padding: 5px;"> <p>Note These ANI and DNIS numbers would be translated if the gateway is configured to do that. See <i>Gateway Trunk and Carrier Based Routing Enhancements</i> for a description of the number translation processes.</p> </div>
3. ARQ	The GWIN sends an ARQ message to the gatekeeper containing: <ul style="list-style-type: none"> • srcInfo=1234 • dstInfo=5678 • sourceCircuitID=GroupA • destinationCircuitID=NULL

Table 1 Call Routing Process for a Zone Gatekeeper (continued)

Step	Description
4. GKTMP Request REQUEST-ARQ	The gatekeeper sends a GKTMP Request message to the GKTMP server application containing: <ul style="list-style-type: none"> • srcInfo=1234 • dstInfo=5678 • sourceCarrier/source TrunkGroup=GroupA • destinationCarrier/destination TrunkGroup=NULL
5. GKTMP Response RESPONSE-ARQ	The GKTMP server application searches its databases for the appropriate route and returns a GKTMP Response message to the gatekeeper containing: <ul style="list-style-type: none"> • srcInfo=1234 • dstInfo=5678 • sourceCarrier/source TrunkGroup=GroupA • destinationCarrier/destination TrunkGroup=GroupC
6. ACF	The gatekeeper sends an ACF message to the GWIN containing: <ul style="list-style-type: none"> • CSA=GWOUT • sourceCircuitID=GroupA • destinationCircuitID=GroupC
7. H.225 Setup	The gateway sends a Setup message to the GWOUT containing: <ul style="list-style-type: none"> • srcInfo=1234 • dstInfo=5678 • sourceCircuitID=GroupA • destinationCircuitID=GroupC
8. ARQ	The GWOUT sends a verifying ARQ message to the gatekeeper containing: <ul style="list-style-type: none"> • answerCall=TRUE • srcInfo=1234 • dstInfo=5678 • sourceCircuitID=GroupA • destinationCircuitID=GroupC
9. ACF	The gatekeeper sends an ACF message back to the GWOUT.
10. The call goes out the destination gateway.	The GWOUT sends the call out on GroupC.

Figure 4 Call Routing Process for a Directory Gatekeeper

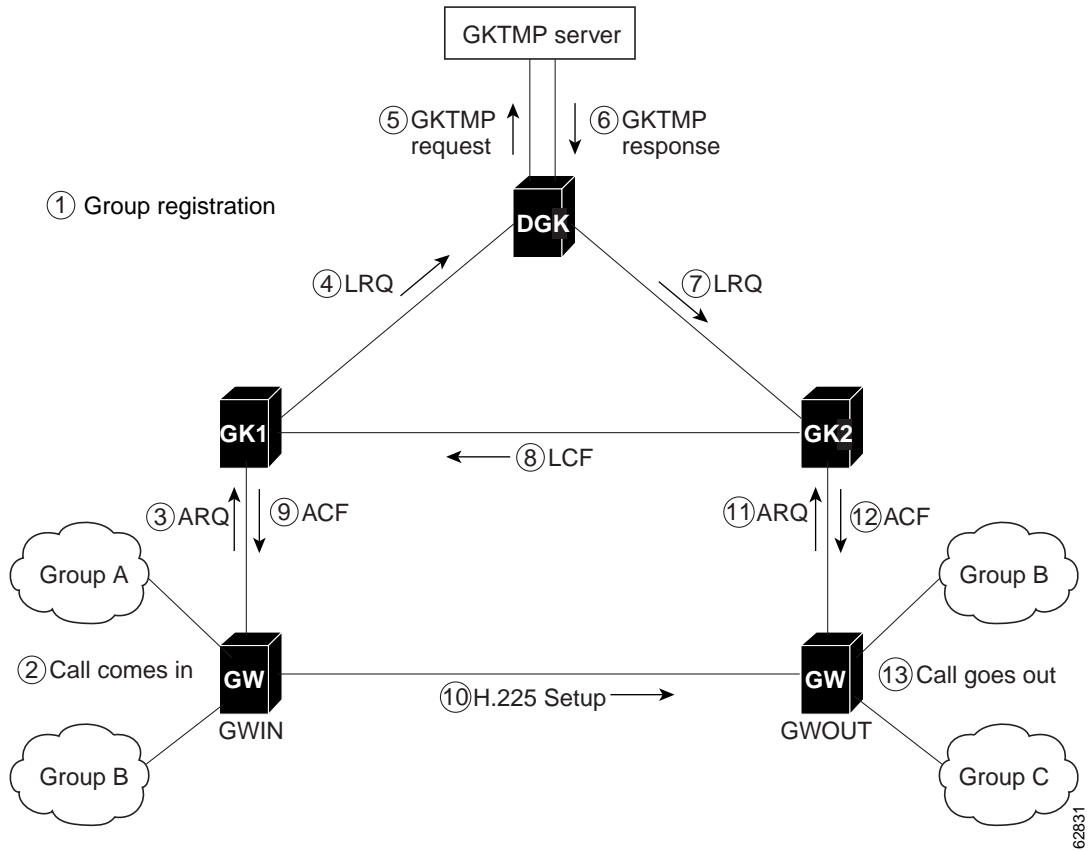


Table 2 explains the steps in the directory gatekeeper call routing process. For clarity, assume the calling party (ANI) is 1234 and the called party (DNIS) is 5678. Groups A, B, and C have circuit identifiers GroupA, GroupB, and GroupC, respectively. (Circuit identifiers represent trunk group labels or carrier IDs.)

Table 2 Call Routing Process for a Directory Gatekeeper

Step	Description
1. The circuit identifiers are registered using RRQ messages.	The zone gatekeepers GK1 and GK2 create a list of registered circuit identifiers.
1a. Ingress Zone	GWIN registers circuit identifiers GroupA and GroupB with the ingress zone gatekeeper GK1.
1b. Egress Zone	GWOUT registers circuit identifiers GroupB and GroupC with the egress zone gatekeeper GK2.
2. The call comes into the gateway.	The call arrives at GWIN on GroupA, ANI = 1234 and DNIS = 5678.

Table 2 Call Routing Process for a Directory Gatekeeper (continued)

Step	Description
3. ARQ	The GWIN sends an ARQ message to GK1 containing: <ul style="list-style-type: none"> • srcInfo=1234 • dstInfo=5678 • sourceCircuitID=GroupA • destinationCircuitID=NULL
4. LRQ	GK1 is configured for forwarding all route requests to the directory gatekeeper (DGK). GK1 sends an LRQ message to the DGK containing: <ul style="list-style-type: none"> • srcInfo=1234 • dstInfo=5678 • sourceCircuitID=GroupA • destinationCircuitID=NULL
5. GKTMP Request REQUEST-LRQ	GK1 sends a GKTMP Request message to the GKTMP server application containing: <ul style="list-style-type: none"> • srcInfo=1234 • dstInfo=5678 • sourceCarrier/source TrunkGroup=GroupA • destinationCarrier/destination TrunkGroup=NULL
6. GKTMP Response RESPONSE-LRQ	The GKTMP server application searches its databases for the appropriate route and returns a GKTMP Response message to GK1 containing: <ul style="list-style-type: none"> • srcInfo=1234 • dstInfo=5678 • sourceCarrier/source TrunkGroup=GroupA • destinationCarrier/destination TrunkGroup=GroupC with the remote zone gatekeeper's (GK2's) RAS address
7. LRQ	The DGK sends an LRQ message to GK2 containing: <ul style="list-style-type: none"> • srcInfo=1234 • dstInfo=5678 • sourceCircuitID=GroupA • destinationCircuitID=GroupC
8. LCF	GK2 sends an LCF message to GK1 containing: <ul style="list-style-type: none"> • CSA=GWOUT • sourceCircuitID=GroupA • destinationCircuitID=GroupC

Table 2 Call Routing Process for a Directory Gatekeeper (continued)

Step	Description
9. ACF	GK1 sends an ACF message to GWIN containing: <ul style="list-style-type: none"> • CSA=GWOUT • sourceCircuitID=GroupA • destinationCircuitID=GroupC
10. H.225 Setup	GWIN sends a Setup message to GWOUT containing: <ul style="list-style-type: none"> • srcInfo=1234 • dstInfo=5678 • sourceCircuitID=GroupA • destinationCircuitID=GroupC
11. ARQ	GWOUT sends a verifying ARQ message to GK2 containing: <ul style="list-style-type: none"> • answerCall=TRUE • srcInfo=1234 • dstInfo=5678 • sourceCircuitID=GroupA • destinationCircuitID=GroupC
12. ACF	GK2 sends an ACF message back to GWOUT.
13. The call goes out the destination gateway.	GWOUT sends the call out on GroupC.

Call Routing on the Gateway

The gateway receives calls on the PSTN side through a single voice port interface (DS-0) or a logical group of physical interfaces (DS-0 or DS-1) called a *trunk group*. This feature allows you to route calls by trunk groups or by carriers. To route by carriers, you assign the trunk groups to carriers and specify an identifier or descriptor to each carrier. A carrier can have several trunk groups assigned to it.



Note Trunk group and dial peer enhancements and their configuration on the gateway are described in detail in *Gateway Trunk and Carrier Based Routing Enhancements*.

After receiving the routing information in the admission confirm (ACF) message from the gatekeeper, the gateway sends the call to the next gateway.

Registering with the Gatekeeper

For each carrier assigned to it, the gateway sends to its gatekeeper the carrier ID, the maximum number of calls the carrier can handle, and the number of currently available calls on the carrier. The gatekeeper and the GKTMP server application use this data to determine an appropriate route for an incoming call.

This feature also allows call routing using the trunk groups configured on the gateway without assigning the trunk groups to carriers. The gateway sends the call capacity information for each trunk group to the gatekeeper for route processing. Trunk group routing requires that all trunk groups on a gateway be identified using a trunk group identifier rather than a carrier identifier.



Note The gateway uses the capacities field in the H.323 Version 4 Registration Request (RRQ) message to register the maximum call capacity for each trunk group or carrier. H.323 Version 4 allows the capacities field to refer to several types of calls, such as voice, H.323, and T.120 data. For this feature, a gateway registers only voice calls.

Identifiers

In this document, *circuit identifier* refers to either a trunk group identifier or a carrier identifier.

A *source circuit identifier* specifies the trunk group or carrier sending the incoming PSTN call or the service provider sending an incoming VoIP call. The gateway sends this source circuit identifier, the calling party (ANI), and the called party number (DNIS) to the gatekeeper in the admission request (ARQ) RAS message.

If zones are used in the network, the gateway uses an inter-zone clearToken (IZCT) in the ARQ message to send the source zone identifier to gatekeeper.

Call Routing on the Gatekeeper

Receiving a Call Request

The gatekeeper receives source circuit identifiers from the gateway for circuits that are assigned to the gateway. Gateways send this information as part of the ARQ message.

For Cisco gateways running a Cisco IOS version prior to this release and non-Cisco gateways that cannot send circuit identifiers, this feature provides the gatekeeper with a CLI command (**endpoint circuit-id h323id**) that assigns a circuit identifier to the gateway. Using this command restricts the gateway to the specified circuit. Similarly, for VoIP calls coming to the gatekeeper from a non-Cisco gatekeeper and not from a gateway, this feature provides the gatekeeper with the **zone circuit-id** command that associates a circuit identifier to the zone and an IP address of the call origination.

Processing the Call Request

Once the gatekeeper receives the source circuit identifier, the ANI number, and the DNIS number, it works with the GKTMP server application to determine the *destination circuit identifier*, which specifies the PSTN or service provider resource to be used for the outgoing call.

The gatekeeper sends a GKTMP message to the GKTMP server application with the ARQ data. The GKTMP server application searches its databases for an one or more egress circuits, and sends the destination circuit identifier back to the gatekeeper in a RESPONSE ARQ message.

If zones are used in the network, the GKTMP server application may determine that the egress circuit is in another zone. In that case, GKTMP server sends back a remote zone list with the RESPONSE ARQ message.

The gatekeeper uses the destination circuit identifiers and any zone lists to locate an available egress gateway for the call. The gatekeeper checks local gateways first. If none are available and GKTMP server sent remote zones, the gatekeeper sends a location request (LRQ) message to the gatekeeper in each zone on the list to find an available gateway. The LRQs are sent in sequential order and the circuits are sorted in priority order. A gatekeeper with an available egress gateway sends back an acknowledge confirmed (ACF) message to the original gatekeeper.

When a gatekeeper receives an LRQ, it tries to find an egress gateway that supports the circuit identifier. If the LRQ does not include any destination circuit information, the gateway uses the zone definitions and technology prefixes (identifiers for gateways in a zone) to determine an egress circuit. If the gatekeeper must return an LRQ in response to the received LRQ, **lrq forward-queries** must be enabled in its configuration.

Returning a Destination Endpoint

After finding an available egress gateway, the gatekeeper sends this information to the originating gateway in the admission confirm (ACF) RAS message.

If the egress gateway is in a remote zone, the gatekeeper includes an IZCT with the destination zone and the *intermediate circuit identifier* in the ACF message. The intermediate circuit identifier specifies the carrier or trunk group of the gateway in the next zone to handle the call. The gatekeeper also sends IZCTs for any alternate endpoints.

GKTMP Server Call Routing



Note

This section provides a general overview of the GKTMP server application. For detailed information about the GKTMP server application, its installation, and its programming, refer to the documents that come with the GKTMP server application.

The GKTMP server application is user-programmable software that runs on a Sun server. GKTMP server sits behind a Cisco IOS gatekeeper. GKTMP server and the gatekeeper communicate using GKTMP. When the gatekeeper sends the GKTMP server an ARQ or LRQ message, the message is formatted into the GKTMP format before the GKTMP server application processes it. Similarly, the GKTMP server application returns its search results in GKTMP format, which is translated back into an ARQ or LRQ message and sent to the gatekeeper.

GKTMP server extracts the source circuit identifier and called party (DNIS) information from the gatekeeper's ARQ message and, in the case of network zones, the IZCT. After searching its databases with user-defined rules, the GKTMP server returns the primary destination circuit identifier and a zone list, if needed, for the primary circuit and any secondary circuits that may be used for routing the call.

The GKTMP server application itself is a set of translation rules that determine the destination circuit identifier and optional zone lists. Each rule consists of a processing definition and data. Three types of rules are specified:

- Origination circuit rejection rule—When triggered, this rule causes the call to be rejected.
- Termination circuit rejection rule—When triggered, this rule eliminates a destination circuit from further consideration while allowing consideration of other destination circuits.
- Termination selection rule—When triggered, this rule selects the best circuit to terminate the call.

The user must provision the GKTMP server application with the following data:

- Circuits in the network
- Destination patterns
- Egress costing attributes
- Ingress costing attributes
- Zones in the network
- Rules for selecting and rejecting destination circuits

The GKTMP server application has GUI commands for maintaining this network data.

Static Triggers

By default, the Cisco IOS gatekeeper does not forward any RAS messages to any external applications, such as the GKTMP server application. If an application is interested in receiving certain RAS messages, it must register this interest with the gatekeeper. To determine which RAS messages the gatekeeper

forwards to the GKTMP server application, you can specify trigger parameters. If the gatekeeper receives a message that satisfies the specified trigger conditions, the message is forwarded to the GKTMP server application. If the message does not meet the trigger conditions, the gatekeeper processes the message according to its usual instructions, but the GKTMP server application does not receive that message.

If multiple trigger conditions are specified in a single registration message, the gatekeeper treats the trigger conditions as “OR” conditions. In other words, if a RAS message received by the gatekeeper meets any of the trigger conditions the message is sent to the GKTMP server application.

Trigger conditions are optional. If the gatekeeper receives a registration that contains no trigger conditions, the gatekeeper forwards all messages of the specified RAS message type to the GKTMP server application.

If the gatekeeper has a registration for a RAS message type and receives another registration for the same RAS message from the same GKTMP server with the same priority, the gatekeeper uses the new registration and discards the previous one. The gatekeeper allows registrations for the same RAS message type with the same priority from multiple servers.

To indicate that the external application is no longer interested in a message, it must unregister its interest. The contents of the unregistration message must match that of the corresponding registration message before the trigger can be removed.

A Cisco IOS gatekeeper can be statically (through a command-line interface) or dynamically (through the gatekeeper API) configured with trigger parameters.



Note

Triggers that are statically configured can be removed only through the command-line interface. Likewise, those triggers that are dynamically configured can be removed or modified only through the gatekeeper API.

Benefits

Improves Call Routing Flexibility

Through the creation of profiles, call routing is more flexible and easier to implement than it was before.

Improves VoIP Interconnect Support

This feature provides the scalability of VoIP interconnections and eases the implementation and maintenance of the networks.

Provides a Common Architecture

This feature is based on Cisco’s open architecture, which permits easier application development than proprietary environments.

Restrictions

Features Not Supported

- Ability to download carrier ID settings from the GKTMP server application, rather than configuring them on the gateway
- Support for ITSP-to-ITSP carrier sensitive routing
- Any H.323 Version 4 capabilities except call capacities

Static Triggers

Carrier-sensitive routing (CSR) does not accept static trigger request (REQ) messages. CSR sets up the triggers dynamically.

Related Features and Technologies

- Voice over IP (VoIP)
- Gateway Trunk and Carrier Based Routing Enhancements

Related Documents

General reference documents:

- [Cisco IOS Voice, Video, and Fax Configuration Guide](#), Release 12.2
- [Cisco IOS Voice, Video, and Fax Command Reference](#), Release 12.2

Feature documents:

- *Gateway Trunk and Carrier Based Routing Enhancements*
- *GKTMP Application Programmer's Interface Guide*

Related Feature Documents

- *Inter-Domain Gatekeeper Security Enhancement*

Supported Platforms

Gatekeepers

- Cisco 3660 multiservice platform
- Cisco 7200 series routers

Gateways

- Cisco 3660 multiservice platforms
- Cisco AS5300 universal access server
- Cisco AS5350 universal gateway
- Cisco AS5400 universal gateway
- Cisco AS5850 universal gateway

Supported Standards, MIBs, and RFCs

Standards

- ITU H.323 Version 4 (call capacities only)

MIBs

No new or modified MIBs are supported by this feature.

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

RFCs

No new or modified RFCs are supported by this feature.

Prerequisites

Complete these tasks before configuring the gatekeeper for trunk and carrier based routing enhancements feature functionality:

- Configure IP routing.

For more information on IP routing, refer to *Cisco IOS IP Configuration Guide*, Release 12.2

- Configure voice ports.

For more information on configuring voice ports, refer to *Cisco IOS Voice, Video, and Fax Configuration Guide*, Release 12.2

- Configure voice over IP.

For more information on configuring Voice over IP, refer to *Cisco IOS Voice, Video, and Fax Configuration Guide*, Release 12.2

- Configure trunks and dial peers on the gateway.

See *Gateway Trunk and Carrier Based Routing Enhancements* for the details on configuring the trunks and dial peers on the gateway.

- Configure the GKTMP server application.

Refer to the GKTMP server documentation for information and procedures.

Configuration Tasks

See the following sections for configuration tasks for this routing feature. Each task in the list is identified as either required or optional.

- [Configuring the Gatekeeper](#) (required)
- [Configuring Additional Gatekeeper Capabilities](#) (optional)
- [Verifying the Gatekeeper Configuration](#) (optional)

Configuring the Gatekeeper

To configure the gatekeeper, follow these steps beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# gatekeeper	Initiates gatekeeper configuration mode.
Step 2	Router(config-gk)# zone local <i>gatekeeper-name</i> <i>domain-name</i> [<i>ras-IP-address</i>]	Specifies the zone controlled by the gatekeeper.
Step 3	Router(config-gk)# no shutdown	Enables the gatekeeper.
Step 4	Router(config-gk)# server registration-port <i>port-number</i>	Configures the listener port for the server to establish a connection with the gatekeeper.
Step 5	Router(config-gk)# exit	Ends the gatekeeper configuration mode.

Configuring Additional Gatekeeper Capabilities

To configure the optional capabilities for the gatekeeper, follow these steps beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# gatekeeper	Initiates gatekeeper configuration mode.
Step 2	Router(config-gk)# gw-type-prefix <i>type-prefix</i> [[<i>hopoff gkid1</i>] [<i>hopoff gkid2</i>] [<i>hopoff gkidn</i>] [<i>seq</i> <i>blast</i>]] [<i>default-technology</i>] [[<i>gw ipaddr ipaddr</i> [<i>port</i>]] ...]	(Optional) Configures a technology prefix in the gatekeeper.
Step 3	Router(config-gk)# zone prefix <i>gatekeeper-name</i> <i>e164-prefix</i> [<i>blast</i> <i>seq</i>] [<i>gw-priority priority gw-alias</i> [<i>gw-alias, ...</i>]]	(Optional) Adds one or more prefixes to the gatekeeper zone list. Enter a separate command entry for each prefix.
Step 4	Router(config-gk)# zone remote <i>other-gatekeeper-name other-domain-name</i> <i>other-gatekeeper-ip-address</i> [<i>port-number</i>] [<i>cost cost-value</i> [<i>priority priority-value</i>]] [<i>foreign-domain</i>]	(Optional) Assigns a remote zone to an incoming call if a source carrier identifier is not available for the call.
Step 5	Router(config-gk)# zone circuit-id <i>remote-zone-name</i> <i>circuit-id</i>	(Optional) Assigns a circuit descriptor to a remote zone.
Step 6	Router(config-gk)# lrq reject-unknown-circuit	(Optional) Enables gatekeeper rejection of LRQ messages that contain an unknown destination circuit descriptor.
Step 7	Router(config-gk)# endpoint circuit-id <i>h323id</i> <i>endpoint-h323id circuit-id</i> [<i>max-calls number</i>]	(Optional) Assigns a circuit ID to a non-Cisco or an older Cisco endpoint for use by the GKTMP server application.
Step 8	Router(config-gk)# endpoint resource threshold <i>onset high-water-mark abatement low-water-mark</i>	(Optional) Sets call volume thresholds in the gatekeeper for monitoring its gateway.
Step 9	Router(config-gk)# server routing { <i>both</i> <i>carrier</i> <i>trunk-group</i> }	(Optional) Enables routing of only carrier or trunk-group information to the GKTMP server.
Step 10	Router(config-gk)# server flow-control [<i>onset</i> <i>high-water-mark</i> <i>abatement low-water-mark</i> <i>qcount</i> <i>number</i>]	(Optional) Turns on flow control and failure detection in the gatekeeper.

	Command	Purpose
Step 11	<pre>Router(config-gk)# server trigger arq <i>gkid priority server-id server-ipaddress server-port</i> Router(config-gk)# server trigger brq <i>gkid priority server-id server-ipaddress server-port</i> Router(config-gk)# server trigger drq <i>gkid priority server-id server-ipaddress server-port</i> Router(config-gk)# server trigger irr <i>gkid priority server-id server-ipaddress server-port</i> Router(config-gk)# server trigger lcf <i>gkid priority server-id server-ipaddress server-port</i> Router(config-gk)# server trigger lrj <i>gkid priority server-id server-ipaddress server-port</i> Router(config-gk)# server trigger lrq <i>gkid priority server-id server-ipaddress server-port</i> Router(config-gk)# server trigger rai <i>gkid priority server-id server-ipaddress server-port</i> Router(config-gk)# server trigger rrq <i>gkid priority server-id server-ipaddress server-port</i> Router(config-gk)# server trigger urq <i>gkid priority server-id server-ipaddress server-port</i></pre>	(Optional) Statically configures the RAS triggers on the gatekeeper. Each trigger type has submode commands that are used for configuring trigger conditions.
Step 12	<pre>Router(config-gk)# security izct password <i>password</i>}</pre>	(Optional) Enables IZCT authentication and authorization on the gatekeeper.
Step 13	<pre>Router(config-gk)# security {password default <i>password</i> password separator <i>character</i>}</pre>	(Optional) Enables a security password for the authentication and authorization function on the gatekeeper.
Step 14	<pre>Router(config-gk)# exit</pre>	Ends gatekeeper configuration mode.

Verifying the Gatekeeper Configuration

Use the following commands to verify the gatekeeper configuration. Refer to the command's reference page later in this document for sample output and its description.

Command	Description
show run	Displays the current gatekeeper configuration.
show gatekeeper circuits	Displays information about the circuits (carriers) registered with the gatekeeper.
show gatekeeper endpoint circuits	Displays information about the endpoint circuits registered with the gatekeeper.
show gatekeeper servers	Displays information about the servers registered with the gatekeeper.

Monitoring and Maintaining

Command	Description
Router# <code>debug cch323 capacity</code>	Tracks and displays the call capacity on the gatekeeper.
Router# <code>show run</code>	Displays the current gatekeeper configuration.

Configuration Examples

This section provides the following configuration examples:

```
Router# show run

Current configuration : 1628 bytes
!
version 12.2
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname alpha
!
logging buffered 500000 debugging
logging rate-limit console 10 except errors
!
memory-size iomem 20
ip subnet-zero
!
!
!
no ip dhcp-client network-discovery
!
!
!
!
!
interface Ethernet0/0
 ip address 172.18.125.10 255.255.0.0
 no ip route-cache
 no ip mroute-cache
 half-duplex
 no cdp enable
!
interface Serial0/0
 no ip address
 no ip mroute-cache
 shutdown
 no fair-queue
!
interface Ethernet0/1
 no ip address
 shutdown
 half-duplex
!
interface Serial0/1
 no ip address
 shutdown
!
```

```

interface Serial0/2
  no ip address
  shutdown
  !
ip classless
ip route 0.0.0.0 0.0.0.0 172.18.125.1
ip http server
!
snmp-server packetsize 4096
!
dial-peer cor custom
!
!
!
dial-peer voice 1 pots
  destination-pattern 5666001
!
dial-peer voice 2 pots
!
dial-peer voice 100 pots
  destination-pattern 103
!
dial-peer voice 123 pots
  destination-pattern 5553007
!
dial-peer voice 3141 pots
!
!
gatekeeper
  zone local alpha zebra.com 172.18.125.10
  zone remote beta zebra.com 172.18.125.10 1719 foreign-domain
  zone prefix beta 319...
  zone prefix alpha 387... gw-priority 10 gateway-1
  zone prefix alpha 5553001* gw-priority 8 gateway-east
  zone prefix alpha 5553002* gw-priority 7 gateway-west
  security izct password myname
  gw-type-prefix 1#* default-technology gw ipaddr 172.18.138.69 1720
  no shutdown
  server registration-port 5055
!
!
line con 0
  exec-timeout 0 0
line aux 0
line vty 0 4
  password lab
  login
line vty 5 15
  login
!
!
end

```

Command Reference

This section documents new and modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.2 command reference publications.

New Commands

- [debug cch323 capacity](#)
- [endpoint circuit-id h323id](#)
- [endpoint resource threshold](#)
- [lrq reject-unknown-circuit](#)
- [server flow-control](#)
- [server routing](#)
- [show gatekeeper circuits](#)
- [zone circuit-id](#)

Modified Commands

- [gw-type-prefix](#)
- [security](#)
- [server registration-port](#)
- [server trigger arq](#)
- [server trigger brq](#)
- [server trigger drq](#)
- [server trigger irr](#)
- [server trigger lcf](#)
- [server trigger lrj](#)
- [server trigger lrq](#)
- [server trigger rai](#)
- [server trigger rrq](#)
- [server trigger urq](#)
- [show gatekeeper endpoint circuits](#)
- [show gatekeeper endpoints](#)
- [show gatekeeper servers](#)
- [zone local](#)
- [zone prefix](#)
- [zone remote](#)

debug cch323 capacity

To track the call capacity on the gatekeeper, use the **debug cch323 capacity** command in privileged EXEC mode. To turn off debugging, use the **no** form of this command.

debug cch323 capacity

no debug cch323 capacity

Syntax Description This command has no keywords or arguments.

Defaults No default behavior or values

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(2)XU	This command was introduced.

Usage Guidelines Use the **debug cch323 capacity** command to track the maximum and current call capacity values in the RAS messages and to debug capacity-related problems while sending RAS messages. The command lists the values for current and maximum call capacity provided by the trunk group capacity resource manager if and when the H.323 Service Provider Interface (SPI) requests the information for all or specific groups of circuits.

Examples The following example illustrates the debug output. Descriptions of the output follow the example.

```
Router# debug cch323 capacity
Call Capacity Information tracing is enabled

5d00h: cch323_process_carrier_update: Registered = 0x, Event = 1,
      Reason = 1
5d00h: cch323_process_carrier_update: CarrierId = CARRIERA_NEWENGLAND
5d00h: cch323_fill_crm_CallCapacities: Reason = 1, Carrier_ID = CARRIERA_NEWENGLAND
5d00h: cch323_fill_crm_CallCapacities: MAX_CAPACITY:Max = 0, In_voice = 0, Out_voice = 0,
      In_data = 0, Out_data = 0,
      CURR_CAPACITY:Max = 0, In_voice = 0, Out_voice = 0,
      In_data = 0, Out_data = 0
      Egress Disconnect pending = 2
```

The gatekeeper displays this output when trunk groups are added, deleted, or modified or when circuits in a trunk group are deactivated or activated (similar to ISDN layer 2 down/up).

```
5d00h: cch323_process_carrier_update: Registered = 0, Event = 1,
      Reason = 1
5d00h: cch323_process_carrier_update: CarrierId = CARRIERA_NEWENGLAND
```

Table 3 describes the fields shown in this section of the **debug cch323 capacity** sample output:

Table 3 *debug cch323 capacity Update Fields*

Field	Description
Registered	Gateway registration: <ul style="list-style-type: none"> • 0=gateway is not registered to the gatekeeper • 1=gateway is registered to the gatekeeper at the time of the change
Event	Carriers updated: <ul style="list-style-type: none"> • 0=all carriers updated • 1=single carrier updated
Reason	Reason for the update notification: <ul style="list-style-type: none"> • 0=CURRENT_CAPACITY_UPDATE • 1=MAX_CAPACITY_UPDATE • 2=BOTH_CAPACITY_UPDATE
CarrierID	ID of the trunk group or carrier to which the change applies.

The gatekeeper displays this output whenever call capacity information is sent to the gatekeeper.

```
5d00h: cch323_fill_crm_CallCapacities: MAX_CAPACITY:Max = 0, In_voice = 0, Out_voice = 0,
      In_data = 0, Out_data = 0,
      CURR_CAPACITY:Max = 0, In_voice = 0, Out_voice = 0,
      In_data = 0, Out_data = 0
      Egress Disconnect pending = 2
```

Table 4 describes the fields shown in this section of the **debug cch323 capacity** sample output:

Table 4 *debug cch323 capacity Call Capacity Fields*

Field	Description
MAX_CAPACITY	Indicates the values for maximum capacity.
Max	Maximum physical (or configured) circuits.
In_voice	Count of allowed incoming voice calls.
Out_voice	Count of allowed outgoing voice calls.
In_data	Count of allowed incoming data calls.
Out_data	Count of allowed outgoing data calls.
CURR_CAPACITY	Indicates the values for current used capacity.
Max	Maximum physical (or configured) circuits. This field is not used for current capacity computation.
In_voice	Count of active incoming voice calls.
Out_voice	Count of active outgoing voice calls.
In_data	Count of active incoming data calls.

Table 4 *debug cch323 capacity Call Capacity Fields (continued)*

Field	Description
Out_data	Count of active outgoing data calls.
Egress Disconnect pending	Count of calls released on the H.323 side to which the telephony circuits are yet to be idled.

Based on the values in this example, the RAS call capacities values are:

```

maximumCallCapacity
{
  voiceGwCallsAvailable
  {
    {
      calls 23
      group "CARRIERA_NEWENGLAND"
    },
  }
}
currentCallCapacity
{
  voiceGwCallsAvailable
  {
    {
      calls 1
      group "CARRIERA_NEWENGLAND"
    }
  }
}

```

Related Commands

Command	Description
endpoint circuit-id h323id	Associates a carrier with a non-Cisco endpoint.

endpoint circuit-id h323id

To associate a circuit with an older Cisco or a non-Cisco endpoint, use the **endpoint circuit-id h323id** command in gatekeeper configuration mode. To delete the association, use the **no** form of this command.

endpoint circuit-id h323id *endpoint-h323id* *circuit-id* [**max-calls** *number*]

no endpoint circuit-id h323id *endpoint-h323id* *descriptor* [**max-calls** *number*]

Syntax Description		
	<i>endpoint-h323id</i>	Specifies the ID of the H.323 endpoint.
	<i>circuit-id</i>	Specifies the circuit assigned to the H.323 endpoint.
	max-calls <i>number</i>	(Optional) Specifies the maximum number of calls this endpoint can handle. Valid values are 1 to 10000.

Defaults No default behavior or values

Command Modes Gatekeeper configuration

Command History	Release	Modification
	12.2(2)XU	This command was introduced.

Usage Guidelines The **endpoint circuit-id h323id** command allows the gatekeeper and GKTMP server application to work with Cisco gateways running a Cisco IOS version prior to this release and non-Cisco gateways that cannot identify incoming circuits. This command permits only one circuit to be associated with the endpoint.

Examples The following example associates a non-Cisco endpoint **first** with a circuit **westcoast**, and assigns a maximum of 2750 calls to the endpoint:

```
Router(config)# gatekeeper
Router(config-gk)# endpoint circuit-id h323-id first westcoast maxcalls 2750
```

Related Commands	Command	Description
	show gatekeeper endpoint circuits	Displays the information of all registered endpoints for a gatekeeper.

endpoint resource threshold

To set a gateway's call capacity thresholds in the gatekeeper, use the **endpoint resource threshold** command in gatekeeper configuration mode. To delete the thresholds, use the **no** form of this command.

endpoint resource threshold [*onset high-water-mark* | **abatement** *low-water-mark*]

no endpoint resource threshold [*onset high-water-mark* | **abatement** *low-water-mark*]

Syntax Description	onset <i>high-water-mark</i>	(Optional) Specifies the gateway's maximum call volume usage, as a percent. Valid values are 1 to 99 percent.
	abatement <i>low-water-mark</i>	(Optional) Specifies the gateway's minimum call volume usage, as a percent. Valid values are 1 to 99 percent.

Defaults	High-water-mark: 90 percent Low-water-mark: 70percent
----------	--

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

Command History	Release	Modification
	12.2(2)XU	This command was introduced.

Usage Guidelines	<p>The gatekeeper monitors the call volume in each of its gateways. If the call volume usage in a particular gateway exceeds the high-water-mark threshold, the gatekeeper stops sending calls to that gateway. When the gateway's active call volume falls below the low-water-mark threshold, the gatekeeper resumes sending new calls to the gateway.</p> <p>These thresholds are global values and affect all gateways registered with the gatekeeper.</p> <p>If neither threshold is set, the gatekeeper uses the default values.</p>
------------------	--

Examples	The following example sets the high and low call volume thresholds for all of its gateways:
----------	---

```
Router(config)# gatekeeper
Router(config-gk)# endpoint resource-threshold onset 85 abatement 65
```

Related Commands	Command	Description
	show gatekeeper endpoint circuits	Displays the information of all registered endpoints for a gatekeeper.

gw-type-prefix

To configure a technology prefix in the gatekeeper, use the **gw-type-prefix** command in gatekeeper configuration mode. To remove the technology prefix, use the **no** form of this command.

```
gw-type-prefix type-prefix [[hopoff gkid1] [hopoff gkid2] [hopoff gkidn] [seq | blast]]
[default-technology] [[gw ipaddr ipaddr [port]]...]
```

```
no gw-type-prefix type-prefix [[hopoff gkid1] [hopoff gkid2] [hopoff gkidn] [seq | blast]]
[default-technology] [[gw ipaddr ipaddr [port]]...]
```

Syntax Description	
<i>type-prefix</i>	A technology prefix is recognized and is stripped before checking for the zone prefix. Cisco strongly recommends that you select technology prefixes that are clearly distinct from zone prefixes. To avoid confusion, use the # character to terminate technology prefixes, for example, 3#.
hopoff <i>gkid</i>	(Optional) Use this option to specify the gatekeeper where the call is to hop off, regardless of the zone prefix in the destination address. The <i>gkid</i> argument refers to a gatekeeper previously configured using the zone local or zone remote command. You can enter this keyword and argument multiple times to configure redundant gatekeepers for a given technology prefix.
seq blast	(Optional) If you list multiple hopoffs, this setting indicates that the LRQs should be sent sequentially (seq) or simultaneously (blast) to the gatekeepers according to the order in which they were listed. The default is seq .
default-technology	(Optional) Gateways registering with this prefix option are used as the default for routing any addresses that are otherwise unresolved.
gw ipaddr <i>ipaddr</i> [<i>port</i>]	(Optional) Use this option to associate a gateway with the technology prefix. <i>ipaddr</i> is the IP address of the gateway to associate with the prefix and <i>port</i> is the gateway's call signaling port. This option is available for gateways that are incapable of registering technology prefixes. When a gateway registers, the gatekeeper adds the gateway to the group for this type prefix. This parameter can be repeated to associate more than one gateway with a technology prefix.

Defaults By default, no technology prefix is defined, and LRQs are sent sequentially to all the gatekeepers listed.

Command Modes Gatekeeper configuration

Command History	Release	Modification
	11.3(6)NA2	This command was introduced on the Cisco 2500 and Cisco 3600 series routers and the Cisco AS5300 universal access server.
	12.1(1)T	This command was modified to allow the user to specify multiple hopoffs.

Release	Modification
12.1(2)T	This command was modified to allow the user to specify whether LRQs should be sent simultaneously or sequentially to the gatekeepers.
12.2(2)XU	This command was extended to the Cisco 2600 series, Cisco MC3810, and Cisco 7200 platforms.

Usage Guidelines

More than one gateway can register with the same technology prefix. In such cases, a random selection is made of one of them.

You do not have to define a technology prefix to a gatekeeper if there are gateways configured to register with that prefix and if there are no special flags (**hopoff gkid** or **default-technology**) that you want to associate with that prefix.

You need to configure the gateway type prefix of all remote technology prefixes that will be routed through this gatekeeper.

Examples

The following example defines two gatekeepers for technology zone 3:

```
Router(config)# gatekeeper
Router(config-gk)# gw-type-prefix 3#* hopoff c2600-1-gk hopoff c2514-1-gk
```

Related Commands

Command	Description
show gatekeeper gw-type-prefix	Displays the list of currently defined technology zones and the gatekeepers responsible for each.
zone prefix	Configures the gatekeeper with knowledge of its own prefix and the prefix of any remote zone.

lrq reject-unknown-circuit

To enable the gatekeeper to reject an LRQ message containing an unknown destination circuit, use the **lrq reject-unknown-circuit** command in gatekeeper configuration mode. To disable the rejection, use the **no** form of this command.

lrq reject-unknown-circuit

no lrq reject-unknown-circuit

Syntax Description This command has no keywords or arguments.

Defaults Disabled

Command Modes Gatekeeper configuration

Release	Modification
12.2(2)XU	This command was introduced.

Usage Guidelines The gatekeeper checks the destination circuit field in each location request (LRQ) message. If the field contains a circuit unknown to the gatekeeper and **lrq reject-unknown-circuit** is enabled, the gatekeeper rejects the LRQ request. If **lrq reject-unknown-circuit** is disabled, the gatekeeper tries to resolve the alias without considering the circuit.

Examples The following example enables gatekeeper rejection of unknown carriers in an LRQ request:

```
Router(config)# gatekeeper
Router(config-gk)# lrq reject-unknown-circuit
```

Command	Description
show gatekeeper endpoint circuits	Displays the information of all registered endpoints for a gatekeeper.
endpoint circuit-id h323id	Assigns a circuit to a non-Cisco endpoint.

security

To enable authentication and authorization on a gatekeeper, use the **security** command in gatekeeper configuration mode. To disable security, use the **no** form of this command.

security { **any** | **h323-id** | **e164** } { **password default** *password* | **password separator** *character* }

no security { **any** | **h323-id** | **e164** } { **password default** *password* | **password separator** *character* }

Syntax Description		
any		Uses the first alias of an incoming registration, admission, and status (RAS) protocol registration, regardless of its type, as the means of identifying the user to RADIUS/TACACS+.
h323-id		Uses the first H.323 ID type alias as the means of identifying the user to RADIUS/TACACS+.
e164		Uses the first E.164 address type alias as the means of identifying the user to RADIUS/TACACS+.
password default <i>password</i>		Specifies the default password that the gatekeeper associates with endpoints when authenticating them with an authentication server. The <i>password</i> must be identical to the password on the authentication server.
password separator <i>character</i>		Specifies the character that endpoints use to separate the H.323-ID from the piggybacked password in the registration. Specifying this character allows each endpoint to supply a user-specific password. The separator character and password will be stripped from the string before it is treated as an H.323-ID alias to be registered. Note that passwords may only be piggybacked in the H.323-ID, not the E.164 address, because the E.164 address allows a limited set of mostly numeric characters. If the endpoint does not wish to register an H.323-ID, it can still supply an H.323-ID consisting of just the separator character and password. This H.323-ID consisting of just the separator character and password will be understood to be a password mechanism and no H.323-ID will be registered.

Defaults No default behavior or values

Command Modes Gatekeeper configuration

Command History	Release	Modification
	11.3(2)NA	This command was introduced.
	12.2(2)XU	This command was extended to the Cisco 3660 and Cisco 7200 platforms.

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. Although the **no security password** command undefines the password mechanism, it leaves the security type unchanged, so security is still enabled. However, the **no security** command disables security entirely, including removing any existing password definitions.

Examples

The following example enables identification of registrations using the first H.323 ID found in any registration:

```
Router(config)# gatekeeper
Router(config-gk)# security h323id
```

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

```
Router(config)#gatekeeper
Router(config-gk)# security h323-id
Router(config-gk)# security password qwerty2x
```

The next example enables security, authenticating all users by using their H.323-IDs and the password entered by the user in the H.323-ID alias he or she registers:

```
Router(config)#gatekeeper
Router(config-gk)# security h323-id
Router(config-gk)# security password separator !
```

Now 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 point is not found, the user is authenticated with the default password, or a null password if no default has been configured.

The following example enables security, authenticating all users by using their E.164 IDs and the password entered by the user in the H.323-ID alias he or she registers:

```
Router(config)#gatekeeper
Router(config-gk)# security e164
Router(config-gk)# security password separator !
```

Now if a user registers with an E.164 address of 5551212 and an H.323-ID of !hs8473q6, the gatekeeper authenticates user 5551212 and password hs8473q6. Because the H.323-ID string supplied by the user begins with the separator character, no H.323-ID is registered, and the user is known only by the E.164 address.

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.

server flow-control

To enable the gatekeeper to monitor flow control and failure detection on the server, use the **server flow-control** command in gatekeeper configuration mode. To disable flow control, use the **no** form of this command.

server flow-control [**onset** *high-water-mark* | **abatement** *low-water-mark* | **qcount** *number*]

no server flow-control [**onset** *high-water-mark* | **abatement** *low-water-mark* | **qcount** *number*]

Syntax Description

onset <i>high-water-mark</i>	Specifies the maximum server usage as a percent of the maximum delay tolerated. Valid values are 1 percent to 100 percent.
abatement <i>low-water-mark</i>	Specifies the minimum server usage as a percent of the maximum delay tolerated. Valid values are 1 percent to 100 percent.
qcount <i>number</i>	Specifies the number of messages waiting to be delivered to the server. Valid values are 1 to 2000.

Defaults

onset high-water-mark: 80 percent
 abatement low-water-mark: 50 percent
 qcount messages: 400 messages

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.2(2)XU	This command was introduced.

Usage Guidelines

The gatekeeper monitors two characteristics of the GKTMP server:

- How much the server is being used, as a percentage of its total capacity
- The number of messages waiting to be sent to the server.

When the server usage exceeds the high-water-mark value or when the number of waiting messages exceeds the configured number, the gatekeeper stops sending messages to the server. When the server's usage falls below the low-water-mark value or when the number of waiting messages falls below the specified number, the gatekeeper resumes sending messages to the server.

Examples

The following example enables flow control on the gatekeeper:

```
Router(config)# gatekeeper
Router(config-gk)# server flow-control onset 85 abatement 45 qcount 500
```

Related Commands	Command	Description
	show gatekeeper servers	Displays the triggers configured on the gatekeeper.

server registration-port

To configure the listener port on the gatekeeper for establishing connections with the server, use the **server registration-port** command in gatekeeper configuration mode. To force the gatekeeper to close the listening socket so that no more new registrations take place, use the **no** form of this command.

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

No registration port is configured.



Note If the gatekeeper is to communicate with network servers, a registration port must be configured on it.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(2)XU	This command was extended to the Cisco 3660 and Cisco 7200 platforms.

Usage Guidelines

Use this command to configure a server registration port that polls 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

The following example port 20000 as the gatekeeper's listening port that servers use to register with the gatekeeper:

```
Router(config)# gatekeeper
Router(config-gk)# 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.
show gatekeeper servers	Displays the triggers configured on the gatekeeper.

server routing

To specify the type of circuit messages sent to the GKTMP server, use the **server routing** command in gatekeeper configuration mode. To return to the default, use the **no** form of this command.

server routing { **both** | **carrier** | **trunk-group** }

no server routing { **both** | **carrier** | **trunk-group** }

Syntax Description	both	Sends both types of information in the GKTMP messages.
	carrier	Sends only carrier information in GKTMP messages.
	trunk-group	Sends only trunk group information in GKTMP messages.

Defaults carrier

Command Modes Gatekeeper configuration

Command History	Release	Modification
	12.2(2)XU	This command was introduced.

Usage Guidelines Use the **server routing** command to route carrier and trunk group messages from the gatekeeper to the GKTMP server.

The **carrier** parameter uses the “I” and “J” tags in the GKTMP messages. The **trunk-group** parameter uses “P” and “Q” tags in the GKTMP messages. The **both** parameter sends both sets of tags.

Examples The following example enables trunk group information to be sent in GKTMP messages from the gatekeeper:

```
Router(config)# gatekeeper
Router(config-gk)# server routing trunk-group
```

Related Commands	Command	Description
	show gatekeeper servers	Displays the triggers configured on the gatekeeper.

server trigger arq

To configure the Admission Request (ARQ) trigger statically on the gatekeeper, use the **server trigger arq** command in gatekeeper configuration mode. Submode commands are available after entering the **server trigger arq** command. To delete a single static trigger on the gatekeeper, use the **no** form of this command. To delete all static triggers on the gatekeeper, use the **all** form of the command.

server trigger arq *gkid* *priority* *server-id* *server-ipaddress* *server-port*

submode commands:

info-only

shutdown

destination-info { **e164** | **email-id** | **h323-id** } *value* |

redirect-reason *reason_number*

no server trigger arq *gkid* *priority* *server-id* *server-ipaddress* *server-port*

no server trigger all

Syntax Description

all	Deletes all CLI configured triggers.
<i>gkid</i>	The local gatekeeper identifier.
<i>priority</i>	The priority for each trigger. The range is 1 to 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.

Submode commands

After entering the **server trigger arq** command, the software enters a submode that permits you to configure additional filters on the RAS message. These filters are optional and you may configure any of them, one per command line.

info-only	Use the info-only submode command to indicate to the Cisco IOS gatekeeper that messages that meet the specified trigger parameters should be sent to the GKTMP server application as notifications only and that the gatekeeper should not wait for a response from the GKTMP server application.
shutdown	Use the shutdown submode command to temporarily disable a trigger. The gatekeeper does not consult triggers in a shutdown state when determining what message to forward to the GKTMP server application.

destination-info { e164 email-id h323-id } <i>value</i>	<p>Use the destination-info submode command to send ARQ RAS messages containing a specified destination to the GKTMP server application. Configure one of the following conditions</p> <ul style="list-style-type: none"> • e164—Indicates that the destination is an E.164 address. • email-id—Indicates that the destination is an e-mail ID. • h323-id—Indicates that the destination is an H.323 ID. • <i>value</i>—Specifies the value against which to compare the destination address in the RAS messages. For E.164 addresses, the following wildcards can be used: <ul style="list-style-type: none"> – A trailing series of periods, each of which represents a single character. – A trailing asterisk, which represents one or more characters.
redirect-reason <i>reason_number</i>	<p>Use the redirect-reason submode command to send ARQ RAS messages containing a specific redirect reason to the GKTMP server application.</p> <ul style="list-style-type: none"> • <i>reason_number</i>—Valid values are 0 to 65535. Currently-used values are: <ul style="list-style-type: none"> – 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

Defaults

No trigger servers are set

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(2)XB	The drq , rai , and brq triggers were added.
12.2(2)XU	The irr trigger was added and the command was extended to the Cisco 3660 and Cisco 7200 platforms.

Usage Guidelines

Use the **server trigger arq** command and its optional submode commands to configure the admission request (ARQ) static server trigger. The gatekeeper checks incoming gateway ARQ messages for the configured trigger information. If an incoming ARQ message contains the specified trigger information, the gatekeeper sends the ARQ message to the GKTMP server application. In addition, the gatekeeper processes the message according to its programmed instructions. If the ARQ message does not contain the specified information, the gatekeeper processes the message but does not send it to the GKTMP server application.

If no submode commands are configured for the ARQ messages, the gatekeeper sends all ARQ messages to the GKTMP server application.

If the gatekeeper receives an ARQ trigger registration message containing several trigger conditions, the conditions are treated as “OR” conditions. In other words, if an incoming ARQ RAS message meets any one of the conditions, the gatekeeper sends the RAS message to the GKTMP server.

If the gatekeeper receives two ARQ trigger registration messages with the same priority for the same GKTMP server, the gatekeeper retains the second registration and discards the first one.

If the gatekeeper receives two ARQ trigger registration messages with different priorities for the same GKTMP server, the gatekeeper checks incoming ARQ messages against the conditions on the higher priority registration before using the lower priority registration.

If the gatekeeper receives more than one ARQ trigger registration message with the same priority but for different GKTMP servers, the gatekeepers retains all of the registrations.

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

The following example configures a trigger registration on gatekeeper sj.xyz.com to send all ARQ messages to GKTMP server Server-123:

```
Router(config-gk)# server trigger arq sj.xyz.com 1 Server-123 1.14.93.130 1751
Router(config-gk_arqtrigger)# exit
```

The following example configures an ARQ trigger registration on gatekeeper alpha, which will send to GKTMP server Server-west any ARQ message containing an H.323 ID 3660-gw1, an email ID joe.xyz.com, or a redirect reason 1. All other ARQ messages will not be sent to the GKTMP server application.

```
Router(config-gk)# server trigger arq alpha 1 Server-west 10.10.10.10 1751
Router(config-gk-arqtrigger)# destination-info h323-id 3660-gw1
Router(config-gk-arqtrigger)# destination-info email-id joe.xyz.com
Router(config-gk-arqtrigger)# redirect-reason 1
Router(config-gk-arqtrigger)# exit
```

If the ARQ registration message defined above for gatekeeper alpha is configured and the gatekeeper receives the following trigger registration:

```
Router(config-gk)# server trigger arq alpha 2 Server-west 10.10.10.10 1751
Router(config-gk_arqtrigger)# destination-info e164 1800...
Router(config-gk_arqtrigger)# exit
```

then gatekeeper alpha checks all incoming ARQ messages for the destination H.323 ID, email ID, or redirect reason before checking for the E.164 address 1800 (for example, 18005551212). If any one of those conditions is met, the gatekeeper sends the ARQ message to the GKTMP server Server-west.

If the second gatekeeper alpha ARQ trigger registration had been defined with a priority 1 instead of priority 2, then the second server trigger definition would have overridden the first one. In other words, the gatekeeper alpha would send to GKTMP server Server-west only those ARQ messages that contain a destination E.164 address starting with 1800. All other ARQ messages would not be sent to the GKTMP server.

Related Commands

Command	Description
show gatekeeper servers	Displays the triggers configured on the gatekeeper.
server registration-port	Configures the server listening port on the gatekeeper.

server trigger brq

To configure the bandwidth request (BRQ) trigger statically on the gatekeeper, use the **server trigger brq** command in gatekeeper configuration mode. Submode commands are available after entering the **server trigger brq** command. To delete a single static trigger on the gatekeeper, use the **no** form of this command. To delete all static triggers on the gatekeeper, use the **all** form of the command.

server trigger brq *gkid* *priority* *server-id* *server-ipaddress* *server-port*

submode commands:

info-only

shutdown

redirect-reason *reason_number*

no server trigger brq *gkid* *priority* *server-id* *server-ipaddress* *server-port*

no server trigger all

Syntax	Description
all	Deletes all CLI configured triggers.
<i>gkid</i>	The local gatekeeper identifier.
<i>priority</i>	The priority for each trigger. The range is 1 to 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.

Submode commands

After entering the **server trigger brq** command, the software enters a submode that permits you to configure additional filters on the RAS message. These filters are optional and you may configure any of them, one per command line.

info-only	Use the info-only submode command to indicate to the Cisco IOS gatekeeper that messages that meet the specified trigger parameters should be sent to the GKTMP server application as notifications only and that the gatekeeper should not wait for a response from the GKTMP server application.
------------------	--

shutdown	Use the shutdown submode command to temporarily disable a trigger. The gatekeeper does not consult triggers in a shutdown state when determining what message to forward to the GKTMP server application.
redirect-reason <i>reason_number</i>	Use the redirect-reason submode command to send BRQ RAS messages containing a specific redirect reason to the GKTMP server application. <ul style="list-style-type: none"> • <i>reason_number</i>—Valid values are 0 to 65535. Currently-used values are: <ul style="list-style-type: none"> – 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

Defaults

No trigger servers are set

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(2)XB	The drq , rai , and brq triggers were added.
12.2(2)XU	The irr trigger was added and the command was extended to the Cisco 3660 and Cisco 7200 platforms.

Usage Guidelines

Use the **server trigger brq** command and its optional submode commands to configure the bandwidth request (BRQ) static server trigger. The gatekeeper checks incoming gateway BRQ messages for the configured trigger information. If an incoming BRQ message contains the specified trigger information, the gatekeeper sends the BRQ message to the GKTMP server application. In addition, the gatekeeper processes the message according to its programmed instructions. If the BRQ message does not contain the specified information, the gatekeeper processes the message but does not send it to the GKTMP server application.

If no submode commands are configured for the BRQ messages, the gatekeeper sends all BRQ messages to the GKTMP server application.

If the gatekeeper receives an BRQ trigger registration message containing several trigger conditions, the conditions are treated as “OR” conditions. In other words, if an incoming BRQ RAS message meets any one of the conditions, the gatekeeper sends the RAS message to the GKTMP server.

If the gatekeeper receives two BRQ trigger registration messages with the same priority for the same GKTMP server, the gatekeeper retains the second registration and discards the first one.

If the gatekeeper receives two BRQ trigger registration messages with different priorities for the same GKTMP server, the gatekeeper checks incoming BRQ messages against the conditions on the higher priority registration before using the lower priority registration.

If the gatekeeper receives more than one BRQ trigger registration message with the same priority but for different GKTMP servers, the gatekeepers retains all of the registrations.

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

The following example configures a trigger registration on gatekeeper sj.xyz.com to send all BRQ messages to GKTMP server Server-123:

```
Router(config-gk)# server trigger brq sj.xyz.com 1 Server-123 1.14.93.130 1751
Router(config-gk_brqtrigger)# exit
```

The following example configures an BRQ trigger registration on gatekeeper alpha, which will send to GKTMP server Server-west any BRQ message containing a redirect reason 1 or a redirect reason 2. All other BRQ messages will not be sent to the GKTMP server application.

```
Router(config-gk)# server trigger brq alpha 1 Server-west 10.10.10.10 1751
Router(config-gk_brqtrigger)# redirect-reason 1
Router(config-gk_brqtrigger)# redirect-reason 2
Router(config-gk_brqtrigger)# exit
```

If the BRQ registration message defined above for gatekeeper alpha is configured and the gatekeeper receives the following trigger registration:

```
Router(config-gk)# server trigger brq alpha 2 Server-west 10.10.10.10 1751
Router(config-gk_brqtrigger)# redirect-reason 10
Router(config-gk_brqtrigger)# exit
```

then gatekeeper alpha checks all incoming BRQ messages for redirect reasons 1 or 2 before checking for redirect reason 10. If any one of those conditions is met, the gatekeeper sends the BRQ message to the GKTMP server Server-west.

If the second gatekeeper alpha BRQ trigger registration had been defined with a priority 1 instead of priority 2, then the second server trigger definition would have overridden the first one. In other words, the gatekeeper alpha would send to GKTMP server Server-west only those BRQ messages that contain a redirect reason 10. All other BRQ messages would not be sent to the GKTMP server.

Related Commands

Command	Description
show gatekeeper servers	Displays the triggers configured on the gatekeeper.
server registration-port	Configures the server listening port on the gatekeeper.

server trigger drq

To configure the disengage request (DRQ) trigger statically on the gatekeeper, use the **server trigger drq** command in gatekeeper configuration mode. Submode commands are available after entering the **server trigger drq** command. To delete a single static trigger on the gatekeeper, use the **no** form of this command. To delete all static triggers on the gatekeeper, use the **all** form of the command.

server trigger drq *gkid priority server-id server-ipaddress server-port*

submode commands:

info-only

shutdown

destination-info { **e164** | **email-id** | **h323-id** } *value*

no server trigger drq *gkid priority server-id server-ipaddress server-port*

no server trigger all

Syntax Description

all	Deletes all CLI configured triggers.
<i>gkid</i>	The local gatekeeper identifier.
<i>priority</i>	The priority for each trigger. The range is 1 to 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.

Submode commands

After entering the **server trigger drq** command, the software enters a submode that permits you to configure additional filters on the RAS message. These filters are optional and you may configure any of them, one per command line.

info-only	Use the info-only submode command to indicate to the Cisco IOS gatekeeper that messages that meet the specified trigger parameters should be sent to the GKTMP server application as notifications only and that the gatekeeper should not wait for a response from the GKTMP server application.
------------------	--

shutdown	Use the shutdown submode command to temporarily disable a trigger. The gatekeeper does not consult triggers in a shutdown state when determining what message to forward to the GKTMP server application.
destination-info { e164 email-id h323-id } <i>value</i>	Use the destination-info submode command to send ARQ RAS messages containing a specified destination to the GKTMP server application. Configure one of the following conditions <ul style="list-style-type: none"> • e164—Indicates that the destination is an E.164 address. • email-id—Indicates that the destination is an e-mail ID. • h323-id—Indicates that the destination is an H.323 ID. • <i>value</i>—Specifies the value against which to compare the destination address in the RAS messages. For E.164 addresses, the following wildcards can be used: <ul style="list-style-type: none"> – A trailing series of periods, each of which represents a single character. – A trailing asterisk, which represents one or more characters.

Defaults No trigger servers are set

Command Modes Gatekeeper configuration

Command History	Release	Modification
	12.1(1)T	This command was introduced.
	12.2(2)XB	The drq , rai , and brq triggers were added.
	12.2(2)XU	The irr trigger was added and the command was extended to the Cisco 3660 and Cisco 7200 platforms.

Usage Guidelines Use the **server trigger drq** command and its optional submode commands to configure the disengage request (DRQ) static server trigger. The gatekeeper checks incoming gateway DRQ messages for the configured trigger information. If an incoming DRQ message contains the specified trigger information, the gatekeeper sends the DRQ message to the GKTMP server application. In addition, the gatekeeper processes the message according to its programmed instructions. If the DRQ message does not contain the specified information, the gatekeeper processes the message but does not send it to the GKTMP server application.

If no submode commands are configured for the DRQ messages, the gatekeeper sends all DRQ messages to the GKTMP server application.

If the gatekeeper receives an DRQ trigger registration message containing several trigger conditions, the conditions are treated as “OR” conditions. In other words, if an incoming DRQ RAS message meets any one of the conditions, the gatekeeper sends the RAS message to the GKTMP server.

If the gatekeeper receives two DRQ trigger registration messages with the same priority for the same GKTMP server, the gatekeeper retains the second registration and discards the first one.

If the gatekeeper receives two DRQ trigger registration messages with different priorities for the same GKTMP server, the gatekeeper checks incoming DRQ messages against the conditions on the higher priority registration before using the lower priority registration.

If the gatekeeper receives more than one DRQ trigger registration message with the same priority but for different GKTMP servers, the gatekeepers retains all of the registrations.

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

The following example configures a trigger registration on gatekeeper sj.xyz.com to send all DRQ messages to GKTMP server Server-123:

```
Router(config-gk)# server trigger drq sj.xyz.com 1 Server-123 1.14.93.130 1751
Router(config-gk_drqtrigger)# exit
```

The following example configures an DRQ trigger registration on gatekeeper alpha, which will send to GKTMP server Server-west any DRQ message containing an H.323 ID 3660-gw1 or an email ID joe.xyz.com. All other DRQ messages will not be sent to the GKTMP server application.

```
Router(config-gk)# server trigger drq alpha 1 Server-west 10.10.10.10 1751
Router(config-gk_drqtrigger)# destination-info h323-id 3660-gw1
Router(config-gk_drqtrigger)# destination-info email-id joe.xyz.com
Router(config-gk_drqtrigger)# exit
```

If the DRQ registration message defined above for gatekeeper alpha is configured and the gatekeeper receives the following trigger registration:

```
Router(config-gk)# server trigger drq alpha 2 Server-west 10.10.10.10 1751
Router(config-gk_drqtrigger)# destination-info e164 1800...
Router(config-gk_drqtrigger)# exit
```

then gatekeeper alpha checks all incoming DRQ messages for the destination H.323 ID or email ID before checking for the E.164 address 1800 (for example, 18005551212). If any one of those conditions is met, the gatekeeper sends the DRQ message to the GKTMP server Server-west.

If the second gatekeeper alpha DRQ trigger registration had been defined with a priority 1 instead of priority 2, then the second trigger registration would have overridden the first one. In other words, the gatekeeper alpha would send to GKTMP server Server-west only those DRQ messages that contain a destination E.164 address starting with 1800. All other DRQ messages would not be sent to the GKTMP server.

Related Commands

Command	Description
show gatekeeper servers	Displays the triggers configured on the gatekeeper.
server registration-port	Configures the server listening port on the gatekeeper.

server trigger irr

To configure the information request response (IRR) trigger statically on the gatekeeper, use the **server trigger irr** command in gatekeeper configuration mode. Submode commands are available after entering the **server trigger irr** command. To delete a single static trigger on the gatekeeper, use the **no** form of this command. To delete all static triggers on the gatekeeper, use the **all** form of the command.

server trigger irr *gkid priority server-id server-ipaddress server-port*

submode commands:

info-only

shutdown

destination-info { **e164** | **email-id** | **h323-id** } *value* |

redirect-reason *reason_number*

no server trigger irr *gkid priority server-id server-ipaddress server-port*

no server trigger all

Syntax Description

all	Deletes all CLI configured triggers.
<i>gkid</i>	The local gatekeeper identifier.
<i>priority</i>	The priority for each trigger. The range is 1 to 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.

Submode commands

After entering the **server trigger irr** command, the software enters a submode that permits you to configure additional filters on the RAS message. These filters are optional and you may configure any of them, one per command line.

info-only	Use the info-only submode command to indicate to the Cisco IOS gatekeeper that messages that meet the specified trigger parameters should be sent to the GKTMP server application as notifications only and that the gatekeeper should not wait for a response from the GKTMP server application.
shutdown	Use the shutdown submode command to temporarily disable a trigger. The gatekeeper does not consult triggers in a shutdown state when determining what message to forward to the GKTMP server application.

destination-info { e164 email-id h323-id } <i>value</i>	<p>Use the destination-info submode command to send IRR RAS messages containing a specified destination to the GKTMP server application. Configure one of the following conditions</p> <ul style="list-style-type: none"> • e164—Indicates that the destination is an E.164 address. • email-id—Indicates that the destination is an e-mail ID. • h323-id—Indicates that the destination is an H.323 ID. • <i>value</i>—Specifies the value against which to compare the destination address in the RAS messages. For E.164 addresses, the following wildcards can be used: <ul style="list-style-type: none"> – A trailing series of periods, each of which represents a single character. – A trailing asterisk, which represents one or more characters.
redirect-reason <i>reason_number</i>	<p>Use the redirect-reason submode command to send IRR RAS messages containing a specific redirect reason to the GKTMP server application.</p> <ul style="list-style-type: none"> • <i>reason_number</i>—Valid values are 0 to 65535. Currently-used values are: <ul style="list-style-type: none"> – 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

Defaults

No trigger servers are set

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(2)XB	The drq , rai , and brq triggers were added.
12.2(2)XU	The irr trigger was added and the command was extended to the Cisco 3660 and Cisco 7200 platforms.

Usage Guidelines

Use the **server trigger irr** command and its optional submode commands to configure the information request response (IRR) static server trigger. The gatekeeper checks incoming gateway IRR messages for the configured trigger information. If an incoming IRR message contains the specified trigger information, the gatekeeper sends the IRR message to the GKTMP server application. In addition, the IRR message does not contain the specified information, the gatekeeper processes the message but does not send it to the GKTMP server application.

If no submode commands are configured for the IRR messages, the gatekeeper sends all IRR messages to the GKTMP server application.

If the gatekeeper receives an IRR trigger registration message containing several trigger conditions, the conditions are treated as “OR” conditions. In other words, if an incoming IRR RAS message meets any one of the conditions, the gatekeeper sends the RAS message to the GKTMP server.

If the gatekeeper receives two IRR trigger registration messages with the same priority for the same GKTMP server, the gatekeeper retains the second registration and discards the first one.

If the gatekeeper receives two IRR trigger registration messages with different priorities for the same GKTMP server, the gatekeeper checks incoming IRR messages against the conditions on the higher priority registration before using the lower priority registration.

If the gatekeeper receives more than one IRR trigger registration message with the same priority but for different GKTMP servers, the gatekeepers retains all of the registrations.

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

The following example configures a trigger registration on gatekeeper sj.xyz.com to send all IRR messages to GKTMP server Server-123:

```
Router(config-gk)# server trigger irr sj.xyz.com 1 Server-123 1.14.93.130 1751
Router(config-gk_irrtrigger)# exit
```

The following example configures an IRR trigger registration on gatekeeper alpha, which will send to GKTMP server Server-west any IRR message containing an H.323 ID 3660-gw1, an email ID joe.xyz.com, or a redirect reason 1. All other IRR messages will not be sent to the GKTMP server application.

```
Router(config-gk)# server trigger irr alpha 1 Server-west 10.10.10.10 1751
Router(config-gk_irrtrigger)# destination-info h323-id 3660-gw1
Router(config-gk_irrtrigger)# destination-info email-id joe.xyz.com
Router(config-gk_irrtrigger)# redirect-reason 1
Router(config-gk_irrtrigger)# exit
```

If the IRR registration message defined above for gatekeeper alpha is configured and the gatekeeper receives the following trigger registration:

```
Router(config-gk)# server trigger irr alpha 2 Server-west 10.10.10.10 1751
Router(config-gk_irrtrigger)# destination-info e164 1800....
Router(config-gk_irrtrigger)# exit
```

then gatekeeper alpha checks all incoming IRR messages for the destination H.323 ID, email ID, or redirect reason before checking for the E.164 address 1800 (for example, 18005551212). If any one of those conditions is met, the gatekeeper sends the IRR message to the GKTMP server Server-west.

If the second gatekeeper alpha IRR trigger registration had been defined with a priority 1 instead of priority 2, then the second server trigger definition would have overridden the first one. In other words, the gatekeeper alpha would send to GKTMP server Server-west only those IRR messages that contain a destination E.164 address starting with 1800. All other IRR messages would not be sent to the GKTMP server.

Related Commands

Command	Description
show gatekeeper servers	Displays the triggers configured on the gatekeeper.
server registration-port	Configures the server listening port on the gatekeeper.

server trigger lcf

To configure the location confirm (LCF) trigger statically on the gatekeeper, use the **server trigger lcf** command in gatekeeper configuration mode. Submode commands are available after entering the **server trigger lcf** command. To delete a single static trigger on the gatekeeper, use the **no** form of this command. To delete all static triggers on the gatekeeper, use the **all** form of the command.

server trigger lcf *gkid* *priority* *server-id* *server-ipaddress* *server-port*

submode commands:

info-only

shutdown

destination-info { **e164** | **email-id** | **h323-id** } *value* |

remote-ext-address **e164** *value*

no server trigger lcf *gkid* *priority* *server-id* *server-ipaddress* *server-port*

no server trigger all

Syntax Description

all	Deletes all CLI configured triggers.
<i>gkid</i>	The local gatekeeper identifier.
<i>priority</i>	The priority for each trigger. The range is 1 to 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.

Submode commands

After entering the **server trigger lcf** command, the software enters a submode that permits you to configure additional filters on the RAS message. These filters are optional and you may configure any of them, one per command line.

info-only	Use the info-only submode command to indicate to the Cisco IOS gatekeeper that messages that meet the specified trigger parameters should be sent to the GKTMP server application as notifications only and that the gatekeeper should not wait for a response from the GKTMP server application.
shutdown	Use the shutdown submode command to temporarily disable a trigger. The gatekeeper does not consult triggers in a shutdown state when determining what message to forward to the GKTMP server application.

destination-info { e164 email-id h323-id } <i>value</i>	<p>Use the destination-info submode command to send LCF RAS messages containing a specified destination to the GKTMP server application. Configure one of the following conditions</p> <ul style="list-style-type: none"> • e164—Indicates that the destination is an E.164 address. • email-id—Indicates that the destination is an e-mail ID. • h323-id—Indicates that the destination is an H.323 ID. • <i>value</i>—Specifies the value against which to compare the destination address in the RAS messages. For E.164 addresses, the following wildcards can be used: <ul style="list-style-type: none"> – A trailing series of periods, each of which represents a single character. – A trailing asterisk, which represents one or more characters.
remote-ext-address e164 <i>value</i>	<p>Use the remote-address submode command to send LCF RAS messages containing a specified remote extension address to the GKTMP server application.</p> <ul style="list-style-type: none"> • e164—Indicates that the remote extension address is an E.164 address. • <i>value</i>—Specifies the value against which to compare the destination address in the RAS messages. The following wildcards can be used: <ul style="list-style-type: none"> – A trailing series of periods, each of which represents a single character. – A trailing asterisk, which represents one or more characters.

Defaults No trigger servers are set

Command Modes Gatekeeper configuration

Command History	Release	Modification
	12.1(1)T	This command was introduced.
	12.2(2)XB	The drq , rai , and brq triggers were added.
	12.2(2)XU	The irr trigger was added and the command was extended to the Cisco 3660 and Cisco 7200 platforms.

Usage Guidelines

Use the **server trigger lcf** command and its optional submode commands to configure the location confirm (LCF) static server trigger. The gatekeeper checks incoming gateway LCF messages for the configured trigger information. If an incoming LCF message contains the specified trigger information, the gatekeeper sends the LCF message to the GKTMP server application. In addition, the gatekeeper processes the message according to its programmed instructions. If the LCF message does not contain the specified information, the gatekeeper processes the message but does not send it to the GKTMP server application.

If no submode commands are configured for the LCF messages, the gatekeeper sends all LCF messages to the GKTMP server application.

If the gatekeeper receives an LCF trigger registration message containing several trigger conditions, the conditions are treated as “OR” conditions. In other words, if an incoming LCF RAS message meets any one of the conditions, the gatekeeper sends the RAS message to the GKTMP server.

If the gatekeeper receives two LCF trigger registration messages with the same priority for the same GKTMP server, the gatekeeper retains the second registration and discards the first one.

If the gatekeeper receives two LCF trigger registration messages with different priorities for the same GKTMP server, the gatekeeper checks incoming LCF messages against the conditions on the higher priority registration before using the lower priority registration.

If the gatekeeper receives more than one LCF trigger registration message with the same priority but for different GKTMP servers, the gatekeepers retains all of the registrations.

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

The following example configures a trigger registration on gatekeeper sj.xyz.com to send all LCF messages to GKTMP server Server-123:

```
Router(config-gk)# server trigger lcf sj.xyz.com 1 Server-123 1.14.93.130 1751
Router(config-gk_lcftrigger)# exit
```

The following example configures an LCF trigger registration on gatekeeper alpha, which will send to GKTMP server Server-west any LCF message containing an H.323 ID 3660-gw1, an email ID joe.xyz.com, or a remote extension address starting with 1408. All other LCF messages will not be sent to the GKTMP server application.

```
Router(config-gk)# server trigger lcf alpha 1 Server-west 10.10.10.10 1751
Router(config-gk_lcftrigger)# destination-info h323-id 3660-gw1
Router(config-gk_lcftrigger)# destination-info email-id joe.xyz.com
Router(config-gk_lcftrigger)# remote-ext-address e164 1408...
Router(config-gk_lcftrigger)# exit
```

If the LCF registration message defined above for gatekeeper alpha is configured and the gatekeeper receives the following trigger registration:

```
Router(config-gk)# server trigger lcf alpha 2 Server-west 10.10.10.10 1751
Router(config-gk_lcftrigger)# remote-ext-address e164 1800...
Router(config-gk_lcftrigger)# exit
```

then gatekeeper alpha checks all incoming LCF messages for the destination H.323 ID, email ID, or remote extension address 1408 before checking for the remote extension address 1800 (for example, 18005551212). If any one of those conditions is met, the gatekeeper sends the LCF message to the GKTMP server Server-west.

If the second gatekeeper alpha LCF trigger registration had been defined with a priority 1 instead of priority 2, then the second trigger registration would have overridden the first one. In other words, the gatekeeper alpha would send to GKTMP server Server-west only those LCF messages that contain a remote extension address E.164 address starting with 1800. All other LCF messages would not be sent to the GKTMP server.

Related Commands	Command	Description
	show gatekeeper servers	Displays the triggers configured on the gatekeeper.
	server registration-port	Configures the server listening port on the gatekeeper.

server trigger lrj

To configure the location reject (LRJ) trigger statically on the gatekeeper, use the **server trigger lrj** command in gatekeeper configuration mode. Submode commands are available after entering the **server trigger lrj** command. To delete a single static trigger on the gatekeeper, use the **no** form of this command. To delete all static triggers on the gatekeeper, use the **all** form of the command.

```
server trigger lrj gkid priority server-id server-ipaddress server-port
submode commands:
info-only
shutdown
destination-info { e164 | email-id | h323-id } value
```

```
no server trigger lrj gkid priority server-id server-ipaddress server-port
```

```
no server trigger all
```

Syntax Description

all	Deletes all CLI configured triggers.
<i>gkid</i>	The local gatekeeper identifier.
<i>priority</i>	The priority for each trigger. The range is 1 to 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.

Submode commands

After entering the **server trigger lrj** command, the software enters a submode that permits you to configure additional filters on the RAS message. These filters are optional and you may configure any of them, one per command line.

info-only	Use the info-only submode command to indicate to the Cisco IOS gatekeeper that messages that meet the specified trigger parameters should be sent to the GKTMP server application as notifications only and that the gatekeeper should not wait for a response from the GKTMP server application.
------------------	--

shutdown	Use the shutdown submode command to temporarily disable a trigger. The gatekeeper does not consult triggers in a shutdown state when determining what message to forward to the GKTMP server application.
destination-info { e164 email-id h323-id } <i>value</i>	Use the destination-info submode command to send LRJ RAS messages containing a specified destination to the GKTMP server application. Configure one of the following conditions <ul style="list-style-type: none"> • e164—Indicates that the destination is an E.164 address. • email-id—Indicates that the destination is an e-mail ID. • h323-id—Indicates that the destination is an H.323 ID. • <i>value</i>—Specifies the value against which to compare the destination address in the RAS messages. For E.164 addresses, the following wildcards can be used: <ul style="list-style-type: none"> – A trailing series of periods, each of which represents a single character. – A trailing asterisk, which represents one or more characters.

Defaults No trigger servers are set

Command Modes Gatekeeper configuration

Release	Modification
12.1(1)T	This command was introduced.
12.2(2)XB	The drq , rai , and brq triggers were added.
12.2(2)XU	The irr trigger was added and the command was extended to the Cisco 3660 and Cisco 7200 platforms.

Usage Guidelines Use the **server trigger lrj** command and its optional submode commands to configure the location reject (LRJ) static server trigger. The gatekeeper checks incoming gateway LRJ messages for the configured trigger information. If an incoming LRJ message contains the specified trigger information, the gatekeeper sends the LRJ message to the GKTMP server application. In addition, the gatekeeper processes the message according to its programmed instructions. If the LRJ message does not contain the specified information, the gatekeeper processes the message but does not send it to the GKTMP server application.

If no submode commands are configured for the LRJ messages, the gatekeeper sends all LRJ messages to the GKTMP server application.

If the gatekeeper receives an LRJ trigger registration message containing several trigger conditions, the conditions are treated as “OR” conditions. In other words, if an incoming LRJ RAS message meets any one of the conditions, the gatekeeper sends the RAS message to the GKTMP server.

If the gatekeeper receives two LRJ trigger registration messages with the same priority for the same GKTMP server, the gatekeeper retains the second registration and discards the first one.

If the gatekeeper receives two LRJ trigger registration messages with different priorities for the same GKTMP server, the gatekeeper checks incoming LRJ messages against the conditions on the higher priority registration before using the lower priority registration.

If the gatekeeper receives more than one LRJ trigger registration message with the same priority but for different GKTMP servers, the gatekeepers retains all of the registrations.

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

The following example configures a trigger registration on gatekeeper sj.xyz.com to send all LRJ messages to GKTMP server Server-123:

```
Router(config-gk)# server trigger lrj sj.xyz.com 1 Server-123 1.14.93.130 1751
Router(config-gk_lrjtrigger)# exit
```

The following example configures an LRJ trigger registration on gatekeeper alpha, which will send to GKTMP server Server-west any LRJ message containing an H.323 ID 3660-gw1 or an email ID joe.xyz.com. All other LRJ messages will not be sent to the GKTMP server application.

```
Router(config-gk)# server trigger lrj alpha 1 Server-west 10.10.10.10 1751
Router(config-gk_lrjtrigger)# destination-info h323-id 3660-gw1
Router(config-gk_lrjtrigger)# destination-info email-id joe.xyz.com
Router(config-gk_lrjtrigger)# exit
```

If the LRJ registration message defined above for gatekeeper alpha is configured and the gatekeeper receives the following trigger registration:

```
Router(config-gk)# server trigger lrj alpha 2 Server-west 10.10.10.10 1751
Router(config-gk_lrjtrigger)# destination-info e164 1800...
Router(config-gk_lrjtrigger)# exit
```

then gatekeeper alpha checks all incoming LRJ messages for the destination H.323 ID or email ID before checking for the E.164 address 1800 (for example, 18005551212). If any one of those conditions is met, the gatekeeper sends the LRJ message to the GKTMP server Server-west.

If the second gatekeeper alpha LRJ trigger registration had been defined with a priority 1 instead of priority 2, then the second trigger registration would have overridden the first one. In other words, the gatekeeper alpha would send to GKTMP server Server-west only those LRJ messages that contain a destination E.164 address starting with 1800. All other LRJ messages would not be sent to the GKTMP server.

Related Commands

Command	Description
show gatekeeper servers	Displays the triggers configured on the gatekeeper.
server registration-port	Configures the server listening port on the gatekeeper.

server trigger lrq

To configure the location request (LRQ) trigger statically on the gatekeeper, use the **server trigger lrq** command in gatekeeper configuration mode. Submode commands are available after entering the **server trigger lrq** command. To delete a single static trigger on the gatekeeper, use the **no** form of this command. To delete all static triggers on the gatekeeper, use the **all** form of the command.

server trigger lrq *gkid* *priority* *server-id* *server-ipaddress* *server-port*

submode commands:

info-only

shutdown

destination-info { **e164** | **email-id** | **h323-id** } *value* |

redirect-reason *reason_number*

no server trigger lrq *gkid* *priority* *server-id* *server-ipaddress* *server-port*

no server trigger all

Syntax Description

all	Deletes all CLI configured triggers.
<i>gkid</i>	The local gatekeeper identifier.
<i>priority</i>	The priority for each trigger. The range is 1 to 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.

Submode commands

After entering the **server trigger lrq** command, the software enters a submode that permits you to configure additional filters on the RAS message. These filters are optional and you may configure any of them, one per command line.

info-only	Use the info-only submode command to indicate to the Cisco IOS gatekeeper that messages that meet the specified trigger parameters should be sent to the GKTMP server application as notifications only and that the gatekeeper should not wait for a response from the GKTMP server application.
shutdown	Use the shutdown submode command to temporarily disable a trigger. The gatekeeper does not consult triggers in a shutdown state when determining what message to forward to the GKTMP server application.

destination-info { e164 email-id h323-id } <i>value</i>	<p>Use the destination-info submode command to send LRQ RAS messages containing a specified destination to the GKTMP server application. Configure one of the following conditions</p> <ul style="list-style-type: none"> • e164—Indicates that the destination is an E.164 address. • email-id—Indicates that the destination is an e-mail ID. • h323-id—Indicates that the destination is an H.323 ID. • <i>value</i>—Specifies the value against which to compare the destination address in the RAS messages. For E.164 addresses, the following wildcards can be used: <ul style="list-style-type: none"> – A trailing series of periods, each of which represents a single character. – A trailing asterisk, which represents one or more characters.
redirect-reason <i>reason_number</i>	<p>Use the redirect-reason submode command to send LRQ RAS messages containing a specific redirect reason to the GKTMP server application.</p> <ul style="list-style-type: none"> • <i>reason_number</i>—Valid values are 0 to 65535. Currently-used values are: <ul style="list-style-type: none"> – 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

Defaults

No trigger servers are set

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(2)XB	The drq , rai , and brq triggers were added.
12.2(2)XU	The irr trigger was added and the command was extended to the Cisco 3660 and Cisco 7200 platforms.

Usage Guidelines

Use the **server trigger lrq** command and its optional submode commands to configure the location request (LRQ) static server trigger. The gatekeeper checks incoming gateway LRQ messages for the configured trigger information. If an incoming LRQ message contains the specified trigger information, the gatekeeper sends the LRQ message to the GKTMP server application. In addition, the gatekeeper processes the message according to its programmed instructions. If the LRQ message does not contain the specified information, the gatekeeper processes the message but does not send it to the GKTMP server application.

If no submode commands are configured for the LRQ messages, the gatekeeper sends all LRQ messages to the GKTMP server application.

If the gatekeeper receives an LRQ trigger registration message containing several trigger conditions, the conditions are treated as “OR” conditions. In other words, if an incoming LRQ RAS message meets any one of the conditions, the gatekeeper sends the RAS message to the GKTMP server.

If the gatekeeper receives two LRQ trigger registration messages with the same priority for the same GKTMP server, the gatekeeper retains the second registration and discards the first one.

If the gatekeeper receives two LRQ trigger registration messages with different priorities for the same GKTMP server, the gatekeeper checks incoming LRQ messages against the conditions on the higher priority registration before using the lower priority registration.

If the gatekeeper receives more than one LRQ trigger registration message with the same priority but for different GKTMP servers, the gatekeepers retains all of the registrations.

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

The following example configures a trigger registration on gatekeeper sj.xyz.com to send all LRQ messages to GKTMP server Server-123:

```
Router(config-gk)# server trigger lrq sj.xyz.com 1 Server-123 1.14.93.130 1751
Router(config-gk_lrqtrigger)# exit
```

The following example configures an LRQ trigger registration on gatekeeper alpha, which will send to GKTMP server Server-west any LRQ message containing an H.323 ID 3660-gw1, an email ID joe.xyz.com, or a redirect reason 1. All other LRQ messages will not be sent to the GKTMP server application.

```
Router(config-gk)# server trigger lrq alpha 1 Server-west 10.10.10.10 1751
Router(config-gk_lrqtrigger)# destination-info h323-id 3660-gw1
Router(config-gk_lrqtrigger)# destination-info email-id joe.xyz.com
Router(config-gk_lrqtrigger)# redirect-reason 1
Router(config-gk_lrqtrigger)# exit
```

If the LRQ registration message defined above for gatekeeper alpha is configured and the gatekeeper receives the following trigger registration:

```
Router(config-gk)# server trigger lrq alpha 2 Server-west 10.10.10.10 1751
Router(config-gk_lrqtrigger)# destination-info e164 1800...
Router(config-gk_lrqtrigger)# exit
```

then gatekeeper alpha checks all incoming LRQ messages for the destination H.323 ID, email ID, or redirect reason before checking for the E.164 address 1800 (for example, 18005551212). If any one of those conditions is met, the gatekeeper sends the LRQ message to the GKTMP server Server-west.

If the second gatekeeper alpha LRQ trigger registration had been defined with a priority 1 instead of priority 2, then the second server trigger definition would have overridden the first one. In other words, the gatekeeper alpha would send to GKTMP server Server-west only those LRQ messages that contain a destination E.164 address starting with 1800. All other LRQ messages would not be sent to the GKTMP server.

Related Commands

Command	Description
show gatekeeper servers	Displays the triggers configured on the gatekeeper.
server registration-port	Configures the server listening port on the gatekeeper.

server trigger rai

To configure the resources available indicator (RAI) trigger statically on the gatekeeper, use the **server trigger rai** command in gatekeeper configuration mode. Submode commands are available after entering the **server trigger rai** command. To delete a single static trigger on the gatekeeper, use the **no** form of this command. To delete all static triggers on the gatekeeper, use the **all** form of the command.

```
server trigger rai gkid priority server-id server-ipaddress server-port
  submode commands:
    info-only
    shutdown
    endpoint-type value | supported-prefix value
```

```
no server trigger rai gkid priority server-id server-ipaddress server-port
```

```
no server trigger all
```

Syntax Description

all	Deletes all CLI configured triggers.
<i>gkid</i>	The local gatekeeper identifier.
<i>priority</i>	The priority for each trigger. The range is 1 to 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.

Submode commands

After entering the **server trigger rai** command, the software enters a submode that permits you to configure additional filters on the RAS message. These filters are optional and you may configure any of them, one per command line.

info-only	Use the info-only submode command to indicate to the Cisco IOS gatekeeper that messages that meet the specified trigger parameters should be sent to the GKTMP server application as notifications only and that the gatekeeper should not wait for a response from the GKTMP server application.
shutdown	Use the shutdown submode command to temporarily disable a trigger. The gatekeeper does not consult triggers in a shutdown state when determining what message to forward to the GKTMP server application.

endpoint-type *value*

Use the **endpoint-type** submode command to send RAI RAS messages containing a particular endpoint type to the GKTMP server application.

- *value*—Specifies the value against which to compare the endpoint-type in the RAS messages. Valid endpoint types are:
 - **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 terminal.
 - **voice-gateway**—The endpoint is a voice gateway.

supported-prefix *value*

Use the **supported-prefix** submode command to send RAI RAS messages containing a specific supported prefix to the GKTMP server application.

- *value*—Specifies the value against which to compare the supported prefix in the RAS messages. The possible values are any E.164 pattern used as a gateway technology prefix. The value string can contain any of the following: 0123456789#*.

Defaults

No trigger servers are set

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(2)XB	The drq , rai , and brq triggers were added.
12.2(2)XU	The irr trigger was added and the command was extended to the Cisco 3660 and Cisco 7200 platforms.

Usage Guidelines

Use the **server trigger rai** command and its optional submode commands to configure the resources available indicator (RAI) static server trigger. The gatekeeper checks incoming gateway RAI messages for the configured trigger information. If an incoming RAI message contains the specified trigger information, the gatekeeper sends the RAI message to the GKTMP server application. In addition, the gatekeeper processes the message according to its programmed instructions. If the RAI message does not contain the specified information, the gatekeeper processes the message but does not send it to the GKTMP server application.

If no submode commands are configured for the RAI messages, the gatekeeper sends all RAI messages to the GKTMP server application.

If the gatekeeper receives an RAI trigger registration message containing several trigger conditions, the conditions are treated as “OR” conditions. In other words, if an incoming RAI RAS message meets any one of the conditions, the gatekeeper sends the RAS message to the GKTMP server.

If the gatekeeper receives two RAI trigger registration messages with the same priority for the same GKTMP server, the gatekeeper retains the second registration and discards the first one.

If the gatekeeper receives two RAI trigger registration messages with different priorities for the same GKTMP server, the gatekeeper checks incoming RAI messages against the conditions on the higher priority registration before using the lower priority registration.

If the gatekeeper receives more than one RAI trigger registration message with the same priority but for different GKTMP servers, the gatekeepers retains all of the registrations.

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

The following example configures a trigger registration on gatekeeper sj.xyz.com to send all RAI messages to GKTMP server Server-123:

```
Router(config-gk)# server trigger rai sj.xyz.com 1 Server-123 1.14.93.130 1751
Router(config-gk_raitrigger)# exit
```

The following example configures an RAI trigger registration on gatekeeper alpha, which will send to the GKTMP server Server-west any RAI message containing an MCU endpoint, an H.323 proxy endpoint, or a supported prefix 1#. All other RAI messages will not be sent to the GKTMP server.

```
Router(config-gk)# server trigger rai alpha 1 Server-west 10.10.10.10 1751
Router(config-gk-raitrigger)# endpoint-type mcu
Router(config-gk-raitrigger)# endpoint-type proxy
Router(config-gk-raitrigger)# supported-prefix 1#
Router(config-gk-raitrigger)# exit
```

If the RAI registration message defined above for gatekeeper alpha is configured and the gatekeeper receives the following trigger registration:

```
Router(config-gk)# server trigger rai alpha 2 Server-west 10.10.10.10 1751
Router(config-gk_raitrigger)# supported-prefix 1234*
Router(config-gk_raitrigger)# exit
```

then gatekeeper alpha checks all incoming RAI messages for the MCU or H.323 proxy endpoint or supported prefix 1# before checking for the supported prefix 1234*. If any one of those conditions is met, the gatekeeper sends the RAI message to the GKTMP server Server-west.

If the second gatekeeper alpha RAI trigger registration had been defined with a priority 1 instead of priority 2, then the second trigger registration would have overridden the first one. In other words, the gatekeeper alpha would send to GKTMP server Server-west only those RAI messages that contain a supported prefix of 1234*. All other RAI messages would not be sent to the GKTMP server.

Related Commands	Command	Description
	show gatekeeper servers	Displays the triggers configured on the gatekeeper.
	server registration-port	Configures the server listening port on the gatekeeper.

server trigger rrq

To configure the registration request (RRQ) trigger statically on the gatekeeper, use the **server trigger rrq** command in gatekeeper configuration mode. Submode commands are available after entering the **server trigger rrq** command. To delete a single static trigger on the gatekeeper, use the **no** form of this command. To delete all static triggers on the gatekeeper, use the **all** form of the command.

```
server trigger rrq gkid priority server-id server-ipaddress server-port
  submode commands:
    info-only
    shutdown
    endpoint-type value | supported-prefix value
```

```
no server trigger rrq gkid priority server-id server-ipaddress server-port
```

```
no server trigger all
```

Syntax Description

all	Deletes all CLI configured triggers.
<i>gkid</i>	The local gatekeeper identifier.
<i>priority</i>	The priority for each trigger. The range is 1 to 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.

Submode commands

After entering the **server trigger rrq** command, the software enters a submode that permits you to configure additional filters on the RAS message. These filters are optional and you may configure any of them, one per command line.

info-only	Use the info-only submode command to indicate to the Cisco IOS gatekeeper that messages that meet the specified trigger parameters should be sent to the GKTMP server application as notifications only and that the gatekeeper should not wait for a response from the GKTMP server application.
shutdown	Use the shutdown submode command to temporarily disable a trigger. The gatekeeper does not consult triggers in a shutdown state when determining what message to forward to the GKTMP server application.

endpoint-type <i>value</i>	<p>Use the endpoint-type submode command to send RRQ RAS messages containing a particular endpoint type to the GKTMP server application.</p> <ul style="list-style-type: none"> • <i>value</i>—Specifies the value against which to compare the endpoint-type in the RAS messages. Valid endpoint types are: <ul style="list-style-type: none"> – 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 terminal. – voice-gateway—The endpoint is a voice gateway.
supported-prefix <i>value</i>	<p>Use the supported-prefix submode command to send RRQ RAS messages containing a specific supported prefix to the GKTMP server application.</p> <ul style="list-style-type: none"> • <i>value</i>—Specifies the value against which to compare the supported prefix in the RAS messages. The possible values are any E.164 pattern used as a gateway technology prefix. The value string can contain any of the following: 0123456789#*.

Defaults No trigger servers are set

Command Modes Gatekeeper configuration

Command History	Release	Modification
	12.1(1)T	This command was introduced.
	12.2(2)XB	The drq , rai , and brq triggers were added.
	12.2(2)XU	The irr trigger was added and the command was extended to the Cisco 3660 and Cisco 7200 platforms.

Usage Guidelines

Use the **server trigger rrq** command and its optional submode commands to configure the registration request (RRQ) static server trigger. The gatekeeper checks incoming gateway RRQ messages for the configured trigger information. If an incoming RRQ message contains the specified trigger information, the gatekeeper sends the RRQ message to the GKTMP server application. In addition, the gatekeeper processes the message according to its programmed instructions. If the RRQ message does not contain the specified information, the gatekeeper processes the message but does not send it to the GKTMP server application.

If no submode commands are configured for the RRQ messages, the gatekeeper sends all RRQ messages to the GKTMP server application.

If the gatekeeper receives an RRQ trigger registration message containing several trigger conditions, the conditions are treated as “OR” conditions. In other words, if an incoming RRQ RAS message meets any one of the conditions, the gatekeeper sends the RAS message to the GKTMP server.

If the gatekeeper receives two RRQ trigger registration messages with the same priority for the same GKTMP server, the gatekeeper retains the second registration and discards the first one.

If the gatekeeper receives two RRQ trigger registration messages with different priorities for the same GKTMP server, the gatekeeper checks incoming RRQ messages against the conditions on the higher priority registration before using the lower priority registration.

If the gatekeeper receives more than one RRQ trigger registration message with the same priority but for different GKTMP servers, the gatekeepers retains all of the registrations.

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

The following example configures a trigger registration on gatekeeper sj.xyz.com to send all RRQ messages to GKTMP server Server-123:

```
Router(config-gk)# server trigger rrq sj.xyz.com 1 Server-123 1.14.93.130 1751
Router(config-gk_rrqtrigger)# exit
```

The following example configures an RRQ trigger registration on gatekeeper alpha, which will send to the GKTMP server Server-west any RRQ message containing an MCU endpoint, an H.323 proxy endpoint, or a supported prefix 1#. All other RRQ messages will not be sent to the GKTMP server.

```
Router(config-gk)# server trigger rrq alpha 1 Server-west 10.10.10.10 1751
Router(config-gk_rrqtrigger)# endpoint-type mcu
Router(config-gk_rrqtrigger)# endpoint-type proxy
Router(config-gk_rrqtrigger)# supported-prefix 1#
Router(config-gk_rrqtrigger)# exit
```

If the RRQ registration message defined above for gatekeeper alpha is configured and the gatekeeper receives the following trigger registration:

```
Router(config-gk)# server trigger rrq alpha 2 Server-west 10.10.10.10 1751
Router(config-gk_rrqtrigger)# supported-prefix 1234*
Router(config-gk_rrqtrigger)# exit
```

then gatekeeper alpha checks all incoming RRQ messages for the MCU or H.323 proxy endpoint or supported prefix 1# before checking for the supported prefix 1234*. If any one of those conditions is met, the gatekeeper sends the RRQ message to the GKTMP server Server-west.

If the second gatekeeper alpha RRQ trigger registration had been defined with a priority 1 instead of priority 2, then the second trigger registration would have overridden the first one. In other words, the gatekeeper alpha would send to GKTMP server Server-west only those RRQ messages that contain a supported prefix of 1234*. All other RRQ messages would not be sent to the GKTMP server.

Related Commands	Command	Description
	show gatekeeper servers	Displays the triggers configured on the gatekeeper.
	server registration-port	Configures the server listening port on the gatekeeper.

server trigger urq

To configure the unregistration request (URQ) trigger statically on the gatekeeper, use the **server trigger urq** command in gatekeeper configuration mode. Submode commands are available after entering the **server trigger urq** command. To delete a single static trigger on the gatekeeper, use the **no** form of this command. To delete all static triggers on the gatekeeper, use the **all** form of the command.

```
server trigger urq gkid priority server-id server-ipaddress server-port
  submode commands:
    info-only
    shutdown
    endpoint-type value | supported-prefix value
```

```
no server trigger urq gkid priority server-id server-ipaddress server-port
```

```
no server trigger all
```

Syntax Description

all	Deletes all CLI configured triggers.
<i>gkid</i>	The local gatekeeper identifier.
<i>priority</i>	The priority for each trigger. The range is 1 to 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.

Submode commands

After entering the **server trigger urq** command, the software enters a submode that permits you to configure additional filters on the RAS message. These filters are optional and you may configure any of them, one per command line.

info-only	Use the info-only submode command to indicate to the Cisco IOS gatekeeper that messages that meet the specified trigger parameters should be sent to the GKTMP server application as notifications only and that the gatekeeper should not wait for a response from the GKTMP server application.
shutdown	Use the shutdown submode command to temporarily disable a trigger. The gatekeeper does not consult triggers in a shutdown state when determining what message to forward to the GKTMP server application.

endpoint-type *value*

Use the **endpoint-type** submode command to send URQ RAS messages containing a particular endpoint type to the GKTMP server application.

- *value*—Specifies the value against which to compare the endpoint-type in the RAS messages. Valid endpoint types are:
 - **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 terminal.
 - **voice-gateway**—The endpoint is a voice gateway.

supported-prefix *value*

Use the **supported-prefix** submode command to send URQ RAS messages containing a specific supported prefix to the GKTMP server application.

- *value*—Specifies the value against which to compare the supported prefix in the RAS messages. The possible values are any E.164 pattern used as a gateway technology prefix. The value string can contain any of the following: 0123456789#*.

Defaults

No trigger servers are set

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(2)XB	The drq , rai , and brq triggers were added.
12.2(2)XU	The irr trigger was added and the command was extended to the Cisco 3660 and Cisco 7200 platforms.

Usage Guidelines

Use the **server trigger urq** command and its optional submode commands to configure the unregistration request (URQ) static server trigger. The gatekeeper checks incoming gateway URQ messages for the configured trigger information. If an incoming URQ message contains the specified trigger information, the gatekeeper sends the URQ message to the GKTMP server application. In addition, the gatekeeper processes the message according to its programmed instructions. If the URQ message does not contain the specified information, the gatekeeper processes the message but does not send it to the GKTMP server application.

If no submode commands are configured for the URQ messages, the gatekeeper sends all URQ messages to the GKTMP server application.

If the gatekeeper receives an URQ trigger registration message containing several trigger conditions, the conditions are treated as “OR” conditions. In other words, if an incoming URQ RAS message meets any one of the conditions, the gatekeeper sends the RAS message to the GKTMP server.

If the gatekeeper receives two URQ trigger registration messages with the same priority for the same GKTMP server, the gatekeeper retains the second registration and discards the first one.

If the gatekeeper receives two URQ trigger registration messages with different priorities for the same GKTMP server, the gatekeeper checks incoming URQ messages against the conditions on the higher priority registration before using the lower priority registration.

If the gatekeeper receives more than one URQ trigger registration message with the same priority but for different GKTMP servers, the gatekeepers retains all of the registrations.

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

The following example configures a trigger registration on gatekeeper sj.xyz.com to send all URQ messages to GKTMP server Server-123:

```
Router(config-gk)# server trigger urq sj.xyz.com 1 Server-123 1.14.93.130 1751
Router(config-gk_urqtrigger)# exit
```

The following example configures an URQ trigger registration on gatekeeper alpha, which will send to the GKTMP server Server-west any URQ message containing an MCU endpoint, an H.323 proxy endpoint, or a supported prefix 1#. All other URQ messages will not be sent to the GKTMP server.

```
Router(config-gk)# server trigger urq alpha 1 Server-west 10.10.10.10 1751
Router(config-gk_urqtrigger)# endpoint-type mcu
Router(config-gk_urqtrigger)# endpoint-type proxy
Router(config-gk_urqtrigger)# supported-prefix 1#
Router(config-gk_urqtrigger)# exit
```

If the URQ registration message defined above for gatekeeper alpha is configured and the gatekeeper receives the following trigger registration:

```
Router(config-gk)# server trigger urq alpha 2 Server-west 10.10.10.10 1751
Router(config-gk_urqtrigger)# supported-prefix 1234*
Router(config-gk_urqtrigger)# exit
```

then gatekeeper alpha checks all incoming URQ messages for the MCU or H.323 proxy endpoint or supported prefix 1# before checking for the supported prefix 1234*. If any one of those conditions is met, the gatekeeper sends the URQ message to the GKTMP server Server-west.

If the second gatekeeper alpha URQ trigger registration had been defined with a priority 1 instead of priority 2, then the second trigger registration would have overridden the first one. In other words, the gatekeeper alpha would send to GKTMP server Server-west only those URQ messages that contain a supported prefix of 1234*. All other URQ messages would not be sent to the GKTMP server.

Related Commands	Command	Description
	show gatekeeper servers	Displays the triggers configured on the gatekeeper.
	server registration-port	Configures the server listening port on the gatekeeper.

show gatekeeper circuits

To display the circuit information on the gatekeeper, use the **show gatekeeper circuits** command in privileged EXEC mode.

```
show gatekeeper circuits [ [ {begin | exclude | include} expression]
```

Syntax Description	begin	Display all circuits, beginning with the line containing <i>expression</i> .
	exclude	Display all circuits, excluding those containing <i>expression</i> .
	include	Display all circuits, including those containing <i>expression</i> .
	<i>expression</i>	(Optional) Word or phrase used to determine what lines will be displayed.

Defaults No default behavior or values

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(2)XU	This command was introduced.

Usage Guidelines Use the **show gatekeeper circuits** command to display current configuration information about the circuits registered with the gatekeeper.

Examples The following command displays the carrier information for the gatekeeper:

```
Router# show gatekeeper circuits

Circuit      Endpoint    Max Calls Avail Calls Resources      Zone
-----
CarrierA     Total Endpoints: 2
              3640-gw1   25         25         Available
              5400-gw1   23         19         Unavailable
CarrierB     Total Zones: 1
                                                    MsPacmanGK
```

[Table 5](#) describes the fields shown in the `show gatekeeper circuits` sample output.

Table 5 *show gatekeeper carriers Fields*

Field	Description
Circuit	Name of the each circuit connected to the gatekeeper.
Endpoint	Name of each H.323 endpoint.
Max Calls	The maximum number of calls that circuit can handle.

Table 5 show gatekeeper carriers Fields

Field	Description
Avail Calls	The number of new calls that the circuit can handle at the current time.
Resources	Indicates whether the circuit's resources have exceeded the defined threshold limits. The endpoint resource threshold command defines these thresholds.
Zone	The zone that supports the endpoint. The zone circuit-id command assigns a zone to an endpoint.
Total Endpoints	Total number of endpoints supported by the circuit.
Total Zones	Total number of zones supported by the circuit.

Related Commands

Command	Description
endpoint resource threshold	Sets a gateway's capacity thresholds in the gatekeeper.
zone circuit-id	Assigns a remote zone to a carrier.

show gatekeeper endpoint circuits

To display the information of all registered endpoints and carriers or trunk groups for a gatekeeper, use the **show gatekeeper endpoint circuit** command in privileged EXEC mode.

```
show gatekeeper endpoint circuits [ | {begin | exclude | include} expression]
```

Syntax Description	begin	Display all circuits, beginning with the line containing <i>expression</i> .
	exclude	Display all circuits, excluding those containing <i>expression</i> .
	include	Display all circuits, including those containing <i>expression</i> .
	<i>expression</i>	(Optional) Word or phrase used to determine what lines will be displayed.

Defaults No default behavior or values

Command Modes Privileged EXEC

Command History	Release	Modification
	11.3(2)NA	This command was introduced.
	12.0(5)T	The display format was modified for H.323 Version 2.
	12.2(2)XU	The display form was modified for show the E164-ID, carrier and trunk group data, and total number of active calls.

Usage Guidelines Use the **show gatekeeper endpoint circuit** command to display current configuration information about the endpoints and carriers registered with the gatekeeper.

Examples The following command displays the circuit information for the gatekeeper:

```
Router# show gatekeeper endpoint circuits
```

```

                                GATEKEEPER ENDPOINT REGISTRATION
                                =====
CallSignalAddr  Port  RASignalAddr  Port  Zone Name      Type  Flags
-----
172.18.195.120  1720  172.18.195.120  51059  LavenderGK     VOIP-GW
      E164-ID: 4081234
      H323-ID: 3640-gw1
      Carrier: CarrierA, Max Calls: 25, Available: 25
172.18.197.143  1720  172.18.197.143  57071  LavenderGK     VOIP-GW
      H323-ID: 5400-gw1
      Carrier: CarrierB, Max Calls: 23, Available: 19
      Carrier: CarrierA, Max Calls: 25, Available: 25
Total number of active registrations = 2

```

Table 6 describes the fields shown in the `show gatekeeper endpoint circuits` sample output.

Table 6 *show gatekeeper endpoint circuits Fields*

Field	Description
CallSignalAddr	Call signaling IP address of the endpoint. If the endpoint is also registered with an alias, a list of all aliases registered for that endpoint should be listed on the line below.
Port	Call signaling port number of the endpoint.
RASSignalAddr	RAS IP address of the endpoint.
Port	RAS port number of the endpoint.
Zone Name	Zone name (gatekeeper ID) that this endpoint registered in.
Type	The endpoint type (for example, terminal, gateway, or MCU).
Flags	S—Indicates that the endpoint is statically entered from the alias command rather than being dynamically registered through RAS messages. O—Indicates that the endpoint, which is a gateway, has sent notification that it is nearly out of resources.
E164-ID	The E.164 ID of the endpoint.
H323-ID	The H.323 ID of the endpoint.
Carrier	The carrier associated with the endpoint.
Max Calls	The maximum number of calls the circuit can handle.
Available	The number of new calls the circuit can handle currently.

Related Commands

Command	Description
endpoint circuit-id h323id	Assigns a circuit to a non-Cisco endpoint.
endpoint resource threshold	Sets a gateway's capacity thresholds in the gatekeeper.
zone circuit-id	Assigns a circuit to a remote zone.

show gatekeeper endpoints

To display the call capacities of all registered endpoints for a gatekeeper, use the **show gatekeeper endpoints** command in privileged EXEC mode.

show gatekeeper endpoints

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes Privileged EXEC

Command History	Release	Modification
	11.3(2)NA	This command was introduced.
	12.0(5)T	The display format was modified for H.323 Version 2.
	12.2(2)XU	The registration and call capacities were added to the display.

Usage Guidelines Use this command to display the registered endpoints and total call capacities for all trunk groups or carriers supported by a gatekeeper. Use the [show gatekeeper endpoint circuits](#) command to display carrier or trunk group call capacity information.

Examples The following example displays the registered endpoints and call capacities for a gatekeeper:

```
Router# show gatekeeper endpoints

                                GATEKEEPER ENDPOINT REGISTRATION
                                =====
CallsignalAddr  Port  RASSignalAddr  Port  Zone Name  Type  Flags
-----
172.21.127.8    1720  172.21.127.8   57787  sj-gk      VOIP-GW
                H323-ID:joe@cisco.com
                Voice Capacity Max.=23  Avail.=23
                Total number of active registrations = 1
```

[Table 7](#) describes the fields in the **show gatekeeper endpoints** display.

Table 7 *show gatekeeper endpoints Field Descriptions*

Field	Description
CallSignalAddr	Call signaling IP address of the endpoint. If the endpoint is also registered with alias, a list of all aliases registered for that endpoint should be listed on the line below.
Port	Call signaling port number of the endpoint.
RASSignalAddr	Registration, admission, and status (RAS) protocol IP address of the endpoint.
Port	RAS port number of the endpoint.
Zone Name	Zone name (gatekeeper ID) that this endpoint registered in.
Type	The endpoint type (for example, terminal, gateway, or MCU).
Flags	S—Indicates that the endpoint is statically entered from the alias command rather than being dynamically registered through RAS messages. O—Indicates that the endpoint, which is a gateway, has sent notification that it is nearly out of resources.

Related Commands

Command	Description
show gatekeeper endpoint circuits	Displays endpoint and carrier or trunk group call capacities.
endpoint resource threshold	Sets a gateway's capacity thresholds in the gatekeeper.

show gatekeeper servers

To see a list of currently registered and statically configured triggers on this gatekeeper, enter the **show gatekeeper servers** command in privileged EXEC mode.

```
show gatekeeper servers [gkid] [ | { begin | exclude | include } expression]
```

Syntax Description		
	<i>gkid</i>	(Optional) The local gatekeeper name to which this trigger applies.
	begin	Display all circuits, beginning with the line containing <i>expression</i> .
	exclude	Display all circuits, excluding those containing <i>expression</i> .
	include	Display all circuits, including those containing <i>expression</i> .
	<i>expression</i>	(Optional) Word or phrase used to determine what lines will be displayed.

Defaults No default behavior or values

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(1)T	This command was introduced.
	12.2(2)XU	The server timeout and GKTMP version values were added.

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 zones on this gatekeeper appear.

Examples The following example shows the server triggers for the gatekeeper zone named tree:

```
Router# show gatekeeper servers tree

      GATEKEEPER SERVERS STATUS
      =====

Gatekeeper Server listening port: 5055
Gatekeeper Server timeout value: 30 (100ms)
GateKeeper GKTMP version: 4.1

Gatekeeper-ID: 5400-gk1
-----
```

[Table 8](#) describes the fields shown in the **show gatekeeper server** command output.

Table 8 *show gatekeeper servers Fields*

Field	Description
Gatekeeper Server listening port	The gatekeeper port configured to receive calls.
Gatekeeper Server timeout value	The timeout value configured on the gatekeeper.
GateKeeper GKTMP version	The version of GKTMP used installed on the gatekeeper.
Gatekeeper-ID	The name of the gatekeeper.

Related Commands

Command	Description
debug cch323 capacity	Tracks call capacity information on the gatekeeper.
server trigger arq	Configures static triggers on the gatekeeper.
server registration-port	Configures a listening port on the gatekeeper for server registration.

zone circuit-id

To associate a remote zone with a circuit, use the **zone circuit-id** command in gatekeeper configuration mode. To delete the zone, use the **no** form of this command.

zone circuit-id *remote-zone-name* *circuit-id*

no zone circuit-id *remote-zone-name* *circuit-id*

Syntax Description		
	<i>remote-zone-name</i>	Name of the remote zone.
	<i>circuit-id</i>	ID of the circuit to be associated with the remote zone.

Defaults No default behavior or values

Command Modes Gatekeeper configuration

Command History	Release	Modification
	12.2(2)XU	This command was introduced.

Usage Guidelines When VoIP calls come to the gatekeeper from a non-Cisco gatekeeper in a remote zone (for example, from an ITSP), the LRQ message does not include a source circuit identifier. This command allows the gatekeeper to assign a circuit identifier to the zone and an IP address of the call origination. The GKTMP server application uses this data to determine a route for the call.

Examples The following example configures the remote zone GKout with a circuit ID CarrierA:

```
Router(config)# gatekeeper
Router(config-gk)# zone circuit-id GKout CarrierA
```

Related Commands	Command	Description
	show gatekeeper circuits	Displays the circuit information on the gatekeeper.
	show gatekeeper endpoint circuits	Displays information for all registered endpoints and carriers for the gatekeeper.
	endpoint circuit-id h323id	Assigns a circuit to a non-Cisco endpoint.

zone local

To specify a zone controlled by a gatekeeper, use the **zone local** command in gatekeeper configuration mode. To remove a zone controlled by a gatekeeper, use the **no** form of this command.

zone local *gatekeeper-name domain-name [ras-IP-address]*

no zone local *gatekeeper-name domain-name [ras-IP-address]*

Syntax Description

<i>gatekeeper-name</i>	The gatekeeper's name or zone name. This is usually the fully domain-qualified host name of the gatekeeper. For example, if the domain-name is cisco.com, the <i>gatekeeper-name</i> might be gk1.cisco.com. However, if the gatekeeper is controlling multiple zones, the <i>gatekeeper-name</i> for each zone should be some unique string that has a mnemonic value.
<i>domain-name</i>	The domain name served by this gatekeeper.
<i>ras-IP-address</i>	(Optional) The IP address of one of the interfaces on the gatekeeper. When the gatekeeper responds to gatekeeper discovery messages, it signals the endpoint or gateway to use this address in future communications.



Note

Setting this address for one local zone makes it the address used for all local zones.

Defaults

No local zone is defined.



Note

The gatekeeper cannot operate without at least one local zone definition. Without local zones, the gatekeeper goes to an inactive state when the **no shutdown** command is issued.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
11.3(2)NA	This command was introduced on Cisco 2500 and Cisco 3600 series routers.
12.2(2)XU	This command was extended to the Cisco MC3810 and Cisco 7200 series routers.

Usage Guidelines

Multiple local zones can be defined. The gatekeeper manages all configured local zones. Intrazone and interzone behavior remains the same (zones are controlled by the same or different gatekeepers).

Only one *ras-IP-address* argument can be defined for all local zones. You cannot configure each zone to use a different RAS IP address. If you define this in the first zone definition, you can omit it for all subsequent zones, which automatically pick up this address. If you set it in a subsequent **zone local** command, it changes the RAS address of all previously configured local zones as well. Once defined, you can change it by reissuing any **zone local** command with a different *ras-IP-address* argument.

If the *ras-IP-address* argument is a Hot Standby Router Protocol (HSRP) virtual address, it automatically puts the gatekeeper into HSRP mode. In this mode, the gatekeeper assumes standby or active status according to whether the HSRP interface is on standby or active status.

You cannot remove a local zone if there are endpoints or gateways registered in it. To remove the local zone, shut down the gatekeeper first, which forces unregistration.

Multiple zones are controlled by multiple logical gatekeepers on the same Cisco IOS platform.

The maximum number of local zones defined in a gatekeeper should not exceed 100.

This command can also be used to change the IP address used by the gatekeeper.

Examples

The following example creates a zone controlled by the easterngk gatekeeper in the domain called cisco.com:

```
Router(config)# gatekeeper
Router(config-gk)# zone local easterngk.cisco.com cisco.com
```

Related Commands


Command	Description
show proxy h323 calls	Displays a list of each active call on the proxy.
zone subnet	Specifies a zone controlled by a gatekeeper.

zone prefix

To add a prefix to the gatekeeper zone list, use the **zone prefix** command in gatekeeper configuration mode. To remove knowledge of a zone prefix, use the **no** form of this command with the gatekeeper name and prefix. To remove the priority assignment for a specific gateway, use the **no** form of this command with the **gw-priority** option.

```
zone prefix gatekeeper-name e164-prefix [blast | seq] [gw-priority priority
gw-alias [gw-alias, ...]]
```

```
no zone prefix gatekeeper-name e164-prefix [blast | seq] [gw-priority priority
gw-alias [gw-alias, ...]]
```

Syntax Description	
<i>gatekeeper-name</i>	The name of a local or remote gatekeeper, which was previously defined by using the zone local or zone remote command.
<i>e164-prefix</i>	An E.164 prefix in standard form followed by dots (.). Each dot represents a number in the E.164 address. For example, 212..... is matched by 212 and any seven numbers.
	 <p>Note Although a dot representing each digit in an E.164 address is the preferred configuration method, you can also enter an asterisk (*) to match any number of digits.</p>
blast	(Optional) If you list multiple hopoffs, this indicates that the LRQs should be sent simultaneously to the gatekeepers based on the order in which they were listed. The default is seq .
seq	(Optional) If you list multiple hopoffs, this indicates that the LRQs should be sent sequentially to the gatekeepers based on the order in which they were listed. The default is seq .
gw-priority <i>priority</i> <i>gw-alias</i>	<p>(Optional) Use the gw-priority option to define how the gatekeeper selects gateways in its local zone for calls to numbers beginning with prefix <i>e164-prefix</i>. Do not use this option to set priority levels for a prefix assigned to a remote gatekeeper.</p> <p>Use values from 0 to 10. A 0 value prevents the gatekeeper from using the gateway <i>gw-alias</i> for that prefix. Value 10 places the highest priority on gateway <i>gw-alias</i>. If you do not specify a priority value for a gateway, the value 5 is assigned.</p> <p>To assign the same priority value for one prefix to multiple gateways, list all the gateway names after the <i>priority</i> value.</p> <p>The <i>gw-alias</i> name is the H.323 ID of a gateway that is registered or will register with the gatekeeper. This name is set on the gateway with the h323-gateway voip h.323-id command.</p>

Defaults

No prefixes are defined.
Gateway priority is 5.

Command Modes Gatekeeper configuration

Command History

Release	Modification
11.3(6)Q	This command was introduced.
11.3(7)NA	This command was modified for H.323 Version 1.
12.0(5)T	The display format was modified for H.323 Version 2.
12.2(2)XU	This command was extended to include the Cisco 3660 and Cisco 7200 platforms.

Usage Guidelines

A gatekeeper can handle more than one zone prefix, but a zone prefix cannot be shared by more than one gatekeeper. If you have defined a zone prefix as being handled by a gatekeeper and now define it as being handled by a second gatekeeper, the second assignment cancels the first.

If you need a gatekeeper to handle more than one prefix, but for cost reasons you want to be able to group its gateways by prefix usage, there are two ways to do it.

The first method is simpler, has less overhead, and is recommended if your gateways can be divided into distinct groups, in which each group is to be used for a different set of prefixes. For instance, if a group of gateways is used for calling area codes 408 and 650, and another group is used for calling area code 415, you can use this method. In this case, you define a local zone for each set of prefixes, and have the group of gateways to be used for that set of prefixes register with that specific local zone. Do not define any gateway priorities. All gateways in each local zone are treated equally in the selection process.

However, if your gateways cannot be cleanly divided into non-intersecting groups (for instance if one gateway is used for calls to 408 and 415 and another gateway is used for calls to 415 and 650, and so on), you can put all these gateways in the same local zone and use the **gw-priority** option to define which gateways will be used for which prefixes.

When choosing a gateway, the gatekeeper first looks for the longest zone prefix match; then it uses the priority and the gateway status to select from the gateways.

If all gateways are available, the gatekeeper chooses the highest priority gateway. If all the highest-priority gateways are busy (see the gateway **resource threshold** command), a lower-priority gateway is selected.



Note The **zone prefix** command matches a prefix to a gateway. It does not register the gateway. The gateway must register with the gatekeeper before calls can be completed through that gateway.

Examples

The following example shows how you can define multiple local zones for separating your gateways:

```
Router (config)# gatekeeper
Router(config-gk)# zone local gk408or650 xyz.com
Router(config-gk)# zone local gk415 xyz.com
Router(config-gk)# zone prefix gk408or650 408.....
Router(config-gk)# zone prefix gk408or650 650.....
Router(config-gk)# zone prefix gk415 415.....
```

Now you need to configure all the gateways to be used for area codes 408 or 650 to register with gk408or650 and all gateways to be used for area code 415 to register with gk415. On Cisco voice gateways, you configure the gateways to register with the appropriate gatekeepers by using the **h323 voip id** command.

The following example shows how you can put all your gateways in the same zone but use the **gw-priority** keyword to determine which gateways are used for calling different area codes:

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

The commands shown accomplish the following tasks:

- 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; 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 gateway 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.

The following example changes gateway gw2 from priority 10 for zone 415..... to the default priority 5:

```
Router(config)# gatekeeper
Router(config-gk)# no zone prefix localgk 415..... gw-pri 10 gw2
```

The following example changes both gateways gw1 and gw2 from priority 10 for zone 415..... to the default priority 5:

```
Router(config)# gatekeeper
Router(config-gk)# no zone prefix localgk 415..... gw-pri 10 gw1 gw2
```

In the preceding example, the prefix 415..... remains assigned to gatekeeper localgk. All gateways that do not specify a priority level for this prefix are assigned a default priority of 5. The following example removes the prefix and all associated gateways and priorities from this gatekeeper:

```
Router(config)# gatekeeper
Router(config-gk)# no zone prefix localgk 415.....
```

Related Commands	Command	Description
	register	Configures a gateway to register or unregister a fully qualified dial-peer E.164 address with a gatekeeper.
	resource threshold	Configures a gateway to report H.323 resource availability to the gatekeeper of the gateway.
	show call resource voice threshold	Displays the threshold configuration settings and status for an H.323 gateway.
	show gateway	Displays the current gateway status.
	zone local	Specifies a zone controlled by a gatekeeper.
	zone remote	Statically specifies a remote zone if DNS is unavailable or undesirable.

zone remote

To configure a zone in the gatekeeper's remote zone list, use the **zone remote** command in gatekeeper configuration mode. To delete the zone, use the **no** form of this command.

```
zone remote other-gatekeeper-name other-domain-name other-gatekeeper-ip-address
[port-number] [cost cost-value [priority priority-value]] [foreign-domain]
```

```
no zone remote other-gatekeeper-name other-domain-name other-gatekeeper-ip-address
[port-number] [cost cost-value [priority priority-value]] [foreign-domain]
```

Syntax Description		
<i>other-gatekeeper-name</i>	Name of the remote gatekeeper.	
<i>other-domain-name</i>	Domain of the remote gatekeeper.	
<i>other-gatekeeper-ip-address</i>	IP address and port of the remote gatekeeper.	
<i>port-number</i>	RAS signaling port number. Valid values are 1 to 65535.	
cost	(Optional) Cost of the remote zone.	
<i>cost-value</i>	(Optional) Cost value. Range is 1 through 100. Default is 50.	
priority	(Optional) Priority of the remote zone.	
<i>priority-value</i>	(Optional) Priority value. Range is 1 through 100. Default is 50.	
foreign-domain	(Optional) Indicates the zone is part of a foreign domain.	

Defaults	
	No remote zone is defined.
	Default RAS port is 1719.
	Cost-value is 50.
	Priority-value is 50.

Command Modes	
	Gatekeeper configuration

Command History	Release	Modification
	11.3(2)NAand 12.0(3)T	This command was introduced on Cisco 2500 and Cisco 3600 series routers.
	12.1(5)XM	The cost and priority keywords were added.
	12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
	12.2(2)XA	The foreign-domain keyword was added.
	12.2(4)T	The new and modified commands introduced in Cisco IOS Release 12.2(2)XA were integrated into Cisco IOS Release 12.2(4)T. Support for the Cisco AS5300 is not included in this release.
	12.2(2)XB1	This command was implemented on the Cisco AS5850 platform.
	12.2(2)XU	This command was extended to the Cisco AS5400 and Cisco 7200 series platforms.

Usage Guidelines

All gatekeepers do not have to be in DNS. For those that are not, use the **zone remote** command so that the local gatekeeper knows how to access them. In addition, you may wish to improve call response time slightly for frequently accessed zones. If the **zone remote** command is configured for a particular zone, you do not need to make a DNS lookup transaction.

The maximum number of zones defined on a gatekeeper varies depending on the mode or the call model or both. For example, a directory gatekeeper may be in the mode of being responsible for forwarding location request (LRQ) messages and not handling any local registrations and calls; the call model might be E.164 addressed calls instead of H.323-ID addressed calls.

For a directory gatekeeper that does not handle local registrations and calls, the maximum remote zones defined should not exceed 10,000; an additional 4 MB of memory is required to store this maximum number of remote zones.

For a gatekeeper that handles local registrations and only E.164-addressed calls, the number of remote zones defined should not exceed 2000.

For a gatekeeper that handles H.323-ID calls, the number of remote zones defined should not exceed 200.

When there are several remote zones configured, they can be ranked by cost and priority value. A zone with a lower cost value and a higher priority value is given preference over others.

Examples

The following example assigns the remote zone GK10 to the domain Zone1:

```
Router(config)# gatekeeper
Router(config-gk)# zone remote GK10 Zone1 209.165.200.224 cost 20 priority 5
```

Related Commands

Command	Description
show proxy h323 calls	Displays a list of each active call on the proxy.
zone local	Specifies the zones controlled by a gatekeeper.

Glossary

- ACF**—admission confirmation RAS message
- ANI**—Automatic Number Identification, representing the calling party's telephone number
- ARQ**—admission request RAS message
- ASP**—Application Service Provider
- BRQ**—bandwidth request RAS message
- CAS**—channel-associated signaling
- CDR**—call detail record
- Circuit identifier**—a trunk group label or a carrier ID
- CSA**—H.323 call signaling address of the gateway or endpoint
- CSR**—carrier sensitive routing
- DNIS**—Dialed Number Identification Service, representing the called party's telephone number
- DRQ**—disengage request RAS message
- GK**—gatekeeper
- GKTMP**—Gatekeeper Transaction Message Protocol. This is a proprietary Cisco protocol that allows third-party applications to influence the operation of the Cisco IOS Gatekeeper.
- GW**—gateway
- HSRP**—hot standby router protocol
- IRR**—information request response RAS message
- ITSP**—Internet Telephony Service Provider
- IVR**—interactive voice response
- IZCT**—Interzone clearToken. This is a new clearToken format introduced in this feature to identify the source and destination zones of an interzone call.
- LCF**—location confirmation RAS message
- LRJ**—location reject RAS message
- LRQ**—location request RAS message
- OGK**—originating gatekeeper
- OGW**—originating gateway
- OSS**—operations support system
- POP**—point of presence
- PSTN**—Public Switched Telephone Network
- RAI**—resources available indicator RAS message
- RAS**—H.225 Registration, Admission, and Status Protocol, which is the communication protocol between H.323 gateways and their gatekeepers.
- RRQ**—registration request RAS message
- SPI**—service provider interface
- TDM**—time-division multiplexing
- TGK**—terminating gatekeeper

TGW—terminating gateway

URQ—unregistration request RAS message

VSA—vendor-specific attribute. This is a nonstandard attribute tag used by RADIUS to enhance the gateway-to-gatekeeper CDR format.