



# VoIP Gatekeeper Trunk and Carrier Based Routing Enhancements

## Feature History

Release	Modification
12.2(11)T	This feature was introduced on the Cisco 2600 series, Cisco 3600 series, Cisco 3700 series, Cisco 7200 series, and Cisco MC3810 for the gatekeeper.
12.3	This feature was integrated into Cisco IOS Release 12.3.

This feature module describes the VoIP Gatekeeper Trunk and Carrier Based Routing Enhancements feature functionality in Cisco IOS Release 12.2(11)T, and includes the following sections:

- [Feature Overview, page 1](#)
- [Supported Platforms, page 14](#)
- [Supported Standards, MIBs, and RFCs, page 14](#)
- [Prerequisites, page 14](#)
- [Configuration Tasks, page 15](#)
- [Monitoring and Maintaining, page 19](#)
- [Configuration Examples, page 19](#)
- [Command Reference, page 22](#)

For information about routing enhancements on the gateway, refer to *VoIP 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 VoIP Gatekeeper Trunk and Carrier Based Routing Enhancements feature enables the H.323 gatekeeper to collect information about the PSTN-side interfaces and the call capacity statistics for those interfaces on a per-call basis from the H.323 gateway and endpoint. This feature also enables the H.323 gateway to report the PSTN-side interfaces for incoming and outgoing calls to the H.323 gatekeeper to help in routing decisions.

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.

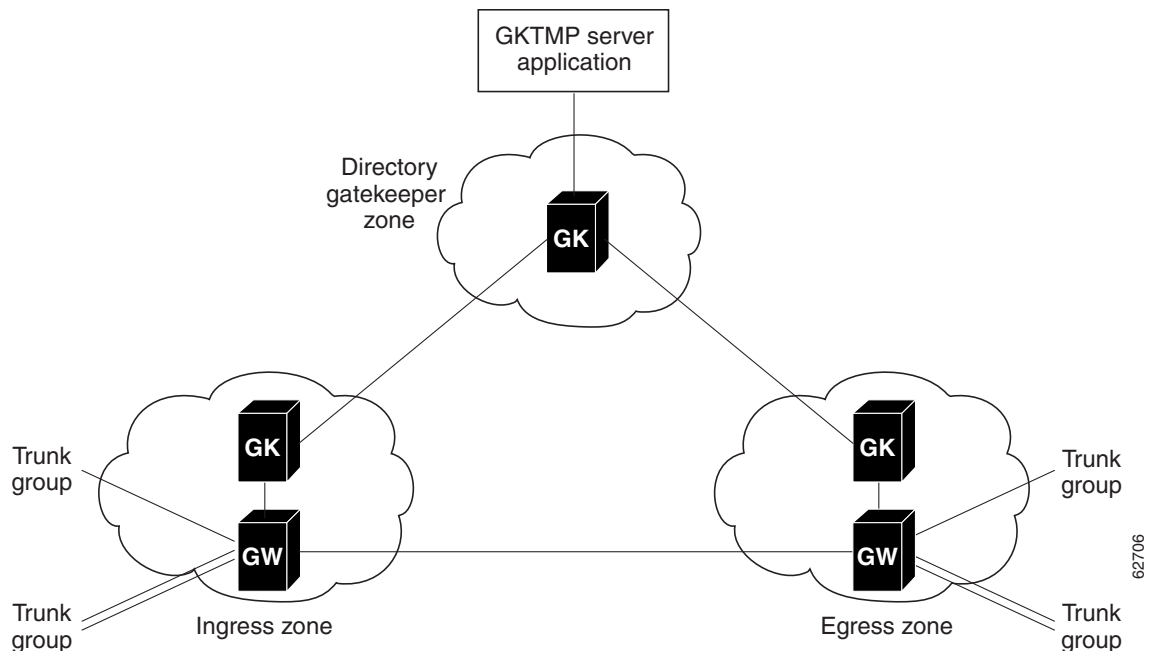


**Note** This feature refers to *circuits* in the network. Circuits can be DS-0 trunks, trunk groups, or carrier IDs. Call routing is done using either carrier IDs or trunk group labels.

- 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.



**Note** This document provides a high-level overview of the new gateway functionality. The gateway enhancements are described in detail in *VoIP 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
- Vendor-specific attributes (VSAs)
- 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

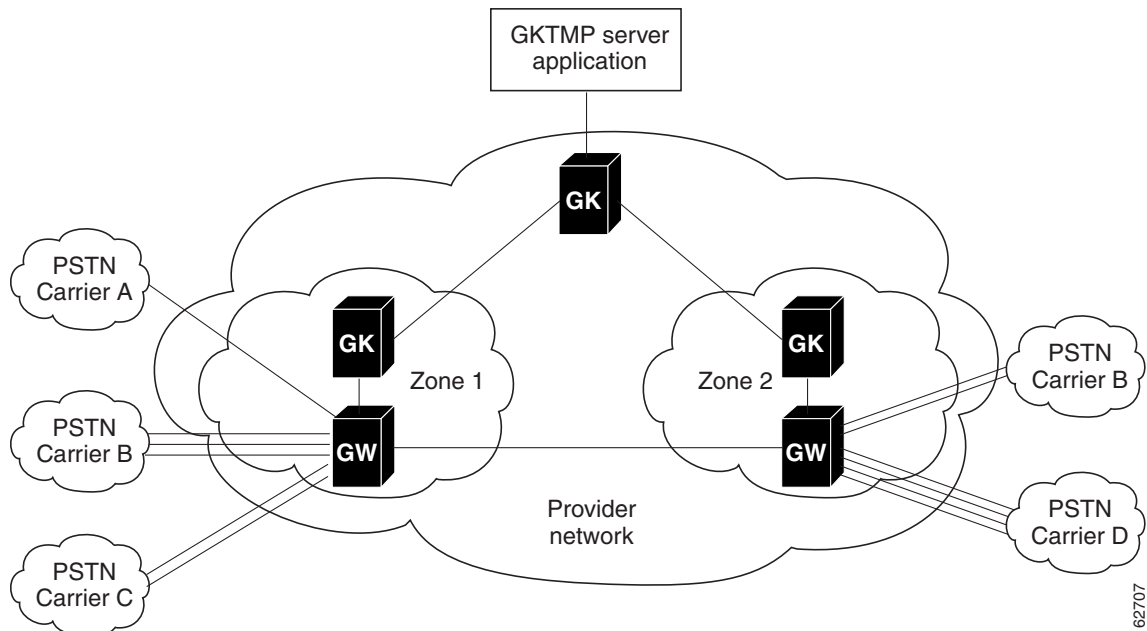
The next section, [Wholesale Voice Network Scenario](#), describes the network configuration that incorporates these features. See [Call Routing, page 4](#) for more detailed descriptions of the new routing functions on the gateways, gatekeepers, and GKTMP server application.

## 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.

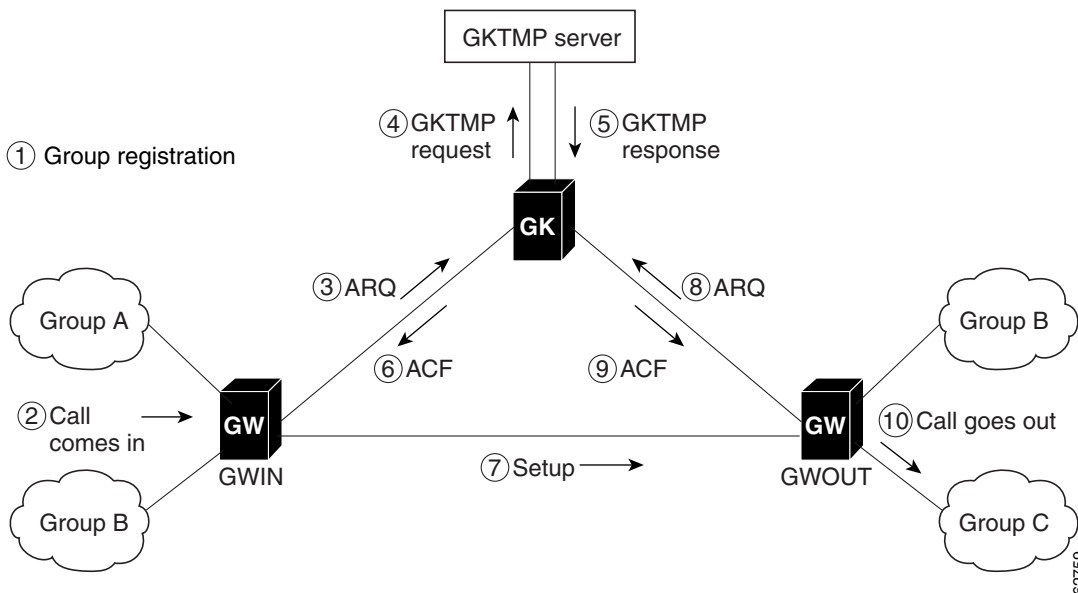
## Call Routing

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 typically requires connection to a local operations support system (OSS) for accurate tracking of current calls. The call routing process is shown in Figure 3.

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

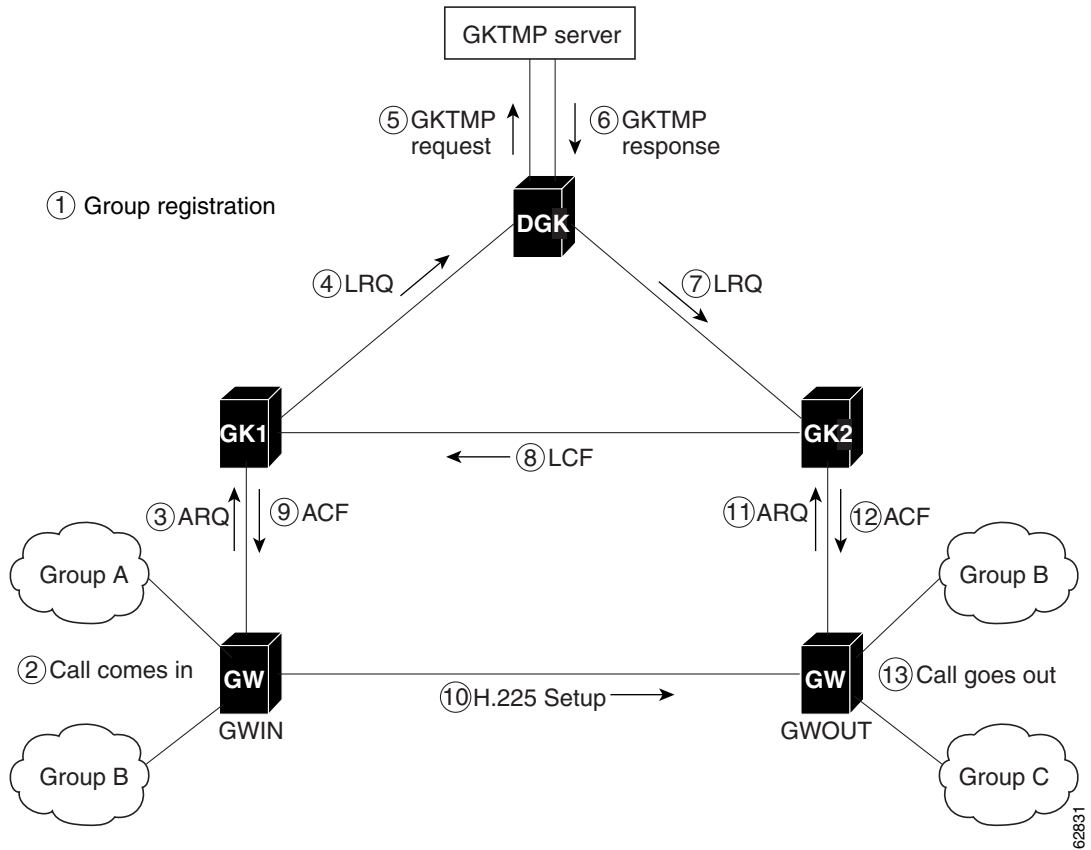


The following table explains the steps in the zone gatekeeper call routing process. For clarity, assume the calling party (ANI) is 1234 and the called party (DNIS) is 5678. Groups A, B, and C have circuit identifiers GroupA, GroupB, and GroupC, respectively. (Circuit identifiers represent trunk group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

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.  <b>Note</b> These ANI and DNIS numbers would be translated if the gateway is configured to do that. Refer to <i>VoIP Gateway Trunk and Carrier Based Routing Enhancements</i> for a description of the number translation processes.
3. ARQ	The GWIN sends an ARQ message to the gatekeeper containing: <ul style="list-style-type: none"> <li>• srcInfo=1234</li> <li>• dstInfo=5678</li> <li>• sourceCircuitID=GroupA</li> <li>• destinationCircuitID=NULL</li> </ul>

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"> <li>• srcInfo=1234</li> <li>• dstInfo=5678</li> <li>• sourceCarrier/source TrunkGroup=GroupA</li> <li>• destinationCarrier/destination TrunkGroup=NULL</li> </ul>
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"> <li>• srcInfo=1234</li> <li>• dstInfo=5678</li> <li>• sourceCarrier/source TrunkGroup=GroupA</li> <li>• destinationCarrier/destination TrunkGroup=GroupC</li> </ul>
6. ACF	The gatekeeper sends an ACF message to the GWIN containing: <ul style="list-style-type: none"> <li>• CSA=GWOUT</li> <li>• sourceCircuitID=GroupA</li> <li>• destinationCircuitID=GroupC</li> </ul>
7. H.225 Setup	The gateway sends a Setup message to the GWOUT containing: <ul style="list-style-type: none"> <li>• srcInfo=1234</li> <li>• dstInfo=5678</li> <li>• sourceCircuitID=GroupA</li> <li>• destinationCircuitID=GroupC</li> </ul>
8. ARQ	The GWOUT sends a verifying ARQ message to the gatekeeper containing: <ul style="list-style-type: none"> <li>• answerCall=TRUE</li> <li>• srcInfo=1234</li> <li>• dstInfo=5678</li> <li>• sourceCircuitID=GroupA</li> <li>• destinationCircuitID=GroupC</li> </ul>
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



The following table 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.)

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.
3. ARQ	The GWIN sends an ARQ message to GK1 containing: <ul style="list-style-type: none"> <li>• srcInfo=1234</li> <li>• dstInfo=5678</li> <li>• sourceCircuitID=GroupA</li> <li>• destinationCircuitID=NULL</li> </ul>
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"> <li>• srcInfo=1234</li> <li>• dstInfo=5678</li> <li>• sourceCircuitID=GroupA</li> <li>• destinationCircuitID=NULL</li> </ul>
5. GKTMP Request REQUEST-LRQ	GK1 sends a GKTMP Request message to the GKTMP server application containing: <ul style="list-style-type: none"> <li>• srcInfo=1234</li> <li>• dstInfo=5678</li> <li>• sourceCarrier/source TrunkGroup=GroupA</li> <li>• destinationCarrier/destination TrunkGroup=NULL</li> </ul>
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"> <li>• srcInfo=1234</li> <li>• dstInfo=5678</li> <li>• sourceCarrier/source TrunkGroup=GroupA</li> <li>• destinationCarrier/destination TrunkGroup=GroupC with the remote zone gatekeeper's (GK2's) RAS address</li> </ul>
7. LRQ	The DGK sends an LRQ message to GK2 containing: <ul style="list-style-type: none"> <li>• srcInfo=1234</li> <li>• dstInfo=5678</li> <li>• sourceCircuitID=GroupA</li> <li>• destinationCircuitID=GroupC</li> </ul>

Step	Description
8. LCF	GK2 sends an LCF message to GK1 containing: <ul style="list-style-type: none"> <li>• CSA=GWOUT</li> <li>• sourceCircuitID=GroupA</li> <li>• destinationCircuitID=GroupC</li> </ul>
9. ACF	GK1 sends an ACF message to GWIN containing: <ul style="list-style-type: none"> <li>• CSA=GWOUT</li> <li>• sourceCircuitID=GroupA</li> <li>• destinationCircuitID=GroupC</li> </ul>
10. H.225 Setup	GWIN sends a Setup message to GWOUT containing: <ul style="list-style-type: none"> <li>• srcInfo=1234</li> <li>• dstInfo=5678</li> <li>• sourceCircuitID=GroupA</li> <li>• destinationCircuitID=GroupC</li> </ul>
11. ARQ	GWOUT sends a verifying ARQ message to GK2 containing: <ul style="list-style-type: none"> <li>• answerCall=TRUE</li> <li>• srcInfo=1234</li> <li>• dstInfo=5678</li> <li>• sourceCircuitID=GroupA</li> <li>• destinationCircuitID=GroupC</li> </ul>
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 using trunk group identifiers or by carrier identifiers in addition to existing routing mechanisms. To route by carriers, you create the trunk groups and specify an identifier or descriptor to represent a carrier on those trunk groups. 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 *VoIP 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 the gatekeeper and gateways are configured for the use of inter-zone clearToken (IZCT), the RAS, ACF, LRQ, LCF, and the H.225.0 Setup messages will include the IZCT, which consists of the circuit identifiers for the call.

## Call Routing on the Gatekeeper

### Receiving a Call Request

The gatekeeper receives source circuit identifiers from the gateway for the originating call, derived from the voice interface (DS-0). 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 IZCT functionality is enabled, the gatekeeper includes an IZCT with the source, destination, and *intermediate circuit identifiers*. If the egress gateway is in a remote zone with the IZCT functionality enabled, the gatekeeper includes a destination zone in the IZCT as well. 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.

#### Carrier-Based Routing Without a GKTMP Application Server

Carrier-based routing is possible without the presence of the GKTMP application server, if you have Cisco IOS Release 12.3(8)T1, Cisco IOS Release 12.3(11)T, or higher. The trunk group label or carrier ID of the terminating gateway can also be provided by the destination circuitInfo field in ARQ. Incoming ARQ to the gatekeeper has the destination circuitInfo field. When both GKTMP and incoming ARQ provide the trunk group ID or carrier ID, the ID provided by the GKTMP server is accepted. The GKTMP server can also add, modify, or delete the trunk group ID or carrier ID present in ARQ using a RESPONSE ARQ or ACF message. If the RESPONSE ARQ or the ACF message does not include a trunk group label (Q tag) or carrier ID (J tag), only the Q tag or the J tag provided by the incoming ARQ is used for routing.

## 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 works in conjunction with a Cisco IOS gatekeeper. The GKTMP server and the gatekeeper communicate using GKTMP protocol. When the gatekeeper sends the GKTMP server an ARQ or LRQ request 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, called response messages, in GKTMP format. The gatekeeper uses these response messages to proceed further with the routing decisions and send RAS response messages back to the gateway or to the next gatekeeper.

GKTMP server receives the source circuit identifier and called party (DNIS) information from the gatekeeper in the GKTMP message. The gatekeeper extracts the same information from the ARQ and LRQ messages or IZCT, as applicable. 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

GKTMP server call routing offers the following 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

The following restrictions apply to GKTMP server call routing.

**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

**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)
- [VoIP Gateway Trunk and Carrier Based Routing Enhancements](#)

## Related Documents

**General reference documents:**

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

**Feature documents:**

- [VoIP Gateway Trunk and Carrier Based Routing Enhancements](#)
- [Cisco Gatekeeper External Interface Reference](#), Version 4.1

**Related Feature Documents**

- [Inter-Domain Gatekeeper Security Enhancement](#)

**Platform Documents**

- [Cisco 2600 Series product documentation](#)

- [Cisco 3600 Series product documentation](#)
- [Cisco 7202 product documentation](#)
- [Cisco MC3810 product documentation](#)

## Supported Platforms

- Cisco 2600 series modular access routers
- Cisco 3600 series modular access routers
- Cisco 7200 series routers
- Cisco MC3810 multiservice access concentrators

## 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.  
Refer to *VoIP 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)# <b>gatekeeper</b>	Enters gatekeeper configuration mode.
Step 2	Router(config-gk)# <b>zone local</b> <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)# <b>no shutdown</b>	Enables the gatekeeper.
Step 4	Router(config-gk)# <b>server registration-port</b> <i>port-number</i>	Configures the listener port for the server to establish a connection with the gatekeeper.
Step 5	Router(config-gk)# <b>exit</b>	Ends 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)# <b>gatekeeper</b>	Enters gatekeeper configuration mode.
Step 2	Router(config-gk)# <b>gw-type-prefix</b> <i>type-prefix</i> [ [ <b>hopoff</b> <i>gkid1</i> ] [ <b>hopoff</b> <i>gkid2</i> ] [ <b>hopoff</b> <i>gkidn</i> ] [ <b>seq</b>   <b>blast</b> ] ] [ <b>default-technology</b> ] [[ <b>gw ipaddr</b> <i>ipaddr</i> [ <i>port</i> ]] ...]	(Optional) Configures a technology prefix in the gatekeeper.
Step 3	Router(config-gk)# <b>zone prefix</b> <i>gatekeeper-name</i> <i>e164-prefix</i> [ <b>blast</b>   <b>seq</b> ] [ <b>gw-priority</b> <i>priority</i> <i>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.

	Command	Purpose
Step 4	Router(config-gk)# <b>zone remote</b> <i>other-gatekeeper-name other-domain-name</i> <i>other-gatekeeper-ip-address [port-number]</i> [ <b>cost</b> <i>cost-value</i> [ <b>priority</b> <i>priority-value</i> ]] [ <b>foreign-domain</b> ]	(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)# <b>zone circuit-id</b> <i>remote-zone-name</i> <i>circuit-id</i>	(Optional) Assigns a circuit descriptor to a remote zone.
Step 6	Router(config-gk)# <b>lrq reject-unknown-circuit</b>	(Optional) Enables gatekeeper rejection of LRQ messages that contain an unknown destination circuit descriptor.
Step 7	Router(config-gk)# <b>endpoint circuit-id</b> <b>h323id</b> <i>endpoint-h323id circuit-id</i> [ <b>max-calls</b> <i>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)# <b>endpoint resource-threshold</b> <b>onset</b> <i>high-water-mark</i> <b>abatement</b> <i>low-water-mark</i>	(Optional) Sets call volume thresholds in the gatekeeper for monitoring its gateway.
Step 9	Router(config-gk)# <b>server routing</b> { <b>both</b>   <b>carrier</b>   <b>trunk-group</b> }	(Optional) Enables routing of only carrier or trunk-group information to the GKTMP server.
Step 10	Router(config-gk)# <b>server flow-control</b> [ <b>onset</b> <i>high-water-mark</i>   <b>abatement</b> <i>low-water-mark</i>   <b>qcount</b> <i>number</i> ]	(Optional) Turns on flow control and failure detection in the gatekeeper.
Step 11	Router(config-gk)# <b>server trigger arq</b> <i>gkid priority</i> <i>server-id server-ipaddress server-port</i>  Router(config-gk)# <b>server trigger brq</b> <i>gkid priority</i> <i>server-id server-ipaddress server-port</i>  Router(config-gk)# <b>server trigger drq</b> <i>gkid priority</i> <i>server-id server-ipaddress server-port</i>  Router(config-gk)# <b>server trigger irr</b> <i>gkid priority</i> <i>server-id server-ipaddress server-port</i>  Router(config-gk)# <b>server trigger lcf</b> <i>gkid priority</i> <i>server-id server-ipaddress server-port</i>  Router(config-gk)# <b>server trigger lrj</b> <i>gkid priority</i> <i>server-id server-ipaddress server-port</i>  Router(config-gk)# <b>server trigger lrq</b> <i>gkid priority</i> <i>server-id server-ipaddress server-port</i>  Router(config-gk)# <b>server trigger rai</b> <i>gkid priority</i> <i>server-id server-ipaddress server-port</i>  Router(config-gk)# <b>server trigger rrq</b> <i>gkid priority</i> <i>server-id server-ipaddress server-port</i>  Router(config-gk)# <b>server trigger urq</b> <i>gkid priority</i> <i>server-id server-ipaddress server-port</i>	(Optional) Statically configures the RAS triggers on the gatekeeper. Each trigger type has submode commands that are used for configuring trigger conditions.
Step 12	Router(config-gk)# <b>security izct password</b> <i>password</i> }	(Optional) Enables IZCT authentication and authorization on the gatekeeper.
Step 13	Router(config-gk)# <b>exit</b>	Ends gatekeeper configuration mode.

## Verifying the Gatekeeper Configuration

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

- Enter **show run** to display the current gatekeeper configuration.

```
gatekeeper
zone local area1 alpha.com 172.18.193.39
zone remote hatteras alpha.com 172.18.193.32 1718 foreign-domain
zone cluster remote 387_cluster alpha.com
  element planet 172.18.193.29 1719
  element hatteras 172.18.193.32 1719
!
zone cluster remote 319_cluster alpha.com
  element planet 172.18.193.29 1719
  element newbridge 172.18.193.38 1719
!
zone prefix area1 319....
zone prefix area1 387....
zone circuit-id hatteras foreign-carrier
security izct password myname
gw-type prefix 1#* default-technology gw ipaddr 172.18.138.69.1720
lrq reject-unknown-circuit
endpoint resource-threshold onset 95 abatement 75
endpoint circuit-id h323id sales-gw-1 MAIN max-calls 1000
server routing carrier
server registration-port 5055
server flow-control onset 95 abatement 75 qcount 1000
```

- Enter **show gatekeeper circuits** to display information about the circuits (carriers) registered with the gatekeeper.

```
Router# show gatekeeper circuits
Circuit      Endpoint      Max Calls Avail Calls Resources      Zone
-----
MAIN         Total Endpoints: 1
             sales-gw-1 1000          1000          Available
```

- Enter **show gatekeeper endpoint circuits** to display information about the endpoint circuits registered with the gatekeeper.

```
Router# show gatekeeper endpoint circuits
GATEKEEPER ENDPOINT REGISTRATION
=====
CallSignalAddr  Port  RASignalAddr  Port  Zone Name      Type      Flags
-----
172.18.193.32   1720  172.18.195.69  54805  area1          VOIP-GW
H323-ID: sales-gw-1
Voice Caapcity Max.=1000 Avail.=1000
Carrier: MAIN, Max Calls: 1000, Available: 1000
Total number of active registrations = 1
```

In the example above, the Voice Capacity Max. and Avail. values represent the total voice call capacity maximum and active calls for all carriers on the gateway.

The Carrier Max Calls and Available values represent the voice call capacity maximum and active calls for the specific carrier ID configured or registered by the gateway.

- Enter **show gatekeeper servers** to display information about the servers registered with the gatekeeper.

```
GATEKEEPER SERVERS STATUS
```

```

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

Gatekeeper-ID: areal
-----
ARQ Priority: 1
  Server-ID:CSR01
  Server IP address: 172.18.197.220:59212
  Server type:dynamically registered
  Connection Status: active
  Trigger Information:
    Trigger unconditionally

Server Statistics:
  REQUEST ARQ Sent=1000
  RESPONSE ARQ Received=900
  RESPONSE ACF Received=60
  RESPONSE ARJ Received=30
  timeout Encountered=10
  Average response time(ms)=6
  Server Usable=TRUE

LRQ Priority: 1
  Server-ID:CSR01
  Server IP address:172.18.197.220:59212
  Server type:dynamically registered
  Connection Status:active
  Trigger Information:
    Trigger undonditionally

Server Statistics:
  REQUEST LRQ Sent=160
  RESPONSE LRQ Received=80
  RESPONSE LCF Received=20
  RESPONSE LRJ Received=30
  Timeout Encountered=30
  Average response time(ms)=6
  Server Usable=TRUE

```

- Enter **debug gatekeeper server** to display the messages between the Cisco IOS gatekeeper and the external application.

```

Router# debug gatekeeper server
1w6d:GK TMSG encoded to writer bugger:
REQUEST ARQ
Version-id:401
From:areal
TO:CSR01
Transaction-Id:815C9FB0000002D0
Content-Length:168

i=I:172.18.195.69:1720
s=E:3870008 H:sales-gw-1
d=E:3190008
b=1280
A=F
C=B6E2A7F2-2883-11CC-8014-D7E9930F170D
c=B6E2A7F2-2883-11CC-8015-D7E9930F170D
m=T
L=CarrierA
1w6d: GK:processing server msg:

```

```

RESPONSE ARQ
Version-id:401
From:CSR01
To:areal
Transaction-Id:815C9FB000002D0
Content-Length:46

J={i:MAIN z:{r:I:172.18.193.22:1719 c:1 p:1})

```

In this display, CarrierA represents the source carrier ID, MAIN is the destination carrier, and z{ } is the destination zone override information.

Refer to the *Cisco Gatekeeper External Interface Reference*, Version 3.2 for a description of the **show gatekeeper server** output fields.

## Monitoring and Maintaining

Command	Description
Router# <b>debug gatekeeper server</b>	Displays all messages between the gatekeeper and external applications.
Router# <b>show run</b>	Displays the current gatekeeper configuration.

## Configuration Examples

The following example illustrates the gatekeeper routing configuration. Dial peer configurations are done on the gateway(s) linked to the gatekeeper.

```

Router# show run

Current configuration : 1889 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname main-ny
!
logging buffered 500000 debugging
!
memory-size iomem 20
ip subnet-zero
!
interface Ethernet0/0
 ip address 172.18.193.39 255.255.255.0
 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 0.0.0.0 172.18.193.1
ip route 0.0.0.0 0.0.0.0 172.18.193.0
ip route 0.0.0.0 0.0.0.0 172.18.195.1
ip route 10.2.0.0 255.255.255.0 Ethernet0/0
no ip http server
ip pim bidir-enable
!
!
snmp-server packetsize 4096
snmp-server enable traps tty
!
dial-peer cor custom
!
gatekeeper
zone local main-ny alpha.com 172.18.193.39
zone remote hatteras cisco.com 172.18.193.32 1718 foreign-domain
zone cluster remote 387_cluster cisco.com
  element planet 172.18.193.29 1719
  element hatteras 172.18.193.32 1719
!
zone cluster remote 319_cluster cisco.com
  element planet 172.18.193.29 1719
  element goldengate 172.18.193.38 1719
!
zone prefix main-ny 319....
zone prefix main-ny 387....
zone circuit-id hatteras foreign-carrier
security izct password myname
gw-type-prefix 1#* default-technology gw ipaddr 172.18.138.69 1720
lrq reject-unknown-circuit
endpoint resource-threshold onset 95 abatement 75
endpoint circuit-id h323id sales-gw-1 MYTEL max-calls 1000
server routing carrier
server registration-port 5055
server flow-control onset 95 abatement 75 qcount 1000
!
!
line con 0
  exec-timeout 0 0
line aux 0
line vty 0 4
  exec-timeout 0 0
  password lab
  login
line vty 5 15
  login
!
!
end

```



# Command Reference

All commands used with this feature are documented in the [Cisco IOS Voice Command Reference, Release 12.3](#).