



Cisco High-Performance Gatekeeper

Document Update Alert

This document was originally produced for Cisco IOS Release 12.2(2)T. This feature has been updated in subsequent releases, and more recent documentation is available.

If you are using Cisco IOS Release 12.2(2)T or higher, refer to the following documentation in the Configuring H.323 Gatekeepers and Proxies chapter of the [Cisco IOS H.323 Configuration Guide](#), Cisco IOS Voice Configuration Library, Release 12.3:

- Configuring Load Balancing and Alternate Gatekeeper

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/callc_c/h323_c/323config/4gkconf.htm#1057867

- Configuring Remote Clusters

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/callc_c/h323_c/323config/4gkconf.htm#1060291

Feature History

Release	Modification
12.1(5)XM	This feature was introduced on the Cisco 2500, Cisco 2600, and Cisco 7200 series, and the Cisco MC3810.
12.2(2)T	This feature was integrated into Cisco IOS Release 12.2(2)T.

This feature module describes the High-Performance Gatekeeper (GK) feature for Cisco IOS Release 12.2(2)T and includes information on the benefits of the new feature, supported platforms, related documents, and new and updated feature command syntax.

This document includes the following sections:

- [Feature Overview, page 2](#)
- [Supported Platforms, page 4](#)
- [Supported Standards, MIBs, and RFCs, page 5](#)
- [Prerequisites, page 6](#)
- [Configuration Tasks, page 7](#)
- [Monitoring and Maintaining Gatekeepers and Endpoints, page 17](#)

- [Configuration Examples, page 18](#)
- [Command Reference, page 19](#)
- [Glossary, page 54](#)

Feature Overview

The *Cisco High-Performance Gatekeeper* feature introduces new gatekeeper functionality and modifications for facilitating carrier class reliability, security, and performance into the Cisco Voice Network solution portfolio. These H.323 standard-based features have carrier grade reliability and performance characteristics with a robust open application protocol interface to enable development of enhanced applications like voice Virtual Private Networks (VPNs) and wholesale voice solutions.

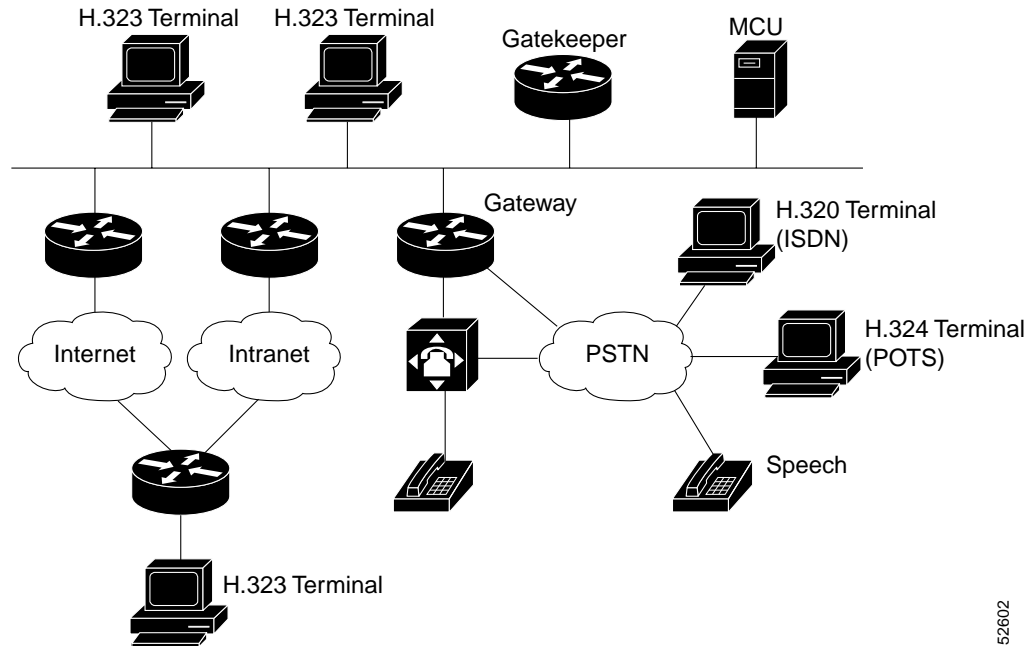
The new gatekeeper is characterized by the following:

- Increased support for back end applications.
- Increased performance on a single gatekeeper.
- Alternate gatekeeper support to the gatekeeper. Each alternate gatekeeper, or GK node, shares its local zone information so that the cluster can effectively manage all local zones within the cluster. Each alternate gatekeeper has a unique local zone. Clusters provide a mechanism for distributing call processing seamlessly across a converged IP network infrastructure to support IP telephony, facilitate redundancy, and provide feature transparency and scalability.

This feature addresses the scalability, redundancy, and performance aspects of the gatekeeper as part of the Cisco Multimedia Conference Manager (MCM) to present a complete Cisco solution. The Cisco H.323 MCM provides the network administrator with the ability to identify H.323 traffic and to apply appropriate policies. The Cisco H.323 Multimedia Conference Manager is implemented on Cisco IOS software and enables a network manager to do the following:

- Limit the H.323 traffic on the LAN and WAN.
- Provide user accounting for records based on the service utilization.
- Inject quality of service (QoS) parameters for the H.323 traffic generated by applications such as VoIP, and data and video conferencing.
- Provide the mechanism to implement security for H.323 communications.

Figure 1 Cisco H.323/Gatekeeper Overview



52602

Benefits

Alternate Gatekeepers

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

Alternate Endpoints

A calling endpoint can recover from a call setup failure by sending a setup message to one of the alternate endpoints so that it is possible for a call to finish even if a gateway goes down and the gatekeeper is not yet aware of the problem. Cisco supports a maximum of 20 alternates for each endpoint, and any alternates received through registration, admission, and status protocol (RAS) messages are merged with those entered manually in the GK command-line interface (CLI). If more than 20 alternates are submitted, the total list of alternates reverts back to 20.

Enhancements to GKTMP Messages

The Gatekeeper Transaction Message Protocol (GKTMP) servers can set triggers for disengage request (DRQ) and resource availability indication (RAI) messages. Other messages are extended to contain more parameters for added call control.

Gatekeeper Billing Information

The gatekeeper sends detailed call information to a RADIUS distributed client/server system that can be used for billing purposes. RADIUS servers use the vendor-specific attribute (VSA) capability to configure features for individual users.

Improved Performance

Optimizations in the gatekeeper data structures and algorithms provide increased performance.

Least Cost Routing

Cost and priority fields are included with each remote zone definition, which ensures that the zones with lower cost are given an advantage over zones with higher cost.

Load-Balancing

Load balancing allows the gatekeeper to move registered H.323 endpoints to an alternate gatekeeper or to reject new calls and registrations once a certain threshold is met.

Restrictions

- Gatekeepers other than Cisco gatekeepers and Cisco gatekeeper images that were shipped prior to the release of this feature, which was originally supported on Cisco IOS Release 12.1(5)XM do not contain the clustering ability provided by the Cisco proprietary protocol.
- This feature does not work with Cisco IOS software released before Cisco IOS release 12.1(5)XM.

Related Documents

- *Cisco IOS Multiservice Applications Configuration Guide*
- *Configuration Guides and Command References, Cisco IOS Release 12.2*
- *Configuring Gatekeepers (Multimedia Conference Manager)*
- [Configuring H.323 VoIP Gateway for Cisco Access Platforms](#)
- *H.323 Version 2 Phase 2, Cisco IOS Release 12.2*

Supported Platforms

- Cisco 2600 series
- Cisco 3600 series
- Cisco 3620
- Cisco 3640
- Cisco 3660
- Cisco AS5850
- Cisco MC3810
- Cisco 7200 series

Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that are supported on specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

<http://www.cisco.com/go/fn>

Availability of Cisco IOS Software Images

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or, if supported, Cisco Feature Navigator.

Supported Standards, MIBs, and RFCs

Standards

- T.120 within an H.323 call
- ITU-T Recommendation H.323
- ITU-T Recommendation H.225.0

MIBs

- CISCO-GATEKEEPER-MIB
- CISCO-PROXY-CONTROL-MIB
- GATEKEEPER MIB

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

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

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

RFCs

No new or modified RFCs are supported by this feature.

Prerequisites

You must be running Cisco IOS Software Release 12.2(2)T.

Configuration Tasks

See the following sections for configuration tasks for the Cisco High-Performance Gatekeeper feature. Each task in the list indicates if the task is optional or required.

- [Configuring the Gatekeeper](#) (Required)
- [Configuring Load Balancing and Alternate Gatekeepers](#) (Required)
- [Configuring Remote Clusters](#) (Required)
- [Configuring Server Triggers](#) (Required)
- [Verifying Configuration](#)

Configuring the Gatekeeper

To configure the gatekeeper to support zones, use the following commands, beginning in global configuration mode.

	Command	Purpose
Step 1	Router(config)# gatekeeper	Enters gatekeeper configuration mode.
Step 2	Router(config-gk)# zone local <i>zone-name</i> <i>domain-name</i> [<i>rasIPAddress</i>] [<i>port number</i>]	<p>Defines 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 gatekeeper-name might be gk1.cisco.com. However, if the gatekeeper is controlling multiple zones, the <i>gatekeeper-name</i> for each zone is a unique string that has a mnemonic value.</p> <p><i>The domain-name argument specifies</i> the domain name served by this gatekeeper.</p> <p><i>The rasIPAddress argument</i> specifies 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. This is an optional command.</p> <p>Note Setting this address for one local zone makes it the address used for all local zones.</p> <p>(Optional) <i>port number</i> is the RAS signaling port number for the local zone. Value ranges from 1 to 65535. If no port number is specified, the default is 1719.</p>

Command	Purpose
Step 3 Router(config-gk)# zone remote zone-name domain-name ip-address [port number] [cost cost-value [priority priority-value]]	<p>Defines the remote zone cluster.</p> <p><i>zone-name</i> is the name (ID) of the remote zone.</p> <p><i>domain-name</i> is the name (ID) of the domain the remote zone is serving.</p> <p><i>ip-address</i> is the IP address for the remote gatekeeper.</p> <p><i>port number</i> is an optional parameter to indicate the RAS signaling port number for the remote zone. Value ranges from 1 to 65535. If this is not set, the default is the well-known RAS port number 1719.</p> <p>cost sets the cost of the zone.</p> <p><i>cost-value</i> is the cost value. Range is 1 through 100. Default is 50.</p> <p>priority sets the priority of the zone.</p> <p><i>priority-value</i> is the priority value. Range is 1 through 100. Default is 50.</p> <p>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.</p>

Command	Purpose
<p>Step 4</p> <pre>Router(config-gk)# zone prefix zone-name e164-prefix [gw-priority pri-0-to-10 gw-alias [gw-alias, ...]]</pre>	<p><i>zone-name</i> specifies the name of a local or remote gatekeeper, which must have been defined by using the zone local or zone remote command.</p> <p>To route all incoming calls to a remote zone, use the zone remote zone-name* command.</p> <p>The <i>e164-prefix</i> argument represents 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> <p>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> <p>The GK uses the longest match criteria from among the known prefixes to select one or more terminating zones. So a dialed number 9193926823 will match a 919392* prefix rather than a 919* prefix.</p> <p>The local zone (where the endpoint is registered) is given preference over other zones. So if the dialed number matches the prefix criteria for the local zone, the local zone will be selected. For example, a dialed number of 6823 will match the local zone prefix of 919392.... rather than a remote prefix of 68*.</p> <p>Note The dots (.) following the 919392 prefix is standard form.</p> <p>If a match is found, the call is routed to a local zone, and a gateway (GW) is selected from that zone. If the call is routed to a remote zone, an LRQ is sent to that zone. If no match is found, the local zone is used unless the reject-unknown-prefix is configured.</p> <p>Use the gw-priority option to define how the gatekeeper selects gateways in its local zone for calls to numbers beginning with the <i>e164-prefix</i> argument. 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 gw-alias for that prefix. Value 10 places the highest priority on gateway gw-alias. 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>pri-0-to-10</i> value. The gw-alias 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>

	Command	Purpose
Step 5	Router(config-gk)# use-proxy <i>local zone remote-zone remote-zone-name outbound-from gateway</i>	Specifies that all calls originating from gateways in the local zone and bound to the remote zone, route through a proxy, which should be registered with the gatekeeper.
Step 6	Router(config-gk)# no shutdown	Activates the gatekeeper.

Configuring Load Balancing and Alternate Gatekeepers

If a gatekeeper fails, the endpoint might use alternate gatekeepers to continue operation. The example below creates a local cluster associated with a local zone and defines an alternate GK within the cluster.

To configure alternate gatekeepers and load balancing, perform the following steps starting in global configuration mode.

	Command	Purpose
Step 1	Router(config)# gatekeeper	Enters gatekeeper configuration mode.
Step 2	Router(config-gk)# zone local <i>local-zone-name domain-name [rasIPAddress]</i>	Defines the gatekeeper's name or zone name. This is usually the fully domain-qualified host name of the gatekeeper.
Step 3	Router(config-gk)# zone cluster local <i>cluster-name local-zone-name</i>	Defines a local cluster for the local zone.
Step 4	Router(config-gk-cluster)# element <i>alternateGK IP address [port number]</i>	Defines the alternate gatekeeper in the local cluster. The alternate gatekeeper is an alternate gatekeeper to the local zone. (Optional) <i>port number</i> defaults to 1719 if not set.
Step 5	Router(config-gk-cluster)# exit	Exits from gatekeeper cluster configuration mode and returns to gatekeeper configuration mode.
Step 6	Router(config-gk)# load-balance [endpoints <i>max-endpoints</i>] [calls <i>max-calls</i>] [cpu <i>max-%cpu</i>] [memory <i>max-%mem-used</i>]	Configures load balancing. The following commands are optional: endpoints <i>max-endpoints</i> sets the maximum number of endpoints. calls <i>max-calls</i> sets the maximum number of calls. cpu <i>max-%cpu</i> sets the maximum percentage of CPU usage. memory <i>max-%mem-used</i> sets the maximum percentage of memory used.

Configuring Remote Clusters

The following commands define a group of associated gatekeepers in a remote cluster. This remote cluster can then be addressed using the **zone prefix** command in the same way that a remote gatekeeper would be addressed to route calls. However, rather than individually addressing each remote gatekeeper within the cluster, you can address the cluster as a single entity. Additionally, location requests (LRQs) are now sent round-robin to each gatekeeper within the remote cluster.

To configure remote clusters, perform the following steps starting in global configuration mode.

	Command	Purpose
Step 1	Router(config)# gatekeeper	Enters gatekeeper configuration mode.
Step 2	Router(config-gk)# zone local <i>zone-name</i> <i>domain-name</i> [<i>rasIPAddress</i>] [<i>port number</i>]	<p>Defines 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 gatekeeper-name might be gk1.cisco.com. However, if the gatekeeper is controlling multiple zones, the <i>gatekeeper-name</i> for each zone is a unique string that has a mnemonic value.</p> <p><i>Domain-name</i> specifies the domain name served by this gatekeeper.</p> <p><i>rasIPAddress</i> specifies 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. This is an optional command.</p> <p>Note Setting this address for one local zone makes it the address used for all local zones.</p> <p>(Optional) <i>port number</i> is the RAS signaling port number for the local zone. Value ranges from 1 to 65535. If no port number is specified, the default is 1719.</p>
Step 3	Router(config-gk)# zone cluster remote <i>remote-cluster-name</i> <i>domain-name</i> [cost <i>cost-value</i>] [priority <i>priority-value</i>]	<p>Defines a remote cluster.</p> <p><i>remote-cluster-name</i> defines the remote cluster name.</p> <p><i>domain-name</i> is the name (ID) of the domain the remote cluster is serving.</p> <p>cost sets the cost.</p> <p><i>cost-value</i> defines the cost value. Range is 1 through 100. Default is 50.</p> <p>priority sets the priority.</p> <p><i>priority-value</i> defines the priority value. Range is 1 through 100. Default is 50.</p>
Step 4	Router(config-gk-cluster)# element <i>gatekeeper-name</i> <i>ip-address</i> [<i>port number</i>]	<p>Defines component elements of local or remote clusters</p> <p><i>gatekeeper-name</i> defines the gatekeeper name.</p> <p><i>ip-address</i> defines the IP address for this interface.</p> <p>(Optional) <i>port number</i> defines the port number. Default is 1719.</p>

Command	Purpose
Step 5 Router(config-gk-cluster)# exit	Exits from gatekeeper cluster configuration mode and returns to gatekeeper configuration mode.
Step 6 Router(config-gk)# zone prefix <i>remote-cluster-name</i> <i>e164-prefix [gw-priority pri-0-to-10 gw-alias</i> <i>[gw-alias, ...]]</i>	<p><i>remote-cluster-name</i> specifies the name of a local or remote cluster, which must have been defined by using the zone local or zone remote command.</p> <p><i>e164-prefix</i> represents an E.164 prefix in standard form followed by dots (.). Each dot represent a number in the E.164 address. For example, 212..... is matched by 212 and any seven numbers.</p> <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> <p>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>pri-0-to-10</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>

Configuring Server Triggers

You can configure your gatekeepers to connect to a specific back end server at startup or to listen to any server that wants to connect to it. You can also set the triggers in the gatekeeper configuration so that they send only the specified messages. Servers can also dynamically register their triggers with a gatekeeper.

To configure server triggers, perform the following tasks starting in global configuration mode.

	Command	Purpose
Step 1	Router(config)# gatekeeper	Enters gatekeeper configuration mode.
Step 2	Router(config-gk)# zone local <i>zone-name domain-name</i> [<i>rasIPAddress</i>] [<i>port number</i>]	<p>Defines 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 gatekeeper-name might be gk1.cisco.com. However, if the gatekeeper is controlling multiple zones, the <i>gatekeeper-name</i> for each zone is a unique string that has a mnemonic value.</p> <p><i>Domain-name</i> specifies the domain name served by this gatekeeper.</p> <p><i>rasIPAddress</i> specifies 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. This is an optional command.</p> <p>Note Setting this address for one local zone makes it the address used for all local zones.</p> <p>(Optional) <i>port number</i> is the RAS signaling port number for the local zone. Value ranges from 1 to 65535. If no port number is specified, the default is 1719.</p>
Step 3	Router(config-gk)# timer server timeout <i>time-in-100-millisecond-units</i>	Specifies the timeout value for a response from a back end GKTMP server. The time is specified as the number of milliseconds in 100 ms units. Range is 1 through 50 (0.1 seconds through 5 seconds).

	Command	Purpose
Step 4	<pre>Router(config-gk)# server trigger {arq drq lcf lrj lrq rai rrq urq} <i>zone-name</i> <i>priority</i> <i>server-id</i> <i>server-ipaddress</i> <i>server-port</i></pre>	<p>Configures triggering on RAS message types.</p> <p><i>all</i> deletes all CLI configured triggers.</p> <p>arq, drq, lcf, lrj, lrq, rai, rrq, urq—RAS message types. Use these message types to specify a submode in the gatekeeper configuration mode where you configure a trigger for the gatekeeper to act upon. Specify only one message type per server trigger command. There is a different trigger submode for each message type. Each trigger submode has its own set of applicable commands.</p> <p><i>zone-name</i> is the local gatekeeper identifier.</p> <p><i>priority</i> is the priority for each trigger. The range is from 1 through 20, with 1 being the highest priority.</p> <p><i>server-id</i> is the external application's ID number.</p> <p><i>server-ipaddress</i> is the server's IP address.</p> <p><i>server-port</i> is the port on which the Cisco IOS gatekeeper listens for messages from the external server connection.</p>
Step 5	<pre>Router(config-gk_raitrigger)# info-only</pre>	<p>Information only; no need to wait for acknowledgement.</p>

Verifying Configuration

- Step 1** Enter the **show gatekeeper endpoints [alternates]** command. For each endpoint, if there are any alternate endpoints for it, they are displayed in the second half of the output. Then the alternate endpoints are displayed, one per line, whether or not they correspond to a registered endpoint.

```
Router# show gatekeeper endpoints [alternates]
```

```
GATEKEEPER ENDPOINT REGISTRATION
```

```
=====
```

```
CallSignalAddr  Port  RASSignalAddr  Port  Zone Name          Type  F
-----
209.165.200 1720 209.165.54 52661 RoseGK              VOIP-GW
      H323-ID:GW-156-2600-fxs@cisco.com
      E164-ID:10052
209.165.200 1720 209.165.54 57040 RoseGK              VOIP-GW
      H323-ID:GW-158-2600-fxs
      E164-ID:10042
```

```
Total number of active registrations = 2
```

```
ALL CONFIGURED ALTERNATE ENDPOINTS
```

```
=====
```

```
Endpoint H323 ID          RAS Signal Addr  Port
-----
GW-156-2600-fxs@cisco.com 209.5.4.3        1111
```

Step 2 Enter the **show gatekeeper servers** command to display triggers:

```
Router# show gatekeeper servers

GATEKEEPER SERVERS STATUS
=====
Gatekeeper Server listening port:0
Gatekeeper Server timeout value:20 (100ms)

Gatekeeper-ID:RoseGK
-----
DRQ Priority:1
  Server-ID:TMPServer
  Server IP address:209.165.201.1:4000
  Server type:CLI-configured
  Connection Status:inactive
  Trigger Information:
    Informational only
    Trigger unconditionally

RAI Priority:1
  Server-ID:TMPServer
  Server IP address:209.165.201.1:4000
  Server type:CLI-configured
  Connection Status:inactive
  Trigger Information:
    Endpoint-type:voip-gateway
```

Step 3 Enter the **show gatekeeper status** command to see if load balancing is configured and if accounting vendor-specific attributes (VSAs) are enabled. The last five lines, starting with Load Balance Count, are displayed only when load balancing is enabled.

```
Router# show gatekeeper status
Gatekeeper State: UP
Load Balancing: ENABLED
Zone Name: RoseGK
Zone Name: PurpleGK
Accounting: DISABLED
Security: DISABLED
Maximum Remote Bandwidth: unlimited
Current Remote Bandwidth: 0 kbps
Current Remote Bandwidth (w/Alt GKs): 0 kbps
Load Balance Count: 0
Calls: 0/unlimited
Endpoints: 0/unlimited
Memory: 0%/90%
CPU: 0%/80%
```

Step 4 Enter the **show gatekeeper performance statistics** command to verify performance statistics:

```
Router-1-gk# show gatekeeper performance statistics
Performance statistics captured since:19:00:12 EST Sun Feb 28 1993

RAS inbound message counters:
  Originating ARQ:426   Terminating ARQ:306   LRQ:154
RAS outbound message counters:
  ACF:731   ARJ:1   LCF:154   LRJ:0
  ARJ due to overload:0
  LRJ due to overload:0

Load balancing events:0
Real endpoints:5
```

Enter the **show gatekeeper status cluster** command to display each element of a cluster. This command shows the health of the elements in a cluster and reports on the percentage of memory and CPU usage, the number of active calls, and the number of endpoints registered on the element. The Last Announce field tells you the time since the last announcement message was received from the alternate gatekeeper. In this example, MsPacman and LavenderGK are part of a local cluster:

```
Router# show gatekeeper status cluster
```

```

                CLUSTER INFORMATION
                =====
Hostnme         %Mem   %CPU   Active  Endpoint  Last
-----         -
MsPacman        17     2      0       1          Local Host
LavenderGK      30     1      0       4          14s

```

Step 5 Enter the **show gatekeeper zone status** command to display the bandwidth information for all zones.

```
Router# show gatekeeper zone status
```

```

                GATEKEEPER ZONES
                =====
GK name         Domain Name   RAS Address   PORT  FLAGS
-----         -
RoseGK          cisco.com     209.165.201.30 1719  LS
BANDWIDTH INFORMATION (kbps) :
  Maximum interzone bandwidth :unlimited
  Current interzone bandwidth :0
  Current interzone bandwidth (w/ Alt GKs) :0
  Maximum total bandwidth :unlimited
  Current total bandwidth :0
  Current total bandwidth (w/ Alt GKs) :0
  Maximum session bandwidth :unlimited
SUBNET ATTRIBUTES :
  All Other Subnets :(Enabled)
PROXY USAGE CONFIGURATION :
  Inbound Calls from all other zones :
    to terminals in local zone RoseGK :use proxy
    to gateways in local zone RoseGK :do not use proxy
  Outbound Calls to all other zones :
    from terminals in local zone RoseGK :use proxy
    from gateways in local zone RoseGK :do not use proxy

```

Step 6 Enter the **show gatekeeper zone cluster** command to display information about alternate gatekeepers. PRI represents the priority value assigned to an alternate gatekeeper. This field ranges from 0 to 127, with 127 representing the lowest priority.

```
Router# show gatekeeper zone cluster
```

```

ALTERNATE GATEKEEPER INFORMATION
=====
LOCAL GK NAME  ALT GK NAME  PRI  TOT BW  INT BW  REM BW  LAST ANNOUNCE  ALT GK STATUS
-----
RoseGK         LilacGK      120  0       0       0       7s            CONNECTED

```

Step 7 Enter the **show proxy h323 status** command to display information about the proxy such as the T.120 mode and what port is being used.

```
Router# show proxy h323 status
```

```
H.323 Proxy Status
```

```

=====
H.323 Proxy Feature:Enabled
Proxy interface = Ethernet0:UP
Proxy IP address = 209.165.200.254
Proxy IP port = 11720
Application Specific Routing:Disabled
RAS Initialization:Complete
Proxy aliases configured:
  H323_ID:PROXY
Proxy aliases assigned by Gatekeeper:
  H323_ID:PROXY
Gatekeeper multicast discovery:Disabled
Gatekeeper:
  Gatekeeper ID:DVM1
  IP address:209.165.200.254
Gatekeeper registration succeeded
T.120 Mode:PROXY
RTP Statistics:OFF
Number of calls in progress:0

```

- Step 8** Enter the **show gatekeeper cluster** command to display all clusters defined in the gatekeeper and with their component elements.

```

gatekeeper
  zone local RTPGK1cisco.com
  zone cluster local RTPCluster RTPGK1
    element RTPGK2 209.165.200 1719
    element RTPGK3 209.165.200 1719
  zone cluster remote SJCluster cisco.com
    element SJGK1 209.18.79.23 1719
    element SJGK2 209.18.79.24 1719
    element SJGK3 209.18.79.25 1719
no shutdown

```

Router# **show gatekeeper cluster**

```

                CONFIGURED CLUSTERS
                =====
Cluster Name   Type      Local Zone  Elements  IP
-----
RTPCluster    Local    RTPGK1     RTPGK2    209.165.200.254 1719
                RTPGK3    209.165.200.223 1719
SJCluster     Remote
                SJGK1    209.165.200.257 1719
                SJGK2    209.165.200.258 1719
                SJGK3    209.165.200.259 1719

```

Monitoring and Maintaining Gatekeepers and Endpoints

To monitor and maintain gatekeepers and endpoints, use the following **show** commands in privileged EXEC mode.

Command	Purpose
Router# show gatekeeper cluster	Displays information about all the clusters defined in the gatekeeper along with their component elements.
Router# show gatekeeper endpoints [alternates]	Displays information about alternate endpoints.

Command	Purpose
Router# <code>show gatekeeper performance statistics</code>	Displays statistics about gatekeeper performance.
Router# <code>show gatekeeper status cluster</code>	Displays the health of each element of all local clusters
Router# <code>show gatekeeper zone cluster</code>	Displays the dynamic status of all local clusters.

Configuration Examples

This section provides the following configuration examples:

- [Least-Cost Routing](#)
- [Accounting Enabled](#)

Least-Cost Routing

The following example shows configuration output for least-cost routing. For more information about cost priority commands, see the [zone remote](#) command.

```
gatekeeper
zone local RoseGK cisco.com 209.165.201.30
zone remote LilacGK cisco.com 209.165.201.1 cost 20 priority 10
zone remote LavenderGK cisco.com 209.165.202.129 1719 cost 10 priority 10
zone prefix LilacGK 408*
zone prefix LavenderGK 408*
no shutdown
```

Accounting Enabled

The following configuration output example shows accounting enabled using VSA. VSA defines a private extension to the attributes that can be passed across to a RADIUS server. For more information about VSA accounting, see the [accounting \(gatekeeper\)](#) command.

```
gatekeeper
zone local RoseGK cisco.com 209.165.201.30
zone remote LilacGK cisco.com 209.165.201.1 cost 20 priority 10
zone remote LavenderGK cisco.com 209.165.202.129 1719 cost 10 priority 10
zone cluster local RoseGK PurpleGK 209.165.202.158 1719
accounting vsa
load-balance endpoints 200 calls 100 cpu 75 memory 80
no shutdown
server trigger drq RoseGK 1 TMPServer 209.165.201.1 4000
info-only
!
server trigger rai RoseGK 1 TMPServer 209.165.201.1 4000
endpoint-type voice-gateway
!
```

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

- **clear h323 gatekeeper statistics**
- **debug gatekeeper gup**
- **debug gatekeeper load**
- **element**
- **endpoint alt-ep h323id**
- **endpoint ttl**
- **load-balance**
- **show gatekeeper cluster**
- **show gatekeeper performance statistics**
- **show gatekeeper status cluster**
- **show gatekeeper zone cluster**
- **timer cluster-element announce**
- **timer lrq seq delay**
- **timer lrq window**
- **timer server timeout**
- **zone cluster local**
- **zone cluster remote**
- **zone remote**

Modified Commands

- **accounting (gatekeeper)**
- **bandwidth (gatekeeper)**
- **bandwidth remote**
- **server trigger**
- **show gatekeeper endpoints**

accounting (gatekeeper)

To configure the VSA method of accounting, use the **accounting vsa** gatekeeper configuration command. To disable, use the **no** form of this command.

accounting [vsa]

no accounting [vsa]

Syntax Description	vsa (Optional) Configures the vendor-specific attribute (VSA) method of accounting.								
Defaults	Accounting is disabled.								
Command Modes	Gatekeeper configuration								
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>11.3T</td> <td>This command was introduced for gatekeeper configuration.</td> </tr> <tr> <td>12.1(5)XM</td> <td>The vsa keyword was added.</td> </tr> <tr> <td>12.2(2)T</td> <td>This command was integrated into Cisco IOS Release 12.2(2)T.</td> </tr> </tbody> </table>	Release	Modification	11.3T	This command was introduced for gatekeeper configuration.	12.1(5)XM	The vsa keyword was added.	12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
Release	Modification								
11.3T	This command was introduced for gatekeeper configuration.								
12.1(5)XM	The vsa keyword was added.								
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.								
Usage Guidelines	Use the accounting (gatekeeper) vsa command to enable accounting for sending VSA encoded values.								
Examples	<p>The following example enables VSA accounting:</p> <pre>Router(config-gk)# accounting vsa</pre>								
Related Commands	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>bandwidth (gatekeeper)</td> <td>Specifies the maximum aggregate bandwidth for H.323 traffic.</td> </tr> </tbody> </table>	Command	Description	bandwidth (gatekeeper)	Specifies the maximum aggregate bandwidth for H.323 traffic.				
Command	Description								
bandwidth (gatekeeper)	Specifies the maximum aggregate bandwidth for H.323 traffic.								

bandwidth (gatekeeper)

To specify the maximum aggregate bandwidth for H.323 traffic, use the **bandwidth** gatekeeper configuration command. To disable, use the **no** form of this command.

bandwidth { **interzone** | **total** | **session** } { **default** | **zone** *zone-name* } *bandwidth-size*

no bandwidth { **interzone** | **total** | **session** } { **default** | **zone** *zone-name* } *bandwidth-size*

Syntax	Description
interzone	Specifies the total amount of bandwidth for H.323 traffic from the zone to any other zone.
total	Specifies the total amount of bandwidth for H.323 traffic allowed in the zone.
session	Specifies the maximum bandwidth allowed for a session in the zone.
default	Specifies the default value for all zones.
zone	Specifies a particular zone.
<i>zone-name</i>	Names the particular zone.
<i>bandwidth-size</i>	Maximum bandwidth. For interzone and total , the range is from 1 to 10,000,000 kbps. For session , the range is from 1 to 5,000 kbps.

Defaults None

Command Modes Gatekeeper configuration

Command History	Release	Modification
	12.1(3)XI	This command was introduced.
	12.1(5)XM	The bandwidth command is recognized without using the zone gatekeeper command.
	12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.

Usage Guidelines In previous Cisco IOS software releases, the functionality of the **bandwidth** command was obtained by using the **zone gatekeeper** command.

Examples The following example configures the maximum bandwidth for the zone to 5,000 kbps:

```
Router(config)# gatekeeper
Router(config-gk)# bandwidth total default 5000
```

Related Commands

■ bandwidth (gatekeeper)

Command	Description
bandwidth remote	Specifies the total bandwidth for H.323 traffic between this gatekeeper and any other gatekeeper.

bandwidth remote

To specify the total bandwidth for H.323 traffic between this gatekeeper and any other gatekeeper, use the **bandwidth remote** gatekeeper configuration command. To disable, use the **no** form of this command.

bandwidth remote *bandwidth-size*

no bandwidth remote

Syntax Description	<i>bandwidth-size</i>	Maximum bandwidth. Range is 1 to 10,000,000 kbps.
--------------------	-----------------------	---------------------------------------------------

Defaults	None.
----------	-------

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

Command History	Release	Modification
	12.1(3)XI	This command was introduced.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.	

Usage Guidelines	The functionality of this command in previous Cisco IOS software releases was obtained by using the zone gatekeeper command.
------------------	-------------------------------------------------------------------------------------------------------------------------------------

Examples	The following example configures the remote maximum bandwidth to 100,000 kbps:
----------	--------------------------------------------------------------------------------

```
Router(config)# gatekeeper
Router(config-gk)# bandwidth remote 100000
```

Related Commands	Command	Description
	bandwidth (gatekeeper)	Specifies the maximum aggregate bandwidth for H.323 traffic from a zone to another zone, within a zone, or for a session in a zone.

clear h323 gatekeeper statistics

To clear statistics about gatekeeper performance, use the **clear h323 gatekeeper statistics** privileged EXEC command.

clear h323 gatekeeper statistics

Syntax Description There are no keywords or arguments for this command.

Defaults No default behavior or values.

Command Modes EXEC

Command History	Release	Modification
	12.1(5)XM	This command was introduced.
	12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.

Usage Guidelines This command resets the gatekeeper performance counters to zero and records the time when the last clear was performed.

Examples The following example shows output for the [show gatekeeper performance statistics](#) command after the [clear h323 gatekeeper statistics](#) command has been applied. See the [show gatekeeper performance statistics](#) command for more information.

```
Router# clear h323 gatekeeper statistics
Router# show gatekeeper performance statistics

RAS inbound message counters:

Originating ARQ: 0 Terminating ARQ: 0 LRQ: 0

RAS outbound message counters:

ACF: 2 ARJ: 0 LCF: 2 LRJ: 0

ARJ due to overload: 0

LRJ due to overload: 0

Load balancing events: 0

Real endpoints: 2
```

Related Commands

Command	Description
show gatekeeper performance statistics	Displays statistics about gatekeeper performance.

debug gatekeeper gup

To display the Gatekeeper Update Protocol (GUP) events or Abstract Syntax Notation 1 (ASN.1) details, use the **debug gatekeeper gup** privileged EXEC command. To disable debugging output, use the **no** form of the command.

```
debug gatekeeper gup {events | asn1}
```

```
no debug gatekeeper gup
```

Syntax Description

events	Displays a message whenever a GUP announcement is sent or received. GUP is the protocol used between individual gatekeepers in a cluster, which keeps all of the gatekeepers synchronized with all endpoints registered on the cluster.
asn1	ASN.1 library. ASN.1 is an ITU standard for protocol syntax and message encoding. Entering this keyword causes a packet dump of all GUP announcement messages.

Defaults

Debugging is not enabled.

Command History

Release	Modification
12.1(5)XM	This command was introduced.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.

Examples

The following example shows how to enable a packet dump of all GUP announcement messages:

```
Paris# debug gatekeeper gup asn1
Paris# 00:10:21:ENCODE BUFFER::= 00 0A2A8648 86F70C0A 00000120 001E8001
86A08001 86A00547 656E6576 614E0000 00000142 80004700 65006E00 65007600
61080050 00610072 00690073 00000000 0000
00:10:21:
00:10:21:PDU ::=

value GUP_Information ::=

protocolIdentifier { 1 2 840 113548 10 0 0 1 }
message announcementIndication :

announcementInterval 30
endpointCapacity 100000
callCapacity 100000
hostName '47656E657661'H
percentMemory 39
percentCPU 0
currentCalls 0
currentEndpoints 0
zoneInformation

gatekeeperIdentifier {"Geneva"}
altGKIdentifier {"Paris"}
```

```

totalBandwidth 0
interzoneBandwidth 0
remoteBandwidth 0

RAW_BUFFER::=
00 0A2A8648 86F70C0A 00000120 001E800B 858A8001 86A00144 80007400 6F007200 6E006100
64006F00 2D006700 6B120063 00790063 006C006F 006E0065 002D0067 006B0000 00000000
*Mar  3 15:40:31:
*Mar  3 15:40:31:Sending GUP ANNOUNCEMENT INDICATION to 172.18.195.140RAW_BUFFER::=
00 0A2A8648 86F70C0A 00000120 001E800A EF8A8001 86A00144 80006300 79006300 6C006F00
6E006500 2D006700 6B120074 006F0072 006E0061 0064006F 002D0067 006B0000 00000000
*Mar  3 15:40:31:PDU DATA = 60EAB248

value GUP_Information ::=

protocolIdentifier { 1 2 840 113548 10 0 0 1 }
message announcementIndication :
{
announcementInterval 30
endpointCapacity 716682
callCapacity 100000
zoneInformation

gatekeeperIdentifier {"cyclone-gk"}
altGKIdentifier {"tornado-gk"}
totalBandwidth 0
interzoneBandwidth 0
remoteBandwidth 0

Mar  3 15:40:31:Received GUP ANNOUNCEMENT INDICATION from 172.18.195.140
Router#
Router# u all
All possible debugging has been turned off

```

Related Commands

Command	Description
load-balance	Moves an endpoint registered on the gatekeeper to another gatekeeper in the local cluster, if the source gatekeeper becomes overloaded and the target gatekeeper is able to take the load off the endpoint. This command sets the threshold values for performing load balancing.

debug gatekeeper load

To display gatekeeper load-balancing debug events, use the **debug gatekeeper load** privileged EXEC command. To disable debugging output, use the **no** form of the command.

debug gatekeeper load {events}

no debug gatekeeper load

Syntax Description	events	Displays a message whenever a load-balancing message is sent or received.
--------------------	--------	---------------------------------------------------------------------------

Defaults Debugging is not enabled.

Command History	Release	Modification
	12.1(5)XM	This command was introduced.
	12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.

Examples The following example shows output for the **debug gatekeeper load** command.



Note

The following output examples are independent of each other and would not ordinarily be seen at the same time.

```
cyclone-gk# debug gatekeeper load
cyclone-gk#
cyclone-gk#

cyclone-gk# show deb
gk load-balancing debug level = Events
cyclone-gk#
cyclone-gk#

gk_load_overloaded:Overloaded, 5-second CPU utilization too high

gk_load_overloaded:Overloaded due to excessive calls/endpoints

gk_load_balance_endpt_request:load balance occurred. New load_balance_count=2
```

Related Commands	Command	Description
	load-balance	Moves an endpoint registered on the gatekeeper to another gatekeeper in the local cluster, if the source gatekeeper gets overloaded and the target gatekeeper is able to take the load off the endpoint. This command sets the threshold values for performing load balancing.

element

To define component elements of local or remote clusters, use the **element** gatekeeper configuration command. To disable, use the **no** form of this command.

element *gatekeeper-name ip-address port*

no element

Syntax	Description
<i>gatekeeper-name</i>	Defines the name of the gatekeeper component to be added to the local or remote cluster.
<i>ip-address</i>	Defines the IP address of the gatekeeper to be added to the local or remote cluster.
<i>port number</i>	(Optional) RAS signalling port number for the remote zone. Value ranges from 1 to 65535. If this is not set, the default is the well-known RAS port number 1719.

Defaults No default behavior or values.

Command Modes Zone cluster configuration.

Command History	Release	Modification
	12.1(5)XM	This command was introduced.
	12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.

Examples The following example places the GenevaGK gatekeeper into the specified local or remote cluster:

```
Router(config-gk_cluster)# element GenevaGK 209.165.202.158 1719
```

Related Commands	Command	Description
	zone cluster local	Defines a local group of gatekeepers, including the gatekeeper you are configuring.
	zone cluster remote	Defines a remote group of gatekeepers, including the gatekeeper you are configuring.

endpoint alt-ep h323id

To configure alternate endpoints, use the **endpoint alt-ep h323id** gatekeeper configuration command. To disable, use the **no** form of this command.

endpoint alt-ep h323id *h323-id ip-address* [*port number*]

no endpoint alt-ep h323id

Syntax Description		
<i>h323-id</i>	H.323 name (ID) of the endpoint for which an alternate address is being supplied. This ID is used by this gateway when this gateway communicates with the gatekeeper. Usually, this H.323 ID is the name given to the gateway with the gatekeeper domain name appended to the end.	
<i>ip-address</i>	The IP address of an alternate for this endpoint.	
<i>port number</i>	The port number associated with the address of the alternate. Default is 1720.	

Defaults No default behavior or values.

Command Modes Gatekeeper configuration

Command History	Release	Modification
	12.1(5)XM	This command was introduced.
	12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.

Usage Guidelines This command defines the IP address for an alternate endpoint for the primary endpoint identified by its H.323ID. The IP address is returned in the alternate endpoint field whenever the primary endpoint is returned in an ACF or LCF. The alternate endpoint gives an alternate address to place the call in case the call to the primary endpoint fails.

This command provides a failover mechanism if a gateway becomes disabled for a period of time before the gatekeeper becomes aware of the problem. After receiving an admission confirmation (ACF) from the gatekeeper with an alternate endpoint list, the Cisco gateway may attempt to use an alternate if a SETUP message results in no reply from the destination. This command causes the alternate endpoints specified to be sent in all subsequent ACF/location confirmation (LCF) messages for the endpoint named in the *h323-id* argument. Gatekeepers that support this **endpoint alt-ep h323id** command also support receiving alternate endpoint information using RAS messages. The gatekeeper accepts IP and port call signal address information in endpoint registration request (RRQ) messages. The gatekeeper list of alternates for a given endpoint is the union of the configured alternates and alternates received in RRQs from that endpoint.

Examples The following example shows the endpoint at 209.9.53.15 1719 as an alternate for GW10:

```
Router(config-gk)# endpoint alt-ep h323id GW10 209.9.53.15 1719
```

Related Commands

Command

Description

show gatekeeper endpoints [alternates] Displays information about alternate endpoints.

endpoint ttl

To enable the gatekeeper to assign Time To Live (TTL) to the endpoint when it registers with the gatekeeper, use the **endpoint ttl** gatekeeper configuration command. To disable, use the **no** form of this command.

endpoint ttl *time to live*

no endpoint ttl

Syntax Description

time to live When an endpoint registers with the gatekeeper and does not provide a TTL value, the gatekeeper assigns this value as the Time To Live. When the TTL expires, the endpoint becomes subject to removal. However, the endpoint is queried a few times in an attempt to communicate with the device. If the device appears active, the registration does not expire. If the device is unresponsive after a few communication attempts, the endpoint is removed.

The Time To Live value can range from 60 to 3600 seconds.

Defaults

1800 seconds.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.1(5)XM	This command was introduced.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.

Usage Guidelines

This command specifies endpoint registration. Use this command to set the interval that the gatekeeper requires of an endpoint that does not supply its own value. Use a lower value to make the gatekeeper clear the registration of an unresponsive endpoint more quickly.

Examples

The following example enables time to live:

```
Router(config-gk)# endpoint ttl time to live
```

Related Commands

Command	Description
timer cluster-element announce	Specifies the announcement period.
timer lrq seq delay	Specifies the timer for sequential LRQs.
timer lrq window	Specifies the window timer for LRQs.

load-balance

To configure load balancing, use the **load-balance** gatekeeper configuration command. To disable, use the **no** form of this command.

```
load-balance [endpoints max-endpoints] [calls max-calls] [cpu max-%cpu]
[memory max-%mem-used]
```

Syntax Description	endpoints <i>max-endpoints</i>	(Optional) Maximum number of endpoints.
	calls <i>max-calls</i>	(Optional) Maximum number of calls.
	cpu <i>max-%cpu</i>	(Optional) Maximum percentage of CPU utilization.
	memory <i>max-%mem-used</i>	(Optional) Maximum percentage of memory used.

Defaults Load balancing is performed by the gatekeeper.

Command Modes Gatekeeper configuration

Command History	Release	Modification
	12.1(2)XM	This command was introduced.
	12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.

Usage Guidelines Load balancing occurs when one gatekeeper reaches the default or the configured load level. Upon reaching the load-level threshold, the gatekeeper begins sending alternate gatekeeper information in RAS messages, and the gateways then attempt to migrate from the loaded gatekeeper to its least busy alternate. The move is permanent; endpoints are not actively moved back to the original gatekeeper if it stabilizes. However, they might return to that gatekeeper if the new gatekeeper reaches a load threshold and transfers them again. The gatekeepers share the load, but they might not have an equal load. This process allows for more effective zone management.

Examples The following example configures load balancing:

```
Router(config-gk)# load-balance endpoints 200 calls 100 cpu 75 memory 80
```

Related Commands	Command	Description
	zone cluster local	Configures alternate gatekeepers for each zone.

server trigger

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

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

```
no server trigger {arq | lcf | lrj | lrq | rai | rrq | urq} zone-name priority
```

```
no server trigger all
```

Syntax Description

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

Defaults

No server triggers are set.

Command Modes

Gatekeeper configuration.

Usage Guidelines

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

In ARQ submode, enter the following syntax:

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

In DRQ submode, enter the following syntax:

```
Router(config-gk)#server trigger drq zone-name priority
server-id server-ipaddress
server-port
```

```
Router(config-gk-lcftrigg)#
```

In LCF submode, enter the following syntax:

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

In LRJ submode, enter the following syntax:

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

In LRQ submode, enter the following syntax:

```
Router(config-gk)#server trigger lrq zone-name priority
server-id server-ipaddress
server-port
Router(config-gk-lrqtrigg)#
```

In RAI submode, enter the following syntax:

```
Router(config-gk)#server trigger rai zone-name priority
server-id server-ipaddress
server-port
Router(config-gk-lrqtrigg)#
```

In RRQ submode, enter the following syntax:

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

In URQ submode, enter the following syntax:

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

The following options are available in all submodes:

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

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

<i>destination-info</i>	Configure <i>destination-info</i> to trigger one of the following conditions:
<i>e164</i>	Configure an E.164 pattern.
<i>email-id</i>	Configure an email ID.
<i>h323-id</i>	Configure an H.323 ID.
<i>word</i>	When configuring the e164 address option, the email-id option, or the h323-id option above, the E.164 address can end in a trailing '.', 's, or '*'.

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

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

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

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

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

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

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

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

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

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.1(5)XM	The drq and rai keywords were added.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.

Usage Guidelines

Server triggers are used to set the trigger points for an external application and are set for the messages that are of interest to that application. Processing of these RAS messages trips the trigger that causes the gatekeeper to send a GKTMP REQUEST message to the external application.

Examples

The following example shows the server trigger enabled.

```

gatekeeper
  zone local RoseGK cisco.com 209.165.201.30
  zone remote LilacGK cisco.com 209.165.201.1 cost 20 priority 10
  zone remote LavenderGK cisco.com 209.165.202.129 1719 cost 10 priority 10
  zone cluster local RoseGK PurpleGK 209.165.202.158 1719
  accounting vsa
  load-balance endpoints 200 calls 100 cpu 75 memory 80
  no shutdown
  server trigger drq RoseGK 1 TMPServer 209.165.201.1 4000
    info-only
  !
  server trigger rai RoseGK 1 TMPServer 209.165.201.1 4000
    endpoint-type voice-gateway
  !

```

Related Commands

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

show gatekeeper cluster

To display all the configured clusters and to provide validation of the configuration, use the **show gatekeeper cluster** privileged EXEC command.

show gatekeeper cluster

Syntax Description There are no arguments or keywords for this command.

Defaults No default behavior or values.

Command Modes EXEC

Command History	Release	Modification
	12.1(5)XM	This command was introduced.
	12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.

Examples The following example shows configured clusters:

```
Router# show gatekeeper cluster
```

```

                CONFIGURED CLUSTERS
                =====
Cluster Name   Type      Local Zone  Elements  IP
-----
RTPCluster    Local    RTPGK1     RTPGK2    209.165.200.254 1719
                RTPGK3    209.165.200.223 1719
SJCluster     Remote
                SJGK1     209.165.200.257 1719
                SJGK2     209.165.200.258 1719
                SJGK3     209.165.200.259 1719

```

Related Commands	Command	Description
	show gatekeeper endpoints	Configures alternate endpoints.
	show gatekeeper performance statistics	Displays information about the number of calls accepted and rejected, and finds the number of endpoints sent to other gatekeepers
	show gatekeeper zone cluster	Displays the dynamic status of all local clusters.

show gatekeeper endpoints

To enable printing of alternate endpoint information, use the **show gatekeeper endpoints** privileged EXEC command.

show gatekeeper endpoints [alternates]

Syntax Description	alternates (Optional) Includes information about alternates in the display. All information normally included with the show gatekeeper endpoints command is also displayed.										
Defaults	No default behavior or values.										
Command Modes	EXEC										
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>11.3(2) NA</td> <td>This command was introduced.</td> </tr> <tr> <td>12.0(5)T</td> <td>The display format was modified for H.323, version 2.</td> </tr> <tr> <td>12.1(5)XM</td> <td>The alternates keyword was added.</td> </tr> <tr> <td>12.2(2)T</td> <td>This command was integrated into Cisco IOS Release 12.2(2)T.</td> </tr> </tbody> </table>	Release	Modification	11.3(2) NA	This command was introduced.	12.0(5)T	The display format was modified for H.323, version 2.	12.1(5)XM	The alternates keyword was added.	12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
Release	Modification										
11.3(2) NA	This command was introduced.										
12.0(5)T	The display format was modified for H.323, version 2.										
12.1(5)XM	The alternates keyword was added.										
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.										
Usage Guidelines	Having alternate endpoints allows calls destined for an unresponsive gateway to complete using one of the alternate endpoints before the gatekeeper is aware of the problem.										

Examples

The following example shows output for the gatekeeper endpoints and then for alternate endpoints:

```
Router# show gatekeeper endpoints alternates

GATEKEEPER ENDPOINT REGISTRATION
=====
CallSignalAddr  Port  RASSignalAddr  Port  Zone Name          Type  F
-----
209.165.201.1  1720  209.165.201.1  58801 Zone3              VOIP-GW
      H323-ID:GW1
      E164-ID:60001
      E164-ID:60002
      ALT_EP: 209.16.0.0 <1111>
Total number of active registrations = 1

ALL CONFIGURED ALTERNATE ENDPOINTS
=====
Endpoint H323 Id          RASSignalAddr  Port
-----
GW1                209.16.0.0    1111
```

■ show gatekeeper endpoints

Related Commands	Command	Description
	endpoint alt-ep h323id	Configures alternate endpoints.

show gatekeeper performance statistics

To display information about the number of calls accepted and rejected, and to find the number of endpoints sent to other gatekeepers, use the **show gatekeeper performance statistics** privileged EXEC command.

show gatekeeper performance statistics

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes EXEC

Command History	Release	Modification
	12.1(5)XM	This command was introduced.
	12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.

Usage Guidelines This command displays the number of calls accepted, the number of calls rejected due to overload, and the number of endpoints sent to other gatekeepers.

Examples The following example displays output for the **show gatekeeper performance statistics** command:

```
Router show gatekeeper performance statistics
Performance statistics captured since:00:14:02 UTC Mon Mar 1 1993

RAS inbound message counters:
    Originating ARQ:4    Terminating ARQ:1    LRQ:7
RAS outbound message counters:
    ACF:5  ARJ:0  LCF:7  LRJ:0
    ARJ due to overload:0
    LRJ due to overload:0

Load balancing events:0
Real endpoints:2
```

When you enter the **show gatekeeper performance statistics** command, the statistical data relating to the router is displayed. You can identify the amount of call initiation events using the following:

- Automatic repeat request (ARQ)
- Admissions confirmation (ACF)
- Admission rejection (ARJ)

You can identify endpoint contact information events that have been requested and have either been confirmed or rejected on the router by using the following:

 ■ show gatekeeper performance statistics

- Location request (LRQ)
- Location confirmation request (LCF)
- Location reject (LRJ)

The counts associated with overload, and the number of endpoints sent to alternate gatekeepers that are associated with overload conditions, are also displayed. Only when the router experiences an overload condition do these counters reveal a value other than zero. The real endpoint count simply displays the amount of endpoints registered on this router platform. The timestamp displays the start time when the counters started capturing the data. When you want to request a new start period, enter the **clear h323 gatekeeper statistics**. The counters are reset, and the timestamp is updated with the new time.

 Related Commands

Command	Description
clear h323 gatekeeper statistics	Clears statistics about gatekeeper performance.

show gatekeeper status cluster

To display the health of each element of all local clusters such as the amount of memory used, the number of active calls, and the number of endpoints registered on the element, use the **show gatekeeper status cluster** privileged EXEC command.

show gatekeeper status cluster

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes EXEC

Command History	Release	Modification
	12.1(5)XM	This command was introduced.
	12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.

Examples The following example displays output for the **show gatekeeper status cluster** command. In this example, MsPacman and LavenderGK are part of a local cluster:

```
Router# show gatekeeper status cluster
```

```

                CLUSTER INFORMATION
                =====
                Active  Endpoint  Last
                Calls   Count    Announce
-----
Hostname    %Mem    %CPU
-----
MsPacman    17      2      0      1      Local Host
LavenderGK  30      1      0      4      14s

```

Related Commands	Command	Description
	show gatekeeper endpoints	Configures alternate endpoints.
	show gatekeeper performance statistics	Displays information about the number of calls accepted and rejected, and finds the number of endpoints sent to other gatekeepers
	show gatekeeper zone cluster	Displays the dynamic status of all local clusters.

show gatekeeper zone cluster

To display the dynamic status of all local clusters, use the **show gatekeeper zone cluster** privileged EXEC command.

show gatekeeper zone cluster

Syntax Description There are no arguments or keywords.

Defaults No default behavior or values.

Command Modes EXEC

Command History	Release	Modification
	12.1(5)XM	This command was introduced.
	12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.

Examples Enter this command to display information about the current bandwidth values and when the last announcement message from the alternate gatekeeper was received. In the following examples, PRI represents the priority value assigned to an alternate gatekeeper. This field ranges from 0 to 127, with 127 representing the lowest priority.

```
Router# show gatekeeper zone cluster
```

```

LOCAL CLUSTER INFORMATION, 6t
=====
          TOT BW   INT BW   REM BW   LAST   ALT GK
LOCAL GK NAME ALT GK NAME PRI (kbps) (kbps) (kbps) ANNOUNCE STATUS
-----
ParisGK      GenevaGK    120    0        0        7s    CONNECTED
NiceGK       ZurichGK   100    0        0        7s    CONNECTED

```

Related Commands	Command	Description
	timer cluster-element announce	Defines the time interval between successive announcement messages exchanged between elements of a local cluster.
	zone cluster local	Configures alternate gatekeepers for each zone.
	zone remote	Defines the remote zone.

timer cluster-element announce

To define the time interval between successive announcement messages exchanged between elements of a local cluster, use the **timer cluster-element announce** gatekeeper configuration command. To reset to the default value, use the **no** form of this command.

timer cluster-element announce *time-in-seconds*

no timer cluster-element announce

Syntax Description	<i>time-in-seconds</i>	Number of seconds between announcement periods. When a gatekeeper comes on line, it announces its presence on a periodic basis, 3 seconds by default.
---------------------------	------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------

Defaults	30 seconds
-----------------	------------

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

Command History	Release	Modification
	12.1(5)XM	This command was introduced.
	12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.

Usage Guidelines

The announcement indication is exchanged every set interval of time, and carries information about the call and endpoint capacity for the zone. This allows the alternate gatekeepers to manage the bandwidth for a single zone, even though the gatekeepers are in separate physical devices.

The gatekeeper assumes that the alternate gatekeeper has failed (and assumes that any previously allocated bandwidth is now available), if the gatekeeper does not receive an announcement message within six announcement periods, or if the Transmission Control Protocol (TCP) connection with the gatekeeper is detected to be broken.

Lower this value for closer tracking between the elements. Raise it to lower the messaging overhead.

Examples

The following command sets the announcement period to 20 seconds:

```
Router(config-gk) # timer cluster-element announce 20
```

The following command resets the announcement period to the default value of 30 seconds:

```
Router(config-gk) # no timer cluster-element announce
```

Related Commands

Command	Description
zone cluster local	Configures alternate gatekeepers for each zone.
zone remote	Defines the remote zone.

timer lrq seq delay

To define the time interval between successive sequential LRQs, use the **timer lrq seq delay** gatekeeper configuration command. To reset to the default value, use the **no** form of this command.

timer lrq seq delay *time-in-100-millisecond-units*

no timer lrq seq delay

Syntax Description	<i>time-in-100-millisecond-units</i> Number of milliseconds in 100 ms units. Range is 1 through 10.						
Defaults	5 (500 milliseconds).						
Command Modes	Gatekeeper configuration						
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.1(5)XM</td> <td>This command was introduced.</td> </tr> <tr> <td>12.2(2)T</td> <td>This command was integrated into Cisco IOS Release 12.2(2)T.</td> </tr> </tbody> </table>	Release	Modification	12.1(5)XM	This command was introduced.	12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
Release	Modification						
12.1(5)XM	This command was introduced.						
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.						
Usage Guidelines	<p>The LRQ sequential timing source (SEQ) delay is used to set the time between sending LRQs to remote gatekeepers for address resolution. To resolve an address, the gatekeeper might have several remote zones configured, and it can send the LRQs simultaneously (blast) or sequentially (seq). The gatekeeper chooses the best route based on availability and cost. Using LRQs sequentially results in lower network traffic, but can increase latency of calls when the most preferred route is unavailable.</p> <p>Lowering the time will increase traffic on the network but might reduce the call setup time.</p>						
Examples	<p>The following command sets the LRQ delay timer to 100 milliseconds:</p> <pre>Router(config-gk)# timer lrq seq delay 1</pre> <p>The following command resets the LRQ delay timer to the default value:</p> <pre>Router(config-gk)# no timer lrq seq delay</pre>						
Related Commands	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>timer lrq window</td> <td>Specifies the window timer for LRQs.</td> </tr> </tbody> </table>	Command	Description	timer lrq window	Specifies the window timer for LRQs.		
Command	Description						
timer lrq window	Specifies the window timer for LRQs.						

timer lrq window

To define the time window during which the gatekeeper will collect responses to one or more outstanding LRQs, use the **timer lrq window** gatekeeper configuration command. To reset to the default value, use the **no** form of this command.

timer lrq window *time-in-seconds*

no timer lrq window

Syntax Description	<i>time-in-seconds</i>	Number of seconds. Range is 1 through 15.
Defaults	3 seconds.	
Command Modes	Gatekeeper configuration	
Command History	Release	Modification
	12.1(5)XM	This command was introduced.
	12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
Usage Guidelines	Increasing the time can increase the call success rate but might reduce the overall time for call setup.	
Examples	<p>The following command sets the timer to five seconds:</p> <pre>Router(config-gk)# timer lrq window 5</pre> <p>The following command sets the timer to the default value:</p> <pre>Router(config-gk)# no timer lrq window</pre>	
Related Commands	Command	Description
	timer lrq seq delay	Specifies the timer for sequential LRQs.

timer server timeout

To specify the timeout value for a response from a back end GKTMP server, use the **timer server timeout** gatekeeper configuration command. To reset to the default value, use the **no** form of this command.

timer server timeout *time-in-100-millisecond-units*

no timer server timeout

Syntax Description	<i>time-in-100-millisecond-units</i>	Number of milliseconds in 100 ms units. Range is 1 through 50 (0.1 seconds through 5 seconds).
Defaults	30 seconds.	
Command Modes	Gatekeeper configuration	
Command History	Release	Modification
	12.1(2)XM	This command was introduced.
	12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
Examples	<p>The following command sets the timeout value to four seconds:</p> <pre>Router(config-gk)# timer server timeout 4</pre> <p>The following command resets the announcement period to the default value of three seconds:</p> <pre>Router(config-gk)# no timer server timeout</pre>	
Related Commands	Command	Description
	server registration-port	Defines a port number for the gatekeeper to open and listen for incoming TCP connections from back end GKTMP servers.
	server trigger	Connects the gatekeeper to a GKTMP server at startup.

zone cluster local

To define a local grouping of gatekeepers, including the gatekeeper that you are configuring, use the **zone cluster local** gatekeeper configuration command. To disable, use the **no** form of this command.

zone cluster local *cluster-name local-zone-name*

no zone cluster local

Syntax Description		
	<i>cluster-name</i>	Defines the cluster name.
	<i>local-zone-name</i>	Defines the local zone name.

Defaults No default behavior or values.

Command Modes Gatekeeper configuration

Command History	Release	Modification
	12.1(5)XM	This command was introduced.
	12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.

Usage Guidelines Use this command to define a local cluster of gatekeepers that are alternates of each other. Each of these gatekeepers must be configured in a compatible manner for the cluster to work effectively.

Examples The following example shows how to define a local grouping of gatekeepers:

```
Router(config-gk)# zone cluster local EuropeCluster ParisGK
```

Related Commands	Command	Description
	element	Defines component elements of local or remote clusters.
	zone cluster remote	Defines a remote group of gatekeepers including the gatekeeper that you are configuring.

zone cluster remote

To define a remote grouping of gatekeepers, including the gatekeeper that you are configuring, use the **zone cluster remote** gatekeeper configuration command. To disable, use the **no** form of this command.

zone cluster remote *cluster name* [**cost** *cost-value* [**priority** *priority-value*]]

no zone cluster remote

Syntax Description

<i>cluster name</i>	Defines the cluster name.
cost	Sets the cost.
<i>cost-value</i>	Defines the cost value. Range is 1 through 100. Default is 50.
priority	Sets the priority.
<i>priority-value</i>	Defines the priority value. Range is 1 through 100. Default is 50.

Defaults

No default behavior or values.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.1(5)XM	This command was introduced.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.

Usage Guidelines

Use this command to define a set of remote gatekeepers that are alternates of each other and to form a local cluster. This command causes the gatekeeper to optimize these remote gatekeepers by round-robin sending of LRQs.

Examples

The following example shows how to define a remote grouping of gatekeepers:

```
Router(config-gk) # zone cluster remote AsiaCluster cost 70 priority 10
```

Related Commands

Command	Description
element	Defines component elements of local or remote clusters.
zone cluster local	Defines a local group of gatekeepers including the gatekeeper that you are configuring.
zone local	Defines the gatekeeper's name or zone name. This is usually the fully domain-qualified host name of the gatekeeper.

zone remote

To statically specify a remote zone if domain name service (DNS) is unavailable or undesirable, use the **zone remote** command in gatekeeper configuration mode. To remove the remote 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]]
```

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

Syntax Description

<i>other-gatekeeper-name</i>	Name of the remote gatekeeper.
<i>other-domain-name</i>	Domain name of the remote gatekeeper.
<i>other-gatekeeper-ip-address</i>	IP address of the remote gatekeeper.
<i>port number</i>	(Optional) RAS signaling port number for the remote zone. Value ranges from 1 to 65535. If this is not set, the default is the well-known RAS port number 1719.
cost	Sets the cost of the zone.
<i>cost-value</i>	Cost value. Range is 1 through 100. Default is 50.
priority	Sets the priority of the zone.
<i>priority-value</i>	Priority value. Range is 1 through 100. Default is 50.

Defaults

No remote zone is defined. DNS locates the remote zone.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
11.3 (2)NA and 12.0(3)T	This command was introduced.
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.

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 LRQs 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 “zone remotes” 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 shows how to configure the cost and priority for the gatekeeper GK10 serving zone 1:

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

Related Commands

zone local	Defines the gatekeeper's name or zone name. This is usually the fully domain-qualified host name of the gatekeeper.
-------------------	---------------------------------------------------------------------------------------------------------------------

Glossary

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

ACF—admission confirmation.

ARJ—admission rejection.

ARQ—automatic repeat request.

ASN.1—Abstract Syntax Notation 1. A standard to represent information exchanged between computers.

CDR—call detail record.

CLI—command-line interface.

DRQ—disengage request.

gatekeeper—A gatekeeper maintains a registry of devices in the multimedia network. The devices register with the gatekeeper at startup and request admission to a call from the gatekeeper.

The gatekeeper is an H.323 entity on the LAN that provides address translation and control access to the LAN for H.323 terminals and gateways. The gatekeeper can provide other services to the H.323 terminals and gateways, such as bandwidth management and locating gateways.

gatekeeper cluster—A group of alternate gatekeepers.

gatekeeper node—An individual gatekeeper within a cluster. Also called a GK.

gateway—A gateway allows H.323 terminals to communicate with non-H.323 terminals by converting protocols. A gateway is the point where a circuit-switched call is encoded and repackaged into IP packets.

An H.323 gateway is an endpoint on the LAN that provides real-time, two-way communications between H.323 terminals on the LAN and other ITU-T terminals in the WAN or to another H.323 gateway.

GKAPI—Gatekeeper Application Programming Interface. The API provided on the back end servers for applications to use to communicate with the gatekeeper.

GKTMP—Gatekeeper Transaction Message Protocol. The protocol used to communicate with back end servers other than Cisco IOS servers.

GUP—Gatekeeper Update Protocol.

ITU-T—International Telecommunication Union Telecommunication Standardization Sector.

IVR—Interactive voice response. When someone dials in, IVR responds with a prompt to get a personal identification number (PIN), and so on.

LCF—Location confirmation request.

LRJ—location reject.

LRQ—location requests.

MCU—multipoint control unit.

SEQ—sequential timing source.

PIN—Personal identification number. Password used with account number for authentication.

POTS—Plain old telephone service. Basic telephone service supplying standard single-line telephones, telephone lines, and access to the PSTN.

PSTN—Public Switched Telephone Network. PSTN refers to the local telephone company.

RADIUS—Remote Access Dial-In User Service. Database for authenticating modem and ISDN connections and for tracking connection time.

RAI— resource availability indication.

RAS—registration, admission, and status protocol. Protocol used in the H.323 protocol suite for discovering and interacting with a gatekeeper.

RRQ—registration request.

TTL—Time To Live. Field in an IP header that indicates how long a packet is considered valid.

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

VPN—Virtual Private Network, which Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses “tunneling” to encrypt all information at the IP level.

VSA—vendor-specific attribute method of accounting.

