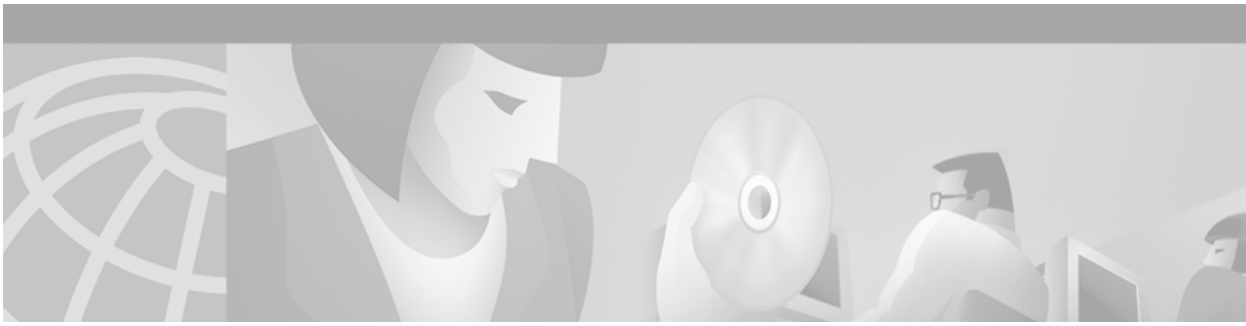


Inter-Domain Gatekeeper Security Enhancement

Feature History

Release	Modification
12.2(2)XA	The Inter-Domain Gatekeeper Security Enhancement was introduced for Cisco 2600, Cisco 3600 series, Cisco 7200, and Cisco MC3810. **Note** The Cisco AS5300 supports this feature by providing *gateway* functionality, but does not itself provide *gatekeeper* functionality.
12.2(4)T	The new and modified commands introduced in Cisco IOS Release 12.2(2)XA were integrated into Cisco IOS Release 12.2(4)T. **Note** Support for the Cisco AS5300 as a universal gateway is not included in this release.
12.2(2)XB1	This feature was implemented on the Cisco AS5850 as a universal gateway.
12.2(11)T	This feature was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5300 and Cisco AS5850 as universal gateways.

This document describes the Inter-Domain Gatekeeper Security Enhancement, including information about the benefits of the feature, supported platforms, related documents, and so on.

This document includes the following sections:

Feature Overview

The Inter-Domain Gatekeeper Security Enhancement provides a means of authenticating and authorizing H.323 calls between the administrative domains of Internet Telephone Service Providers (ITSPs).

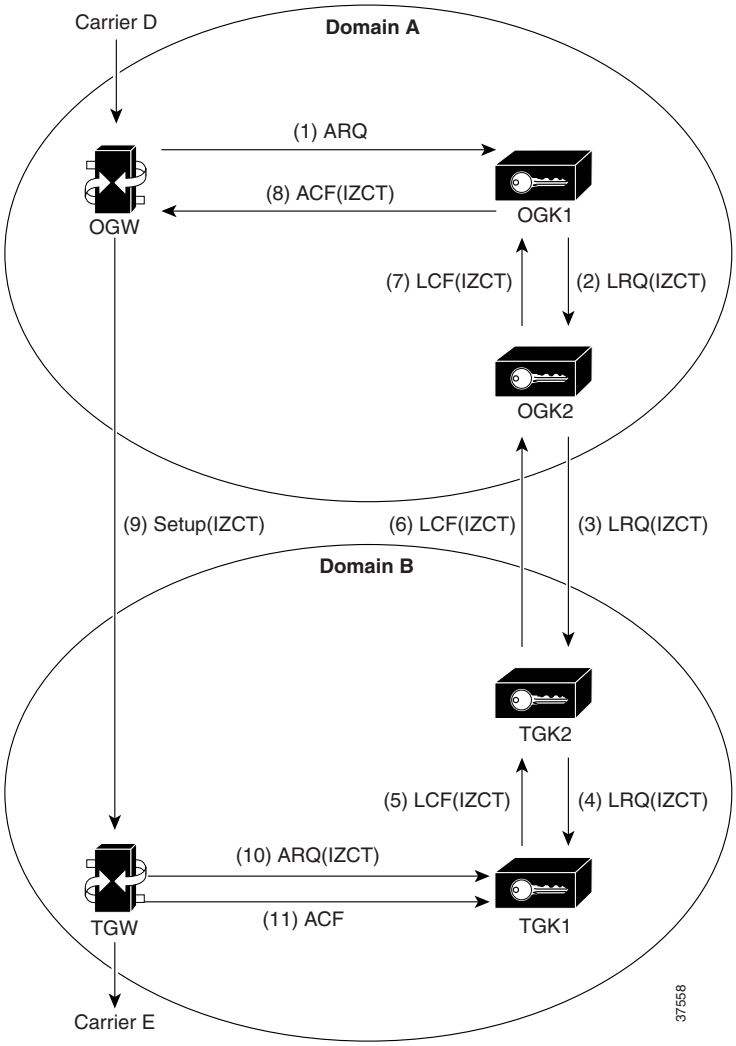
An interzone ClearToken (IZCT) is generated in the originating gatekeeper when a location request (LRQ) is initiated or an admission confirmation (ACF) is about to be sent for an intrazone call within an ITSP's administrative domain. As the IZCT traverses through the routing path, each gatekeeper stamps the IZCT's destination gatekeeper ID with its own ID. This identifies when the IZCT is being passed over to another ITSP's domain. The IZCT is then sent back to the originating gateway in the location confirmation (LCF) message. The originating gateway passes the IZCT to the terminating gateway in the SETUP message. The terminating gatekeeper forwards the IZCT in the admission request (ARQ) answerCall field to the terminating gatekeeper, which then validates it.

Within the IZCT format, the following information is required:

- srcCarrierID —Source carrier identification
- dstCarrierID — Destination carrier identification
- intCarrierID — Intermediate carrier identification
- srcZone — Source zone
- dstZone — Destination zone
- interzone type
  - INTRA_DOMAIN_CISCO
  - INTER_DOMAIN_CISCO
  - INTRA_DOMAIN_TERM_NOT_CISCO
  - INTER_DOMAIN_ORIG_NOT_CISCO

Figure 1 shows a simple inter-ITSP diagram of the IZCT flow.

Figure 1 Inter-ITSP Diagram of the Inter-Domain Gatekeeper Security Enhancement Flow



1. The originating gateway sends an ARQ message with an interface description as a nonstandard field to originating gatekeeper 1 (OGK1). The interface description is treated as a source carrier identifier.
2. Upon receiving the ARQ, OGK1 creates an IZCT with the following:
   - srcCarrierID— source carrier identification, received from the ARQ
   - dstCarrierID—destination carrier identification, received from the CSR
   - intCarrierID—intermediate carrier identification, received from the CSR
   - srcZone—source zone name or a cluster name if the GK is member of a cluster
   - dstZone—destination zone is set to null
   - interZoneType—interzone type is set to INTRA_DOMAIN_CISCO

   The IZCT is sent in an LRQ to OGK2.
3. OGK2 determines that the LRQ did not come from a foreign domain, replaces the IZCT's srcZoneID with its ID (or cluster name, if the gatekeeper is member of a cluster), and forwards the LRQ with the updated IZCT to terminating gatekeeper 2 (TGK2).

4. TGK2 determines that the LRQ came from a foreign domain, updates the IZCT's dstZone with its own ID (or cluster name, if the GK is member of a cluster) and the interZoneType as INTER_DOMAIN_CISCO, and passes the updated IZCT to TGK1. TGK2 treats the zone from which an LRQ is received as foreign-domain zone in either of the following two scenarios:
   a. The TGK2's remote zone list does not contain the zone from which an LRQ is received.
   b. The TGK2's remote zone list contains the zone from which an LRQ is received and the zone is marked with a foreign-domain flag. For details on how to mark a zone as foreign-domain, refer to the "Configuration Tasks" section on page 6.
5. TGK1 updates the IZCT's dstCarrierID to Carrier E, which is determined by the routing process; generates a hash with the IZCT's password; and sends an LCF with the updated IZCT in it. If TGK1 is a clustered GK, then the IZCT password is identical across the cluster.
6. TGK2 forwards the LCF to OGK2.
7. OGK2 forwards the LCF to OGK1.
8. OGK1 extracts the IZCT from the LCF and sends it in an ACF to the OGW.
9. The OGW sends the IZCT to the TGW in the H.225 SETUP message.
10. The TGW passes the IZCT to the TGK1 in an ARQ answerCall.
11. TGK1 authenticates the destination IZCT successfully, because TGK1generated the hash in the IZCT.

Note In the case of an inter-ITSP call, border zones (in the above example, OGK2 and TGK2) are identified as the srcZone and dstZone of the IZCT that is returned in the ACF to the OGW. If the call is intra-ITSP, leaf zones are identified as the srcZone and dstZone of the IZCT that is returned in the ACF to the OGW.

Benefits

- Provides security for wholesale providers by supporting authentication and authorization capability for internet telephony calls between foreign other ITSP domains.
- Provides the security functionality necessary for billing and settlement.

Related Features and Technologies

- Settlements for Packet Voice, Phase 2

Related Documents

Cisco customer documentation:

- *Settlements for Packet Voice, Phase 2*
- *Cisco IOS Voice, Video, and Fax Configuration Guide*, Release 12.2
- *Voice Features for Cisco 3600 Series Routers*
- *Configuring H.323 VoIP Gateway for Cisco Access Platforms*
- *Configuring H.323 VoIP Gatekeeper for Cisco Access Platforms*

- *Configuring Interactive Voice Response for Cisco Access Platforms*
- *Certification Authority Interoperability*
- *Cisco IOS Security Configuration Guide*
- *Cisco IP Security and Encryption Overview*

Other documentation:

- *Token Card and Cisco Secure Authentication Support*
- *The SSL Protocol Version 3.0 as amended SSL 3.0 Errata of August 26, 1996*

Supported Platforms

These platforms support Gatekeeper functionality for this feature:

- Cisco 2600
- Cisco 3600 series (includes the 3620, 3640, and 3660)
- Cisco 7200
- Cisco MC3810

Table 1 Platforms and Images That Support Gatekeeper Functionality

Platform	Images Required for Gatekeeper Functionality
Cisco 2600	ix, jsx
Cisco 3600 series	ix, jsx
Cisco 7200	a3jk8s, a3jk9s, a3js, dk8o3s, dk8s, dk9o3s, do3s, ds, ik8o3s, ik8s, ik9o3s, ik9s, io3s, is, jk8o3s, jk8s, jk9o3s, jk9s, jo3s, js, jx2
Cisco MC3810	a2jsv5x

These platforms support Gateway functionality for this feature:

- Cisco 2600
- Cisco 3600 series
- Cisco 7200
- Cisco AS5300(gateway functionality only)
- Cisco AS5850 (gateway functionality only)

Table 2 Cisco IOS Release and Platform Support for this Feature

Platform	12.2(2)XA	12.2(4)T	12.2(2)XB1	12.2(11)T
Cisco 2600	X	X	Not supported	X
Cisco 3600 series	X	X	Not supported	X
Cisco AS5300 (gateway functionality only)	Not supported	Not supported	Not supported	X
Cisco AS5850 (gateway functionality only)	Not supported	Not supported	X	X
Cisco 7200 series	X	X	Not supported	X
Cisco MC3810	X	X	Not supported	X

Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that support 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 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 at 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

No new or modified standards are supported by this feature.

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 web site on Cisco Connection Online (CCO) at http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

RFCs

No new or modified RFCs are supported by this feature.

Configuration Tasks

See the following section for configuration tasks for the Inter-Domain Gatekeeper Security Enhancement.

- Configuring the Domain Zones and IZCT Password (Required)

Configuring the Domain Zones and IZCT Password

The main tasks are marking foreign and local domain zones and setting up an IZCT password for use in all the zones. To configure the domain zones and IZCT password, perform the following steps beginning in global configuration mode.

	Command	Purpose
Step 1	`Router# config terminal`	Enters the global configuration mode.
Step 2	`Router(config)# gatekeeper`	Enters gatekeeper configuration mode.
Step 3	`Router(config-gk)# zone local` *gatekeeper-name domain-name*	Specifies a zone controlled by a gatekeeper.
Step 4	`Router(config-gk)# zone remote` *other-gatekeeper-name other-domain-name other-ip-address* [*port-number*] [**cost** cost-value [**priority** priority-value]] [**foreign-domain**]	Statically specifies a remote zone if Domain Name System (DNS) is unavailable or undesirable. The arguments and keyword have the following meanings: *other-gatekeeper-name*—Name of the remote gatekeeper. *other-domain-name*—Domain name of the remote gatekeeper. *other-gatekeeper-ip-address*—IP address of the remote gatekeeper. *port number*—(Optional) RAS signaling port number for the remote zone. Value ranges from 1 to 65535. The default is the well-known RAS port number 1719. **cost—**Sets the cost of the zone. *cost-value*—Cost value. Range is 1 through 100. Default is 50. **priority—**Sets the priority of the zone. *priority-value*—Priority value. Range is 1 through 100. Default is 50. **foreign-domain—**Indicates that the cluster is in a different administrative domain.

	Command	Purpose
Step 5	`Router(config-gk)# zone prefix gatekeeper-name e164-prefix [gw-priority pri-0-to-0 gw-alias [gw-alias, ...]]`	Adds a prefix to the gatekeeper zone list. Enter this command for the local gatekeepers and the remote gatekeepers declared in the **zone local** and **zone remote** commands. To remove a zone prefix, use the **no** form of this command with the gatekeeper name and prefix. To remove the priority assignment for a specific gateway, use the no form of this command with the **gw-priority** option. The **zone prefix** arguments have the following meanings: *e164-prefix*—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. **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. **gw-priority** *pri-0-to-10 gw-alias*—(optional) Use the **gw-priority** option to define how the gatekeeper selects gateways in its local zone for calls to numbers beginning with prefix *e164-prefix*. Do not use this option to set priority levels for a prefix assigned to a remote gatekeeper. 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. To assign the same priority value for one prefix to multiple gateways, list all the gateway names after the *pri-0-to-10* 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.
Step 6	`Router(config-gk)# security izct password password`	Enter the IZCT password. The password must be from six to eight alphanumeric characters. To disable the IZCT featurette, enter the **no** form of the command.

	Command	Purpose
Step 7	`Router(config-gk)# gw-type-prefix type-prefix [hopoff gkid][default-technology][gw ipaddr ipaddr [port]]`	Configures a technology prefix for gatekeepers. To remove the technology prefix, use the **no** form of the command. The **gw-type-prefix** arguments and keywords have the following meanings: *type-prefix*—A technology prefix is recognized and is stripped before checking for the zone prefix. It is strongly recommended that you select technology prefixes that do not lead to ambiguity with zone prefixes. Do this by using the # character to terminate technology prefixes, for example, 3#. **hopoff** *gkid* — (optional) Specifies the gatekeeper or zone where the call is to hop off, regardless of the zone prefix in the destination address. The *gkid* argument refers to a zone previously configured using the zone local or zone remote comment. **default-technology**—(optional) Gateways registering with this prefix option are used as the default for routing any addresses that are otherwise unresolved. **gw ipaddr** *ipaddr* [*port*]—(optional) Indicates that the gateway is incapable of registering technology prefixes. When it registers, it adds the gateway to the group for this type-prefix, just as if it had sent the technology prefix in its registration. This parameter can be repeated to associate more than one gateway with a technology prefix.
Step 8	`Router(config-gk)# lrq forward-queries`	Enables a gatekeeper to forward location requests (LRQs) that contain E.164 addresses that match zone prefixes controlled by remote gatekeepers.
Step 9	`Router(config-gk)# no shutdown`	Ensures that the gatekeepers are activated.

Verifying that the IZCT Is Enabled

To verify that the IZCT is enabled, use the **show run** command. The following **show run** example shows that an IZCT password is enabled.

```
gatekeeper
 zone local 35_dirgk cisco.com 172.18.198.196
 zone remote 40_gatekeeper cisco.com 172.18.198.91 1719
 zone remote 34_dirgk cisco.com 172.18.198.197 1719 foreign-domain
 zone prefix 40_gatekeeper 408*
 zone prefix 34_dirgk *
 security izct password ABCDEF
 lrq forward-queries
 no shutdown
```

Configuration Examples

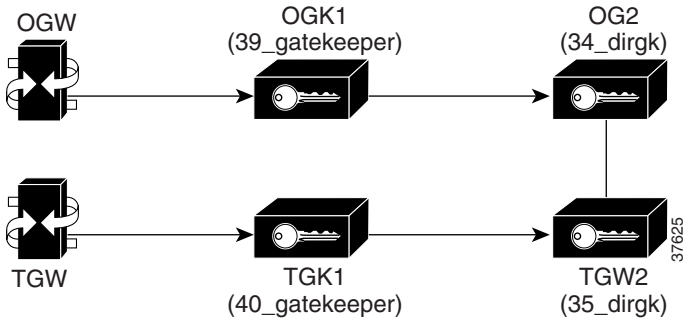
This section provides the following configuration examples:

- Originating Gatekeeper 1 Example
- Terminating Gatekeeper 1 Example
- Originating Gatekeeper 2 Example
- Terminating Gatekeeper 2 Example

Originating Gatekeeper 1 Example

All of the configuration examples are for the set-up diagram shown in Figure 2. One IZCT password is enabled for all of the gatekeepers.

Figure 2 Set-Up Diagram for the Example Configuration




```
config terminal
gatekeeper
 zone local 39_gatekeeper cisco.com 172.18.198.92
 zone remote 34_dirgk cisco.com 172.18.198.197 1719
 zone prefix 39_gatekeeper 919*
 zone prefix 34_dirgk *
 security izct password cisco
 gw-type-prefix 1#* default-technology
 no shutdown
```

Terminating Gatekeeper 1 Example

```
config terminal
gatekeeper
zone local 40_gatekeeper cisco.com 172.18.198.91
 zone remote 35_dirgk cisco.com 172.18.198.196 1719
 zone prefix 40_gatekeeper 408*
 zone prefix 35_dirgk *
 security izct password cisco
 gw-type-prefix 1#* default-technology
 no shutdown
```

Originating Gatekeeper 2 Example

```
config terminal
gatekeeper
zone local 34_dirgk cisco.com 172.18.198.197
 zone remote 39_gatekeeper cisco.com 172.18.198.92 1719
 zone remote 35_dirgk cisco.com 172.18.198.196 1719
 zone prefix 39_gatekeeper 919*
 zone prefix 35_dirgk *
 security izct password cisco
 lrq forward-queries
 no shutdown
```

Terminating Gatekeeper 2 Example

```
config terminal
gatekeeper
 zone local 35_dirgk cisco.com 172.18.198.196
 zone remote 40_gatekeeper cisco.com 172.18.198.91 1719
 zone remote 34_dirgk cisco.com 172.18.198.197 1719 foreign-domain
 zone prefix 40_gatekeeper 408*
 zone prefix 34_dirgk *
 security izct password cisco
 lrq forward-queries
 no shutdown
```

Command Reference

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

New Command:

- **security izct password**

Modified Commands:

- **zone cluster remote**
- **zone remote**

security izct password

To enable generation of the interzone ClearToken (IZCT) password, use the **security izct password** command. To disable IZCT generation, use the **no** form of this command.

security izct password *password*

no security izct password *password*

Syntax Description

password	The password must be between six and eight alphanumeric characters.

Defaults

No default behavior or values.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.2(2)XA	This command was introduced for the Cisco 2600, Cisco 3600 series, and Cisco 7200. **Note** The Cisco AS5300 supports this feature by providing *gateway* functionality, but does not itself provide *gatekeeper* functionality.
12.2(4)T	The new and modified commands introduced in Cisco IOS Release 12.2(2)XA were integrated into Cisco IOS Release 12.2(4)T. **Note** Support for the Cisco AS5300 universal gateway is not included in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850 as a universal gateway.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5300 and Cisco AS5850 as universal gateways.

Usage Guidelines

After the **security izct password** command is issued the technology prefix for the gatekeepers must be configured for the gateways. The gatekeeper must be enabled to forward Location Requests (LRQs) that contain E.164 addresses matching zone prefixes controlled by remote gatekeepers.

Note All the gatekeepers in a cluster should have the same izct password.

Examples

The following example shows how to enable an IZCT password:

```
Router(config-gk)# security izct password cisco
```

Related Commands

Command	Description
show run	Displays the IZCT password, indicating that the password is active.
zone local	Declares local domain name.
zone remote	Declares foreign domain name.
zone prefix	Adds a prefix to the gatekeeper zone list.
gw-type-prefix	Configures a technology prefix for gatekeepers.

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 c*luster name* [**cost** *cost-value* [**priority** *priority-value*]] [**foreign-domain**]

no zone cluster remote

Syntax Description

c*luster name*	Defines the cluster name.
cost	Sets the cost.
cost-value	Defines the cost value. Range is 1 through 100. Default is 50.
priority	Sets the priority.
priority-value	Defines the priority value. Range is 1 through 100. Default is 50.
foreign-domain	Indicates that the cluster is in a different administrative domain.

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.
12.2(2)XA	The **foreign-domain** keyword was added.
12.2(4)T	The new and modified commands introduced in Cisco IOS Release 12.2(2)XA were integrated into Cisco IOS Release 12.2(4)T. **Note** Support for the Cisco AS5300 universal gateway is not included in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850 as a universal gateway.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5300 and Cisco AS5850 as universal gateways.

Usage Guidelines

Use this command to define a set of remote gatekeepers that act as alternates to each other and 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*]] [**foreign-domain**]

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

Syntax Description

other-gatekeeper-name	Name of the remote gatekeeper.
other-domain-name	Domain name of the remote gatekeeper.
other-gatekeeper-ip-address	IP address of the remote gatekeeper.
port number	(Optional) RAS signaling port number for the remote zone. Value ranges from 1 to 65535. The default is the well-known RAS port number 1719.
cost	Sets the cost of the zone.
cost-value	Cost value. Range is 1 through 100. Default is 50.
priority	Sets the priority of the zone.
priority-value	Priority value. Range is 1 through 100. Default is 50.
foreign-domain	Indicates that the cluster is in a different administrative domain.

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.
12.2(2)XA	The **domain-foreign** keyword was added.
12.2(4)T	The new and modified commands introduced in Cisco IOS Release 12.2(2)XA were integrated into Cisco IOS Release 12.2(4)T. **Note** Support for the Cisco AS5300 universal gateway is not included in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850 as a universal gateway.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and support was added for the Cisco AS5300 and Cisco AS5850 as universal gateways.

Usage Guidelines

Not all gatekeepers 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 2000.

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

Examples

The following example 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

ACF—RAS message sent as an admission confirmation.

answer call— When an ARQ is sent by the terminating gateway.

ARQ—RAS message sent as an admission request.

ClearToken—Token that provides data in a clear text format.

CSR—Carrier-Sensitive Routing

domain—A portion of the naming hierarchy tree that refers to general groupings of networks based on organization-type or geography.

ITSP—Internet Telephony Service Providers

IZCT—Interzone ClearToken (IZCT)

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

LCF—RAS message sent as a location confirmation.

LRQ—RAS message sent as a location 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 that provides address translation and control access to the network for H.323 terminals and gateways. The gatekeeper may provide other services to the H.323 terminals and gateways, such as bandwidth management and locating gateways.

gatekeeper cluster—A group of alternate gatekeepers.

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

GK—Gatekeeper (see gatekeeper)

OGK—Originating gatekeeper where the packet is issued (see also gatekeeper).

OGW—Originating gateway, see gateway

OSP—Open Settlement Protocol

RAS—Registration, admission, and status protocol. This is the protocol that is used between endpoints and the gatekeeper to perform management functions. The RAS signaling function performs registration, admissions, bandwidth changes, status, and disengage procedures between the VoIP gateway and the gatekeeper.

TGK—Terminating gatekeeper, see gatekeeper

TGW—Terminating gateway, see gateway

token—A frame that contains control information. Possession of the token allows a network device to transmit data onto the network.

zone—A collection of components, such as terminals and gateways, managed by a single gatekeeper.