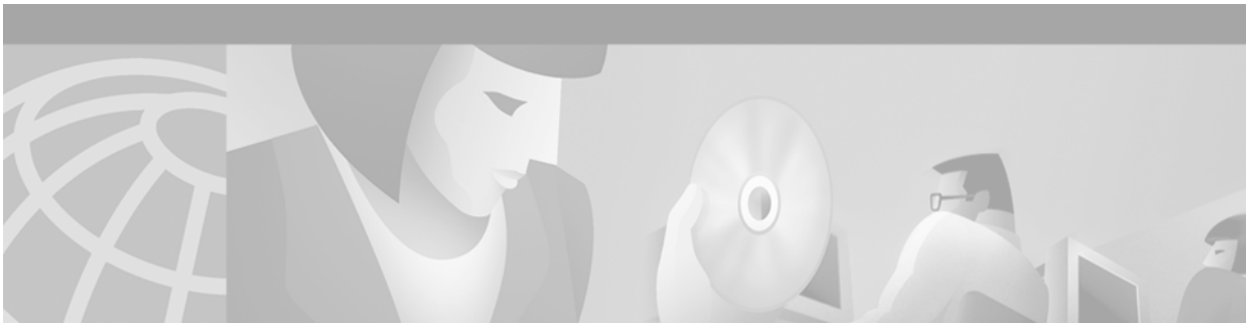

Gatekeeper-to-Gatekeeper Authentication

Feature History

Release	Modification
12.2(11)T	This feature was introduced on the Cisco 2600 series, the Cisco 3660, the Cisco 7200 series, and the Cisco MC3810.
12.2(11)T2	The **encrypted** keyword was added to the **seccurity password-group** command.

This document describes the Gatekeeper-to-Gatekeeper Authentication feature in Cisco IOS Release 12.2(11)T and includes the following sections:

Feature Overview

The Gatekeeper-to-Gatekeeper Authentication feature provides additional security for H.323 networks by introducing the ability to validate intradomain and interdomain gatekeeper-to-gatekeeper Location Request (LRQ) messages on a per-hop basis. When used in conjunction with per-call security using the interzone ClearToken (IZCT), network resources are protected from attackers and security holes are prevented. The IZCT was introduced in the Inter-Domain Gatekeeper Security Enhancement feature released in Cisco IOS Release 12.2(2)XA and Cisco IOS Release 12.2(4)T. For more information on the IZCT, refer to the *Inter-Domain Gatekeeper Security Enhancement* documentation.

The Gatekeeper-to-Gatekeeper Authentication feature provides a Cisco Access Token (CAT) to carry authentication within zones. The CAT is used by adjacent gatekeepers to authenticate each other and is configured on a per-zone basis. In addition, service providers can specify inbound passwords to authenticate LRQ messages that come from foreign domains and outbound passwords to be included in LRQ messages to foreign domains.

The call flows illustrated in Figure 1 and Figure 2 show the steps that occur with a successful LRQ authentication and with an unsuccessful LRQ authentication.

Note Although the IZCT is not required for use with the Gatekeeper-to-Gatekeeper Authentication feature, it is recommended and is shown below in the call flow examples.

Figure 1 Call Flow with Successful LRQ Authentication

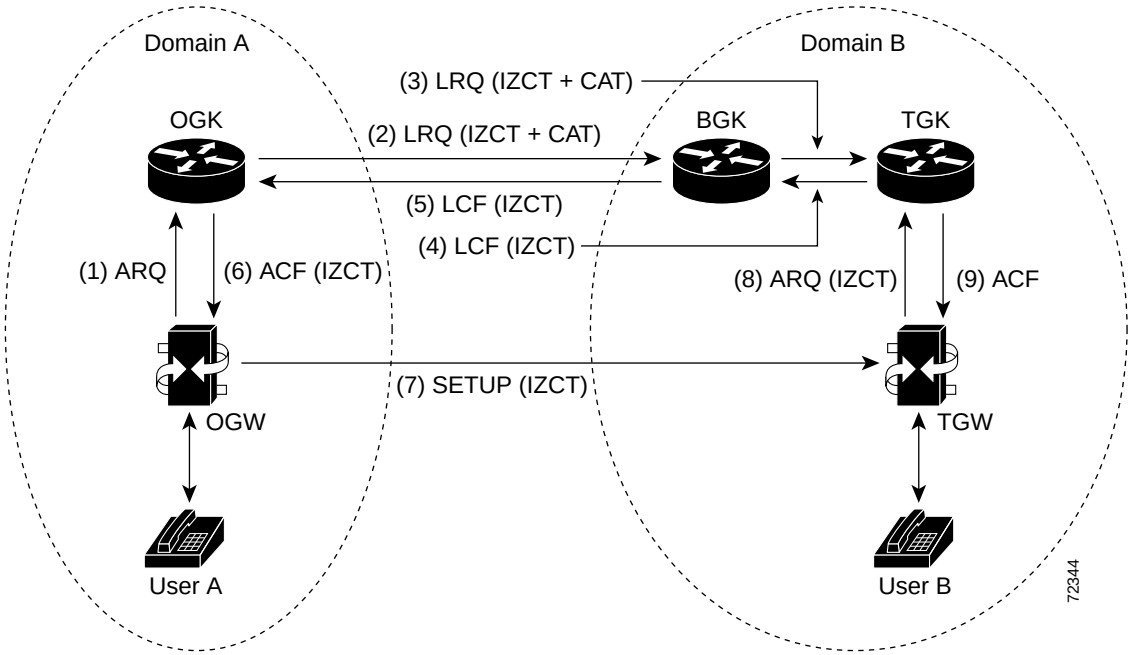

Table 1 shows what occurs in the call flow:

Table 1 Call Flow with Successful LRQ Authentication Description

Step	Action
1.	User A calls User B. The originating dial peer is configured for H.323 Registration, Admission, and Status (RAS) and sends an Admission Request (ARQ) message to the originating gatekeeper (OGK).
2.	Assuming the OGK has security enabled, the OGK generates an IZCT and a CAT to include in the LRQ message. The IZCT is used for per-call authorization while the CAT is used for gatekeeper-to-gatekeeper authentication. The CAT includes the following: • general_id: gatekeeper ID (OGK) • timeStamp: local gatekeeper time • randomValue: a random number • MD5 hash value
3.	The border gatekeeper (BGK) receives the LRQ message, checks its gatekeeper configuration, and determines that the LRQ should be authenticated before forwarding the LRQ message to the terminating gatekeeper (TGK). Once accepted, the BGK creates a new CAT and includes it in the LRQ message sent to the TGK.

Table 1 Call Flow with Successful LRQ Authentication Description

Step	Action
4.	The TGK receives the LRQ message, checks its gatekeeper configuration, and determines that the LRQ should be authenticated. The E.164 address indicates that the destination is a local gateway, so the TGK acknowledges the request by sending a Location Confirmation (LCF) message, including an updated IZCT, to the BGK.
5.	The BGK transfers the LCF to the OGK. Normal call signaling proceeds.
6.	The OGK sends an Admission Confirmation (ACF) message to the OGW. The IZCT is copied to the ACF.
7.	The OGW sends a SETUP message to the terminating gateway (TGW).
8.	The TGW sends an ARQ message to the TGK. The TGK authorizes the call by comparing the IZCT with a locally created IZCT.
9.	The TGK sends an ACF to the TGW. The call is set up between the TGW and User B.

Figure 2 Call Flow with Unsuccessful LRQ Authentication

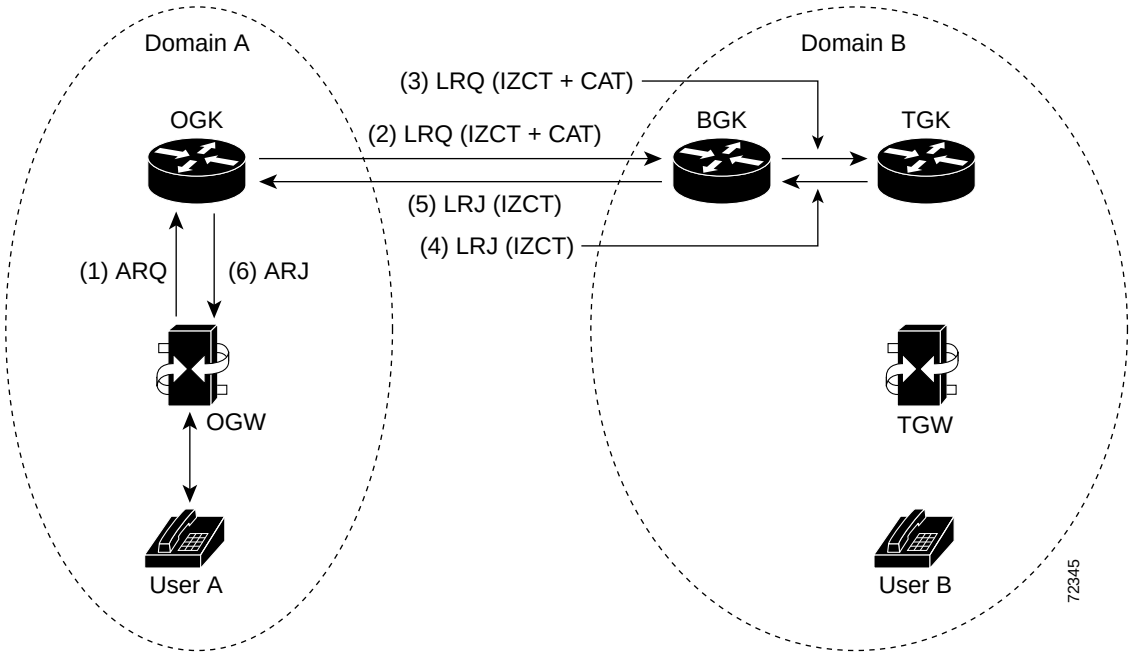

Table 2 shows what occurs in the call flow:

Table 2 Call Flow with Unsuccessful LRQ Authentication Description

Step	Action
1.	User A calls User B. The originating dial peer is configured for H.323 RAS and sends an ARQ to the OGK.
2.	Assuming the OGK has security enabled, the OGK generates an IZCT and a CAT to include in the LRQ message. The IZCT is used for per-call authorization while the CAT is used for gatekeeper-to-gatekeeper authentication. The CAT includes the following: • general_id: gatekeeper ID (OGK) • timeStamp: local gatekeeper time • randomValue: a random number • MD5 hash value
3.	The BGK receives the LRQ message, checks its gatekeeper configuration, and determines that the LRQ should be authenticated before forwarding the LRQ message to the TGK. Once accepted, the BGK creates a new CAT and includes it in the LRQ message sent to the TGK. However, in this example, an incorrect outbound password is used.
4.	The TGK receives the LRQ message, checks its gatekeeper configuration, and determines that the LRQ should be authenticated. Because an incorrect outbound password was used by the BGK, the LRQ CAT and the locally created CAT are not equivalent. The TGK sends a Location Reject (LRJ) message back to the BGK and includes a reject reason of LRJ_INVAL_PERMISSION.
5.	The BGK sends the LRJ to the OGK.
6.	The OGK sends an Admission Reject (ARJ) message to the OGW and signaling is terminated.

Benefits

- Increased security
- Ability to validate gatekeeper-to-gatekeeper requests on a per-hop basis, rather than on an originating and terminating gatekeeper-only basis
- Passwords that are stored in encrypted form locally on the gatekeeper and that do not require a RADIUS server

Restrictions

The CAT is a Cisco-proprietary security mechanism and requires a Cisco solution to receive the full end-to-end benefits of the Gatekeeper-to-Gatekeeper Authentication feature.

LRQ message authentication is done on a hop-by-hop basis. Because a non-Cisco gatekeeper does not support CATs, authentication stops at the non-Cisco gatekeeper. If a non-Cisco gatekeeper can support LRQ forwarding, end-to-end authentication is achieved. However, LRQ message authentication is performed only at the Cisco gatekeepers.

Related Features and Technologies

- Inter-Domain Gatekeeper Security Enhancement
- Cisco High-Performance Gatekeeper

Related Documents

- *Inter-Domain Gatekeeper Security Enhancement*
- *Cisco High-Performance Gatekeeper*
- *Cisco IOS Voice, Video, and Fax Configuration Guide*, Release 12.2
- *Cisco IOS Voice, Video, and Fax Command Reference*, Release 12.2
- Platform support for the Cisco 2600 series:

  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis2600/sw_conf/26_122/12211t/index.htm
- Platform support for the Cisco 3600 series:

  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/cis3600/sw_conf/36_122/12211/index.htm

Supported Platforms

- Cisco 2600 series
- Cisco 3660
- Cisco 7200 series
- Cisco MC3810

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

No new or modified standards are supported by this feature.

MIBs

No new or modified MIBs are supported by this feature.

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 perform the following tasks before configuring this feature in your network:

- Configure VoIP.
- Install Cisco IOS Release 12.2(11)T on your gatekeepers and gateways.
- Configure your gatekeepers.

Note To use this feature, you must configure the same passwords on adjacent gatekeepers. See the "Configuring Gatekeeper-to-Gatekeeper Authentication" section on page 9 for more information.

Configuration Tasks

See the following sections for configuration tasks for the Gatekeeper-to-Gatekeeper Authentication feature. Each task in the list is identified as either required or optional.

- Configuring the Gatekeeper Local and Remote Zones (required)
- Configuring the IZCT (optional)
- Configuring Gatekeeper-to-Gatekeeper Authentication (required)
- Verifying the Remote Zone and Security Features (optional)

Configuring the Gatekeeper Local and Remote Zones

To configure the local and remote zones of the gatekeeper, 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` *zone-name domain-name* [*ras-ip-address*] [*port-number*]	Defines the name or zone name of the gatekeeper. 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 gatekeeper name for each zone is a unique string that has a mnemonic value. The keywords or arguments are as follows: • *zone-name*—The name or zone name of the gatekeeper. • *domain-name*—Specifies the domain name served by this gatekeeper. • *ras-ip-address*—(Optional) 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. **Note** Setting this address for one local zone makes it the address used for all local zones. • *port-number*—(Optional) The RAS signaling port number for the local zone. Values range from 1 to 65535. If no port number is specified, the default is 1719.

	Command	Purpose
Step 3	`Router(config-gk)# zone remote` *zone-name domain-name ip-address* [*port-number*] [**cost** *cost-value*] [**priority** *priority-value*]	Defines the remote zone. The keywords and arguments are as follows: • *zone-name*—Name (ID) of the remote zone. • *domain-name*—Name (ID) of the domain the remote zone is serving. • *ip-address*—IP address for the remote gatekeeper. • *port number*—(Optional) RAS signaling port number for the remote zone. Values range from 1 to 65535. If this argument is not specified, the default is the well-known RAS port number 1719. • **cost—**(Optional) Sets the cost of the zone. • *cost-valu*e—(Optional) The cost value. The range is from 1 to 100. The default is 50. • **priority—**(Optional) Sets the priority of the zone. • *priority-value*—(Optional) The priority value. The range is from 1 to 100. The default is 50. When several remote zones are 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.
Step 4	`Router(config-gk)# no shutdown`	Activates the gatekeeper.

Configuring the IZCT

Although the IZCT is not required for use with the Gatekeeper-to-Gatekeeper Authentication feature, it is recommended. To configure the IZCT password, 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)# security izct password` *password*	Configures the IZCT password. The *password* argument must be from six to eight alphanumeric characters.

Configuring Gatekeeper-to-Gatekeeper Authentication

To configure gatekeeper-to-gatekeeper authentication, 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)# security password-group` *group-name* `lrq {receive` *password* `[encrypted] [effective` *hh:mm day month year*`] | send` *password* `[encrypted]}`	Defines the passwords used by remote gatekeeper zones and associates them with an ID. The keywords and arguments are as follows: • *group-name*—an ID given to a group of passwords. The group can contain inbound and outbound passwords. The group name can include up to 16 characters (any characters on the keyboard). • **lrq receive** *password*—A password that is used to validate any Location Request (LRQ) messages that are received from the specified remote zone. The password can be up to 16 characters (any characters on the keyboard) for cleartext format and 34 characters for encrypted format. • **encrypted**—(Optional). The password is in encrypted format. If the **encrypted** keyword is omitted, the password is defined as being in cleartext format. If the **encrypted** keyword is used, it is assumed that the password is already encrypted. The password will always be displayed in encrypted format. • **effective** *hh:mm day month year*—(Optional) The time and date that the current **lrq receive** *password* will expire. Old and new passwords are valid until the configured time value expires. After expiration, only the new password is valid. The agument values are as follows: – *hh*—The hour the current password will expire. The values are from 0 to 23. – *mm*—The month the current password will expire. The values are from 0 to 59. – *day*—The day the current password will expire. The values are from 1 to 31 and can be one or two digits.

Command	Purpose
	– *month*—The month the current password will expire. The value can be January to December and can be an abbreviation or a full name (for example, Jan or January). – *year*—The year the current password will expire. The value must be four numbers (for example, 2002) and in the range 1993 to 2035. **Note** After you have configured the **effective** keyword and the time associated with the keyword has expired (for example, a day later), the following syslog message will be displayed ("china" is the **password-group** name): `%GK-5-RX_LRQ_PASSWORD_UPDATED:LRQ receive password for security password-group 'china' has been updated.` • **lrq send** *password*—The password that will be contained in the CAT and sent in the outbound LRQ messages. The password can be up to 16 characters (any characters on the keyboard) for cleartext format and 34 characters for encrypted format. **Note** If multiple changes are made to the password groups, the latest update takes precedence.
Step 3 `Router(config-gk)# security zone {zone-name | *} password-group group-name`	Associates a remote zone gatekeeper with a specific password group. If a remote zone sends an LRQ message to the gatekeeper, the gatekeeper checks to see if there is a security password group configured for that remote zone name. If one exists, the gatekeeper gets the password information from the group name configured for that security zone. For example, if you used the command in Step 2 to create a password group named "china," you could use this command to associate one or more of your remote gatekeepers with that password group. The keywords and arguments are as follows: • *zone-name*—Identifies the remote zone gatekeeper. • *****—Using the wildcard (*****) means that remote zones that do not have a security zone configured will default to the security zone password group on the receiving gatekeeper and that the received LRQ message is authenticated using the wildcard-related passwords. Using the wildcard does not affect transmitted LRQ messages. • **password-group** *group-name*—Identifies the password group created using the **security password-group** command.

Verifying the Remote Zone and Security Features

To verify the remote zone and security features, use the **show running-config** command.

```
Router# show running-config

gatekeeper
 zone local tsunamiGK cisco 172.18.195.138
 zone remote laharGK cisco 172.18.195.139 1719
 zone prefix laharGK 987*
 security izct password 123456
 security password-group 1 lrq receive 0257550A5A57 encrypted
 security password-group 1 lrq send 144540595E56 encrypted
 security password-group 2 lrq receive 091F1D5A4A56 encrypted
 security password-group 2 lrq send 135143465F58 encrypted
 security zone larharGK password-group 1
 no shutdown
```

Note For security reasons, the passwords created using the **security password-group** command are encrypted when displayed in the **show running-config** output.

Configuration Examples

This section provides the following configuration examples:

- Originating Gatekeeper Configuration Example
- Border Gatekeeper Configuration Example
- Terminating Gatekeeper Configuration Example
- Gatekeeper Configuration Using the Wildcard Example

The following examples show configuration of the elements illustrated in Figure 1 on page 2.

Note The following examples do not reflect the actual display of the passwords as you would see them in an output. The actual displays show the passwords as being encrypted. The passwords are shown here in cleartext format for clarity purposes only.

Originating Gatekeeper Configuration Example

In this example, LRQ messages received from the border gatekeeper authenticate the LRQ message by using the password “ogk_123.” LRQ messages sent to the border gatekeeper contain the password “bgk_123” in the CAT.

```
gatekeeper
 zone remote bgk china 172.18.195.137 1719 foreign-domain
 security password-group china lrq send bgk_123
 security password-group china lrq receive ogk_123
 security zone bgk password-group china
```

Border Gatekeeper Configuration Example

In this example, LRQ messages received from the originating gatekeeper authenticate the LRQ message by using the password “bgk_123.” LRQ messages sent to the originating gatekeeper contain the password “ogk_123” in the CAT. LRQ messages received from the terminating gatekeeper authenticate the LRQ message by using the password “bgk_123.” LRQ messages sent to the terminating gatekeeper contain the password “tgk_123” in the CAT.

```
gatekeeper
 zone remote ogk usa 172.18.195.138 1719 foreign-domain
 zone remote tgk china 172.18.195.139 1719
 security password-group usa lrq send ogk_123
 security password-group usa lrq receive bgk_123
 security password-group china lrq send tgk_123
 security password-group china lrq receive bgk_123
 security zone ogk password-group usa
 security zone tgk password-group china
```

Terminating Gatekeeper Configuration Example

In this example, LRQ messages received from the border gatekeeper authenticate the LRQ message by using the password “tgk_123.” LRQ messages sent to the border gatekeeper contain the password “bgk_123” in the CAT.

```
gatekeeper
 zone remote bgk china 172.18.195.137 1719
 security password-group china lrq send bgk_123
 security password-group china lrq receive tgk_123
 security zone bgk password-group china
```

Gatekeeper Configuration Using the Wildcard Example

In this example, LRQ messages are received from the terminating gatekeeper, which does not have a password group configured. Therefore, the LRQ messages received are authenticated using the password group configured for the originating gatekeeper (in this example, “ogk_123”).

```
gatekeeper
 zone remote tgk china 172.18.195.137 1719 foreign-domain
 security password-group china lrq send tgk_123
 security password-group china lrq receive ogk_123
 security zone * password-group china
```

Command Reference

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

- **security password-group**
- **security zone**

security password-group

To define the passwords used by gatekeeper zones and associate them with an ID for gatekeeper-to-gatekeeper authentication, use the **security password-group** command in gatekeeper configuration mode. To disable passwords, use the **no** form of this command.

security password-group *group-name* **lrq** {**receive** *password* [**encrypted**] [**effective** *hh*:*mm day month year*] | **send** *password* [**encrypted**]}

no security password-group *group-name* **lrq** {**receive** *password* [**encrypted**] [**effective** *hh*:*mm day month year*] | **send** *password* [**encrypted**]}

Syntax Description

group-name	The *group-name* argument is an ID given to a group of passwords. The group can contain inbound and outbound passwords. The group name can include up to 16 characters (any characters on the keyboard).
lrq receive *password*	A password that is used to validate any Location Request (LRQ) messages received from the specified remote zone. The password can be up to 16 characters (any characters on the keyboard) for cleartext format. The cleartext password will be converted and displayed in encrypted format. The password can be up to 34 characters for passwords that are already encrypted. **Note** The **encrypted** keyword must follow encrypted passwords.
encrypted	(Optional) The password is in encrypted format. If the **encrypted** keyword is omitted, the password is defined as being in cleartext format. If the **encrypted** keyword is used, it is assumed that the password is already encrypted. The password will always be displayed in encrypted format.
effective *hh*:*mm day month year*	(Optional) The time and date that the current **lrq receive** *password* will expire. Old and new passwords are valid until the configured time value expires. After expiration, only the new password is valid. The argument values are as follows: • *hh*—The hour the current password will expire. The values are from 0 to 23. • *mm*—The month the current password will expire. The values are from 0 to 59. • *day*—The day the current password will expire. The values are from 1 to 31 and can be one or two digits. • *month*—The month the current password will expire. The value can be January to December and can be an abbreviation or a full name (for example, Jan or January). • *year*—The year the current password will expire. The value must be four numbers (for example, 2002) and in the range 1993 to 2035. **Note** After you have configured the **effective** keyword and the time associated with the keyword has expired (for example, a day later), the following syslog message will be displayed ("china" is the **password-group** name): `%GK-5-RX_LRQ_PASSWORD_UPDATED:LRQ receive password for security password-group 'china' has been updated.`

lrq send *password*	The password that will be contained in the Cisco Access Token (CAT) and sent in the outbound LRQ messages. The password can be up to 16 characters (any characters on the keyboard) for cleartext format. The cleartext password will be converted and displayed in encrypted format. The password can be up to 34 characters for passwords that are already encrypted. **Note** The **encrypted** keyword must follow encrypted passwords. **Note** If multiple changes are made to the password groups, the latest update takes precedence.

Defaults

No default behavior or values

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

This command associates passwords with a given password group.

Examples

The following example shows two password groups configured for a remote zone gatekeeper. In this example, the **security zone** command associates bgk with the password group "china." LRQ messages received from bgk are authenticated by using the incoming password in the "china" password group, and LRQ messages sent to bgk contain, in the CAT, the outgoing password in the "china" password group.

```
gatekeeper
 zone remote bgk china 172.18.195.137 1719 foreign-domain
 security password-group china lrq send bgk_123
 security password-group china lrq receive ogk_123
 security zone bgk password-group china
```

Note The previous example does not reflect the actual display of the password as you would see it in an output. The actual display would show the password as being encrypted. The passwords bgk_123 and ogk_123 are shown here in cleartext format for clarity purposes only.

The following example shows that the **effective** keyword and *hh***:***mm day month year* argument is being used to set an expiration timer for the inbound LRQ password:

```
gatekeeper
 zone remote bgk china 172.18.195.137 1719 foreign-domain
 security password-group china lrq send bgk_123
 security password-group china lrq receive ogk_123 effective 08:12 09 Dec  2002
 security zone bgk password-group china
```

Note The above example does not reflect the actual display of the password as you would see it in an output. The actual display would show the password as being encrypted. The passwords bgk_123 and ogk_123 are shown here in cleartext format for clarity purposes only.

Related Commands

Command	Description
security izct password	Enables generation of the IZCT password.
security zone	Allows gatekeepers in a zone to use the same passwords for LRQ authentication.

security zone

To configure gatekeeper security zones for gatekeeper-to-gatekeeper authentication, use the **security zone** command in gatekeeper configuration mode. To disable security zones, use the **no** form of this command.

security zone {*zone-name* | *****} **password-group** *group-name*

no security zone

zone-name | *****	Associates a remote zone gatekeeper with a specific password group that is configured using the **security password-group** command. If a remote zone sends an LRQ message to the gatekeeper, the gatekeeper checks to see whether there is a security password group configured for that remote zone name. If one exists, the gatekeeper gets the password information from the group name configured for that security zone. The *zone-name* argument identifies the remote zone gatekeeper. The wildcard (*****) means that remote zones that do not have a security zone configured will default to the security zone password group on the receiving gatekeeper and that the received LRQ message is authenticated using the wildcard-related passwords. Using the wildcard does not affect transmitted LRQ messages.
password-group *group-name*	Identifies the password group created using the **security password-group** command.

Defaults

No default behavior or values

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

Passwords configured with this command are used to create a Cisco Access Token (CAT).

Examples

The following example shows two password groups configured for a remote zone border gatekeeper. In this example, the **security zone** command associates the border gatekeeper with the password group "china." LRQ messages received from the border gatekeeper are authenticated by using the incoming password in the "china" password group, and LRQ messages sent to the border gatekeeper, contain in the CAT, the outgoing password in the "china" password group.

```
gatekeeper
 one remote bgk china 172.18.195.137 1719 foreign-domain
 security password-group china lrq send bgk_123
 security password-group china lrq receive ogk_123
 security zone bgk password-group china
```

Note The above example does not reflect the actual display of the password as you would see it in an output. The actual display would show the password as being encrypted. The passwords bgk_123 and tgk_123 are shown here in cleartext format for clarity purposes only.

In the following example, LRQ messages are received from the terminating gatekeeper, which does not have a password group configured. Therefore, the LRQ messages received are authenticated using the password group configured for the originating gatekeeper (in this example, "ogk_123").

```
gatekeeper
 zone remote tgk china 172.18.195.137 1719 foreign-domain
 security password-group china lrq send tgk_123
 security password-group china lrq receive ogk_123
 security zone * password-group china
```

Note The above example does not reflect the actual display of the password as you would see it in an output. The actual display would show the password as being encrypted. The passwords tgk_123 and ogk_123 are shown here in cleartext format for clarity purposes only.

Related Commands

Command	Description
security izct password	Enables generation of the IZCT password.
security password-group	Configures passwords for gatekeeper zones.