



Gatekeeper Endpoint Control Enhancements

Feature History

Release	Modification
12.2(11)T	This feature was introduced in Cisco IOS Release 12.2(11)T with support for the Cisco 3660 and Cisco MC3810 platforms.

This document describes the Gatekeeper Endpoint Control Enhancements feature in Cisco IOS Release 12.2(11)T and includes the following sections:

- [Feature Overview, page 1](#)
- [Supported Platforms, page 2](#)
- [Supported Standards, MIBs, and RFCs, page 3](#)
- [Prerequisites, page 3](#)
- [Configuration Tasks, page 3](#)
- [Configuration Examples, page 8](#)
- [Command Reference, page 10](#)

Feature Overview

The Gatekeeper Endpoint Control Enhancements feature provides enhancements to the Cisco IOS gatekeeper, including the following:

- Forced unregistration of an endpoint using a command-line interface (CLI) command.
- Forced unregistration of an endpoint using a Gatekeeper Transaction Message Protocol (GKTMP) command from an application server.
- Faster reconnection to a GKTMP server when its TCP connection fails. A new CLI command is provided to enable this feature.
- Rejection of new registrations or calls when a GKTMP server is down or unreachable. A new CLI command is provided to enable this feature.

This document describes the Cisco IOS gatekeeper commands only. The GKTMP enhancements are described in a separate document listed in the [“Related Documents” section on page 2](#).

Benefits

This feature enables finer-grained control of gatekeeper registrations, and enables more capable and robust back-end server applications.

Related Features and Technologies

- Cisco high-performance gatekeeper
- Gatekeeper Transaction Message Protocol Interface Resiliency Enhancement

Related Documents

- [Cisco High-Performance Gatekeeper](#)
- [Gatekeeper Transaction Message Protocol Interface Resiliency Enhancement](#)
- [Cisco IOS Voice, Video, and Fax Configuration Guide](#), Release 12.2
- [Cisco IOS Voice, Video, and Fax Command Reference](#), Release 12.2
- [Cisco Gatekeeper External Interface Reference](#), Version 3.1

Supported Platforms

Table 1 Cisco IOS Release and Platform Support for this Feature

Platform	12.2(11)T
Cisco 2600 series	X
Cisco 3600 series	X
Cisco MC3810	X
Cisco 7200 series	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 website on Cisco.com at the following URL:

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

RFCs

No new or modified RFCs are supported by this feature.

Prerequisites

Before using the Gatekeeper Endpoint Control Enhancements feature, you must perform the following tasks:

- Configure your IP network.
- Install Cisco IOS Release 12.2(11)T on the gateways and gatekeepers in your network.
- Configure gateways and gatekeepers in your network.

For more information on performing these tasks, consult the documentation listed in the “[Related Documents](#)” section on page 2.

Configuration Tasks

See the following sections for configuration tasks for the Gatekeeper Endpoint Control Enhancements feature. Each task in the list is identified as either required or optional.

- [Unregistering an Endpoint](#) (Optional)
- [Setting the Retry Timer for Failed Server Connections](#) (Optional)

- [Configuring Registration or Call Rejection](#) (Optional)
- [Verifying an Unregistered Endpoint](#) (Optional)
- [Verifying the Retry Timer](#) (Optional)
- [Verifying Registration Rejection](#) (Optional)
- [Verifying Call Rejection](#) (Optional)

Unregistering an Endpoint

Command	Purpose
Step 1 Router# clear h323 gatekeeper endpoint { alias { e164 <i>name</i> h323id <i>name</i> } all id <i>number</i> ipaddr <i>address</i> [<i>port</i>]}	<p>Forces the gatekeeper to send an unregistration request (URQ) message to the specified endpoint or all endpoints and removes the endpoint from the gatekeeper registration database.</p> <p>Note The endpoint that was unregistered using this command can come back if it sends the registration request (RRQ) back to the gatekeeper after the unregistration.</p> <p>The following keywords and arguments are used to identify the endpoint:</p> <ul style="list-style-type: none"> • alias e164 name: The E.164 alphanumeric address that is specified in the local alias table. • alias h323id name: The H.323 ID name that is specified in the local alias table and is an alternate way to reach an endpoint. • all: Clears all endpoints. • id number: The ID of the endpoint. • ipaddr address [port]: The call signaling address and port (optional) of the endpoint. If <i>port</i> is not specified, the default is 1720. <p>Note For gatekeeper cluster configurations, this command must be entered on the gatekeeper where the endpoint is registered. Use the show gatekeeper endpoints command to locate the endpoint in a gatekeeper cluster.</p>

Setting the Retry Timer for Failed Server Connections

	Command	Purpose
Step 1	Router(config)# gatekeeper	Enters gatekeeper configuration mode.
Step 2	Router(config-gk)# timer server retry <i>seconds</i>	<p>Sets the gatekeeper's retry timer for failed GKTMP server connections. After the gatekeeper detects that its GKTMP server TCP connection has failed, the gatekeeper retries the server based on the setting of this timer, and keep retrying until the connection is established.</p> <p>The <i>seconds</i> argument configures how many seconds the gatekeeper should wait before retrying the GKTMP server. Valid values are 1 through 300; the default value is 30.</p> <p>Note This timer applies only to deployments where static triggers are used between the gatekeeper and the GKTMP server. If dynamic triggers are used, the server must determine and implement a retry mechanism if the TCP connection to the gatekeeper fails.</p>

Configuring Registration or Call Rejection

	Command	Purpose
Step 1	Router(config)# gatekeeper	Enters gatekeeper configuration mode.
Step 2	Router(config-gk)# server absent reject { rrq arq }	<p>Configures the gatekeeper to reject new registrations or calls when it is unable to reach the GKTMP server because the TCP connection between the gatekeeper and GKTMP server is down. If multiple GKTMP servers are configured, the gatekeeper tries all of them and rejects registrations or calls only if none of the servers respond.</p> <p>The rrq keyword is used to reject registrations by RRQ messages. The arq keyword is used to reject calls by admission request (ARQ) messages.</p> <p>You can also use this feature for security or service denial if a connection with the server is required to complete a registration. By default, this feature is not enabled; the gatekeeper does not reject new registrations or calls.</p> <p>Note This command assumes that RRQ and ARQ triggers are used between the gatekeeper and GKTMP server.</p>

Verifying an Unregistered Endpoint

- Step 1** To verify that an endpoint has been unregistered, make sure that you did not receive an error message after entering the command.

Step 2 Enter the **show gatekeeper endpoints** command to view all endpoints registered to the gatekeeper:

```
Router# show gatekeeper endpoints
```

```
GATEKEEPER ENDPOINT REGISTRATION
```

```
-----  
CallSignalAddr  Port  RASSignalAddr  Port  Zone Name          Type  
  
Flags  
-----  
  
-----  
1.1.1.1          1720  1.1.1.1        1719  gk-e4-2            VOIP-GW S  
      H323-ID: test (static)  
Total number of active registrations = 1
```

Step 3 Verify that the unregistered endpoint is not displayed in the list of endpoints.

Verifying the Retry Timer

- Step 1** To verify the retry timer for failed server connections, use the **show gatekeeper servers** command:

```
Router# show gatekeeper servers

GATEKEEPER SERVERS STATUS
=====

Gatekeeper Server listening port:0
Gatekeeper Server response timeout value:30 (100ms)
Gatekeeper Server connection retry timer value:30 (sec)
Gatekeeper GKTMP version:4.1
```

Verifying Registration Rejection

- Step 1** To verify that the gatekeeper is rejecting new registrations when unable to reach the GKTMP server, use the **show running configuration** command:

```
Router# show running configuration
.
.
.
h323id tet
 gw-type-prefix 1#* default-technology
 gw-type-prefix 9#* gw ipaddr 1.1.1.1 1720
 no shutdown
 server absent reject rrq
.
.
.
```

Verifying Call Rejection

- Step 1** To verify that the gatekeeper is rejecting new calls when unable to reach the GKTMP server, use the **show running configuration** command:

```
Router# show running configuration
.
.
.
h323id tet
 gw-type-prefix 1#* default-technology
 gw-type-prefix 9#* gw ipaddr 1.1.1.1 1720
 no shutdown
 server absent reject arq
.
.
.
```

Configuration Examples

This section provides the following configuration examples:

- [Unregistering an Endpoint Example](#)
- [Retry Timer Example](#)
- [Registration Rejection Example](#)
- [Call Rejection Example](#)

Unregistering an Endpoint Example

The following example shows that all endpoints have been unregistered:

```

GATEKEEPER ENDPOINT REGISTRATION
=====
CallSignalAddr  Port  RASignalAddr  Port  Zone Name          Type  Flags
-----
Total number of active registrations = 0

```

Retry Timer Example

The following example shows that the retry timer has been set to 45 seconds:

```

.
.
.
h323id tet
gw-type-prefix 1#* default-technology
gw-type-prefix 9#* gw ipaddr 1.1.1.1 1720
timer server retry 45
no shutdown
.
.
.

```

Registration Rejection Example

The following example shows that the gatekeeper rejects registrations when it cannot connect to the GKTMP server:

```

.
.
.
h323id tet
gw-type-prefix 1#* default-technology
gw-type-prefix 9#* gw ipaddr 1.1.1.1 1720
no shutdown
server absent reject rrq
.
.
.

```

Call Rejection Example

The following example shows that the gatekeeper rejects calls when it cannot connect to the GKTMP server:

```
.  
. .  
h323id tet  
  gw-type-prefix 1#* default-technology  
  gw-type-prefix 9#* gw ipaddr 1.1.1.1 1720  
  no shutdown  
  server absent reject arq  
. .  
.
```

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.

- [clear h323 gatekeeper endpoint](#)
- [server absent reject](#)
- [timer server retry](#)

clear h323 gatekeeper endpoint

To unregister an endpoint, use the **clear h323 gatekeeper endpoint** command in privileged EXEC mode.

```
clear h323 gatekeeper endpoint {alias e164 digits | alias h323id name | all | id number | ipaddr
address [port]}
```

Syntax Description

alias e164 <i>digits</i>	The E.164 alphanumeric address that is specified in the local alias table.
alias h323id <i>name</i>	The H.323 ID name that is specified in the local alias table and is an alternate way to reach an endpoint.
all	All endpoints.
id <i>number</i>	ID of the endpoint.
ipaddr <i>address</i> [<i>port</i>]	Call signaling address and port (optional) of the endpoint. If <i>port</i> is not specified, the default is 1720.

Defaults

For **ipaddr** *address* [*port*], if *port* is not specified, the default is 1720.

Command Modes

EXEC

Command History

Release	Modification
12.2(11)T	This command introduced in Cisco IOS Release 12.2(11)T with support for the Cisco 3660 and Cisco MC3810 platforms.

Usage Guidelines

Using this command forces the gatekeeper to send an unregistration request (URQ) message to the specified endpoint or all endpoints and removes the endpoint from the gatekeeper registration database.

For gatekeeper cluster configurations, this command must be entered on the gatekeeper where the endpoint is registered. Use the **show gatekeeper endpoints** command to locate the endpoint in a gatekeeper cluster.



Note

The endpoint that was unregistered using this command can come back if it sends the registration request (RRQ) back to the gatekeeper after the unregistration.

Examples

The following example shows how to unregister all endpoints:

```
GK# clear h323 gatekeeper endpoint all
GK# show gatekeeper endpoints
```

```

GATEKEEPER ENDPOINT REGISTRATION
=====
CallSignalAddr  Port  RASSignalAddr  Port  Zone Name          Type  Flags
-----
Total number of active registrations = 0
```

■ clear h323 gatekeeper endpoint

server absent reject

To configure the gatekeeper to reject new registrations or calls when the connection to the Gatekeeper Transaction Message Protocol (GKTMP) server is down, use the **server absent reject** command in gatekeeper configuration mode. To disable, use the **no** form of this command.

```
server absent reject {arq | rrq}
```

```
no server absent reject {arq | rrq}
```

Syntax Description

arq	Reject call admission request (ARQ) messages.
rrq	Reject registration request (RRQ) messages.

Defaults

By default, registrations and calls are not rejected.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.2(11)T	This command introduced in Cisco IOS Release 12.2(11)T with support for the Cisco 3660 and Cisco MC3810 platforms.

Usage Guidelines

Configures the gatekeeper to reject new registrations or calls when it is unable to reach the GKTMP server because the TCP connection between the gatekeeper and GKTMP server is down. If multiple GKTMP servers are configured, the gatekeeper tries all of them and rejects registrations or calls only if none of the servers respond. You can also use this feature for security or service denial if a connection with the server is required to complete a registration.



Note

This command assumes that RRQ and ARQ triggers are used between the gatekeeper and GKTMP server.

Examples

The following example shows that the gatekeeper rejects registrations when it cannot connect to the GKTMP server:

```
Router# show gatekeeper configuration
.
.
.
h323id tet
gw-type-prefix 1#* default-technology
gw-type-prefix 9#* gw ipaddr 1.1.1.1 1720
no shutdown
server absent reject rrq
.
.
```

■ server absent reject

timer server retry

To set the gatekeeper's retry timer for failed Gatekeeper Transaction Message Protocol (GKTMP) connections, use the **timer server retry** command in gatekeeper configuration mode. To reset the timer to its default, use the **no** form of this command or the **default server timer retry** command.

server timer retry *seconds*

no server timer retry

default server timer retry

Syntax Description	<i>seconds</i>	How long the gatekeeper should wait before retrying the GKTMP server. Valid values are 1 through 300; the default value is 30.
---------------------------	----------------	--

Defaults The default timer value is 30 seconds.

Command Modes Gatekeeper configuration

Command History	Release	Modification
	12.2(11)T	This command introduced in Cisco IOS Release 12.2(11)T with support for the Cisco 3660 and Cisco MC3810 platforms.

Usage Guidelines This command sets the gatekeeper's retry timer for failed GKTMP server connections. After the gatekeeper detects that its GKTMP server TCP connection has failed, the gatekeeper will retry the server based on the setting of this timer, and keep retrying until the connection is established.

This timer only applies to deployments where static triggers are used between the gatekeeper and the GKTMP server. If dynamic triggers are used, the server must determine and implement a retry mechanism if the TCP connection to the gatekeeper fails.

Examples The following example shows that the retry timer has been set to 45 seconds:

```
Router# show gatekeeper configuration
.
.
.
h323id tet
 gw-type-prefix 1#* default-technology
 gw-type-prefix 9#* gw ipaddr 1.1.1.1 1720
 timer server retry 45
 no shutdown
.
.
.
```

■ timer server retry

Related Commands

Command	Description
timer server timeout	Specifies the timeout value for a response from a back-end Gatekeeper Transaction Message Protocol (GKTMP) server.
