Cisco 1000 Series Connected Grid Routers System Management Software Configuration Guide

March 2014

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Text Part Number: OL-25633-03

CONTENTS

Configuring NTP

This chapter describes how to configure the Network Time Protocol (NTP) on the Cisco 1000 Series Connected Grid Routers (hereafter referred to as the Cisco CG-OS router).

This chapter includes the following sections:

Information About NTP

This section includes the following topics:

NTP Overview

The Network Time Protocol (NTP) synchronizes the time of day among a set of distributed time servers and clients so that you can correlate events when you receive system logs and other time-specific events from multiple network devices. With the User Datagram Protocol (UDP) as its transport protocol, NTP uses standard Universal Time Coordinated (UTC).

An NTP server usually receives its time from a source such as a radio clock or an atomic clock attached to a time server and then distributes this time across the network. NTP is extremely efficient; no more than one packet per minute is necessary to synchronize two machines to within a millisecond of each other.

NTP uses a stratum to describe the distance between a network device and an authoritative time source:

- A stratum 1 time server is directly attached to an authoritative time source (such as an atomic clock).
- A stratum 2 NTP server receives its time through NTP from a stratum 1 NTP server.

Before synchronizing, NTP compares the time reported by several network devices and does not synchronize with one that is significantly different, even if it is a stratum 1.

Because the Cisco CG-OS software cannot connect to a radio or atomic clock and act as a stratum 1 server, Cisco recommends that you use the public NTP servers available on the Internet.

When the network is isolated from the Internet, the Cisco CG-OS software allows you to configure the time as though it were synchronized through NTP, even though it was not.

When the Cisco CG-OS router loses connectivity with the NTP server, the Cisco CG-OS router uses the latest synchronized time it received from the NTP server.

To use the local clock for the Cisco CG-OS router, you will need to delete the NTP client configuration using the **no** form of the commands (see Configuring an NTP Client, page 1-4).

Stateless Restarts

The Cisco CG-OS router supports stateless restarts for NTP. After a system reboot, the Cisco CG-OS software applies the running configuration to the Cisco CG-OS router.

Prerequisites for NTP

Router must have connectivity to at least one server that is running NTP.

NTP must be configured in the default VDC of the Cisco CG-OS router. No other VDCs are supported on the Cisco CG-OS router.

Guidelines and Limitations

The Cisco CG-OS router supports an NTP client and receives its clock source from an NTP server.

When you have only one NTP server, configure all the devices as clients to that NTP server.

You can configure up to 64 NTP servers.

Default Settings

Table 1-1 lists the default settings for NTP parameters.

Table 1-1 Default NTP Parameters

Parameters	Default
NTP protocol	Enabled
NTP authentication	Disabled

Table 1-1 Default NTP Parameters (continued)

Parameters	Default
NTP access	Enabled
NTP logging	Disabled

Configuring NTP

This section includes the following topics:

Enabling or Disabling the NTP Protocol

You can enable or disable NTP on the Cisco CG-OS router. NTP is enabled by default.

BEFORE YOU BEGIN

Make sure that you are in the default VDC. The Cisco CG-OS router does not support any VDCs beyond the default.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**[no] ntp enable**	Enables or disables the NTP protocol on the Cisco CG-OS router. NTP is enabled by default.
Step 3	**show ntp status**	(Optional) Displays the status of the NTP application.
Step 4	**copy running-config startup-config**	(Optional) Saves the change by copying the running configuration to the startup configuration

EXAMPLE

This example shows how to disable NTP on the Cisco CG-OS router.

```
router# configure terminal
router(config)# no ntp enable
router(config)# copy running-config startup-config
```

Configuring an NTP Client

This section addresses how to configure the Cisco CG-OS router to serve as an NTP client.

BEFORE YOU BEGIN

Identify the IP address or DNS name for each NTP server that you want to define as a possible clocking reference for the Cisco CG-OS router.

When defining multiple NTP servers, determine which server will serve as the primary (preferred) NTP server.

Ensure that you are in the default VDC. The Cisco CG-OS router does not support any VDCs beyond the default.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**[no] ntp server** {*ip-address* | *dns-name*} [**key** *key-id*] [**maxpoll** *max-poll*] [**minpoll** *min-poll*] [**prefer**]	Defines the NTP server that provides the clocking source for the Cisco CG-OS router. You can specify multiple server associations. **key–**Configures a key to use while communicating with the NTP server. The range for the *key-id* argument is from 1 to 65535. **Note**: Only configure the key when you want the NTP server to provide authentication for the Cisco CG-OS router. **maxpoll, minpoll**–Configures the maximum and minimum intervals in which to poll a server. The range for the *max-poll* and *min-poll* arguments is from 4 to 17 seconds, and the default values are 6 and 4, respectively. **prefer**–Assigns the NTP server as the preferred NTP server for the Cisco CG-OS router. **Note**: When you configure a key for use in communicating with the NTP server, be sure that the key exists as a trusted key on the Cisco CG-OS router. For more information on trusted keys, see Configuring NTP Authentication, page 1-5.
Step 3	**[no] ntp source-interface [ethernet | cellular | wimax]** *slot/port*	Configures the interface that connects to the NTP server.
Step 4	**[no] ntp source** *ip-address*	Configures the source IP address for the source-interface that will receive all NTP packets. The *ip-address* must be in IPv4 format.

	Command	Purpose
Step 5	**exit**	Exits to the global configuration mode.
Step 6	**show ntp statistics** {**io** | **local** | **memory** | **peer** {**ipaddr** *ipv4-addr* | **name** *peer-name*}}	(Optional) Displays the configured NTP servers. Enter the NTP server name for the *peer-name* variable.
Step 7	**copy running-config startup-config**	(Optional) Saves the change by copying the running configuration to the startup configuration.

EXAMPLE

This example shows how to configure an IPv4 client and assign the NTP server as the preferred clocking reference; and, define the cellular interface as the path to the NTP server.

```
router# configure terminal
router(config)# ntp server 192.0.2.12 prefer
router(config)# ntp server 192.0.2.10 key 42
router(config)# ntp source-interface cellular 3/1
router(config-if)# exit
router# copy running-config startup-config
```

Configuring NTP Authentication

You can configure the Cisco CG-OS router to authenticate the time sources to which the local clock synchronizes. When you enable NTP authentication, the Cisco CG-OS router synchronizes to a time source only if the source carries one of the authentication keys specified by the **ntp trusted-key** command. The Cisco CG-OS router drops any packets that fail the authentication check and prevents them from updating the local clock.

By default, NTP authentication is disabled on the Cisco CG-OS router.

BEFORE YOU BEGIN

Configure the NTP server(s) with the authentication keys configured on the Cisco CG-OS router in this procedure.

Ensure that you are in the default VDC. The Cisco CG-OS router does not support any VDCs beyond the default.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**ntp authenticate**	Enables the NTP authentication feature. By default, NTP authentication is disabled on the Cisco CG-OS router.

	Command	Purpose
Step 3	**ntp authentication-key number md5** *md5-string*	Defines the authentication key. This key must match the value on the NTP server along with the **ntp trusted-key** *number* value of the Cisco CG-OS router in Step 4 below. The Cisco CG-OS router does not synchronize to the NTP server clocking source unless the **ntp authentication-key** and the **ntp trusted-key** values on the server and the Cisco CG-OS router match. The range for authentication keys is from 1 to 65535. For the MD5 string, you can enter up to eight alphanumeric characters.
Step 4	**ntp trusted-key** *number*	Specifies one or more keys (defined in Step 3) that a time source (NTP server) must provide in its NTP packets in order for the Cisco CG-OS router to synchronize to it. The range for trusted keys is from 1 to 65535. This command provides protection against accidentally synchronizing the Cisco CG-OS router to a time source (NTP server) that is not trusted.
Step 5	**show ntp authentication-keys**	(Optional) Displays the configured NTP authentication keys.
Step 6	**show ntp trusted-keys**	(Optional) Displays the configured NTP trusted keys.
Step 7	**show ntp authentication-status**	(Optional) Displays the status of NTP authentication.
Step 8	**copy running-config startup-config**	(Optional) Saves the change by copying the running configuration to the startup configuration.

EXAMPLE

This example shows how to configure the Cisco CG-OS router to synchronize only to NTP servers that provide authentication key 42 and authentication key 35 in their NTP packets.

```
router# configure terminal
router(config)# ntp authentication-key 42 md5 aNiceKey
router(config)# ntp trusted-key 42
router(config)# ntp authentication-key 35 md5 aBetterKey
router(config)# ntp trusted-key 35
router(config)# ntp authenticate
router(config)# copy running-config startup-config
router(config)#
```

Configuring NTP Access Restrictions

You can control access to NTP services by using access groups. Specifically, you can specify the types of requests that the Cisco CG-OS router allows and the servers from which it accepts responses.

When you do not configure any access groups, NTP access is granted to all devices. When you configure any access groups, NTP access is granted only to the remote device whose source IP address passes the access list criteria.

BEFORE YOU BEGIN

Make sure that you are in the default VDC. The Cisco CG-OS router does not support any VDCs beyond the default.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**ntp access-group peer** *access-list-name*	Creates an access group to control NTP access and applies a basic IP access list. The **peer** keyword allows time requests and NTP control queries and allows the Cisco CG-OS router to synchronize only to a remote device whose IP address passes the access list criteria. The **no** form of this command removes the access group.
Step 3	**show ntp access-groups**	(Optional) Displays the NTP access group configuration.
Step 4	**copy running-config startup-config**	(Optional) Saves the change by copying the running configuration to the startup configuration.

EXAMPLE

This example shows how to configure the Cisco CG-OS router to allow it to synchronize to a NTP server from access group, accesslist1.

```
router# configure terminal
router(config)# ntp access-group peer accesslist1
router(config)# copy running-config startup-config
router(config)#
```

Configuring NTP Logging

You can configure the Cisco CG-OS router to generate significant NTP events to the system log on the Cisco CG-OS router. NTP logging is disabled by default.

BEFORE YOU BEGIN

Make sure that you are in the default VDC. The Cisco CG-OS router does not support any VDCs beyond the default.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**ntp logging**	Enables logging of significant NTP events to the system log on the Cisco CG-OS router. By default, NTP logging is disabled on the Cisco CG-OS router.
Step 3	**show ntp logging-status**	(Optional) Displays the NTP logging configuration status.
Step 4	**copy running-config startup-config**	(Optional) Saves the change by copying the running configuration to the startup configuration.

EXAMPLE

This example shows how to enable NTP logging in order to log significant NTP events to the system log on the Cisco CG-OS router.

```
router# configure terminal
router(config)# ntp logging
router(config)# copy running-config startup-config
```

Discarding NTP Configuration Changes

After making the configuration changes, you can choose to discard the changes instead of committing them. When you discard the changes, the Cisco CG-OS software removes the pending (starting configuration) database changes.

BEFORE YOU BEGIN

Make sure that you are in the default VDC. The Cisco CG-OS router does not support any VDCs beyond the default.

DETAILED STEPS

To discard NTP configuration changes, enter the following command in global configuration mode.

Command	Purpose
ntp abort	Discards the NTP configuration changes in the pending database. Enter this command on the Cisco CG-OS router in which you started the NTP configuration.

Verifying Configuration

To display the NTP configuration, enter any or all of the following commands.

Command	Purpose
show ntp access-groups	Displays the NTP access group configuration.
show ntp authentication-keys	Displays the configured NTP authentication keys.
show ntp authentication-status	Displays the status of NTP authentication.
show ntp internal	Displays internal NTP information.
show ntp logging-status	Displays the NTP logging status.
show ntp peer-status	Displays the status for all NTP servers.
show ntp peers	Displays all the NTP servers.
show ntp source	Displays the configured NTP source IP address.
show ntp source-interface	Displays the configured NTP source interface.
show ntp statistics {**io** | **local** | **memory** | **peer** {**ipaddr** *ipv4-addr* | **name** *peer-name*}}	Displays the NTP statistics. Enter the NTP server name for the *peer-name* variable.
show ntp trusted-keys	Displays the configured NTP trusted keys.
show running-config ntp	Displays date and timestamp of last running configuration update.

Enter the **clear ntp session** command to clear the NTP sessions.

Enter the **clear ntp statistics** command to clear the NTP statistics.

Configuration Example

This example shows how to configure an NTP client, enable NTP authentication, enable NTP logging, and then save the configuration in the startup configuration file so that it is saved across reboots and restarts.

```
router# configure terminal
router(config)# ntp server 192.0.2.12 prefer
router(config)# ntp server 192.0.2.10 key 42
router(config)# ntp source-interface cellular 3/1
router(config-if)# exit
router(config)# ntp authenticate
router(config)# ntp authentication-key 42 md5 aNiceKey
router(config)# ntp trusted-key 42
router(config)# ntp logging
router(config)# copy running-config startup-config
```

Feature History

Table 1-2

Feature Name	Release	Feature Information
Network Time Protocol	Cisco CG-OS Release CG1(1)	Initial support of the feature on the CGR 1000 Series Routers.

Configuring System Message Logging

This chapter describes how to configure system message logging on the Cisco 1000 Series Connected Grid Routers (hereafter referred to as Cisco CG-OS router).

This chapter includes the following sections:

Information About System Message Logging

System message logging allows you to configure the destination device of the system messages and to filter system messages by severity level. System messages can be logged to terminal sessions, a log file, and to syslog servers on remote systems. System message logging is based on RFC5424.

- By default, the Cisco CG-OS router outputs messages to terminal sessions. For information about configuring logging to terminal sessions, see Configuring System Message Logging to Terminal Sessions, page 2-3.
- By default, the Cisco CG-OS router logs system messages to a log file. For information about configuring logging to a file, see Logging System Messages to a File, page 2-4.

Table 2-1 describes the severity levels used in system messages. When you configure the severity level, the system outputs messages at that level and lower.

For example, when security level 4 is configured on the Cisco CG-OS router, the router logs all messages for security levels 1, 2, 3, and 4.

Table 2-1 System Message Severity Levels

Level	Description
0 – emergency	System unusable
1 – alert	Immediate action needed

Table 2-1 System Message Severity Levels (continued)

Level	Description
2 – critical	Critical condition
3 – error	Error condition
4 – warning	Warning condition
5 – notification	Normal but significant condition
6 – informational	Informational message only
7 – debugging	Appears during debugging only

The Cisco CG-OS router logs the most recent 100 messages of severity 0, 1, or 2 to the NVRAM log. You cannot configure logging to the NVRAM.

You can configure which system messages to log based on the facility that generated the message and its severity level. For information about configuring the severity level by module and facility, see Configuring Parameters for Module and Facility Messages Logs, page 2-5.

syslog Servers

The syslog servers run on remote systems that log system messages based on the syslog protocol. You can configure up to eight IPv4 or IPv6 syslog servers. For information about configuring syslog servers, see Configuring syslog Servers, page 2-7.

Note When the Cisco CG-OS router first initializes, the Cisco CG-OS software sends messages to syslog servers only after the network initializes.

Prerequisites

Identify the local or remote device that you want on which you want to log the system messages.

Identify what severity level filtering of system messages, if any, you want to configure on the Cisco CG-OS router.

Guidelines and Limitations

System messages are logged to the console and the logfile by default.

Default Settings

Table 2-2 lists the default settings for system message logging parameters.

Table 2-2 Default System Message Logging Parameters

Parameters	Default
Console logging	Enabled at severity level 2
Monitor logging	Enabled at severity level 5
Log file logging	Enabled to log messages at severity level 5
Module logging	Enabled at severity level 5
Facility logging	Enabled
Time-stamp units	Seconds
syslog server logging	Disabled

Configuring System Message Logging

This section includes the following topics:

Configuring System Message Logging to Terminal Sessions

You can configure the Cisco CG-OS router to log messages by their severity level to console, Telnet, and SSHv2 sessions.

By default, logging is enabled for terminal sessions.

Tip The current critical (default) logging level is maintained if the console baud speed is 9600 baud (default). All attempts to change the console logging level generate an error message. To increase the logging level (above critical), you must change the console baud speed to 38400 baud.

BEFORE YOU BEGIN

No prerequisites.

DETAILED STEPS

	Command	Purpose
Step 1	**terminal monitor**	Enables the Cisco CG-OS router to log messages to the console.
Step 2	**configure terminal**	Enters global configuration mode.

	Command	Purpose
Step 3	**logging console** [*severity-level*]	Configures the Cisco CG-OS router to log messages to the console session based on the defined severity level as well as those security levels with higher numbers. For example, when security level 4 is configured on the Cisco CG-OS router, the router logs all messages for security levels 1, 2, 3, and 4. Severity levels range from 1 to 7 (see Table 2-1). Default severity level setting is 2.
	no logging console [*severity-level*]	Disables the ability of the Cisco CG-OS router to log messages to the console.
Step 4	**show logging console**	(Optional) Displays the console logging configuration.
Step 5	**logging monitor** [*severity-level*]	Enables the Cisco CG-OS router to log messages to the monitor based on the specified severity level and higher. For example, when security level 4 is configured on the Cisco CG-OS router, the router logs all messages for security levels 1, 2, 3, and 4. The configuration applies to Telnet and SSHv2 sessions. Severity level settings range from 0 to 7 (see Table 2-1). Default severity level setting is 2.
	no logging monitor [*severity-level*]	Disables logging messages to Telnet and SSHv2 sessions.
Step 6	**show logging monitor**	(Optional) Displays the monitor logging configuration.
Step 7	**copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

EXAMPLE

This example shows how to log messages by their severity level to a console and monitor (Telnet and SSHv2).

```
router# terminal monitor
router# configure terminal
router(config)# logging console 3
router(config)# logging monitor 3
router(config)# copy running-config startup-config
```

Logging System Messages to a File

You can configure the Cisco CG-OS router to log system messages to a file. By default, system messages are logged to the file log: messages.

For information about displaying and clearing log files, see Displaying and Clearing Log Files, page 2-9.

BEFORE YOU BEGIN

No prerequisites.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**logging logfile** *logfile-name severity-level* [**size** *bytes*]	Configures the name of the log file that stores system messages and the minimum severity level to log. Severity levels are listed in Table 2-1. (Optional) You can also specify a maximum file size. Severity levels are listed in Table 2-1. The file size is from 4096 to 10485760 bytes. The default severity level is 5 and the file size is 10485760.
	no logging logfile [*logfile-name severity-level* [**size** *bytes*]]	Disables logging to the log file.
Step 3	**logging event** {**link-status** | **trunk-status**} {**enable** | **default**}	Logs interface events. **link-status**—Logs all UP/DOWN and CHANGE messages. **enable**—Enables logging on the interface. **default**—Enables the default logging configuration on interfaces that are not implicitly configured (see Table 2-2).
Step 4	**show logging info**	(Optional) Displays the logging configuration.
Step 5	**copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

EXAMPLE

This example shows how to log system messages to a file.

```
router# configure terminal
router(config)# logging logfile my_log 6
router(config)# logging event link-status default
router(config)# copy running-config startup-config
```

Configuring Parameters for Module and Facility Messages Logs

You can configure the severity level and time-stamp units of messages logged by module and facility.

Note All module commands refer to configuration of interface (Ethernet, cellular, WiMax) logging. In some cases, the Cisco CG-OS software might refer to interfaces as line cards.

BEFORE YOU BEGIN

No prerequisites.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**logging module** [*severity-level*]	Enables module log messages that have the specified severity level or higher. For example, when security level 4 is configured on the Cisco CG-OS router, the router logs all messages for security levels 1, 2, 3, and 4. Severity levels, which range from 0 to 7, are listed in Table 2-1. Default severity level setting is 5.
	no logging module [*severity-level*]	Disables module log messages.
Step 3	**show logging module**	(Optional) Displays the module logging configuration.
Step 4	**logging level** *facility severity-level*	Enables logging messages from the specified facility that have the specified severity level or higher. Severity levels, which range from 0 to 7, are listed in Table 2-1. To apply the same severity level to all facilities, use the **all** facility. For defaults, see the **show logging level** command.
	no logging level [*facility severity-level*]	Resets the logging severity level for the specified facility to its default level. When you do not specify a facility and severity level, the Cisco CG-OS router resets all facilities to their default levels.
Step 5	**show logging level** [*facility*]	(Optional) Displays the logging level configuration and the system default level by facility. When you do not specify a facility, the Cisco CG-OS router displays levels for all facilities.
Step 6	**logging timestamp** {**microseconds** | **milliseconds** | **seconds**}	Sets the logging time-stamp units. By default, the units are seconds. **Note**: This command applies to logs that the Cisco CG-OS router stores locally. It does not apply to the external logging server.
	no logging timestamp {**microseconds** | **milliseconds** | **seconds**}	Resets the logging time-stamp units to the default of seconds. **Note**: This command applies to logs that the Cisco CG-OS router stores locally. It does not apply to the external logging server.
Step 7	**show logging timestamp**	(Optional) Displays the logging time-stamp units configured.
Step 8	**copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

EXAMPLE

This example shows how to configure the severity level and time-stamp units of messages logged by modules and facilities.

```
router# configure terminal
router(config)# logging module 3
router(config)# logging level aaa 2
router(config)# logging timestamp milliseconds
router(config)# copy running-config startup-config
```

Configuring syslog Servers

You can configure up to eight syslog servers that reference remote systems to log system messages.

BEFORE YOU BEGIN

No prerequisites.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**logging server** {*hostname* | *ipv4_address* | *ipv6_address}* [*severity-level]*	Configures a syslog server by its specified hostname or IPv4 or IPv6 address. Severity levels, which range from 0 to 7, are listed in Table 2-1. The default outgoing facility is local 7.
	no logging server {*hostname* | *ipv4_address* | *ipv6_address}*	Removes the logging server for the specified host.
Step 3	**logging source-interface loopback** *virtual-interface*	Enables a source interface for the remote syslog server, which in this case is the loopback interface. The range for the *virtual-interface* argument is from 0 to 1023.
Step 4	**show logging server**	(Optional) Displays the syslog server configuration.
Step 5	**copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

EXAMPLE

This example shows how to a configure syslog server with an IPv4 address.

```
router# configure terminal
router(config)# logging server 192.0.2.253 5
router(config)# logging source-interface loopback 5
router(config)# copy running-config startup-config
```

This example shows how to configure a syslog server with an IPv6 address.

```
router# configure terminal
router(config)# logging server 2001::)db*::3 5
router(config)# logging source-interface loopback 5
router(config)# copy running-config startup-config
```

Configuring Syslog Server on UNIX or Linux

You can configure a syslog server on a UNIX or Linux system by adding the following line to the /etc/syslog.conf file:

```
facility.level local1.notice/var/log action
```

Table 2-3 describes the syslog fields that you can configure.

Table 2-3 syslog Fields in syslog.conf

Field	Description
Facility	Creator of the message, which can be auth, authpriv, cron, daemon, kern, lpr, mail, mark, news, syslog, user, local0 through local7, or an asterisk (*) for all. These facility designators allow you to control the destination of messages based on their origin. **Note**: Check your configuration before using a local facility.
Level	Minimum severity level at which messages are logged, which can be debug, info, notice, warning, err, crit, alert, emerg, or an asterisk (*) for all. You can use none to disable a facility.
Action	Destination for messages, which can be a filename, a hostname preceded by the at sign (@), a comma-separated list of users, or an asterisk (*) for all logged-in users.

To configure a syslog server on a UNIX or Linux system, follow these steps:

Step 1 Log debug messages with the local7 facility in the file /var/log/myfile.log by adding the following line to the /etc/syslog.conf file:

```
debug.local7             /var/local1.notice/var/log/myfile.log
```

Step 2 Create the log file by entering these commands at the shell prompt:

```
$ touch /var/log/myfile.log
$ chmod 766 /var/log/myfile.log
```

Step 3 Make sure the system message logging daemon reads the new changes by checking myfile.log after entering this command:

```
$ kill -HUP ~cat /etc/syslog.pid~
```

Displaying and Clearing Log Files

You can display or clear messages in the log file and the NVRAM.

Command	Purpose
show logging last *number-lines*	Displays the last number of lines in the logging file. You can specify from 1 to 9999 for the last number of lines.
show logging logfile [**start-time** *yyyy mmm dd hh:mm:ss*] [**end-time** *yyyy mmm dd hh:mm:ss*]	Displays the messages in the log file that have a time stamp within the span entered. If you do not enter an end time, then the Cisco CG-OS software applies the current time. Enter three characters for the month time field, and digits for the year and day time fields.
show logging nvram [**last** *number-lines*]	Displays the messages in the NVRAM. To limit the number of lines displayed, enter the last number of lines to display. Specify from 1 to 100 for the last number of lines.
clear logging logfile	Clears the contents of the log file.
clear logging nvram	Clears the logged messages in NVRAM.

Verifying the Configuration

To display system message logging configuration information, enter any of all of the following commands.

Command	Purpose
show logging console	Displays the console logging configuration.
show logging info	Displays the logging configuration.
show logging last *number-lines*	Displays the last number of lines of the log file.
show logging level [*facility*]	Displays the facility logging severity level configuration.
show logging logfile [**start-time** *yyyy mmm dd hh:mm:ss*] [**end-time** *yyyy mmm dd hh:mm:ss*]	Displays the messages in the log file.
show logging loopback	Displays loopback information logged.
show logging module	Displays the module logging configuration.
show logging monitor	Displays the monitor logging configuration.
show logging nvram [**last** *number-lines*]	Displays the messages in the NVRAM log.
show logging server	Displays the syslog server configuration.
show logging timestamp	Displays the logging time-stamp units configuration.

For detailed information about the fields in the output from these commands, see the Command Lookup Tool on Cisco.com.

Configuration Example

This example shows how to configure system message logging:

```
configure terminal
  logging console 3
  logging monitor 3
  logging logfile my_log 6
  logging module 3
  logging level aaa 2
  logging timestamp milliseconds
  logging server 172.28.254.253
  logging server 172.28.254.254 5 facility local3
  copy running-config startup-config
```

Feature History

Table 2-4 Feature History for System Message Logging

Feature Name	Release	Feature Information
System Message Logging	Cisco CG-OS Release CG1(1)	Initial support of the feature on the CGR 1000 Series Routers.

Configuring SNMP

This chapter describes how to configure the SNMP feature on Cisco CG-OS routers.

This chapter includes the following sections:

Information About SNMP

The Simple Network Management Protocol (SNMP) is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language used for the monitoring and management of devices in a network.

This section includes the following topics:

SNMP Functional Overview

The SNMP framework consists of three parts:

- An SNMP manager—The system used to control and monitor the activities of network devices using SNMP.
- An SNMP agent—The software component within the managed device that maintains the data for the device and reports these data, as needed, to managing systems. Cisco CG-OS supports the agent and MIB. To enable the SNMP agent, you must define the relationship between the manager and the agent.
- A managed information base (MIB)—The collection of managed objects on the SNMP agent.

SNMP is defined in RFCs 3411 to 3418.

Cisco CG-OS supports SNMPv2c, and SNMPv3. SNMPv2c uses a community-based form of security.

Cisco CG-OS supports SNMP over IPv4 and IPv6.

Note CG-OS does not support multiple VDCs. It always uses the default VDC (VDC 1).

SNMP Notifications

A key feature of SNMP is the ability to generate notifications from an SNMP agent. These notifications do not require that requests be sent from the SNMP manager. Notifications can indicate improper user authentication, restarts, the closing of a connection, loss of a connection to a neighbor router, or other significant events.

Cisco CG-OS generates SNMP notifications as either traps or informs. A trap is an asynchronous, unacknowledged message sent from the agent to the SNMP managers listed in the host receiver table. Informs are asynchronous messages sent from the SNMP agent to the SNMP manager which the manager must acknowledge receipt of.

Traps are less reliable than informs because the SNMP manager does not send any acknowledgment when it receives a trap. Cisco CG-OS cannot determine if the trap was received. An SNMP manager that receives an inform request acknowledges the message with an SNMP response protocol data unit (PDU). If Cisco CG-OS never receives a response, it can send the inform request again.

You can configure Cisco CG-OS to send notifications to multiple host receivers. See the "Configuring SNMP Notification Receivers" section on page 3-10 for more information about host receivers.

SNMPv3

SNMPv3 provides secure access to devices by a combination of authenticating and encrypting frames over the network. The security features provided in SNMPv3 are as follows:

- Message integrity—Ensures that a packet has not been tampered with while it was in-transit.
- Authentication—Determines that the message is from a valid source.
- Encryption—Scrambles the packet contents to prevent it from being seen by unauthorized sources.

SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the role in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet.

This section includes the following topics:

Security Models and Levels for SNMPv2, v3

The security level determines if an SNMP message needs to be protected from disclosure and if the message needs to be authenticated. The various security levels that exist within a security model are as follows:

- noAuthNoPriv—Security level that does not provide authentication or encryption.
- authNoPriv—Security level that provides authentication but does not provide encryption.
- authPriv—Security level that provides both authentication and encryption.

Three security models are available: SNMPv2c, and SNMPv3. The security model combined with the security level determine the security mechanism applied when the SNMP message is processed.

Table 3-1 identifies what the combinations of security models and levels mean.

Table 3-1 SNMP Security Models and Levels

Model	Level	Authentication	Encryption	What Happens
v2c	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
v3	authNoPriv	HMAC-MD5 or HMAC-SHA	No	Provides authentication based on the Hash-Based Message Authentication Code (HMAC) Message Digest 5 (MD5) algorithm or the HMAC Secure Hash Algorithm (SHA).
v3	authPriv	HMAC-MD5 or HMAC-SHA	DES	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides Data Encryption Standard (DES) 56-bit encryption in addition to authentication based on the Cipher Block Chaining (CBC) DES (DES-56) standard.

User-Based Security Model

The SNMPv3 User-Based Security Model (USM) refers to SNMP message-level security and offers the following services:

- Message integrity—Ensures that messages have not been altered or destroyed in an unauthorized manner and that data sequences have not been altered to an extent greater than can occur nonmaliciously.
- Message origin authentication—Ensures that the claimed identity of the user on whose behalf received data was originated is confirmed.
- Message confidentiality—Ensures that information is not made available or disclosed to unauthorized individuals, entities, or processes.

SNMPv3 authorizes management operations only by configured users and encrypts SNMP messages.

Cisco CG-OS uses two authentication protocols for SNMPv3:

- HMAC-MD5-96 authentication protocol
- HMAC-SHA-96 authentication protocol

Cisco CG-OS uses Advanced Encryption Standard (AES) as one of the privacy protocols for SNMPv3 message encryption and conforms with RFC 3826.

The **priv** option offers a choice of DES or 128-bit AES encryption for SNMP security encryption. The **priv** option and the **aes-128** token indicate that this privacy password is for generating a 128-bit AES key.The AES priv password can have a minimum of eight characters. If the passphrases are specified in clear text, you can specify a maximum of 64 case-sensitive alphanumeric characters. If you use the localized key, you can specify a maximum of 130 characters.

Note For an SNMPv3 operation that uses the external AAA server, you must use AES for the privacy protocol in the user configuration on the external AAA server.

CLI and SNMP User Synchronization

SNMPv3 user management can be centralized at the Access Authentication and Accounting (AAA) server level. This centralized user management allows the SNMP agent in Cisco CG-OS to leverage the user authentication service of the AAA server. Once user authentication is verified, the SNMP PDUs are processed further. Additionally, the AAA server is also used to store user group names. SNMP uses the group names to apply the access/role policy that is locally available in the router.

Any configuration changes made to the user group, role, or password results in database synchronization for both SNMP and AAA.

Cisco CG-OS synchronizes user configuration in the following ways:

- The authentication passphrase specified in the **snmp-server user** command becomes the password for the CLI user.
- The password specified in the **username** command becomes the authentication and privacy passphrases for the SNMP user.
- If you create or delete a user using either SNMP or the CLI, the user is created or deleted for both SNMP and the CLI.
- User-role mapping changes are synchronized in SNMP and the CLI.
- Role changes (deletions or modifications) from the CLI are synchronized to SNMP.

Note When you configure a passphrase/password in localized key/encrypted format, Cisco CG-OS does not synchronize the user information (password, roles, and so on).

Cisco CG-OS holds the synchronized user configuration for 60 minutes by default. See the "Modifying the AAA Synchronization Time" section on page 3-18 for information on how to modify this default value.

Group-Based SNMP Access

Note Because *group* is a standard SNMP term used industry-wide, we refer to role(s) as group(s) in this SNMP section.

SNMP access rights are organized by groups. Each group in SNMP is similar to a role through the CLI. Each group is defined with read access or read-write access.

You can begin communicating with the agent once your username is created, your roles are set up by your administrator, and you are added to the roles.

Cisco MIB Locator

To locate and download the MIBs supported by Cisco CG-OS, visit the Cisco MIB Locator page:

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

For a list of supported MIBs and MIB notifications, see Table 3-3.

Default Settings

Table 3-2 lists the default settings for SNMP parameters.

Table 3-2 Default SNMP Parameters

Parameters	Default
LinkUp/LinkDown Notifications	Enabled
Module inserted/removed Notifications	Enabled

Configuring SNMP

This section includes the following topics:

Configuring SNMP Users

You can configure a user for SNMP.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Router enters global configuration mode.
Step 2	**snmp-server user** *name* [**auth** {**md5** | **sha**} *passphrase* [**auto**] [**priv** [**aes-128**] *passphrase*] [**engineID** *id*] [**localizedkey**]]	Configures an SNMP user with authentication and privacy parameters. The passphrase can be any case-sensitive alphanumeric string up to 64 characters. If you use the **localizedkey** keyword, the passphrase can be any case-sensitive alphanumeric string up to 130 characters. The engineID format is a 12-digit colon-separated decimal number.
Step 3	**show snmp user**	(Optional) Displays information about one or more SNMP users.
Step 4	**copy running-config startup-config**	(Optional) Saves this configuration change.

EXAMPLE

This example shows how to configure the SNMP contact and location information:

```
router# configure terminal
router(config)# snmp-server user Admin auth sha abcd1234 priv abcdefgh
router(config-callhome)# show snmp user
router(config)# copy running-config startup-config
```

Enforcing SNMP Message Encryption

You can configure SNMP to require authentication or encryption for incoming requests. By default, the SNMP agent accepts SNMPv3 messages without authentication and encryption. When you enforce privacy, Cisco CG-OS responds with an authorizationError for any SNMPv3 PDU request using securityLevel parameter of either noAuthNoPriv or authNoPriv.

Use the following command in global configuration mode to enforce SNMP message encryption for a user:

Command	Purpose
snmp-server user *name* **enforcePriv** **Example:** router(config)# **snmp-server user Admin enforcePriv**	Enforces SNMP message encryption for this user.

Use the following command in global configuration mode to enforce SNMP message encryption for all users:

Command	Purpose
snmp-server globalEnforcePriv **Example:** router(config)# **snmp-server globalEnforcePriv**	Enforces SNMP message encryption for all users.

Assigning SNMPv3 Users to Multiple Roles

After you configure an SNMP user, you can assign multiple roles for the user.

Note Only users belonging to a network-admin role can assign roles to other users.

Use the following command in global configuration mode to assign a role to an SNMP user:

Command	Purpose
snmp-server user *name group* **Example:** router(config)# **snmp-server user Admin superuser**	Associates this SNMP user with the configured user role.

Creating SNMP Communities

You can create SNMP communities for SNMPv2c.

Use the following command in global configuration mode to create an SNMP community string:

Command	Purpose
snmp-server community *name group* **{ro | rw}** **Example:** router(config)# **snmp-server community public ro**	Creates an SNMP community string.

Filtering SNMP Requests

You can assign an access list (ACL) to a community to filter incoming SNMP requests. If the assigned ACL allows the incoming request packet, SNMP processes the request. If the ACL denies the request, SNMP drops the request and sends a system message.

Create the ACL with the following parameters:

- Source IP address
- Destination IP address
- Source port
- Destination port
- Protocol (UDP or TCP)

See the *Cisco 1000 Series Connected Grid Routers Security Software Configuration Guide* for more information on creating ACLs. The ACL applies to IPv4 over UDP and TCP.

Use the following command in global configuration mode to assign an ACL to a community to filter SNMP requests:

Command	Purpose
snmp-server community *community-name* **use-acl** *acl-name* **Example:** `router(config)# snmp-server community public use-acl my_acl_for_public`	Assigns an ACL to an SNMP community to filter SNMP requests.

Configuring SNMP Notification Receivers

You can configure Cisco CG-OS to generate SNMP notifications to multiple SNMPv2c and SNMPv3 host receivers.

Use the following command in global configuration mode to configure a host receiver for SNMPv2c traps or informs:

Command	Purpose
snmp-server host *ip-address* **{traps | informs} version 2c** *community* [**udp_port** *number*] **Example:** `router(config)# snmp-server host 192.0.2.1 informs version 2c public`	Configures a host receiver for SNMPv2c traps or informs. The *ip-address* can be an IPv4 or IPv6 address, or a domain name. The *community* can be any alphanumeric string up to 255 characters. The UDP port number range is from 0 to 65535.

Use the following command in global configuration mode to configure a host receiver for SNMPv3 traps or informs:

Command	Purpose
snmp-server host *ip-address* **{traps | informs} version 3 {auth | noauth | priv}** *username* **[udp_port number** *port***]** **Example:** `router(config)# snmp-server host 192.0.2.1 informs version 3 auth NMS`	Configures a host receiver for SNMPv3 traps or informs. The *ip-address* can be an IPv4 or IPv6 address, or a domain name. The *username* can be any alphanumeric string up to 255 characters. The UDP port number range is from 0 to 65535.

Note The SNMP manager must know the user credentials (authKey/PrivKey) based on the SNMP engine ID of the Cisco CG-OS device to authenticate and decrypt the SNMPv3 messages.

Configuring a Source Interface for SNMP Notifications

You can configure SNMP to use the IP address of an interface as the source IP address for notifications. When a notification is generated, its source IP address is based on the IP address of this configured interface. You can configure this as follows:

- All notifications sent to all SNMP notification receivers.
- All notifications sent to a specific SNMP notification receiver. This configuration overrides the global source interface configuration.

Note Configuring the source interface IP address for outgoing trap packets does not guarantee that the device will use the same interface to send the trap. The source interface IP address defines the source address inside of the SNMP trap, and the connection is opened with the address of the egress interface as source.

Use the following command in global configuration mode to configure a host receiver on a source interface:

Command	Purpose
snmp-server host *ip-address* **source-interface** *if-type if-number* [**udp_port** *port*] **Example:** `router(config)# snmp-server host 192.0.2.1 source-interface ethernet 2/1`	Configures a host receiver for SNMPv2c traps or informs. The *ip-address* can be an IPv4 address. Use **?** to determine the supported interface types. The UDP port number range is from 0 to 65535. This configuration overrides the global source interface configuration.

Use the following command in global configuration mode to configure a source interface for sending out all SNMP notifications:

Command	Purpose
snmp-server source-interface {traps | informs} *if-type if-number* **Example:** `router(config)# snmp-server source-interface traps ethernet 2/1`	Configures a source interface for sending out SNMPv2c traps or informs. Use **?** to determine the supported interface types.

Use the **show snmp source-interface** command to display information about configured source interfaces.

Configuring the Notification Target User

You must configure a notification target user on the device to send SNMPv3 inform notifications to a notification host receiver.

Cisco CG-OS uses the credentials of the notification target user to encrypt the SNMPv3 inform notification messages to the configured notification host receiver.

Note For authenticating and decrypting the received inform PDU, the notification host receiver should have the same user credentials as configured in Cisco CG-OS to authenticate and decrypt the informs.

Use the following command in global configuration mode to configure the notification target user:

Command	Purpose
snmp-server user name [auth {md5 | sha} *passphrase* **[auto] [priv [aes-128]** *passphrase*] [*engineID id*] **Example:** `router(config)# snmp-server user NMS auth sha abcd1234 priv abcdefgh engineID 00:00:00:63:00:01:00:10:20:15:10:03`	Configures the notification target user with the specified engine ID for the notification host receiver. The engineID format is a 12-digit colon-separated decimal number.

Configuring SNMP to Send Traps Using an Inband Port

You can configure SNMP to send traps using an inband port. To do so, you must configure the source interface (at the global or host level) to send the traps.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Router enters global configuration mode.
Step 2	**snmp-server source-interface traps** *if-type if-number*	Globally configures a source interface for sending out SNMP traps. Use **?** to determine the supported interface types. You can configure the source interface at the global level or at a host level. When the source interface is configured globally, any new host configuration uses the global configuration to send the traps. **Note**: To configure a source interface at the host level, use this command: **snmp-server host** *ip-address* **source-interface** *if-type if-number*.
Step 3	**show snmp source-interface**	(Optional) Displays information about configured source interfaces.
Step 4	**snmp-server host** *ip-address* [**udp_port** *port*]	Configures SNMP to communicate with the host receiver. The *ip-address* can be an IPv4 address. The UDP port number range is from 0 to 65535.

	Command	Purpose
Step 5	**show snmp host**	(Optional) Displays information about configured SNMP hosts.
Step 6	**copy running-config startup-config**	(Optional) Saves this configuration change.

EXAMPLE

This example shows how to configure SNMP to send traps using a globally configured inband port:

```
router# configure terminal
router(config)# snmp-server source-interface traps ethernet 1/2
router(config)# show snmp source-interface
------------------------------------------------------------------------
Notification                    source-interface
------------------------------------------------------------------------
trap                            Ethernet1/2

inform                                -
------------------------------------------------------------------------

router(config)# snmp-server host 171.71.48.164
router(config)# show snmp host
------------------------------------------------------------------------
Host                            Port Version  Level  Type   SecName
------------------------------------------------------------------------
171.71.48.164                    162  v2c      noauth trap   public


Source interface: Ethernet 1/2
------------------------------------------------------------------------
```

Enabling SNMP Notifications

You can enable or disable notifications. If you do not specify a notification name, Cisco CG-OS enables all notifications.

Table 3-3 lists the commands that enable the notifications for Cisco CG-OS MIBs.

Note The **snmp-server enable traps** command enables both traps and informs, depending on the configured notification host receivers.

Table 3-3 Enabling SNMP Notifications

MIB	Related Commands
All notifications	**snmp-server enable traps**
CISCO-AAA-SERVER-MIB	**snmp-server enable traps aaa** **snmp-server enable traps aaa server-state-change**
CISCO-CALLHOME-MIB	**snmp-server enable traps callhome** **snmp-server enable traps callhome event-notify** **snmp-server enable traps callhome smtp-send-fail**
ENTITY-MIB, CISCO-ENTITY-SENSOR-MIB	**snmp-server enable traps entity** **snmp-server enable traps entity fru** **snmp-server enable traps entity entity_sensor** **snmp-server enable traps entity entity_mib_change** **snmp-server enable traps entity entity_module_status_change** **snmp-server enable traps entity entity_power_status_change** **snmp-server enable traps entity entity_module_inserted** **snmp-server enable traps entity entity_module_removed** **snmp-server enable traps entity entity_unrecognised_module** **snmp-server enable traps entity entity_fan_status_change** **snmp-server enable traps entity entity_power_out_change**
IF-MIB	**snmp-server enable traps link** **snmp-server enable traps link linkDown** **snmp-server enable traps link linkUp**
SNMPv2-MIB	**snmp-server enable traps snmp** **snmp-server enable traps snmp authentication**
CISCO-FEATURE-CONTROL-MIB	**snmp-server enable traps feature-control** **snmp-server enable traps feature-control FeatureOpStatusChange**
CISCO-SYSTEM-EXT-MIB	**snmp-server enable traps sysmgr** **snmp-server enable traps sysmgr cseFailSwCoreNotifyExtended**
ITRON-PRISM-C1222-MIB	**snmp-server enable traps c1222r** **snmp-server enable traps c1222r comm_module_idle_too_long** **snmp-server enable traps c1222r comm_module_enable_change**

Use the following commands in global configuration mode to enable the specified notification.

Command	Purpose
snmp-server enable traps **Example:** `router(config)# snmp-server enable traps`	Enables all SNMP notifications.
snmp-server enable traps aaa [**server-state-change**] **Example:** `router(config)# snmp-server enable traps aaa`	Enables the AAA SNMP notifications.
snmp-server enable traps callhome [event-notify] [smtp-send-fail] **Example:** `router(config)# snmp-server enable traps callhome`	Enables the CISCO-CALLHOME-MIB SNMP notifications. Optionally, enables the following specific notifications: • **event-notify**—Enables Call Home external event notifications. • **smtp-send-fail**—Enables SMTP message send fail notifications.
snmp-server enable traps entity [fru] **Example:** `router(config)# snmp-server enable traps entity`	Enables the ENTITY-MIB SNMP notifications.

Disabling LinkUp/LinkDown Notifications on an Interface

You can disable linkUp and linkDown notifications on an individual interface. You can use these limit notifications on a flapping interface (an interface that transitions between up and down repeatedly).

Use the following command in interface configuration mode to disable linkUp/linkDown notifications for the interface:

Command	Purpose
no snmp trap link-status **Example:** `router(config-if)# no snmp trap link-status`	Disables SNMP link-state traps for the interface. This command is enabled by default.

Displaying SNMP ifIndex for an Interface

The SNMP ifIndex is used across multiple SNMP MIBs to link related interface information. The ifIndex is also used by NetFlow to collect information on an interface.

Use the following command in any mode to display the SNMP ifIndex values for interfaces:

Command	Purpose
show interface snmp-ifindex **Example:** `router# show interface snmp-ifindex | grep -i Eth 2/1`	Displays the persistent SNMP ifIndex value from IF-MIB for all interfaces. Optionally, use the | keyword and the grep keyword to search for a particular interface in the output.

Enabling a One-time Authentication for SNMP over TCP

You can enable a one-time authentication for SNMP over a TCP session.

Use the following command in global configuration mode to enable a one-time authentication for SNMP over TCP:

Command	Purpose
snmp-server tcp-session [auth] **Example:** `router(config)# snmp-server tcp-session`	Enables a one-time authentication for SNMP over a TCP session. The default is disabled.

Assigning the SNMP Device Contact and Location Information

You can assign the device contact information, which is limited to 32 characters (without spaces) and the device location.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Router enters global configuration mode.
Step 2	**snmp-server contact** *name*	Configures sysContact, which is the SNMP contact name.
Step 3	**snmp-server location** *name*	Configures sysLocation, which is the SNMP location.
Step 4	**show snmp**	(Optional) Displays information about one or more destination profiles.
Step 5	**copy running-config startup-config**	(Optional) Saves this configuration change.

EXAMPLE

This example shows how to configure the SNMP contact and location information:

```
router# configure terminal
router(config)# snmp-server contact Admin
router(config)# snmp-server location Lab-7
router(config)# copy running-config startup-config
```

Configuring the Context to Network Entity Mapping

You can configure an SNMP context to map to a logical network entity, such as a protocol instance.

BEFORE YOU BEGIN

Determine the logical network entity instance.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Router enters global configuration mode.
Step 2	**snmp-server context** *context-name* **[instance** *instance-name*]**[topology** *topology-name*]	Maps an SNMP context to a protocol instance or topology. The names can be any alphanumeric string up to 32 characters.
Step 3	**snmp-server mib community-map** *community-name* **context** *context-name*	(Optional) Maps an SNMPv2c community to an SNMP context. The names can be any alphanumeric string up to 32 characters.
Step 4	**show snmp context**	(Optional) Displays information about one or more SNMP contexts.
Step 5	**copy running-config startup-config**	(Optional) Saves this configuration change.

EXAMPLE

This example shows how to map OSPF instance Enterprise to the same SNMPv2c public community string.

```
router# configure terminal
router(config)# feature ospf
router(config)# router ospf Enterprise
router(config-router)# exit
router(config)# snmp-server context public1 instance Enterprise
router(config)# snmp-server mib community-map public context public1
router(config)# copy running-config startup-config
```

This example shows how to delete the mapping between an SNMP context and a logical network entity when operating in the global configuration mode.

```
router(config)# no snmp-server context public1
```

Note When deleting a context mapping (see example above), you only enter the context name in the **no snmp-server context** *context-name* command. You do not enter the instance or topology keywords and variable names as you did when configuring the item (see Step 2. If you use the **instance** or **topology** keywords when deleting the context mapping, then you configure a mapping between the context and a zero-length string

Disabling SNMP

You can disable SNMP on a device.

Use the following command in global configuration mode to disable SNMP:

Command	Purpose
no snmp-server protocol enable **Example:** `router(config)# no snmp-server protocol enable`	Disables SNMP. This command is enabled by default.

Modifying the AAA Synchronization Time

You can modify how long Cisco CG-OS holds the synchronized user configuration.

Use the following command in global configuration mode to modify the AAA synchronization time:

Command	Purpose
snmp-server aaa-user cache-timeout *seconds* **Example:** `router(config)# snmp-server aaa-user cache-timeout 1200`	Configures how long the AAA synchronized user configuration stays in the local cache. The range is from 1 to 86400 seconds. The default is 3600.

Verifying Configuration

To display the SNMP configuration information, perform one of the following tasks.

Command	Purpose
show interface snmp-ifidex	Displays the SNMP ifIndex value for all interfaces (from IF-MIB).
show running-config snmp [**all**]	Displays the SNMP running configuration.
show snmp	Displays the SNMP status.
show snmp community	Displays the SNMP community strings.
show snmp context	Displays the SNMP context mapping.
show snmp engineID	Displays the SNMP engineID.
show snmp group	Displays SNMP roles.
show snmp host	Displays information about configured SNMP hosts.
show snmp session	Displays SNMP sessions.
show snmp source-interface	Displays information about configured source interfaces.
show snmp trap	Displays the SNMP notifications enabled or disabled.
show snmp user	Displays SNMPv3 users.

Configuration Examples

This example shows how to configure Cisco CG-OS to send the Cisco linkUp or Down notifications to one notification host receiver and defines two SNMP users, Admin and NMS.

```
router# configure terminal
router(config)# snmp-server contact Admin@company.com
router(config)# snmp-server user Admin auth sha abcd1234 priv abcdefgh
router(config)# snmp-server user NMS auth sha abcd1234 priv abcdefgh engine ID
                00:00:00:63:00:01:00:22:32:15:10:03
router(config)# snmp-server host 192.0.2.1 informs version 3 auth NMS
router(config)# snmp-server enable traps link cisco
```

This example shows how to configure SNMP to send traps using an inband port configured at the host level.

```
router# config t
router(config)# snmp-server host 171.71.48.164 version 2c public
router(config)# snmp-server host 171.71.48.164 source-interface ethernet 1/2
router(config)# show snmp host
-----------------------------------------------------------------------
Host                            Port Version  Level  Type   SecName
-----------------------------------------------------------------------
171.71.48.164                    162  v2c      noauth trap   public

Source interface: Ethernet 1/2
-----------------------------------------------------------------------

router(config)# snmp-server host 171.71.48.164
router(config)# show snmp host
-----------------------------------------------------------------------
Host                            Port Version  Level  Type   SecName
-----------------------------------------------------------------------
171.71.48.164                    162  v2c      noauth trap   public

Source interface: Ethernet 1/2
-----------------------------------------------------------------------
```

Useful Common MIBs

MIBs	MIBs Link
• SNMP-COMMUNITY-MIB • SNMP-FRAMEWORK-MIB • SNMP-NOTIFICATION-MIB • SNMP-TARGET-MIB • SNMPv2-MIB	To locate and download these MIBs, go to the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml Click **SNMPv2 MIBs** to download these MIBs.

Feature History

Table 3-4 Feature History for SNMP

Feature Name	Release	Feature Information
SNMP	Cisco CG-OS Release CG2(1)	Initial support of the feature on the CGR 1000 Series Routers.

Configuring Embedded Event Manager

This chapter describes how to configure Embedded Event Manager (EEM) to detect and handle critical events on the Cisco 1000 Series Connected Grid Routers (hereafter referred to as the Cisco CG-OS router).

This chapter includes the following sections:

Information About EEM

EEM monitors events that occur on your device and takes action to recover or troubleshoot these events, based on your configuration.

This section includes the following topics:

EEM Overview

EEM consists of three major components:

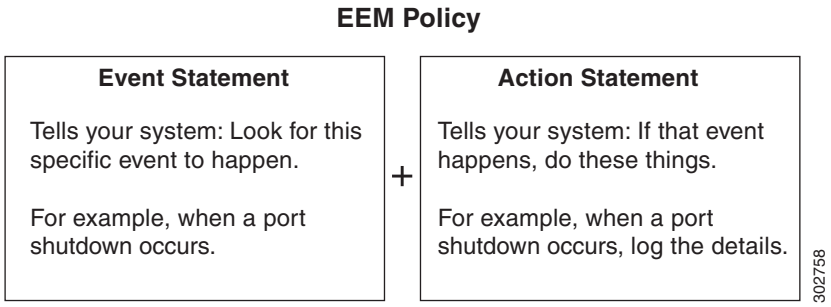
- Event statements—Events to monitor from another Cisco CG-OS component that might require some action, workaround, or notification.
- Action statements —An action that EEM can take, such as sending an e-mail, or disabling an interface, to recover from an event.
- Policies—An event paired with one or more actions to troubleshoot or recover from the event.

Policies

An EEM policy consists of an event statement and one or more action statements. The event statement defines the event to look for as well as the filtering characteristics for the event. The action statement defines the action EEM takes when the event occurs.

Figure 4-1 shows the two basic statements in an EEM policy.

Figure 4-1 EEM Policy Statements



You can configure EEM policies using the CLI or a VSH script.

EEM gives you a device-wide view of policy management. You configure EEM policies on the supervisor, and EEM pushes the policy to the correct module based on the event type. EEM takes any actions for a triggered event either locally on the module or on the supervisor (the default option).

EEM maintains event logs on the Cisco CG-OS router.

Cisco CG-OS has a number of preconfigured system policies. These system policies define many common events and actions for the device. System policy names begin with two underscore characters (__).

You can create user policies to suit your network. If you create a user policy, any actions in your policy occur after EEM triggers any system policy actions related to the same event as your policy. To configure a user policy, see Defining a User Policy, page 4-8.

You can also override some system policies. The overrides that you configure take the place of the system policy. You can override the event or the actions.

Use the **show event manager system-policy** command to view the preconfigured system policies and determine which policies that you can override.

To configure an overriding policy, see the Overriding a Policy, page 4-14.

Note You should use the **show running-config eem** command to check the configuration of each policy. An override policy that consists of an event statement and no action statement triggers no action and no notification of failures.

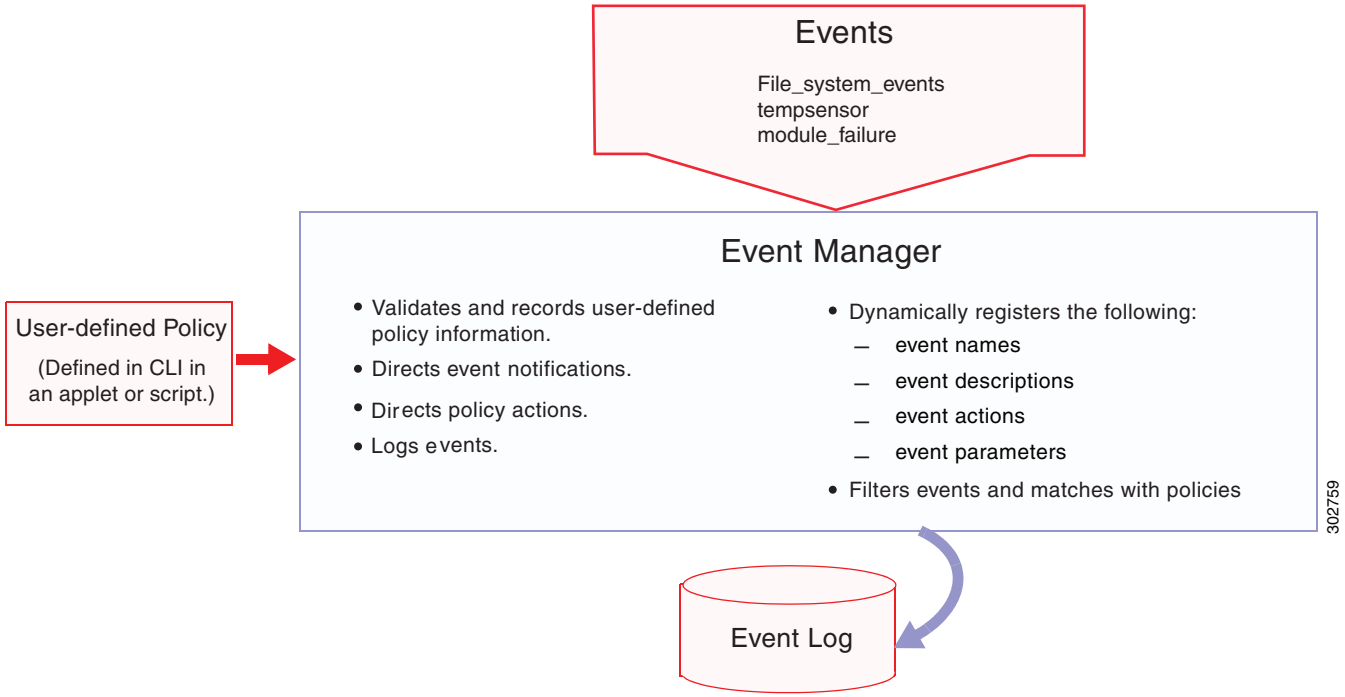
Note Your override policy should always include an event statement. An override policy without an event statement overrides all possible events in the system policy.

Event Statements

An event is any device activity for which some action, such as a workaround or a notification, should be taken. In many cases, these events are related to faults in the device such as when an interface or a fan malfunctions.

EEM defines event filters so only critical events or multiple occurrences of an event within a specified time period trigger an associated action.

Figure 4-2 EEM Overview



Event statements specify the event that triggers a policy to run.

You can configure multiple event triggers. For more information on configuring multiple events, see the EEM Event Correlation, page 4-5.

EEM schedules and runs policies on the basis of event statements. EEM examines the event and action commands and runs them as defined.

Note If you want to allow the triggered event to process any default actions, you must configure the EEM policy to allow the event default action statement.

Action Statements

Action statements describe the action triggered by a policy. Each policy can have multiple action statements. If no action is associated with a policy, EEM still observes events but takes no actions.

EEM supports the following actions in action statements:

- Execute any CLI commands.
- Update a counter.
- Log an exception.
- Force the shutdown of any module.
- Reload the device.
- Shut down specified modules because the power is over budget.
- Generate a syslog message.
- Generate an SNMP notification.
- Use the default action for the system policy.

Note If you want to allow the triggered event to process any default actions, you must configure the EEM policy to allow the default action. For example, if you match a CLI command in a match statement, you must add the event-default action statement to the EEM policy or EEM will not allow the CLI command to execute.

Note Verify that your action statements within your user policy or overriding policy do not negate each other or adversely affect the associated system policy.

VSH Script Policies

You can also write policies in a VSH script, using a text editor. These policies have an event statement and action statement(s) just as other policies, and these policies can either augment or override system policies. After you write your VSH script policy, copy it to the device and activate it. To configure a policy in a VSH script, see the Defining a Policy using a VSH Script, page 4-13.

Environment Variables

You can define environment variables for EEM that are available for all policies. Environment variables are useful for configuring common values that you can use in multiple policies. For example, you can create an environment variable for the IP address of an external e-mail server.

You can use an environment variable in action statements by using the parameter substitution format.

Example 4-1 shows a sample action statement to force a module 1 shutdown, with a reset reason of "EEM action."

Example 4-1 Action Statement

```
router (config-eem-policy)# action 1.0 forceshut module 1 reset-reson "EEM action."
```

If you define an environment variable for the shutdown reason, called default-reason, you can replace that reset reason with the environment variable, as shown in Example 4-2.

Example 4-2 Action Statement with Environment Variable

```
router (config-eem-policy)# action 1.0 foreshut module 1 reset-reason $default-reason
```

You can reuse this environment variable in any policy. For more information on environment variables, see the Defining an Environment Variable, page 4-7.

EEM Event Correlation

You can trigger an EEM policy based on a combination of events. First, you use the **tag** keyword to create and differentiate multiple events in the EEM policy. Then using a set of boolean operators (**and**, **or**, **andnot**), along with the count and time, you can define a combination of these events to trigger a custom action.

Note For information on configuring EEM event correlation, see Defining a User Policy, page 4-8.

Stateless Restarts

Cisco CG-OS software supports stateless restarts for EEM. After a reboot of the Cisco CG-OS router, the CG-OS software applies the running configuration.

Prerequisites for EEM

You must have network-admin or vdc-admin user privileges to configure EEM.

Guidelines and Limitations

Command Rules

The following rules apply to regular command expressions: all keywords must be expanded, and only the * symbol can be used for argument replacement.

Policies

The maximum number of configurable EEM policies is 500.

Action statements within your user policy or overriding policy must not negate each other or adversely affect the associated system policy.

You cannot override event statements. You can only override specific action statements (see Overriding a Policy, page 4-14)

An override policy that consists of an event statement and no action statement triggers no action and no notification of failures.

An override policy without an event statement overrides all possible events in the system policy.

If you want to allow a triggered event to process any default actions, then you must configure the EEM policy to allow the default action. For example, if you match a CLI command in a match statement, you must add the event-default action statement to the EEM policy or EEM will not allow the CLI command to execute.

When more than one event statement is included in an EEM policy, each event statement must have a **tag** keyword with a unique *tag* argument.

Default action execution is not supported for policies that are configured with tagged events.

Event Correlation

EEM event correlation is supported only on the Cisco CG-OS Router, not on individual interfaces.

EEM event correlation is not supported across different interfaces within a single policy.

EEM event correlation supports up to four event statements in a single policy. The event types can be the same or different, but only these event types are supported: cli, counter, syslog, and track.

EEM event correlation does not override the system default policies.

Default Settings

Table 4-1 lists the default settings for EEM parameters.

Table 4-1 Default EEM Parameters

Parameters	Default
System policies	Active

Configuring EEM

You can create policies that contain actions to take based on system policies. To display information about the system policies, use the **show event manager system-policy** command.

This section includes the following topics:

Defining an Environment Variable

You can define a variable to serve as a parameter in an EEM policy.

BEFORE YOU BEGIN

Make sure that you are in the default VDC. The Cisco CG-OS router does not support any VDCs beyond the default.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**event manager environment** *variable-name variable-value*	Creates an environment variable for EEM. The *variable-name* can be any case-sensitive alphanumeric string up to 29 characters. The *variable-value* can be any quoted alphanumeric string up to 39 characters.
Step 3	**show event manager environment** {*variable-name* | **all**}	(Optional) Displays information about the configured environment variables.
Step 4	**copy running-config startup-config**	(Optional) Saves this configuration change.

EXAMPLE

This example shows how to define an environment variable on the Cisco CG-OS router.

```
router# configure terminal
router(config)# event manager environment emailto "admin@anyplace.com"
router(config)# copy running-config startup-config
```

Defining a User Policy

To define a user policy you must define both an event and action statement.

BEFORE YOU BEGIN

Make sure that you are in the default VDC. The Cisco CG-OS router does not support any VDCs beyond the default.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**event manager applet** *applet-name*	Registers the applet with EEM and enters applet configuration mode. The *applet-name* can be any case-sensitive alphanumeric string up to 29 characters.
Step 3	**description** *policy-description*	(Optional) Configures a descriptive string for the policy. The string can be any alphanumeric string up to 80 characters. Enclose the string in quotation marks.
Step 4	**event** *event-statement*	Configures the event statement for the policy and enters the EEM configuration mode. For a list of all supported events statements, see Configuring Event Statements, page 4-9. Repeat Step 4 for multiple event statements.
Step 5	**tag** *tag* {**and** | **andnot** | **or**} *tag* [**and** | **andnot** | **or** {*tag*}] {**happens** *occurs* **in** *seconds*}	(Optional) Correlates multiple events in the policy. The range for the *occurs* argument is from 1 to 4294967295. The range for the *seconds* argument is from 0 to 4294967295 seconds.
Step 6	**action** *number*[**.***number2*] *action-statement*	Configures an action statement for the policy. For a list of all supported action statements, See Configuring Action Statements, page 4-12. Repeat Step 6 for multiple action statements.
	(Optional) **action** *number*[**.***number2*] *action-statement* >> *filename*	Enter this action statement for the policy if you want to export the output of an action statement to a specified flash or a directory. **Note**: The router does not have a default file to log these outputs.

	Command	Purpose
Step 7	**show event manager policy-state** *name* [**module** *module-id*]	(Optional) Displays information about the status of the configured policy.
Step 8	**copy running-config startup-config**	(Optional) Saves this configuration change.

EXAMPLE

This example shows how to define a user policy.

```
router# configure terminal
router(config)# event manager applet monitorShutdown
router(config-applet)# description "Monitors interface shutdown."
router(config-applet)# event cli match "shutdown"
router(config-applet)# tag one or two happens 1 in 10000
router(config-applet)# action 1.0 cli show interface e 2/1 >> action.txt
router(config-applet)# copy running-config startup-config
```

Configuring Event Statements

Use one or more of the following commands in EEM configuration mode to configure an event statement as shown in Step 4 of the Defining a User Policy section.

- **event gold module** {*slot* | **all**} **test** *test-name* [**severity** {**major** | **minor** | **moderate**}] **testing-type** {**bootup** | **monitoring** | **ondemand** | **scheduled**} **consecutive-failure** *count*
- **event memory** {**critical** | **minor** | **severe**}
- **event module** [**tag** *tag*] **status** {**online** | **offline** | **any**} **module** {**all** | *module-num*}
- **event module-failure** [**tag** *tag*] **type** *failure-type* **module** {*slot* | **all**} **count** *repeats* [**time** *seconds*]
- **event policy-default count** [*int coun*t] [**time** *seconds*]
- **event snmp** [**tag** *tag*] **oid** *oid* **get-type** {**exact** | **next**} **entry-op** {**eq** | **ge** | **gt** | **le** | **lt** |**ne**} **entry-val** entry [**exit-comb** {**and** | **or**}] **exit-op** {**eq** | **ge** | **gt** | **le** | **lt** |**ne**} **exit-val** exit **exit-time** *time* **polling-interval** *interval*
- **event temperature** [**module** *slot*] [*sensor numbe*r]

DETAILED STEPS

Command	Purpose
event cli [tag *tag*] **match** *expression* [**count** *repeats* | **time** *seconds*]	Triggers an event if you enter a command that matches the regular expression. **Note**: When using the **event cli match** command, you always use quotes to enclose the expression such as **event cli match** "**show ip int br**" **count 3 time 0** The **tag** *tag* keyword-argument pair identifies this specific event when multiple events are included in the policy. The *repeats* range is from 1 to 65000. The time range, in seconds, is from 0 to 4294967295, where 0 indicates no time limit.
event counter [**tag** *tag*] **name** *counter* **entry-val** *entry* **entry-op {eq | ge | gt | le | lt | ne} [exit-val** *exit* **exit-op {eq | ge | gt | le | lt | ne}]**	Triggers an event if the counter crosses the entry threshold based on the entry operation. The event resets immediately. Optionally, you can configure the event to reset after the counter passes the exit threshold. The **tag** *tag* keyword-argument pair identifies this specific event when multiple events are included in the policy. The *counter* name can be any case-sensitive, alphanumeric string up to 28 characters. The *entry* and *exit* value ranges are from 0 to 2147483647.

Command	Purpose
event track [tag *tag*] *object-number* **state** {**any** | **down** | **up**}	Triggers an event if the tracked object is in the configured state. The **tag** *tag* keyword-argument pair identifies this specific event when multiple events are included in the policy. The *object-numbe*r range is from 1 to 500.
event syslog [**tag** *tag*] [**occurs** | **pattern** *msg-text* | **period** | **priority** [**0-7** | **emergencies** | **alerts** | **critical** | **errors** | **warnings** | **notifications** | **informational** | **debugging**]]	Monitors an event. The **tag** *tag* keyword-argument pair identifies this specific event when multiple events are included in the policy. **occurs** Specifies the number of occurrences. The range is from 1 to 65000. **pattern** *msg-txt*– Specifies the matching regular expression (regex). The pattern can contain character text, an environment variable, or a combination of the two. If the string contains embedded blanks, it is enclosed with double quotation marks. **period**–Specifies the time interval during which the event occurs. The range is from 0 to 4294967295. **priority**–Specifies the priority level of the syslog messages. If this keyword is not selected, all syslog messages are set at the informational priority level. If this keyword is selected, the priority level argument must be defined. The range of values are 0 to 7. **emergencies**–Specifies that the system is unusable. **alerts** Specifies that immediate action is needed. **critical**–Specifies critical conditions. **errors**–Specifies error conditions. **warnings**–Specifies warming conditions. **notifications**–Specifies normal but significant conditions. **informational**–Specifies informational messages. This is the default. **debugging**–Specifies debugging messages

EXAMPLE

This example shows how to configure an event statement.

```
router# configure terminal
router (config-applet)# event cli match "shutdown"
router (config-applet)# event counter name mycounter entry-val 20 gt
router (config-applet)# event track 1 state down
```

Configuring Action Statements

Use the one or more of the following commands in EEM configuration mode to configure action statements as shown in Step 6 of the Defining a User Policy section.

Command	Purpose
action *number*[**.***number2*] **cli** *command1* [*command2...*] [**local**]	Runs the configured CLI commands. You can optionally run the commands on the module where the event occurred. The action label is in the format number1.number2. *number* can be any number up to 16 digits. The range for *number2* is from 0 to 9.
action *number[.number2]* **counter name** counter **value** *val* **op {dec | inc | nop | set}**	Modifies the counter by the configured value and operation. The action label is in the format number1.number2. *number* can be any number up to 16 digits. The range for *number2* is from 0 to 9. The counter name can be any case-sensitive, alphanumeric string up to 28 characters. The *val* can be an integer from 0 to 2147483647 or a substituted parameter.
action *number[.number2]* **event-default**	Executes the default action for the associated event. The action label is in the format number1.number2. *number* can be any number up to 16 digits. The range for *number2* is from 0 to 9.
action *number*[**.***number2*] **syslog** [**priority** *prio-val*] **msg** *error-messag*e	Sends a customized syslog message at the configured priority. *number* can be any number up to 16 digits. The range for *number2* is from 0 to 9. The *error-message* can be any quoted alphanumeric string up to 80 characters.

Note When you want to allow the triggered event to process any default actions, you must configure the EEM policy to allow the default action. For example, if you match a CLI command in a match statement, then you must add the event-default action statement to the EEM policy or EEM will not allow the CLI command to execute. You can use the **terminal event-manager bypass** command to allow all EEM policies with CLI matches to execute the CLI command.

Defining a Policy using a VSH Script

You can define a policy using a VSH script.

BEFORE YOU BEGIN

Make sure that you are in the default VDC. The Cisco CG-OS router does not support any VDCs beyond the default.

Ensure that you are logged in with administrator privileges.

Ensure that your script name is the same name as the script filename.

DETAILED STEPS

Step 1 In a text editor, list the commands that define the policy.

Step 2 Name the text file and save it.

Step 3 Copy the file to the following system directory:

bootflash://eem/user_script_policies

Registering and Activating a VSH Script Policy

You can register and activate a policy defined in a VSH script.

BEFORE YOU BEGIN

Make sure that you are in the default VDC. The Cisco CG-OS router does not support any VDCs beyond the default.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters the global configuration mode.
Step 2	**event manager policy** *policy-script*	Registers and activates an EEM script policy. The *policy-script* can be any case-sensitive alphanumeric string up to 29 characters.
Step 3	**show event manager policy internal** *name*	(Optional) Displays information about the configured policy.
Step 4	**copy running-config startup-config**	(Optional) Saves this configuration change.

EXAMPLE

This example shows how to register and activate a VSH script policy.

```
router# configure terminal
router(config)# event manager policy moduleScript
router(config)# copy running-config startup-config
```

Overriding a Policy

You can override actions statements for a gold system policy.

BEFORE YOU BEGIN

Make sure that you are in the default VDC. The Cisco CG-OS router does not support any VDCs beyond the default.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**event manager applet** *applet-name* **override** *system-policy*	Overrides a system policy and enters applet configuration mode. The *applet-name* can be any case-sensitive alphanumeric string up to 29 characters. The *system-policy* must be one of the existing system policies.
Step 3	**description** *policy-description*	(Optional) Configures a descriptive string for the policy. The string can be any alphanumeric string up to 80 characters. Enclose the string in quotation marks.
Step 4	**action** *number action-statement*	Configures an action statement for the policy. For details on action statements, see Configuring Action Statements, page 4-12. Repeat Step 6 in that section to create multiple action statements.
Step 5	**show event manager policy-state** *name*	(Optional) Displays information about the configured policy.
Step 6	**copy running-config startup-config**	(Optional) Saves this configuration change.

EXAMPLE

This example shows how to override an action statement for a gold system policy.

```
router# configure terminal
router(config)# event manager applet gold module all test monday test-type bootup
                  consecutive-failure 3
router(config-applet)# action 1.0 syslog priority warnings msg "Gold Module bootup
                      consecutive failures."
router(config)# copy running-config startup-config
```

Configuring Syslog as EEM Publisher

You can monitor syslog messages from the router.

Note The maximum number of searchable strings to monitor syslog messages is 10.

BEFORE YOU BEGIN

EEM should be available for registration by syslog.

The syslog daemon must be configured and executed.

Note The maximum number of searchable strings to monitor syslog messages is 10.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**event manager applet** *applet-name*	Registers an applet with EEM and enters applet configuration mode.
Step 3	**event syslog** [**tag** *tag*] {**occurs** *number* | **period** *seconds* | **pattern** *msg-text* | **priority** *priority*}	Monitors syslog messages and invokes the policy based on the search string in the policy. • The **tag** *tag* keyword-argument pair identifies this specific event when multiple events are included in the policy. • The **occurs** *number* keyword-argument pair specifies the number of occurrences. The range is from 1 to 65000. • The **period** *seconds* keyword-argument pair specifies the interval during which the event occurs. The range is from 1 to 4294967295. • The **pattern** *msg-text* keyword-argument pair specifies the matching regular expression. The pattern can contain character text, an environment variable, or a combination of the two. If the string contains embedded blanks, it is enclosed in quotation marks. • The **priority** *priority* keyword-argument pair specifies the priority of the syslog messages. If this keyword is not selected, all syslog messages are set at the informational priority level.
Step 4	**copy running-config startup-config**	(Optional) Saves this configuration change.

EXAMPLE

This example shows how to configure EEM as a publisher.

```
router# configure terminal
router (config-applet)# event manager applet abc
router (config-applet)# event syslog occurs 10
router (config-applet)# copy running-config startup-config
```

Verifying the Configuration

To display EEM configuration information, perform one of the following tasks.

Command	Purpose
show event manager environment [*variable-name* | **all**]	Displays information about the event manager environment variables.
show event manager event-types [*event* | **all** | **module** *slot*]	Displays information about the event manager event types.
show event manager history events [**detail**] [**maximum** *num-events*] [**severity** {**catastrophic** | **minor** | **moderate** | **severe**}]	Displays the history of events for all policies.
show event manager policy internal [*policy-name*] [**inactive**]	Displays information about the configured policies.
show event manager policy-state *policy-name*	Displays information about the policy state, including thresholds.
show event manager script system [*policy-name* | **all**]	Displays information about the script policies.
show event manager system-policy [**all**]	Displays information about the predefined system policies.
show running-config eem	Displays information about the running configuration for EEM.
show startup-config eem	Displays information about the startup configuration for EEM.

Configuration Examples

Note You must add the **event-default** action statement to the EEM policy, or EEM will not allow the CLI command to execute.

This example shows how to override the real_time clock.

```
event manager applet realtime override __real_time_clock
    action 1.0 syslog priority warnings msg Override policy real time clock
    action 1.1 policy-default
```

This example creates an EEM policy that allows the CLI to execute but triggers an SNMP notification when the user enters configuration mode on the router.

```
event manager applet TEST
    event cli match "conf t"
    action 1.0 snmp-trap strdata "Configuration change"
    action 2.0 event-default
```

This example shows how to correlate multiple events in an EEM policy and execute the policy based on a combination of the event triggers. In this example, the software triggers the EEM policy if one of the specified syslog patterns occurs within 120 seconds.

```
event manager applet eem-correlate
    event syslog tag one pattern "copy bootflash:* running-config.*"
    event syslog tag two pattern "copy run start"
    event syslog tag three pattern "hello"
    tag one or two or three happens 1 in 120
    action 1.0 reload module 1
```

Feature History

Table 4-2 Feature History for Embedded Event Manager

Feature Name	Release	Feature Information
Embedded Event Manager	Cisco CG-OS Release CG2(1)	Initial support of the feature on the CGR 1000 Series Routers.

Configuring Backhaul Manager

This chapter describes how to configure the Backhaul Manager to monitor backhauls in order to maximize backhaul uptime, and to take corrective behavior when a backhaul is down on the Cisco 1000 Series Connected Grid Routers (hereafter referred to as the Cisco CG-OS router).

This chapter includes the following sections:

Information About Backhaul Manager

When configured on the Cisco CG-OS router, the Backhaul Manager actively monitors the backhaul between the Cisco CG-OS router and the head-end router.

When a catastrophe affects the backhaul, the Backhaul Manager automatically initiates its configured policies to attempt to recover the backhaul. The first action taken is a reset of interfaces (such as cellular, WiMax, Ethernet) and tunnels on the backhaul. When a reset of the interfaces or tunnels does not restore the backhaul, then a reload of the Cisco CG-OS router occurs.

The following Backhaul Manager policies can be configured on all Cisco CG-OS router interfaces and tunnels.

- Admin-state–Ensures that the Cisco CG-OS router checks the admin-state of all interfaces and tunnels specified by the policy to determine if an administrator has mistakenly configured a shutdown of the interface. When the Cisco CG-OS software detects the shutdown down state, it generates an emergency level syslog event to alert the administrator of the interface or tunnel shutdown state. Using the CLI, the administrator can then enter the **no shutdown** command at the Interface command mode to resolve the issue.

- Backhaul flap–Defines thresholds for the number of allowed backhaul-down events (count) that can occur within a defined period (duration) on a backhaul before the Cisco CG-OS software generates a syslog event (see syslog Events, page 5-6).

Note To define actions to address the backhaul flap beyond reporting a syslog event, add those actions (such as backhaul rest or backhaul reload) to the script (see Defining Backhaul Manager Applets, Track Objects and Scheduler Script, page 5-5).

- Backhaul reset–Defines the period of time that a backhaul must be down before the Cisco CG-OS software resets specific interfaces or tunnels within the backhaul.
- Backhaul reload–When the backhaul does not recover after a backhaul reset and the backhaul remains down after the defined outage threshold expires, then the Cisco CG-OS router reloads. Additionally, this policy ensures that the threshold timer resets when a backhaul recovers before the threshold expires so that no reload of the Cisco CG-OS router occurs.

For detailed configuration steps and examples for the Backhaul Manager policies, see Configuring Backhaul Manager, page 5-2.

Prerequisites

The Backhaul Manager must be configured in the default VDC of the Cisco CG-OS router. No other VDCs are supported on the Cisco CG-OS router.

When you want to collect syslog events locally on the Cisco CG-OS router, you must enable syslog (see Chapter 2, “Configuring System Message Logging”).

Enable the Scheduler on the Cisco CG-OS router (see Defining Backhaul Manager Applets, Track Objects and Scheduler Script, page 5-5).

Guidelines and Limitations

None.

Default Settings

No preset values. The configuration examples indicate the recommended values.

Configuring Backhaul Manager

This section includes the following topics:

Defining Event Manager Environments

Defines environment and threshold policies that the Backhaul Manager can execute to monitor or reset interfaces or tunnels (connections) within the backhaul or to reload the Cisco CG-OS router.

BEFORE YOU BEGIN

Review the "Information About Backhaul Manager" section on page 5-1 and "Prerequisites" section on page 5-2.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**event manager environment bh_iflist** {*"interface slot/port"*| *"***tunnel** *number"***}** ...[*"interface slot/port"*| *"***tunnel** *number"***]**	Creates an environment variable named **bh_iflist**, that defines all the interfaces (such as cellular, Ethernet, or WiMax) or tunnels that the Backhaul Manager monitors (and resets, if necessary) within the backhaul that connects the Cisco CG-OS router and the head-end router. **Note**: Cisco recommends that you list all active interfaces and tunnels within the backhaul. Both the interface type and slot/port number must be enclosed in quotations as well as the tunnel and tunnel number. **Note**: Do not provide a space between the interface type and slot/port (such as "**cellular3/1**"). Likewise, define the tunnel and its number with no space (such as "**tunnel1**"). **Note**: Environment variables have a length limit of 39 characters. To ensure that you can define as many backhaul lists as necessary, the Cisco CG-OS software allows you to define multiple **bh_iflists** such as **bh_iflist1**, **bh_iflist2**, **bh_iflist3**, and so on. Later, the Cisco CG-OS software concatenates the lists.
Step 3	**event manager environment bh_flap_thresh_cnt** *value*	Creates an environment variable named **bh_flap_thresh_cnt** that monitors the backhaul flaps on the Cisco CG-OS router and generates a backhaul-down syslog event when the backhaul-down events exceed the defined count (**cnt** *value*) within a certain duration. *value*–Enter any numeric value; however, it must be enclosed with quotation marks. **Note**: The **event manager environment bh_flap_thresh_duration** command in Step 4 defines the duration.

	Command	Purpose
Step 4	**event manager environment bh_flap_thresh_duration** *"value"*	Defines the maximum period of time (in mins) that a backhaul can remain down before the Cisco CG-OS software generates a backhaul-down syslog event. *value*–Enter any numeric value; however, it must be enclosed with quotation marks.
Step 5	**event manager environment bh_down_reset_thresh "***value"*	Creates an environment variable named **bh_down_reset_thresh** that defines the maximum allowed backhaul outage (in mins) before the Cisco CG-OS software resets defined interfaces and tunnels on the backhaul. *value*–Enter any numeric value; however, it must be enclosed with quotation marks. **Note**: The **event manager environment bh_iflist** command in Step 6 defines which interfaces and tunnels the Cisco CG-OS software resets.
Step 6	**event manager environment bh_iflist {**"*interface slot/port*"**|** "**tunnel** *number*"**}** ...**[**"*interface slot/port*"**|** "**tunnel** *number*"**]**	Creates an environment variable named **bh_iflist** that defines the interfaces and tunnels that the Cisco CG-OS software resets when the **bh_down_reset_thresh** value set in Step 5 is exceeded.
Step 7	**event manager environment bh_down_reload_thresh "***value"*	Creates an environment variable named **bh_down_reload_thresh** that defines the maximum allowed backhaul outage (in mins) before the Cisco CG-OS software reloads the Cisco CG-OS router. *value*–Enter any numeric value; however, it must be enclosed with quotation marks.
Step 8	**copy running-config startup-config**	(Optional) Saves this configuration change.

EXAMPLE

This example shows how to configure the supported Backhaul Manager policies to monitor the backhaul between the Cisco CG-OS router and a head-end router.

```
router# configure terminal
router (config)# event manager environment bh_iflist "cellular3/1 wimax5/1"
router (config)# event manager environment bh_iflist1 "tunnel10 tunnel20"
router (config)# event manager environment bh_flap_thresh_cnt "10"
router (config)# event manager environment bh_flap_thresh_duration "120"
router (config)# event manager environment bh_down_reset_thresh "360"
router (config)# event manager environment bh_down_reload_thresh "720"
router (config)# copy running-config startup-config
```

Defining Backhaul Manager Applets, Track Objects and Scheduler Script

The script reads and applies all the defined event manager environments each time it is invoked by either the scheduler or an event manager environment variable.

BEFORE YOU BEGIN

Define all the event manager environments listed in the Defining Event Manager Environments section.

DETAILED STEPS

At the Cisco CG-OS router command-line prompt, enter the following commands.

Note For more details on the commands and their syntax, refer to the Command Lookup Tool on Cisco.com.

To define the router to monitor (in this case the loopback address of the head-end router), enter the following commands.

```
router(config)# track 1 ip route 20.0.0.1/32 reachability
router(config-track)# delay down 120
router(config-track)# delay up 120
router(config-track)# exit
router(config)# event manager environment bhmgr_track_obj_instance "1"
```

To define the objects to track and report backhaul up and down states, enter the following commands.

```
router(config)# event manager applet bhmgrbhdown
router(config-applet)# event track 1 state down
router(config-applet)# action 1.0 syslog priority critical msg Backhaul is down
router(config-applet)# action 2.0 cli tclsh bootflash:bhmgr.tcl bhmgr_process_bh_down
router(config-applet)# action 3.0 cli command maximum-timeout
router(config-applet)# exit
router(config)# event manager applet bhmgrbhup
router(config-applet)# event track 1 state up
router(config-applet)# action 1.0 syslog priority errors msg Backhaul is up
router(config-applet)# action 2.0 cli tclsh bootflash:bhmgr.tcl bhmgr_process_bh_up
router(config-applet)# action 3.0 cli command maximum-timeout
router(config-applet)# exit
```

Note Object tracking ignores any intermediate state changes before the delay timer expires. The address specified in the **ip route** command is the loopback address of the head-end router and the *delay up* and *down* values are noted in seconds.

To define a job (a set of commands or tcl script) to be executed on a regular schedule enter the following commands.

```
router(config)# feature scheduler
router(config)# scheduler job name bhmgr_monitor
router(config-job)# tclsh bootflash:/bhmgr.tcl bhmgr_monitor
router(config-job)# exit
router(config)# scheduler schedule name bhmgr_monitor_schedule
router(config-job)# job name bhmgr_monitor
router(config-job)# time start now repeat 10
router(config-job)# exit
```

syslog Events

System message logging allows you to configure the destination device of the system messages and to filter system messages by severity level. For more information on the syslog, see Configuring System Message Logging.

Listed below is an example of the critical events reported to the syslog when a backhaul down condition occurs.

```
2012 Jan 6 17:07:31 cgr1000ca %$ VDC-1 %$ %EEM_ACTION-2-CRIT: bhmgr: Backhaul i/f tunnel1
is admin down. Pl *no shut* it immediately.

2012 Jan 6 17:20:07 cgr1000 %$ VDC-1 %$ %EEM_ACTION-2-CRIT: bhmgr: Backhaul is down

2012 Jan 6 17:21:44 cgr1000 %$ VDC-1 %$ %EEM_ACTION-2-CRIT: bhmgr: 3 mins to BH Reset

2012 Jan 6 17:21:44 cgr1000 %$ VDC-1 %$ %EEM_ACTION-2-CRIT: bhmgr: 8 mins to RELOAD

2012 Jan 6 17:23:46 cgr1000 %$ VDC-1 %$ %EEM_ACTION-2-CRIT: bhmgr: 1 mins to BH Reset

2012 Jan 6 17:23:46 cgr1000 %$ VDC-1 %$ %EEM_ACTION-2-CRIT: bhmgr: 6 mins to RELOAD

2012 Jan 6 17:25:48 cgr1000 %$ VDC-1 %$ %EEM_ACTION-2-CRIT: bhmgr: BH Reset policy hit

2012 Jan 6 17:25:59 cgr1000 %$ VDC-1 %$ %EEM_ACTION-2-CRIT: bhmgr: 4 mins to RELOAD

2012 Jan 6 17:28:01 cgr1000 %$ VDC-1 %$ %EEM_ACTION-2-CRIT: bhmgr: 2 mins to RELOAD

2012 Jan 6 17:30:03 cgr1000 %$ VDC-1 %$ %EEM_ACTION-2-CRIT: bhmgr: 0 mins to RELOAD

2012 Jan 6 17:32:05 cgr1000 %$ VDC-1 %$ %EEM_ACTION-0-EMERG: BH RELOAD policy hit.
Performing reload in 30 seconds
```

Verifying the Configuration

To display event manager configuration information, enter the following commands.

Command	Purpose
show event manager environment [*variable-name* | **all**]	Displays information about the event manager environment variables.
show logging logfile | grep -i bhmgr	Displays all the logged syslog events for the Backhaul Manager.

EXAMPLE

Information similar to the information below displays when you enter the **show event manager environment all** command.

```
router (config)# show event manager environment all
bh_down_reload_thresh : 720
bh_down_reset_thresh : 360
bh_flap_thresh_cnt : 10
bh_flap_thresh_duration : 120
bh_iflist : cellular3/1 wimax5/1
bh_iflist1 : tunnel10 tunnel20
bhmgr_track_obj_instance : 1
```

Configuration Example

To configure the Backhaul Manager policies to monitor the backhaul between the Cisco CG-OS router and a head-end router, enter the following commands.

```
router# configure terminal
router (config)# event manager environment bh_iflist "cellular3/1 wimax5/1"
router (config)# event manager environment bh_iflist1 "tunnel10 tunnel20"
router (config)# event manager environment bh_flap_thresh_cnt "10"
router (config)# event manager environment bh_flap_thresh_duration "120"
router (config)# event manager environment bh_down_reset_thresh "360"
router (config)# event manager environment bh_down_reload_thresh "720"
router (config)# copy running-config startup-config
```

After defining the Backhaul Manager policies, enter the following commands to define the script.

```
router(config)# track 1 ip route 20.0.0.1/32 reachability
router(config-track)# delay down 120
router(config-track)# delay up 120
router(config-track)# exit
router(config)# event manager environment bhmgr_track_obj_instance "1"
router(config)# event manager applet bhmgrbhdown
router(config-applet)# event track 1 state down
router(config-applet)# action 1.0 syslog priority critical msg Backhaul is down
router(config-applet)# action 2.0 cli tclsh bootflash:bhmgr.tcl bhmgr_process_bh_down
router(config-applet)# action 3.0 cli command maximum-timeout
router(config-applet)# exit
router(config)# event manager applet bhmgrbhup
router(config-applet)# event track 1 state up
router(config-applet)# action 1.0 syslog priority errors msg Backhaul is up
router(config-applet)# action 2.0 cli tclsh bootflash:bhmgr.tcl bhmgr_process_bh_up
router(config-applet)# action 3.0 cli command maximum-timeout
router(config-applet)# exit
router(config)# feature scheduler
router(config)# scheduler job name bhmgr_monitor
router(config-job)# tclsh bootflash:/bhmgr.tcl bhmgr_monitor
router(config-job)# exit
router(config)# scheduler schedule name bhmgr_monitor_schedule
router(config-job)# job name bhmgr_monitor
router(config-job)# time start now repeat 10
router(config-job)# exit
```

Feature History

Table 5-1 Feature History for Backhaul Manager

Feature Name	Release	Feature Information
Backhaul Manager	Cisco CG-OS Release CG1(1)	Initial support of the feature on the CGR 1000 Series Routers.