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.