CHAPTER 1

Configuring System Message Logging

This chapter describes how to configure system message logging on the switch.

This chapter includes the following sections:

Information About System Message Logging

You can use system message logging to control the destination and to filter the severity level of messages that system processes generate. You can configure logging to terminal sessions, a log file, and syslog servers on remote systems.

By default, the switch outputs messages to terminal sessions. For information about configuring logging to terminal sessions, see the "Configuring System Message Logging to Terminal Sessions" section on page 1-2.

By default, the switch logs system messages to a log file. For information about configuring logging to a file, see the "Configuring System Message Logging to a File" section on page 1-3.

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

Table 1-1 System Message Severity Levels

Level	Description
0 – emergency	System unusable
1 – alert	Immediate action needed
2 – critical	Critical condition
3 – error	Error condition
4 – warning	Warning condition
5 – notification	Normal but significant condition

Table 1-1 System Message Severity Levels (continued)

Level	Description
6 – informational	Informational message only
7 – debugging	Appears during debugging only

The switch 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 should be logged based on the facility that generated the message and its severity level. For information about configuring the severity level by module and facility, see the "Configuring Module and Facility Messages Logged" section on page 1-4.

syslog Servers

syslog servers run on remote systems that are configured to log system messages based on the syslog protocol. You can configure up to three syslog servers. For information about configuring syslog servers, see the "Configuring syslog Servers" section on page 1-5.

To support the same configuration of syslog servers on all switches in a fabric, you can use the Cisco Fabric Services (CFS) to distribute the syslog server configuration. For information about distributing the syslog server configuration, see the "Configuring syslog Server Configuration Distribution" section on page 1-7.

Note When the switch first initializes, messages are sent to syslog servers only after the network is initialized.

Configuring System Message Logging

This section includes the following topics:

Note If you are familiar with the Cisco IOS CLI, be aware that the Cisco NX-OS commands for this feature might differ from the Cisco IOS commands that you would use.

Configuring System Message Logging to Terminal Sessions

You can configure the switch to log messages by their severity level to console, Telnet, and SSH sessions.

By default, logging is enabled for terminal sessions. To configure the switch to log messages, perform this task:

	Command	Purpose
Step 1	`switch# configure terminal`	Enters configuration mode.
Step 2	`switch(config)# logging console [severity-level]`	Enables the switch to log messages to the console session based on a specified severity level or higher. Severity levels, which can range from 0 to 7, are listed in Table 1-1. If the severity level is not specified, the default of 2 is used.
	`switch(config)# no logging console [severity-level]`	Disables the switch's ability to log messages to the console.
Step 3	`switch(config)# show logging console`	(Optional) Displays the console logging configuration.
Step 4	`switch(config)# logging monitor [severity-level]`	Enables the switch to log messages to the monitor based on a specified severity level or higher. The configuration applies to Telnet and SSH sessions. Severity levels, which can range from 0 to 7, are listed in Table 1-1. If the severity level is not specified, the default of 2 is used.
	`switch(config)# no logging monitor [severity-level]`	Disables logging messages to telnet and SSH sessions.
Step 5	`switch(config)# show logging monitor`	(Optional) Displays the monitor logging configuration.
Step 6	`switch(config)# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

The following example shows how to configure a switch to log messages:

```
switch# configure terminal
switch(config)# logging console 3
switch(config)# no logging console
switch(config)# show logging console
switch(config)# logging monitor 3
switch(config)# no logging monitor
switch(config)# show logging monitor
switch(config)# copy running-config startup-config
```

Configuring System Message Logging to a File

You can configure the switch 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 the "Displaying and Clearing Log Files" section on page 1-8.

To configure the switch to log system messages to a file, perform this task:

	Command	Purpose
Step 1	`switch# configure terminal`	Enters configuration mode.
Step 2	`switch(config)# logging logfile` *logfile-name severity-level* [**size** *bytes*]	Configures the name of the log file used to store system messages and the minimum severity level to log. You can optionally specify a maximum file size. The default severity level is 5 and the file size is 10485760. Severity levels are listed in Table 1-1. The file size is from 4096 to 10485760 bytes.
	`switch(config)# no logging logfile` [*logfile-name severity-level* [**size** *bytes*]]	Disables logging to the log file.
Step 3	`switch(config)# show logging info`	(Optional) Displays the logging configuration.
Step 4	`switch(config)# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

The following example shows how to configure a switch to log system messages to a file:

```
switch# configure terminal
switch(config)# logging logfile my_log size 6
switch(config)# no logging logfile
switch(config)# show logging info
switch(config)# copy running-config startup-config
```

Configuring Module and Facility Messages Logged

To configure the severity level and time-stamp units of messages logged by modules and facilities, perform this task:

	Command	Purpose
Step 1	`switch# configure terminal`	Enters configuration mode.
Step 2	`switch(config)# logging module` [*severity-level*]	Enables module log messages that have the specified severity level or higher. Severity levels, which range from 0 to 7, are listed in Table 1-1. If the severity level is not specified, the default of 5 is used.
	`switch(config)# no logging module` [*severity-level*]	Disables module log messages.
Step 3	`switch(config)# show logging module`	(Optional) Displays the module logging configuration.

	Command	Purpose
Step 4	`switch(config)# 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 1-1. To apply the same severity level to all facilities, use the **all** facility. For defaults, see the **show logging level** command.
	`switch(config)# no logging level [facility severity-level]`	Resets the logging severity level for the specified facility to its default level. If you do not specify a facility and severity level, the switch resets all facilities to their default levels.
Step 5	`switch(config)# show logging level [facility]`	(Optional) Displays the logging level configuration and the system default level by facility. If you do not specify a facility, the switch displays levels for all facilities.
Step 6	`switch(config)# logging timestamp {microseconds | milliseconds | seconds}`	Sets the logging time-stamp units. By default, the units are seconds.
	`switch(config)# no logging timestamp {microseconds | milliseconds | seconds}`	Resets the logging time-stamp units to the default of seconds.
Step 7	`switch(config)# show logging timestamp`	(Optional) Displays the logging time-stamp units configured.
Step 8	`switch(config)# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

The following example shows how to configure the severity level and time-stamp units of messages:

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

Configuring syslog Servers

You can configure up to three syslog servers that reference remote systems where you want to log system messages.

For information about distributing the syslog configuration on the fabric, see the "Configuring syslog Server Configuration Distribution" section on page 1-7.

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 <five tab characters> action
```

Table 1-2 describes the syslog fields that you can configure.

Table 1-2 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 host name preceded by the at sign (@), or 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/log/myfile.log
```

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

```
$ touch /var/log/myfile.log
$ chmod 666 /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~
```

To configure syslog servers, perform this task:

	Command	Purpose
Step 1	`switch# configure terminal`	Enters configuration mode.
Step 2	`switch(config)# logging server` *host* [*severity-level* [*facility*]]	Configures a syslog server at the specified host name or IPv4 or IPv6 address. You can limit logging of messages with a minimum severity level and for a specific facility. Severity levels, which range from 0 to 7, are listed in Table 1-1. The default outgoing facility is local7.
	`switch(config)# no logging server` *host*	Removes the logging server for the specified host.
Step 3	Repeat Step 2 for up to three syslog servers.	
Step 4	`switch(config)# show logging server`	(Optional) Displays the syslog server configuration.
Step 5	`switch(config)# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

The following example shows how to configure a syslog server:

```
switch# configure terminal
switch(config)# logging server 172.28.254.254 5 local3
switch(config)# show logging server
switch(config)# copy running-config startup-config
```

Configuring syslog Server Configuration Distribution

You can distribute the syslog server configuration to other switches in the network by using the Cisco Fabric Services (CFS) infrastructure.

For more information about CFS, see the "Information About CFS" section on page 1-1.

After you enable syslog server configuration distribution, you can modify the syslog server configuration and view the pending changes before committing the configuration for distribution. As long as distribution is enabled, the switch maintains pending changes to the syslog server configuration.

Note If the switch is restarted, the syslog server configuration changes that are kept in volatile memory may be lost.

To configure syslog server configuration distribution, perform this task:

	Command	Purpose
Step 1	`switch# configure terminal`	Enters configuration mode.
Step 2	`switch(config)# logging distribute`	Enables distribution of syslog server configuration to network switches using the CFS infrastructure. By default, distribution is disabled.
	`switch(config)# no logging distribute`	Disables distribution of syslog server configuration to network switches using the CFS infrastructure. You cannot disable distribution when configuration changes are pending. See the **logging commit** and **logging abort** commands. By default, distribution is disabled.
Step 3	Enter syslog server configuration commands.	See the "Configuring syslog Servers" section on page 1-5.
Step 4	`switch(config)# show logging pending`	(Optional) Displays the pending changes to the syslog server configuration.
Step 5	`switch(config)# show logging pending-diff`	(Optional) Displays the differences from the current syslog server configuration to the pending changes of the syslog server configuration.

	Command	Purpose
Step 6	`switch(config)# logging commit`	Commits the pending changes to the syslog server configuration for distribution to the switches in the fabric.
	`switch(config)# logging abort`	Cancels the pending changes to the syslog server configuration.
Step 7	`switch(config)# show logging internal info`	(Optional) Displays information about the current state of syslog server distribution and the last action taken.
Step 8	`switch(config)# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Displaying and Clearing Log Files

To display or clear messages in the log file and the NVRAM , perform this task:

	Command	Purpose
Step 1	`switch# 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.
Step 2	`switch# 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, the current time is used. You enter three characters for the month time field, and digits for the year and day time fields.
Step 3	`switch# show logging nvram` [**last** *number-lines*]	Displays the messages in the NVRAM. To limit the number of lines displayed, you can enter the last number of lines to display. You can specify from 1 to 100 for the last number of lines.
Step 4	`switch# clear logging logfile`	Clears the contents of the log file.
Step 5	`switch# clear logging nvram`	Clears the logged messages in NVRAM.

The following example shows how to display or clear messages in a log file:

```
switch# show logging last 40
switch# show logging logfile start-time 2007 nov 1 15:10:0
switch# show logging nvram last 10
switch# clear logging logfile
switch# clear logging nvram
```

Verifying System Message Logging Configuration

To display system message logging configuration information, perform one of the following tasks:

Command	Purpose
show logging console	Displays the console logging configuration.
show logging info	Displays the logging configuration.
show logging internal info	Displays the syslog distribution information.
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 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 pending	Displays the syslog server pending distribution configuration.
show logging pending-diff	Displays the syslog server pending distribution configuration differences.
show logging server	Displays the syslog server configuration.
show logging session	Displays the logging session status.
show logging status	Displays the logging status.
show logging timestamp	Displays the logging time-stamp units configuration.

System Message Logging Example Configuration

The following 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 distribute
  logging server 172.28.254.253
  logging server 172.28.254.254 5 local3
  logging commit
  copy running-config startup-config
```

Default Settings

Table 1-3 lists the default settings for system message logging parameters.

Table 1-3 Default System Message Logging Parameters

Parameters	Default
Console logging	Enabled at severity level 2
Monitor logging	Enabled at severity level 2
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
syslog server configuration distribution	Disabled