CHAPTER 28

Configuring System Message Logging

This chapter describes how to configure system message logging on the Catalyst 2960 switch.

Note For complete syntax and usage information for the commands used in this chapter, see the *Cisco IOS Configuration Fundamentals Command Reference, Release 12.2* **Documentation > Cisco IOS Software 12.2 Mainline Command References**

This chapter consists of these sections:

- Understanding System Message Logging, page 28-1

  Configuring System Message Logging, page 28-2

  Displaying the Logging Configuration, page 28-13

Caution Logging messages to the console at a high rate can cause high CPU utilization and adversely affect how the switch operates.

Understanding System Message Logging

By default, a switch sends the output from system messages and **debug** privileged EXEC commands to a logging process. The logging process controls the distribution of logging messages to various destinations, such as the logging buffer, terminal lines, or a UNIX syslog server, depending on your configuration. The process also sends messages to the console.

The syslog format is compatible with 4.3 BSD UNIX.

When the logging process is disabled, messages are sent only to the console. The messages are sent as they are generated, so message and debug output are interspersed with prompts or output from other commands. Messages appear on the console after the process that generated them has finished.

You can set the severity level of the messages to control the type of messages displayed on the consoles and each of the destinations. You can time-stamp log messages or set the syslog source address to enhance real-time debugging and management. For information on possible messages, see the system message guide for this release.

You can access logged system messages by using the switch command-line interface (CLI) or by saving them to a properly configured syslog server. The switch software saves syslog messages in an internal buffer.

You can remotely monitor system messages by viewing the logs on a syslog server or by accessing the switch through Telnet or through the console port.

Configuring System Message Logging

-
-
-
- , page 28-5 (optional)
- Synchronizing Log Messages, page 28-6 (optional)
- Enabling and Disabling Time Stamps on Log Messages, page 28-7 (optional)

  Enabling and Disabling Sequence Numbers in Log Messages, page 28-8 (optional)

  Defining the Message Severity Level, page 28-8 (optional)

  Limiting Syslog Messages Sent to the History Table and to SNMP, page 28-10 (optional)

  Enabling the Configuration-Change Logger, page 28-10 (optional)

  Configuring UNIX Syslog Servers, page 28-12 (optional)

System Log Message Format

System log messages can contain up to 80 characters and a percent sign (%), which follows the optional sequence number or time-stamp information, if configured. Messages appear in this format:

seq no:timestamp: %facility-severity-MNEMONIC:description

service sequence-numbers **service timestamps log datetime** **service timestamps log datetime** [**localtime**] [ ] [**show-timezone** **service timestamps log uptime**

Table 28-1 System Log Message Elements

Element	Description
	"Enabling and Disabling Sequence Numbers in Log Messages" section on page 28-8.
formats: *mm/dd hh:mm:ss* *hh:mm:ss* *d h*	**datetime | log**
facility	
severity	
MNEMONIC	
description	

This example shows a partial switch system message:

```
00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet0/2, changed state to up
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed
state to down 2
*Mar  1 18:46:11: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
18:47:02: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
*Mar  1 18:48:50.483 UTC: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
```

Default System Message Logging Configuration

Default System Message Logging Configuration

Feature	Default Setting
	Debugging (and numerically lower levels; see Table 28-3 on page 28-9).
Logging file configuration	No filename specified.
Logging buffer size	4096 bytes.
Logging history size	1 message.

Default System Message Logging Configuration (continued)

Time stamps	Disabled.
Synchronous logging	Disabled.
Logging server	Disabled.
Syslog server IP address	None configured.
Configuration change logger	Disabled
Server facility	Local7 (see Table 28-4 on page 28-13).
Server severity	Informational (and numerically lower levels; see Table 28-3 on page 28-9).

Disabling Message Logging

	Command	Purpose
Step 1		
Step 2		
Step 3		
Step 4		Verify your entries.
Step 5		(Optional) Save your entries in the configuration file.

logging synchronous

Return. For more information, see the "Synchronizing Log Messages" section on page 28-6.

To re-enable message logging after it has been disabled, use the global configuration command.

Setting the Message Display Destination Device

	Command	Purpose
Step 1		
Step 2	*size*	**Note** Do not make the buffer size too large because the switch could run out of memory for other tasks. Use the privileged EXEC command to view the free processor memory on the switch. However, this value is the maximum available, and the buffer size should be set to this amount.
		Log messages to a UNIX syslog server host. For , specify the name or IP address of the host to be used as the syslog server. To build a list of syslog servers that receive logging messages, enter this command more than once. For complete syslog server configuration steps, see the "Configuring UNIX Syslog Servers" section on page 28-12.
	logging file flash: *max-file-size min-file-size severity-level-number | type*]	Store log messages in a file in flash memory. For *filename*, enter the log message filename. (Optional) For *max-file-size, s*pecify the maximum logging file size. The range is 4096 to 2147483647. The default is 4096 bytes. (Optional) For *min-file-size, s*pecify the minimum logging file size. The range is 1024 to 2147483647. The default is 2048 bytes. (Optional) For *severity-level-number | type,*
Step 6		
Step 7		
Step 8		

Synchronizing Log Messages

solicited device output and prompts. After the unsolicited messages appear, the console again displays the user prompt.

Beginning in privileged EXEC mode, follow these steps to configure synchronous logging. This procedure is optional.

	Enter global configuration mode.
[|] [ ]	Specify the line to be configured for synchronous logging of messages. Use the keyword for configurations that occur through the switch console port. Use the command to specify which vty lines are to have synchronous logging enabled. You use a vty connection for configurations that occur through a Telnet session. The range of line numbers is from 0 to 15. You can change the setting of all 16 vty lines at once by entering: **line vty 0 15** **line vty 2**

	Command	Purpose
Step 3		• • •
Step 4		
Step 5		
Step 6		

Enabling and Disabling Time Stamps on Log Messages

	Command	Purpose
Step 1		
Step 2		
Step 3		
Step 4		
Step 5		

Enabling and Disabling Sequence Numbers in Log Messages

	Command	Purpose
Step 1		
Step 2		
Step 3		
Step 4		
Step 5		

Defining the Message Severity Level

	Command	Purpose
Step 1		
Step 2		
Step 3		

	Command	Purpose
Step 4		
Step 5		
Step 6		
Step 7		

Note

Table 28-3 Message Logging Level Keywords

Level Keyword	Level	Description	Syslog Definition
			LOG_EMERG
	1	Immediate action needed	LOG_ALERT
	2	Critical conditions	LOG_CRIT
	3	Error conditions	LOG_ERR
	4	Warning conditions	LOG_WARNING
	5	Normal but significant condition	LOG_NOTICE
	6	Informational messages only	LOG_INFO
	7	Debugging messages	LOG_DEBUG

-
-
-

Limiting Syslog Messages Sent to the History Table and to SNMP

	Command	Purpose
Step 1		
Step 2	[1]	*level*
	number	

1. Table 28-3 lists the level keywords and severity level. For SNMP usage, the severity level values increase by 1. For example, *emergencies* equal 1, not 0, and *critical*

Enabling the Configuration-Change Logger

{ | *number* [*end-number*] | *username* [*number*] *number* [*end-number*] | } [ ] privileged EXEC command to display the complete configuration log or the log for specified parameters.

The default is that configuration logging is disabled.

For information about the commands, see the *Cisco IOS Configuration Fundamentals and Network Management Command Reference, Release 12.3 T*

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_command_reference_chapter09186a00801a8086.html#wp1114989

Beginning in privileged EXEC mode, follow these steps to enable configuration logging:

This example shows how to enable the configuration-change logger and to set the number of entries in the log to 500.

```
Switch(config)# archive
                        log config
                                logging enable
                                logging size 500
                                end
```

```
        show archive log config all
 idx    sess           user@line      Logged command
   38     11   unknown user@vty3     |no aaa authorization config-commands
   39     12   unknown user@vty3     |no aaa authorization network default group radius
   40     12   unknown user@vty3     |no aaa accounting dot1x default start-stop group
radius
   41     13   unknown user@vty3     |no aaa accounting system default
   42     14           temi@vty4     |interface GigabitEthernet4/0/1
   43     14           temi@vty4     | switchport mode trunk
   44     14           temi@vty4     | exit
   45     16           temi@vty5     |interface FastEthernet5/0/1
   46     16           temi@vty5     | switchport mode trunk
   47     16           temi@vty5     | exit
```

Configuring UNIX Syslog Servers

Logging Messages to a UNIX Syslog Daemon

Note

Step 1

```
local7.debug /usr/adm/logs/
```

local7

debug

```
$ touch /var/log/
$ chmod 666 /var/log/
```

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

Configuring the UNIX System Logging Facility

	Command	Purpose
Step 1		
Step 2		

	Command	Purpose
Step 3		
Step 4		
Step 5		
Step 6		
Step 7		

facilities, consult the operator's manual for your UNIX operating system.

Table 28-4 Logging Facility-Type Keywords

Facility Type Keyword	Description
kern	Kernel
	Locally defined messages
	Line printer system
	Mail system
	USENET news
sys9-14	
syslog	
user	
uucp	

Displaying the Logging Configuration