



Configuring System Message Logging

This chapter describes how to configure system message logging on the Cisco Industrial Ethernet 2000U Series (IE 2000U) and Connected Grid Switches, hereafter referred to as *switch*.



Note

For complete syntax and usage information for the commands used in this chapter, see the documents listed in the [“Related Documents”](#) section on page 13-17.

This chapter consists of these sections:

- [Information About System Message Logging, page 13-1](#)
- [Prerequisites, page 13-3](#)
- [Guidelines and Limitations, page 13-3](#)
- [Default Settings, page 13-3](#)
- [Configuring System Message Logging, page 13-3](#)
- [Verifying the Configuration, page 13-16](#)
- [Configuration Example, page 13-16](#)
- [Related Documents, page 13-17](#)
- [Feature History, page 13-18](#)

Information About 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.



Note

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, [Cisco System Messages](#).

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.

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

The part of the message preceding the percent sign depends on the setting of the **service sequence-numbers**, **service timestamps log datetime**, **service timestamps log datetime [localtime] [msec] [show-timezone]**, or **service timestamps log uptime** global configuration command.

[Table 13-1](#) describes the elements of syslog messages.

Table 13-1 System Log Message Elements

Element	Description
<i>seq no:</i>	Stamps log messages with a sequence number only if the service sequence-numbers global configuration command is configured. For more information, see the “ Enabling and Disabling Sequence Numbers in Log Messages ” section on page 13-9.
<i>timestamp</i> formats: <i>mm/dd hh:mm:ss</i> or <i>hh:mm:ss</i> (short uptime) or <i>d h</i> (long uptime)	Date and time of the message or event. This information appears only if the service timestamps log [datetime log] global configuration command is configured. For more information, see the “ Enabling and Disabling Time Stamps on Log Messages ” section on page 13-8.
<i>facility</i>	The facility to which the message refers (for example, SNMP, SYS, and so forth). For a list of supported facilities, see Table 13-3 on page 13-15.
<i>severity</i>	Single-digit code from 0 to 7 that is the severity of the message. For a description of the severity levels, see Table 13-2 on page 13-10.
<i>MNEMONIC</i>	Text string that uniquely describes the message.
<i>description</i>	Text string containing detailed information about the event being reported.

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)
```

Prerequisites

Review the “[Information About System Message Logging](#)” section on page 13-1.

Guidelines and Limitations



Caution

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

Default Settings

Feature	Default Setting
System message logging to the console	Enabled.
Console severity	Debugging (and numerically lower levels; see Table 13-2 on page 13-10).
Logging file configuration	No filename specified.
Logging buffer size	4096 bytes.
Logging history size	1 message.
Time stamps	Disabled.
Synchronous logging	Disabled.
Logging server	Disabled.
Syslog server IP address	None configured.
Server facility	Local7 (see Table 13-3 on page 13-15).
Server severity	Informational (and numerically lower levels; see Table 13-2 on page 13-10).

Configuring System Message Logging

- [Disabling Message Logging, page 13-4](#) (optional)
- [Setting the Message Display Destination Device, page 13-5](#) (optional)
- [Synchronizing Log Messages, page 13-6](#) (optional)
- [Enabling and Disabling Time Stamps on Log Messages, page 13-8](#) (optional)
- [Enabling and Disabling Sequence Numbers in Log Messages, page 13-9](#) (optional)

- [Defining the Message Severity Level, page 13-9](#) (optional)
- [Limiting Syslog Messages Sent to the History Table and to SNMP, page 13-11](#) (optional)
- [Enabling the Configuration-Change Logger, page 13-13](#) (optional)
- [Configuring UNIX Syslog Servers, page 13-14](#) (optional)

Disabling Message Logging

Message logging is enabled by default. It must be enabled to send messages to any destination other than the console. When enabled, log messages are sent to a logging process, which logs messages to designated locations asynchronously to the processes that generated the messages.

BEFORE YOU BEGIN

Disabling the logging process can slow down the switch because a process must wait until the messages are written to the console before continuing. When the logging process is disabled, messages appear on the console as soon as they are produced, often appearing in the middle of command output.

The **logging synchronous** global configuration command also affects the display of messages to the console. When this command is enabled, messages appear only after you press Return. For more information, see the [“Synchronizing Log Messages” section on page 13-6](#).

DETAILED STEPS

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	no logging console	Disable message logging.
Step 3	end	Return to privileged EXEC mode.
Step 4	show running-config or show logging	Verify your entries.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

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

EXAMPLE

```
Switch(config)# no logging console
Switch(config)# end
```

Setting the Message Display Destination Device

If message logging is enabled, you can send messages to specific locations in addition to the console. The **logging buffered** global configuration command copies logging messages to an internal buffer. The buffer is circular, so newer messages overwrite older messages after the buffer is full. To display the messages that are logged in the buffer, use the **show logging** privileged EXEC command. The first message displayed is the oldest message in the buffer. To clear the contents of the buffer, use the **clear logging** privileged EXEC command.

BEFORE YOU BEGIN

If message logging is disabled, use the **logging on** global configuration command to re-enable it.

DETAILED STEPS

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	logging buffered <i>[size]</i>	<p>Log messages to an internal buffer on the switch. The default buffer size is 4096. The range is 4096 to 2147483647 bytes.</p> <p>If the switch fails, the log file is lost unless you previously saved it to Flash memory. See Step 4.</p> <p>Note Do not make the buffer size too large because the switch could run out of memory for other tasks. Use the show memory privileged EXEC command to view the free processor memory on the switch. However, this value is the maximum available, and the buffer size should <i>not</i> be set to this amount.</p>
Step 3	logging <i>host</i>	<p>Log messages to a UNIX syslog server host.</p> <p>For <i>host</i>, specify the name or IP address of the host to be used as the syslog server.</p> <p>To build a list of syslog servers that receive logging messages, enter this command more than once.</p> <p>For complete syslog server configuration steps, see the “Configuring UNIX Syslog Servers” section on page 13-14.</p>

	Command	Purpose
Step 4	logging file flash: <i>filename</i> [<i>max-file-size</i> [<i>min-file-size</i>]] [<i>severity-level-number</i> <i>type</i>]	Store log messages in a file in flash memory. <ul style="list-style-type: none"> For <i>filename</i>, enter the log message filename. (Optional) For <i>max-file-size</i>, specify the maximum logging file size. The range is 4096 to 2147483647. The default is 4096 bytes. (Optional) For <i>min-file-size</i>, specify the minimum logging file size. The range is 1024 to 2147483647. The default is 2048 bytes. (Optional) For <i>severity-level-number</i> <i>type</i>, specify either the logging severity level or the logging type. The severity range is 0 to 7. For a list of logging type keywords, see Table 13-2 on page 13-10. By default, the log file receives debugging messages and numerically lower levels.
Step 5	end	Return to privileged EXEC mode.
Step 6	terminal monitor	Log messages to a nonconsole terminal during the current session. Terminal parameter-setting commands are set locally and do not remain in effect after the session has ended. You must perform this step for each session to see the debugging messages.
Step 7	show running-config	Verify your entries.
Step 8	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To disable logging to the console, use the **no logging console** global configuration command. To disable logging to a file, use the **no logging file** [*severity-level-number* | *type*] global configuration command.

EXAMPLE

The following example shows how to enable standard system logging to the local syslog buffer:

```
Switch(config)# logging buffered
```

Synchronizing Log Messages

You can synchronize unsolicited messages and **debug** privileged EXEC command output with solicited device output and prompts for a specific console port line or virtual terminal line. You can identify the types of messages to be output asynchronously based on the level of severity. You can also configure the maximum number of buffers for storing asynchronous messages for the terminal after which messages are dropped.

When synchronous logging of unsolicited messages and **debug** command output is enabled, unsolicited device output appears on the console or printed after solicited device output appears or is printed. Unsolicited messages and **debug** command output appears on the console after the prompt for user input is returned. Therefore, unsolicited messages and **debug** command output are not interspersed with solicited device output and prompts. After the unsolicited messages appear, the console again displays the user prompt.

BEFORE YOU BEGIN

**Caution**

By configuring abnormally large message queue limits and setting the terminal to "terminal monitor" on a terminal that is accessible to intruders, you expose yourself to "denial of service" attacks. An intruder could carry out the attack by putting the terminal in synchronous output mode, making a Telnet connection to a remote host, and leaving the connection idle. This could cause large numbers of messages to be generated and queued, and these messages could consume all available RAM. You should guard against this type of attack through proper configuration.

DETAILED STEPS

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	line [console vty] line-number [ending-line-number]	Specify the line to be configured for synchronous logging of messages. <ul style="list-style-type: none"> Use the console keyword for configurations that occur through the switch console port. Use the line vty line-number 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. <p>You can change the setting of all 16 vty lines at once by entering:</p> <p>line vty 0 15</p> <p>Or you can change the setting of the single vty line being used for your current connection. For example, to change the setting for vty line 2, enter:</p> <p>line vty 2</p> <p>When you enter this command, the mode changes to line configuration.</p>
Step 3	logging synchronous [level [severity-level all] limit number-of-buffers]	Enable synchronous logging of messages. <ul style="list-style-type: none"> (Optional) For level severity-level, specify the message severity level. Messages with a severity level equal to or higher than this value are printed asynchronously. Low numbers mean greater severity and high numbers mean lesser severity. The default is 2. (Optional) Specifying level all means that all messages are printed asynchronously regardless of the severity level. (Optional) For limit number-of-buffers, specify the number of buffers to be queued for the terminal after which new messages are dropped. The range is 0 to 2147483647. The default is 20.

	Command	Purpose
Step 4	end	Return to privileged EXEC mode.
Step 5	show running-config	Verify your entries.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To disable synchronization of unsolicited messages and debug output, use the **no logging synchronous** [**level severity-level** | **all**] [**limit number-of-buffers**] line configuration command.

EXAMPLE

In the following example, synchronous logging for line 4 is enabled with a severity level of 6. Then synchronous logging for line 2 is enabled with a severity level of 7 and is specified with a maximum number of buffer lines of 1,000.

```
Switch(config)# line 4
Switch(config-line)# logging synchronous level 6
Switch(config-line)# exit
Switch(config)# line 2
Switch(config-line)# logging synchronous level 7 limit 1000
Switch(config-line)# end
```

Enabling and Disabling Time Stamps on Log Messages

By default, log messages are not time stamped.

BEFORE YOU BEGIN

Ensure that the system clock is set correctly. For more information, see [Chapter 4, “Administering the Switch.”](#)

DETAILED STEPS

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	service timestamps log uptime or service timestamps log datetime [msec] [localtime] [show-timezone]	Enable log time stamps. The first command enables time stamps on log messages, showing the time since the system was rebooted. The second command enables time stamps on log messages. Depending on the options selected, the time stamp can include the date, time in milliseconds relative to the local time-zone, and the time zone name.
Step 3	end	Return to privileged EXEC mode.
Step 4	show running-config	Verify your entries.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To disable time stamps for both debug and log messages, use the **no service timestamps** global configuration command.

EXAMPLE

This example shows part of a logging display with the **service timestamps log datetime** global configuration command enabled:

```
*Mar  1 18:46:11: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
```

This example shows part of a logging display with the **service timestamps log uptime** global configuration command enabled:

```
00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
```

Enabling and Disabling Sequence Numbers in Log Messages

Because there is a chance that more than one log message can have the same time stamp, you can display messages with sequence numbers so that you can unambiguously see a single message. By default, sequence numbers in log messages are not displayed.

BEFORE YOU BEGIN

Review the [“Information About System Message Logging”](#) section on page 13-1.

DETAILED STEPS

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	service sequence-numbers	Enable sequence numbers.
Step 3	end	Return to privileged EXEC mode.
Step 4	show running-config	Verify your entries.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To disable sequence numbers, use the **no service sequence-numbers** global configuration command.

EXAMPLE

This example shows part of a logging display with sequence numbers enabled:

```
000019: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
```

Defining the Message Severity Level

You can limit messages displayed to the selected device by specifying the severity level of the message. [Table 13-2](#) describes the *level* keywords. It also lists the corresponding UNIX syslog definitions from the most severe level to the least severe level.

Table 13-2 Message Logging Level Keywords

Level Keyword	Level	Description	Syslog Definition
emergencies	0	System unstable	LOG_EMERG
alerts	1	Immediate action needed	LOG_ALERT
critical	2	Critical conditions	LOG_CRIT
errors	3	Error conditions	LOG_ERR
warnings	4	Warning conditions	LOG_WARNING
notifications	5	Normal but significant condition	LOG_NOTICE
informational	6	Informational messages only	LOG_INFO
debugging	7	Debugging messages	LOG_DEBUG

The software generates four other categories of messages:

- Error messages about software or hardware malfunctions, displayed at levels **warnings** through **emergencies**. These types of messages mean that the functionality of the switch is affected. For information on how to recover from these malfunctions, see the system message guide for this release.
- Output from the **debug** commands, displayed at the **debugging** level. Debug commands are typically used only by the Technical Assistance Center.
- Interface up or down transitions and system restart messages, displayed at the **notifications** level. This message is only for information; switch functionality is not affected.

BEFORE YOU BEGIN



Caution

The console is a slow display device. In message storms some logging messages may be silently dropped when the console queue becomes full. Set severity levels accordingly.

DETAILED STEPS

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	logging console <i>level</i>	Limit messages logged to the console. By default, the console receives debugging messages and numerically lower levels (see Table 13-2 on page 13-10).
Step 3	logging monitor <i>level</i>	Limit messages logged to the terminal lines. By default, the terminal receives debugging messages and numerically lower levels (see Table 13-2 on page 13-10).

	Command	Purpose
Step 4	<code>logging trap level</code>	Limit messages logged to the syslog servers. By default, syslog servers receive informational messages and numerically lower levels (see Table 13-2 on page 13-10). For complete syslog server configuration steps, see the “ Configuring UNIX Syslog Servers ” section on page 13-14.
Step 5	<code>end</code>	Return to privileged EXEC mode.
Step 6	<code>show running-config</code> or <code>show logging</code>	Verify your entries.
Step 7	<code>copy running-config startup-config</code>	(Optional) Save your entries in the configuration file.



Note Specifying a *level* causes messages at that level and numerically lower levels to appear at the destination.

To disable logging to the console, use the **no logging console** global configuration command. To disable logging to a terminal other than the console, use the **no logging monitor** global configuration command. To disable logging to syslog servers, use the **no logging trap** global configuration command.

EXAMPLE

The following example shows how to change the level of messages sent to the console terminal to alerts, meaning that messages at levels 0 and 1 are sent:

```
Switch(config)# logging console alerts
```

Limiting Syslog Messages Sent to the History Table and to SNMP

If you enabled syslog message traps to be sent to an SNMP network management station by using the **snmp-server enable trap** global configuration command, you can change the level of messages sent and stored in the switch history table. You also can change the number of messages that are stored in the history table.

Messages are stored in the history table because SNMP traps are not guaranteed to reach their destination. By default, one message of the level **warning** and numerically lower levels (see [Table 13-2 on page 13-10](#)) are stored in the history table even if syslog traps are not enabled.

BEFORE YOU BEGIN

For information about enabling syslog message traps using the **snmp-server enable trap** command, see [Chapter 14, “Configuring SNMP.”](#)

DETAILED STEPS

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	logging history <i>level</i>¹	Change the default level of syslog messages stored in the history file and sent to the SNMP server. See Table 13-2 on page 13-10 for a list of <i>level</i> keywords. By default, warnings , errors , critical , alerts , and emergencies messages are sent.
Step 3	logging history size <i>number</i>	Specify the number of syslog messages that can be stored in the history table. The default is to store one message. The range is 0 to 500 messages.
Step 4	end	Return to privileged EXEC mode.
Step 5	show running-config	Verify your entries.
Step 6	copy running-config startup-config	(Optional) Save your entries in the configuration file.

1. [Table 13-2](#) 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 equals 3, not 2.

When the history table is full (it contains the maximum number of message entries specified with the **logging history size** global configuration command), the oldest message entry is deleted from the table to allow the new message entry to be stored.

To return the logging of syslog messages to the default level, use the **no logging history** global configuration command. To return the number of messages in the history table to the default value, use the **no logging history size** global configuration command.

EXAMPLE

In the following example, the logging history 1 command is used to configure the system to save only level 1 (alert) and level 0 (emergency) messages to the logging history table, and, by extension, to send only these levels in the SNMP notifications. The configuration is then confirmed using the show logging history command.

```
Switch(config)# logging history 1
Switch(config)# snmp-server enable traps syslog
Switch(config)# end
Switch#
4w0d: %SYS-5-CONFIG_I: Configured from console by console
Switch# show logging history
Syslog History Table:1 maximum table entries,
! The following line indicates that 'logging history level 1' (alerts) is configured.
saving level alerts or higher
18 messages ignored, 0 dropped, 0 recursion drops
1 table entries flushed
SNMP notifications enabled, 0 notifications sent
entry number 2 : LINK-3-UPDOWN
Interface FastEthernet0, changed state to up
timestamp: 2766
Switch#
```

Enabling the Configuration-Change Logger

You can enable a configuration logger to keep track of configuration changes made with the command-line interface (CLI). When you enter the **logging enable** configuration-change logger configuration command, the log records the session, the user, and the command that was entered to change the configuration. You can configure the size of the configuration log from 1 to 1000 entries (the default is 100). You can clear the log at any time by entering the **no logging enable** command followed by the **logging enable** command to disable and reenabling logging.

Use the **show archive log config {all | number [end-number] | user username [session number] number [end-number] | statistics}** [provisioning] privileged EXEC command to display the complete configuration log or the log for specified parameters.

The default is that configuration logging is disabled.

BEFORE YOU BEGIN

If you disable configuration logging, all configuration log records that were collected are purged.

DETAILED STEPS

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	archive	Enter archive configuration mode.
Step 3	log config	Enter configuration-change logger configuration mode.
Step 4	logging enable	Enable configuration change logging.
Step 5	logging size <i>entries</i>	(Optional) Configure the number of entries retained in the configuration log. The range is from 1 to 1000. The default is 100. Note When the configuration log is full, the oldest log entry is removed each time a new entry is entered.
Step 6	end	Return to privileged EXEC mode.
Step 7	show archive log config	Verify your entries by viewing the configuration log.

EXAMPLE

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

This is an example of output for the configuration log:

```
Switch# 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

The next sections describe how to configure the UNIX server syslog daemon and how to define the UNIX system logging facility.

Logging Messages to a UNIX Syslog Daemon

Before you can send system log messages to a UNIX syslog server, you must configure the syslog daemon on a UNIX server. This procedure is optional.

BEFORE YOU BEGIN

Some recent versions of UNIX syslog daemons no longer accept by default syslog packets from the network. If this is the case with your system, use the UNIX **man syslogd** command to decide what options must be added to or removed from the syslog command line to enable logging of remote syslog messages.

DETAILED STEPS

Step 1 Log in as root.

Step 2 Add a line such as the following to the file `/etc/syslog.conf`:

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

The **local7** keyword specifies the logging facility to be used; see [Table 13-3 on page 13-15](#) for information on the facilities. The **debug** keyword specifies the syslog level; see [Table 13-2 on page 13-10](#) for information on the severity levels. The syslog daemon sends messages at this level or at a more severe level to the file specified in the next field. The file must already exist, and the syslog daemon must have permission to write to it.

Step 3 Create the log file by entering these commands at the UNIX shell prompt:

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

Step 4 Make sure the syslog daemon reads the new changes:

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

For more information, see the **man syslog.conf** and **man syslogd** commands on your UNIX system.

Configuring the UNIX System Logging Facility

When sending system log messages to an external device, you can cause the switch to identify its messages as originating from any of the UNIX syslog facilities.

Table 13-3 lists the UNIX system facilities supported by the software.

Table 13-3 Logging Facility-Type Keywords

Facility Type Keyword	Description
auth	Authorization system
cron	Cron facility
daemon	System daemon
kern	Kernel
local0-7	Locally defined messages
lpr	Line printer system
mail	Mail system
news	USENET news
sys9-14	System use
syslog	System log
user	User process
uucp	UNIX-to-UNIX copy system

BEFORE YOU BEGIN

For more information about the UNIX system facilities, consult the operator's manual for your UNIX operating system.

DETAILED STEPS

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	logging host	Log messages to a UNIX syslog server host by entering its IP address. To build a list of syslog servers that receive logging messages, enter this command more than once.
Step 3	logging trap level	Limit messages logged to the syslog servers. Be default, syslog servers receive informational messages and lower. See Table 13-2 on page 13-10 for <i>level</i> keywords.
Step 4	logging facility facility-type	Configure the syslog facility. See Table 13-3 on page 13-15 for <i>facility-type</i> keywords. The default is local7 .
Step 5	end	Return to privileged EXEC mode.

	Command	Purpose
Step 6	show running-config	Verify your entries.
Step 7	copy running-config startup-config	(Optional) Save your entries in the configuration file.

To remove a syslog server, use the **no logging host** global configuration command, and specify the syslog server IP address. To disable logging to syslog servers, enter the **no logging trap** global configuration command.

EXAMPLE

In the following example, the user configures the syslog facility to the kernel facility:

```
Switch(config)# logging facility kern
```

Verifying the Configuration

To display the logging configuration and the contents of the log buffer, use the **show logging** privileged EXEC command. For information about the fields in this display, see the [Cisco IOS Configuration Fundamentals Command Reference, Release 15.2M&T](#).

Configuration Example

The following example shows how to enable standard system logging to the local syslog buffer:

```
Switch(config)# logging buffered
```

In the following example, synchronous logging for line 4 is enabled with a severity level of 6. Then synchronous logging for line 2 is enabled with a severity level of 7 and is specified with a maximum number of buffer lines of 1,000.

```
Switch(config)# line 4
Switch(config-line)# logging synchronous level 6
Switch(config-line)# exit
Switch(config)# line 2
Switch(config-line)# logging synchronous level 7 limit 1000
Switch(config-line)# end
```

This example shows part of a logging display with the **service timestamps log datetime** global configuration command enabled:

```
*Mar  1 18:46:11: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
```

This example shows part of a logging display with the **service timestamps log uptime** global configuration command enabled:

```
00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
```

This example shows part of a logging display with sequence numbers enabled:

```
000019: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
```

The following example shows how to change the level of messages sent to the console terminal to alerts, meaning that messages at levels 0 and 1 are sent:


```
Switch(config)# logging console alerts
```

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

In the following example, the **logging history 1** command is used to configure the system to save only level 1 (alert) and level 0 (emergency) messages to the logging history table, and, by extension, to send only these levels in the SNMP notifications. The configuration is then confirmed using the **show logging history** command.

```
Switch(config)# logging history 1
Switch(config)# snmp-server enable traps syslog
Switch(config)# end
Switch#
4w0d: %SYS-5-CONFIG_I: Configured from console by console
Switch# show logging history
Syslog History Table:1 maximum table entries,
! The following line indicates that 'logging history level 1' (alerts) is configured.
saving level alerts or higher
 18 messages ignored, 0 dropped, 0 recursion drops
 1 table entries flushed
SNMP notifications enabled, 0 notifications sent
  entry number 2 : LINK-3-UPDOWN
   Interface FastEthernet0, changed state to up
   timestamp: 2766
Switch#
```

This is an example of output for the configuration log:

```
Switch# 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
```

Related Documents

- [Cisco IOS Configuration Fundamentals Command Reference, Release 15.2M&T](#)
- [Cisco IOS Master Command List, All Releases](#)
- [Cisco System Messages](#)

Feature History

Platform	First Supported Release
IE 2000U	Cisco IOS Release 15.0(2)EH
CGS 2520	Cisco IOS Release 12.2(53)EX
Ethernet Switch Module (ESM) for CGR 2010	Cisco IOS Release 12.2(53)EX