



Configuring System Message Logging

Restrictions for System Message Logging

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

Information About System Message Logging

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.

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 48 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 Enabling and Disabling Sequence Numbers in Log Messages, page 534 . |
| <i>timestamp formats:</i> <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 Enabling and Disabling Time Stamps on Log Messages, page 534 . |
| <i>facility</i> | The facility to which the message refers (for example, SNMP, SYS, and so forth). |
| <i>severity</i> | Single-digit code from 0 to 7 that is the severity of the message. |
| <i>MNEMONIC</i> | Text string that uniquely describes the message. |
| <i>description</i> | Text string containing detailed information about the event being reported. |

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.

Message Severity Levels

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.

[Table 49 on page 529](#) describes the *level* keywords. It also lists the corresponding UNIX syslog definitions from the most severe level to the least severe level.

Table 49 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 these 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.
- 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.

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.

Note: 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.

Log in as root, and perform these steps:

1. 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. The **debug** keyword specifies the syslog level. 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.

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

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

3. 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.

[Table 50 on page 530](#) lists the UNIX system facilities supported by the software. For more information about these facilities, consult the operator's manual for your UNIX operating system.

Table 50 UNIX System Facilities

| 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 |

Default System Message Logging Configuration

| Feature | Default Setting |
|---------------------------------------|---|
| System message logging to the console | Enabled. |
| Console severity | Debugging (and numerically lower levels). |
| 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. |
| Configuration change logger | Disabled. |
| Server facility | Local7. |
| Server severity | Informational (and numerically lower levels). |

How to Configure System Message Logging

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.

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.

| | Command | Purpose |
|----|---------------------------|-----------------------------------|
| 1. | configure terminal | Enters global configuration mode. |
| 2. | no logging console | Disables message logging. |
| 3. | end | Returns to privileged EXEC mode. |

Setting the Message Display Destination Device

If message logging is enabled, you can send messages to specific locations in addition to the console. Beginning in privileged EXEC mode, use one or more of the following commands to specify the locations that receive messages:

| | Command | Purpose |
|----|--|---|
| 1. | configure terminal | Enters global configuration mode. |
| 2. | logging buffered [<i>size</i>] | <p>Logs messages to an internal buffer on the switch. The range is 4096 to 2147483647 bytes. The default buffer size is 4096 bytes.</p> <p>If the switch fails, the log file is lost unless you had 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> |
| 3. | logging host | <p>Logs messages to a UNIX syslog server host.</p> <p><i>host</i>—Specifies 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> |
| 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>] | <p>Stores log messages in a file in flash memory.</p> <ul style="list-style-type: none"> ■ <i>filename</i>—Enters the log message filename. ■ (Optional) <i>max-file-size</i>—Specifies the maximum logging file size. The range is 4096 to 2147483647. The default is 4096 bytes. ■ (Optional) <i>min-file-size</i>—Specifies the minimum logging file size. The range is 1024 to 2147483647. The default is 2048 bytes. ■ (Optional) <i>severity-level-number</i> <i>type</i>—Specifies either the logging severity level or the logging type. The severity range is 0 to 7. By default, the log file receives debugging messages and numerically lower levels. |
| 5. | end | Returns to privileged EXEC mode. |
| 6. | terminal monitor | <p>Logs messages to a nonconsole terminal during the current session.</p> <p>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.</p> |

Synchronizing Log Messages

| | Command | Purpose |
|----|---|--|
| 1. | configure terminal | Enters global configuration mode. |
| 2. | line [console vty] line-number [ending-line-number] | <p>Specifies the line to be configured for synchronous logging of messages.</p> <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> |
| 3. | logging synchronous [level [severity-level all] limit number-of-buffers] | <p>Enables synchronous logging of messages.</p> <ul style="list-style-type: none"> ■ (Optional) level severity-level—Specifies 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) level all—Specifies that all messages are printed asynchronously regardless of the severity level. ■ (Optional) limit number-of-buffers—Specifies 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. |
| 4. | end | Returns to privileged EXEC mode. |

Enabling and Disabling Time Stamps on Log Messages

| | Command | Purpose |
|----|---|---|
| 1. | configure terminal | Enters global configuration mode. |
| 2. | service timestamps log uptime or service timestamps log datetime [msec] [localtime] [show-timezone] | Enables 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. |
| 3. | end | Returns to privileged EXEC mode. |

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.

| | Command | Purpose |
|----|---------------------------------|-----------------------------------|
| 1. | configure terminal | Enters global configuration mode. |
| 2. | service sequence-numbers | Enables sequence numbers. |
| 3. | end | Returns to privileged EXEC mode. |

Defining the Message Severity Level

You can limit messages displayed to the selected device by specifying the severity level of the message, which are described in Table 2.

| | Command | Purpose |
|----|-------------------------------------|--|
| 1. | configure terminal | Enters global configuration mode. |
| 2. | logging console <i>level</i> | Limits messages logged to the console. By default, the console receives debugging messages and numerically lower levels. |
| 3. | logging monitor <i>level</i> | Limits messages logged to the terminal lines. By default, the terminal receives debugging messages and numerically lower levels. |
| 4. | logging trap <i>level</i> | Limits messages logged to the syslog servers. By default, syslog servers receive informational messages and numerically lower levels. |
| 5. | end | Returns to privileged EXEC mode. |

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 are stored in the history table even if syslog traps are not enabled.

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.

| | Command | Purpose |
|----|------------------------------------|---|
| 1. | configure terminal | Enters global configuration mode. |
| 2. | logging history level | Changes the default level of syslog messages stored in the history file and sent to the SNMP server. By default, warnings, errors, critical, alerts, and emergencies messages are sent. |
| 3. | logging history size number | Specifies 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. |
| 4. | end | Returns to privileged EXEC mode. |

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).

| | Command | Purpose |
|----|-----------------------------|---|
| 1. | configure terminal | Enters global configuration mode. |
| 2. | archive | Enters archive configuration mode. |
| 3. | log config | Enters configuration-change logger configuration mode. |
| 4. | logging enable | Enables configuration change logging. |
| 5. | logging size entries | (Optional) Configures 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. |
| 6. | end | Returns to privileged EXEC mode. |

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.

| | Command | Purpose |
|----|---------------------------------------|---|
| 1. | configure terminal | Enters global configuration mode. |
| 2. | logging host | Logs 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. |
| 3. | logging trap level | Limits messages logged to the syslog servers. By default, syslog servers receive informational messages and lower. |
| 4. | logging facility facility-type | Configures the syslog facility. The default is local7 . |
| 5. | end | Returns to privileged EXEC mode. |

Monitoring and Maintaining the System Message Log

| Command | Purpose |
|--------------------------------|---------------------------------|
| show logging | Displays logging messages. |
| show archive log config | Displays the configuration log. |

Configuration Examples for the System Message Log

System Message: Example

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 GigabitEthernet1/17, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet1/18, 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 GigabitEthernet1/17, 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)
```

Logging Display: Examples

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:

Additional References

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

Enabling the Logger: 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
```

Configuration Log Output: Example

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
```

Additional References

The following sections provide references related to switch administration:

Related Documents

| Related Topic | Document Title |
|--|--|
| Cisco IOS basic commands Cisco IOS system management commands | <i>Cisco IOS Configuration Fundamentals Command Reference</i> |
| Syslog server configuration steps | Configuring the UNIX System Logging Facility, page 535 |

Standards

| Standards | Title |
|---|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | – |

MIBs

| MIBs | MIBs Link |
|------|--|
| – | To locate and download MIBs using Cisco IOS XR software, use the Cisco MIB Locator found at the following URL and choose a platform under the Cisco Access Products menu: http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml |

RFCs

| RFCs | Title |
|---|-------|
| No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature. | – |

Technical Assistance

| Description | Link |
|---|---|
| The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | http://www.cisco.com/techsupport |