Configuring System Message Logging and Smart Logging

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About System Message Logging

System Message Logging Process

It is possible to configure system message logging on the switch. The switch also supports Smart Logging to capture packet flows based on configured triggers.

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

By default, a switch sends the output from system messages and **debug** privileged EXEC commands to a logging process.

Stack members can trigger system messages. A stack member that generates a system message appends its hostname in the form of *hostname-n*, where *n* is a switch number from 1 to 9, and redirects the output to the logging process on the stack master. Though the stack master is a stack member, it does *not* append its hostname to system messages.

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. On the switches, messages appear on the active consoles 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 on a standalone switch, and in the case of a switch stack, on the stack master. If a standalone switch or the stack master fails, the log is lost unless you had saved it to flash memory.

You can remotely monitor system messages by viewing the logs on a syslog server or by accessing the switch through Telnet, through the console port, or through the Ethernet management port. In a switch stack, all stack member consoles provide the same console output.

How to Configure System Message Logging

Configuring System Message Logging

It is possible to configure system message logging on the switch.

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

Related Topics

System Log Message Format, on page 2
Default System Message Logging Configuration, on page 3

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:

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 1: System Log Message Elements

Element	Description
seq no:	Stamps log messages with a sequence number only if the **service sequence-numbers** global configuration command is configured.
timestamp formats: *mm/dd hh:mm:ss* or *hh:mm:ss* (short uptime) or *d h* (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.
facility	The facility to which the message refers (for example, SNMP, SYS, and so forth). For a list of supported facilities, see Table 4: Logging Facility-Type Keywords, on page 21
severity	Single-digit code from 0 to 7 that is the severity of the message. For a description of the severity levels, see Table 3: Message Logging Level Keywords, on page 14
MNEMONIC	Text string that uniquely describes the message.
description	Text string containing detailed information about the event being reported.
hostname-n	Hostname of a stack member and its switch number in the stack. Though the stack master is a stack member, it does *not* append its hostname to system messages.

Related Topics

Configuring System Message Logging, on page 2

Default System Message Logging Configuration

The features and their default settings of the System Message Logging are shown in the table below.

Table 2: Default System Message Logging Configuration

Feature	Default Setting
System message logging to the console	Enabled.
Console severity	Debugging (and numerically lower levels; see Table 3: Message Logging Level Keywords, on page 14)
Logging file configuration	No filename specified.
Logging buffer size	4096 bytes.

Feature	Default Setting
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 4: Logging Facility-Type Keywords, on page 21)
Server severity	Informational (and numerically lower levels; see Table 3: Message Logging Level Keywords, on page 14)
Configuration change logger	Disabled.

Related Topics

Configuring System Message Logging, on page 2

Disabling Message Logging

Follow these steps to disable message logging. This procedure is optional.

Before you begin

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.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no logging console**
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**no logging console** **Example:** `Switch(config)# no logging console`	Disables message logging.

Step 4	**end**
	Example:
	`Switch(config)# end`
		Returns to privileged EXEC mode.

Step 5	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 6	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

What to do next

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.

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

Related Topics

Synchronizing Log Messages, on page 8

Setting the Message Display Destination Device

If message logging is enabled, you can send messages to specific locations in addition to the console.

Use one or more of the following commands to specify the locations that receive messages. This procedure is optional.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **logging buffered** [*size*]
4. **logging** [*host*]
5. **logging file flash:***filename* [*max-file-size* [*min-file-size*]] [*severity-level-number* | *type*]
6. **end**
7. **terminal monitor**
8. **show running-config**
9. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**logging buffered** [*size*] **Example:** `Switch(config)# logging buffered [size]`	Logs messages to an internal buffer on the Switch or on a standalone Switch or, in the case of a Switch stack, on the stack master. The range is 4096 to 2147483647 bytes. The default buffer size is 4096 bytes. If a standalone Switch or the stack master fails, the log file is lost unless you previously saved it to flash memory. **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 not be set to this amount.
Step 4	**logging** [*host*] **Example:** `Switch(config)# logging [host]`	Logs messages to a UNIX syslog server host. For *host*, 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.

	Command or Action	Purpose
Step 5	**logging file flash:***filename* [*max-file-size* [*min-file-size*]] [*severity-level-number* | *type*] **Example:** `Switch(config)#`	Stores log messages in a file in flash memory on a standalone Switch or, in the case of a Switch stack, on the stack master. For filename, enter the log message filename. (Optional) For max-file-size, specify the maximum logging file size. The range is 4096 to 2147483647. The default is 4096 bytes. (Optional) For min-file-size, specify the minimum logging file size. The range is 1024 to 2147483647. The default is 2048 bytes. (Optional) For severity-level-number | type, 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 3: Message Logging Level Keywords, on page 14. By default, the log file receives debugging messages and numerically lower levels.

Step 6	**end**
	Example:
	`Switch(config)# end`
		Returns to privileged EXEC mode.

Step 7	**terminal monitor** **Example:**	Logs 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 8	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 9	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

What to do next

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.

Use the **logging event power-inline-status** interface configuration command to enable and to disable logging of Power over Ethernet (PoE) events on specific PoE-capable ports. Logging on these ports is enabled by default.

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.

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.

Follow these steps to configure synchronous logging. This procedure is optional.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **line** [**console** | vty] *line-number* [*ending-line-number*]
4. **logging synchronous** [**level** [*severity-level* | **all**] | **limit** *number-of-buffers*]
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**line** [**console** | vty] *line-number* [*ending-line-number*] **Example:** `Switch(config)# line [console | vty] line-number [ending-line-number]`	Specifies the line to be configured for synchronous logging of messages. Use the **console** keyword for configurations that occur through the Switch console port or the Ethernet management 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. You can change the setting of all 16 vty lines at once by entering: **line vty 0 15** 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: **line vty 2** When you enter this command, the mode changes to line configuration.
Step 4	**logging synchronous** [**level** [*severity-level* | **all**] | **limit** *number-of-buffers*] **Example:**	Enables synchronous logging of messages. (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.

Step 5	**end**
	Example:
	`Switch(config)# end`
		Returns to privileged EXEC mode.

Step 6	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 7	**copy running-config startup-config** **Example:**	(Optional) Saves your entries in the configuration file.

	Command or Action	Purpose
	`Switch# copy running-config startup-config`	

What to do next

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.

Related Topics

Disabling Message Logging, on page 4

Enabling and Disabling Time Stamps on Log Messages

Follow these steps to enable time-stamping of log messages. This procedure is optional.

Before you begin

By default, log messages are not time-stamped.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **service timestamps log uptime** or **service timestamps log datetime** [**msec**] [**localtime**] [**show-timezone**]
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**service timestamps log uptime** or **service timestamps log datetime** [**msec**] [**localtime**] [**show-timezone**] **Example:**	Enables log time stamps. The first command enables time stamps on log messages, showing the time since the system was rebooted.

	Command or Action	Purpose
		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 4	**end**
	Example:
	`Switch(config)# end`
		Returns to privileged EXEC mode.

Step 5	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 6	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

What to do next

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

Related Topics

Examples of System Message Logging, on page 21

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.

Follow these steps to enable sequence numbers in log messages. This procedure is optional.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **service sequence-numbers**
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**service sequence-numbers** **Example:**	Enables sequence numbers.

Step 4	**end**
	Example:
	`Switch(config)# end`
		Returns to privileged EXEC mode.

Step 5	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 6	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

What to do next

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

Related Topics

Examples of System Message Logging, on page 21

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 3: Message Logging Level Keywords, on page 14.

Follow these steps to define the message severity level. This procedure is optional.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **logging console***level*
4. **logging monitor***level*
5. **logging trap***level*
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**logging console***level* **Example:**	Limits messages logged to the console. By default, the console receives debugging messages and numerically lower levels.
Step 4	**logging monitor***level* **Example:**	Limits messages logged to the terminal lines. By default, the terminal receives debugging messages and numerically lower levels.
Step 5	**logging trap***level* **Example:**	Limits messages logged to the syslog servers. By default, syslog servers receive informational messages and numerically lower levels

Step 6	**end**
	Example:
	`Switch(config)# end`
		Returns to privileged EXEC mode.

Step 7	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.

	Command or Action	Purpose
Step 8	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

What to do next

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.

The table shown below describes the *level* keywords. It also lists the corresponding UNIX syslog definitions from the most severe level to the least severe level.

Table 3: 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.

Reload requests and low-process stack messages, displayed at the **informational** level. This message is only for information; Switch functionality is not affected.

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 3: Message Logging Level Keywords, on page 14) are stored in the history table even if syslog traps are not enabled.

Follow these steps to change the level and history table size defaults. This procedure is optional.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **logging history***level*
4. **logging history size** *number*]
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**logging history***level* **Example:**	Changes the default level of syslog messages stored in the history file and sends to the SNMP server. See Table 3: Message Logging Level Keywords, on page 14 for a list of *level* keywords. By default, **warnings**, **errors**, **critical**, **alerts**, and **emergencies** messages are sent.

	Command or Action	Purpose
		Note Table 3: Message Logging Level Keywords, on page 14 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.
Step 4	**logging history size** *number*] **Example:**	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.

Step 5	**end**
	Example:
	`Switch(config)# end`
		Returns to privileged EXEC mode.

Step 6	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 7	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

What to do next

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.

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 re-enable 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.

Follow these steps to enable configuration logging:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **archive**
4. **log config**
5. **logging enable**
6. **logging size** *entries*
7. **end**
8. **show running-config**
9. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**archive** **Example:** `Switch(config)# archive`	Enters archive configuration mode.
Step 4	**log config** **Example:** `Switch(config)# log config`	Enters configuration-change logger configuration mode.
Step 5	**logging enable** **Example:** `Switch(config)# logging enable`	Enables configuration change logging.

	Command or Action	Purpose
Step 6	**logging size** *entries* **Example:** `Switch(config)# logging size 500`	(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.

Step 7	**end**
	Example:
	`Switch(config)# end`
		Returns to privileged EXEC mode.

Step 8	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 9	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Related Topics

Examples of System Message Logging, on page 21

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

Log in as root, and perform these steps:

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.

Before you begin

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.

SUMMARY STEPS

1. **local7.debug /usr/adm/logs/cisco.log**
2. **$ touch /var/log/cisco.log** and **$ chmod 666 /var/log/cisco.log**
3. $ **kill -HUP `cat /etc/syslog.pid`**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**local7.debug /usr/adm/logs/cisco.log** **Example:** `local7.debug /usr/adm/logs/cisco.log`	Add a line such as the following to the file /etc/syslog.conf: The **local7** keyword specifies the logging facility to be used; see Table 4: Logging Facility-Type Keywords, on page 21 for information on the facilities. The **debug** keyword specifies the syslog level; see Table 3: Message Logging Level Keywords, on page 14 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 2	**$ touch /var/log/cisco.log** and **$ chmod 666 /var/log/cisco.log**
	Example:
	`$ touch /var/log/cisco.log`
	`$ chmod 666 /var/log/cisco.log`
		Enter these commands at the UNIX shell prompt.
		Creates the log file.

Step 3	$ **kill -HUP `cat /etc/syslog.pid`** **Example:** ``$ kill -HUP `cat /etc/syslog.pid` ``	Make sure the syslog daemon reads the new changes:

What to do next

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.

Follow these steps to configure UNIX system facility message logging. This procedure is optional.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **logging** *host*
4. **logging trap** *level*
5. **logging facility** *facility-type*
6. **end**

7. **show running-config**
8. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**logging** *host* **Example:** `Switch(config)# logging`	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.
Step 4	**logging trap** *level* **Example:** `Switch(config)#`	Limits messages logged to the syslog servers. Be default, syslog servers receive informational messages and lower. See Table 3: Message Logging Level Keywords, on page 14 for level keywords.
Step 5	**logging facility** *facility-type* **Example:** `Switch(config)# logging enable`	Configures the syslog facility. See Table Table 4: Logging Facility-Type Keywords, on page 21 for facility-type keywords. The default is **local7**.

Step 6	**end**
	Example:
	`Switch(config)# end`
		Returns to privileged EXEC mode.

Step 7	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 8	**copy running-config startup-config** **Example:**	(Optional) Saves your entries in the configuration file.

	Command or Action	Purpose
	`Switch# copy running-config startup-config`	

What to do next

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.

The table below 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 4: 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

Examples of System Message Logging

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) (Switch-2)
```

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
(Switch-2)
```

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)
(Switch-2)
```

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 GigabitEthernet5/0/1
 46    16           temi@vty5   |switchport mode trunk
 47    16           temi@vty5   |exit
```

Related Topics

Enabling and Disabling Time Stamps on Log Messages, on page 10
Enabling and Disabling Sequence Numbers in Log Messages, on page 11
Enabling the Configuration-Change Logger, on page 16

How to Configure Smart Logging

Configuring Smart Logging

Smart logging provides a mechanism to capture and export packet flows based on predefined or user-configured triggers. The Switch supports smart logging for these events:

- DHCP snooping violations
- Dynamic ARP inspection violations
- IP source guard denied traffic
- ACL permitted or denied traffic

To use smart logging, you must first configure a NetFlow exporter that you identify when you enable smart logging.

Smart logging processing creates a NetFlow packet for the configured event and sends the packet to the external NetFlow collector. Smart logging counters reflect the number of packets that are logged. This number is the same as the number of packets sent to the collector if no packets are dropped between the Switch and the NetFlow collector.

If you enable smart logging globally on the Switch, you can then configure specific events to be smart logged.

Related Topics

Enabling Smart Logging, on page 23

Enabling Smart Logging

Follow these steps to globally enable smart logging:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **logging smartlog**
4. **logging smartlog exporter** *exporter_name*
5. **logging packet capture size** *packet_size*
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**logging smartlog** **Example:** `Switch(config)# logging smartlog`	Turns on the smart logging feature.
Step 4	**logging smartlog exporter** *exporter_name* **Example:** `Switch(config)# logging smartlog exporter`	Identify the smart log exporter. You must have already configured the exporter by using the flexible NetFlow CLI. If the exporter name does not exist, you receive an error message. By default, the Switch sends data to the collector every 60 seconds.

	Command or Action	Purpose
Step 5	**logging packet capture size** *packet_size* **Example:** `Switch(config)# logging packet capture size 64`	(Optional) Configure the size of the packet to be sent to the exporter. The range is from 64 to 1024 bytes in 4-byte increments. The default size is 64 bytes. **Note** Increasing the packet capture size reduces the number of flow records per packet.

Step 6	**end**
	Example:
	`Switch(config)# end`
		Returns to privileged EXEC mode.

Step 7	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 8	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Related Topics

Configuring Smart Logging, on page 22

Enabling Smart Logging for DHCP Snooping Violations

DHCP snooping intercepts and inspects DHCP packets entering untrusted ports and either forwards or drops the packets. You can enable DHCP snooping smart logging to send the contents of dropped packets to the NetFlow collector. Follow these steps to enable DHCP snooping smart logging:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp snooping vlan** *vlan-range* **smartlog**
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Switch> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**ip dhcp snooping vlan** *vlan-range* **smartlog** **Example:** `Switch(config)# ip dhcp snooping vlan`	Specifies a VLAN ID or a range of VLANs on which to enable DHCP snooping smart logging.

Step 4	**end**
	Example:
	`Switch(config)# end`
		Returns to privileged EXEC mode.

Step 5	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 6	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Enabling Smart Logging for Dynamic ARP Inspection Violations

Dynamic ARP inspection intercepts ARP packets on untrusted ports and validates them before forwarding. The functionality is similar to DHCP snooping but for ARP packets. You can configure dynamic ARP inspection logging by using the ip arp inspection log-buffer global configuration command. By default, all dropped packets are logged. You can also configure the Switch to apply smart logging to the same packets that are being logged, sending the packet contents packet to the NetFlow collector.

Follow these steps to enable dynamic ARP inspection smart logging:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip arp inspection smartlog**

4. **end**
5. **show running-config**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**ip arp inspection smartlog** **Example:** `Switch(config)# ip arp inspection smartlog`	Specifies that whatever packets are currently being logged (the default is all dropped packets) are also smart-logged.

Step 4	**end**
	Example:
	`Switch(config)# end`
		Returns to privileged EXEC mode.

Step 5	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 6	**copy running-config startup-config** **Example:** `Switch# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Enabling Smart Logging for IP Source Guard Violations

IP source guard is a security feature related to DHCP snooping. You can use IP source guard to filter traffic based on the IP source address or the MAC address. All IP packets with a source address other than the specified address or addresses learned through DHCP snooping are denied. You can enable IP source guard smart logging to send the contents of the denied packets to the NetFlow collector.

Follow these steps to enable IP source guard smart logging:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface***interface-id*
4. **ip verify source smartlog**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Switch# configure terminal`	Enters global configuration mode.
Step 3	**interface***interface-id* **Example:** `Switch(config)# interface`	Specifies an interface and enter interface configuration mode.
Step 4	**ip verify source smartlog** **Example:** `Switch(config)# ip verify source smartlog`	Enables IP source guard smart logging for all packets that are denied by IP source guard.

Step 5	**end**
	Example:
	`Switch(config)# end`
		Returns to privileged EXEC mode.

Step 6	**show running-config** **Example:** `Switch# show running-config`	Verifies your entries.
Step 7	**copy running-config startup-config** **Example:**	(Optional) Saves your entries in the configuration file.

	Command or Action	Purpose
	`Switch# copy running-config startup-config`	

Enabling Smart Logging for Port ACL Deny or Permit Actions

The Switch supports port ACLs, router ACLs, and VLAN ACLs.

- Port ACLs are IP or MAC ACLs applied to a Layer 2 port. Logging is not supported on port ACLs, but smart logging is supported on IP ACLs applied to Layer 2 ports.
- Router ACLs are ACLs applied to Layer 3 ports. Router ACLs support logging but not smart logging.
- VLAN ACLs or VLAN maps are ACLs applied to VLANs. You can configure logging on VLAN maps, but not smart logging.

When you configure any permit or deny ACL, you can configure logging or smart logging as part of the access list, to take place on all traffic that the ACL permits or denies. The type of port that you attach the ACL to determines the type of logging. If you attach an ACL with smart log configured to a router or a VLAN, the ACL is attached, but smart logging does not take affect.

If you configure logging on an ACL attached to a Layer 2 port, the logging keyword is ignored.

You add the smart log configuration option when you create the permit and deny conditions for an ACL.

This example enables smart logging on a numbered access list:

```
Switch(config)# access-list 199 permit ip any any smartlog
```

This example enables smart logging on a named access list:

```
Switch(config)# ip access-list extended test1
Switch(config-ext-nacl)# deny ip host 10.1.1.3 any smartlog
```

Monitoring Logging Information

Monitoring Logging Information

To display the logging configuration and the contents of the log buffer, use the **show logging** privileged EXEC command.

To display smart logging information, use the **show logging smartlog** command.

Additional References

Related Documents

Related Topic	Document Title
System Commands	*Command Reference, Cisco IOS Release 15.2(2)E*

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

Standards and RFCs

Standard/RFC	Title
None	-

MIBs

MIB	MIBs Link
All supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support