Configuring System Message Logging

This chapter describes how to configure system message logging on Cisco MDS 9000 Series switches.

Feature History for System Message Logging

Table 1: Feature History for Configuring SAN Analytics

Feature Name	Release	Feature Information
Secure Remote System Message Logging	9.2(2)	Support for CFS distribution of the **secure** option was added.
Secure Remote System Message Logging	9.2(1)	The Secure Remote System Message Logging feature allows you to securely log system messages to a remote logging server using TLS.

Information About System Message Logging

With the system message logging software, you can save messages in a log file or direct the messages to other devices. By default, the switch logs normal but significant system messages to a log file and sends these messages to the system console. This feature provides you with the following capabilities:

- Provides logging information for monitoring and troubleshooting
- Allows you to select the types of captured logging information
- Allows you to select the destination server to forward the captured logging information properly configured system message logging server.

Note When the switch first initializes, the network is not connected until initialization completes. Therefore, messages are not redirected to a system message logging server for a few seconds.

Log messages are not saved across system reboots. However, a maximum of 100 log messages with a severity level of critical and below (levels 0, 1, and 2) are saved in NVRAM.

Table 2: Internal Logging Facilities , on page 2 describes some samples of the facilities supported by the system message logs.

Table 2: Internal Logging Facilities

Facility Keyword	Description	Standard or Cisco MDS Specific
acl	ACL manager	Cisco MDS 9000 Family specific
all	All facilities	Cisco MDS 9000 Family specific
auth	Authorization system	Standard
authpriv	Authorization (private) system	Standard
bootvar	Bootvar	Cisco MDS 9000 Family specific
callhome	Call Home	Cisco MDS 9000 Family specific
cron	Cron or at facility	Standard
daemon	System daemons	Standard
fcc	FCC	Cisco MDS 9000 Family specific
fcdomain	fcdomain	Cisco MDS 9000 Family specific
fcns	Name server	Cisco MDS 9000 Family specific
fcs	FCS	Cisco MDS 9000 Family specific
flogi	FLOGI	Cisco MDS 9000 Family specific
fspf	FSPF	Cisco MDS 9000 Family specific
ftp	File Transfer Protocol	Standard
ipconf	IP configuration	Cisco MDS 9000 Family specific
ipfc	IPFC	Cisco MDS 9000 Family specific
kernel	Kernel	Standard
local0 to local7	Locally defined messages	Standard
lpr	Line printer system	Standard
mail	Mail system	Standard

Facility Keyword	Description	Standard or Cisco MDS Specific
mcast	Multicast	Cisco MDS 9000 Family specific
module	Switching module	Cisco MDS 9000 Family specific
news	USENET news	Standard
ntp	NTP	Cisco MDS 9000 Family specific
platform	Platform manager	Cisco MDS 9000 Family specific
port	Port	Cisco MDS 9000 Family specific
port-channel	PortChannel	Cisco MDS 9000 Family specific
qos	QoS	Cisco MDS 9000 Family specific
rdl	RDL	Cisco MDS 9000 Family specific
rib	RIB	Cisco MDS 9000 Family specific
rscn	RSCN	Cisco MDS 9000 Family specific
securityd	Security	Cisco MDS 9000 Family specific
syslog	Internal system messages	Standard
sysmgr	System manager	Cisco MDS 9000 Family specific
tlport	TL port	Cisco MDS 9000 Family specific
user	User process	Standard
uucp	UNIX-to-UNIX Copy Program	Standard
vhbad	Virtual host base adapter daemon	Cisco MDS 9000 Family specific
vni	Virtual network interface	Cisco MDS 9000 Family specific
vrrp_cfg	VRRP configuration	Cisco MDS 9000 Family specific
vrrp_eng	VRRP engine	Cisco MDS 9000 Family specific
vsan	VSAN system messages	Cisco MDS 9000 Family specific
vshd	vshd	Cisco MDS 9000 Family specific
wwn	WWN manager	Cisco MDS 9000 Family specific
xbar	Xbar system messages	Cisco MDS 9000 Family specific
zone	Zone server	Cisco MDS 9000 Family specific

Table 3: Error Message Severity Levels , on page 4 describes the severity levels supported by the system message logs.

Table 3: Error Message Severity Levels

Level Keyword	Level	Description	System Message Definition
emergencies	0	System unusable	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

Note Refer to the *Cisco MDS 9000 Family System Messages Reference* for details on the error log message format.

System Message Logging

The System Message Logging feature allows system messages to be logged for later reference. This feature has the following capabilities:

- Provides logging information for monitoring and troubleshooting.
- Allows the user to select the types of captured logging information.
- Allows the user to forward the captured logging information to remote logging servers.

Messages are time stamped to enhance real time debugging and message management.

By default, the switch logs normal but significant system messages to an onboard logfile and the system console as they occur. The onboard logfile is circular and can store up to the last 1200 messages. Messages stored in the onboard logfile can be viewed using the CLI.

System messages may be displayed in real time in a user's session to the switch. This allows real time monitoring of switch events when troubleshooting. The minimum severity of messages to be displayed to sessions is configurable.

System messages may also be logged to remote logging servers. Up to three remote destinations may be configured. These may be a mix of IPv4 and IPv6 addresses. By default, when a remote logging destination is configured, system messages are sent using UDP. From Cisco MDS NX-OS Release 9.2(1), logging over a secure Transport Layer Security (TLS) connection and mutual device authentication is supported. The Cisco MDS device is the TLS client and initiates a connection to the remote logging server. This allows transport encryption for secure logging over an unsecure network. From Cisco MDS NX-OS Release 9.2(2), distribution over Cisco Fabric Services (CFS) of secure syslog server configurations is supported.

Tip To be able to compare system messages from multiple devices ensure that all devices have the correct time. This will allow the sequence of events involving multiple devices to be understood. Device clocks can be synchronised by using NTP.

The system messages to be logged to each destination can be filtered based on the facility and the severity level.

SFP Diagnostics

The error message related to SFP failures is written to the syslog. You can listen to the syslog for events related to SFP failures. The values, low or high alarm, and the warning are checked for the following parameters:

- TX Power
- RX Power
- Temperature
- Voltage
- Current

The SFP notification trap indicates the current status of the alarm and warning monitoring parameters for all the sensors based on the digital diagnostic monitoring information. This notification is generated whenever there is a change in the status of at least one of the monitoring parameters of the sensors on the transceiver in an interface.

The CISCO-INTERFACE-XCVR-MONITOR-MIB contains the SFP notification trap information. Refer to the *Cisco MDS 9000 Family MIB Quick Reference* for more information on this MIB.

Outgoing System Message Logging Server Facilities

All system messages have a logging facility and a level. The logging facility can be thought of as *where* and the level can be thought of as *what*.

The single system message logging daemon (syslogd) sends the information based on the configured **facility** option. If no facility is specified, local7 is the default outgoing facility.

The internal facilities are listed in Table 2: Internal Logging Facilities , on page 2 and the outgoing logging facilities are listed in Table 4: Outgoing Logging Facilities , on page 5.

Table 4: Outgoing Logging Facilities

Facility Keyword	Description	Standard or Cisco MDS Specific
auth	Authorization system	Standard
authpriv	Authorization (private) system	Standard
cron	Cron or at facility	Standard
daemon	System daemons	Standard
ftp	File Transfer Protocol	Standard

Facility Keyword	Description	Standard or Cisco MDS Specific
kernel	Kernel	Standard
local0 to local7	Locally defined messages	Standard (local7 is the default)
lpr	Line printer system	Standard
mail	Mail system	Standard
news	USENET news	Standard
syslog	Internal system messages	Standard
user	User process	Standard
uucp	UNIX-to-UNIX Copy Program	Standard

System Message Logging Configuration Distribution

You can enable fabric distribution for all Cisco MDS switches in the fabric. When you perform system message logging configurations, and distribution is enabled, that configuration is distributed to all the switches in the fabric.

You automatically acquire a fabric-wide lock when you issue the first configuration command after you enabled distribution in a switch. The system message logging server uses the effective and pending database model to store or commit the commands based on your configuration. When you commit the configuration changes, the effective database is overwritten by the configuration changes in the pending database and all the switches in the fabric receive the same configuration. After making the configuration changes, you can choose to discard the changes by terminating the changes instead of committing them. In either case, the lock is released. See Using the CFS Infrastructure for more information on the CFS application.

Fabric Lock Override

If you have performed a system message logging task and have forgotten to release the lock by either committing or discarding the changes, an administrator can release the lock from any switch in the fabric. If the administrator performs this task, your changes to the pending database are discarded and the fabric lock is released.

Tip The changes are only available in the volatile directory and are subject to being discarded if the switch is restarted.

Guidelines and Limitations for System Message Logging

- CFS distribution must be enabled for synchronized distribution of secure syslog configuration across a fabric.
- In Cisco MDS NX-OS Release 9.2(1), you can either configure the secure option for remote system logging servers or CFS distribution of the system logging configuration. You cannot configure both. If

you try configuring a secure remote destination when CFS distribution for logging is enabled, you will be prompted with a message to disable CFS distribution for logging before configuring a secure remote destination, and vice versa.

- CA certificates must be installed for a TLS connection to be used and mutual authentication of secure remote logging server connections. Hence, a warning message is displayed after each secure syslog configuration command. For information on configuring CA certificates, see the "Configuring Certificate Authorities and Digital Certificates" chapter in the Cisco MDS 9000 Series Security Configuration Guide, Release 9.x.
- Any system messages that are logged before any remote syslog servers are reachable (such as supervisor active or online messages) will not be sent to the syslog server.

When merging two fabrics with CFS that have different system message logging configurations, follow these guidelines:

- Be aware that the merged configuration is a union of the existing and received configuration for each switch in the fabric.
- Verify that the merged configuration will only have a maximum of three unique system message logging servers.

Caution If the merged configuration contains more that three servers, the merge will fail.

For detailed concepts on CFS merge, see CFS Merge Support.

Default Settings

Table 5: Default System Message Log Settings , on page 7 lists the default settings for system message logging.

Table 5: Default System Message Log Settings

Parameters	Default
System message logging to the console	Enabled for messages at the critical severity level.
System message logging to sessions	Disabled.
Onboard logging file size	4194304 bytes.
Onboard logging file name	messages
Remote server facility	local7
Remote logging destinations	Not configured.
Unsecure remote server destination port	UDP 514
Secure remote server destination port	TCP 6514

Parameters	Default
CA certificates	Not installed.

Configuring System Message Logging

System logging messages are sent to the console based on the default (or configured) logging facility and severity values.

Task Flow for Configuring System Message Logging

Follow these steps to configure system message logging:

Procedure

Step 1 Enable or disable message logging.
Step 2 Configure console severity level.
Step 3 Configure monitor severity level.
Step 4 Configure module log severity level.
Step 5 Configure facility severity levels.
Step 6 Configure the onboard log file.
Step 7 Configure system message logging servers.
Step 8 Configure system message logging distribution.

Enabling or Disabling Message Logging

You can disable logging to the console or enable logging to a specific Telnet or SSH session.

- When you disable or enable logging to a console session, that state is applied to all future console sessions. If you exit and log in again to a new session, the state is preserved.
- When you enable or disable logging to a Telnet or SSH session, that state is applied only to that session. If you exit and log in again to a new session, the state is not preserved.

To enable or disable the logging state for a Telnet or SSH session, follow these steps:

Procedure

Step 1 switch# **terminal monitor**

Enables logging for a Telnet or SSH session.

Note Logging to the console session is enabled by default.

Step 2 switch# **terminal no monitor**

Disables logging for a Telnet or SSH session.

Note A Telnet or SSH session is disabled by default.

Configuring Console Severity Level

When logging is enabled for a console session (default), you can configure the severity levels of messages that appear on the console. The default severity for console logging is 2 (critical).

Note The current critical (default) logging level is maintained if the console baud speed is 9600 baud (default). All attempts to change the console logging level generates an error message. To increase the logging level (above critical), you must change the console baud speed to 38400 baud.

To configure the severity level for the console session, follow these steps:

Procedure

Step 1 switch# **configure terminal**

Enters configuration mode.

Step 2 switch(config)# **logging console 3**

Configures console logging at level 3 (error). Logging messages with a severity level of 3 or above are displayed on the console.

Step 3 switch(config)# **no logging console**

Reverts console logging to the factory set default severity level of 2 (critical). Logging messages with a severity level of 2 or above are displayed on the console.

Configuring Monitor Severity Level

When logging is enabled for a monitor session (default), you can configure the severity levels of messages that appear on the monitor. The default severity for monitor logging is 5 (notifications).

To configure the severity level for a monitor session, follow these steps:

Procedure

Step 1 switch# **configure terminal**

Enters configuration mode.

Step 2 switch(config)# **logging monitor 3**

Configures monitor logging at level 3 (error). Logging messages with a severity level of 3 or above are displayed on the monitor.

Step 3 switch(config)# **no logging monitor**

Reverts monitor logging to the factory set default severity level of 5 (notifications). Logging messages with a severity level of 5 or above are displayed on the console.

Configuring Module Logging

By default, logging is enabled at level 7 for all modules. You can enable or disable logging for each module at a specified level.

To enable or disable the logging for modules and configure the severity level, follow these steps:

Procedure

Step 1 switch# **configure terminal**

Enters configuration mode.

Step 2 switch(config)# **logging module 1**

Configures module logging at level 1 (alerts) for all modules.

Step 3 switch(config)# **logging module**

Configures module logging for all modules in the switch at the default level 5 (notifications).

Step 4 switch(config)# **no logging module**

Disables module logging.

Configuring Facility Severity Levels

To configure the severity level for a logging facility (see Table 2: Internal Logging Facilities , on page 2), follow these steps:

Procedure

Step 1 switch# **configure terminal**

Enters configuration mode.

Step 2 switch(config)# **logging level kernel 4**

Configures Telnet or SSH logging for the kernel facility at level 4 (warning). As a result, logging messages with a severity level of 4 or above are displayed.

Step 3 switch(config)# **no logging level kernel 4**

Reverts to the default severity level 6 (informational) for the Telnet or SSH logging for the kernel facility.

Note Use the **show logging info** command to display the default logging levels for the facilities listed in Table 2: Internal Logging Facilities , on page 2.

Configuring the Onboard Log File

By default, the switch logs normal but significant system messages to a log file and sends these messages to the system console. Log messages are not saved across system reboots. The logging messages that are generated may be saved to a log file. You can configure the name of this file and restrict its size as required. The default log file name is messages.

The file name can have up to 80 characters and the file size ranges from 4096 bytes to 4194304 bytes.

To send log messages to a file, follow these steps:

Procedure

Step 1 switch# **configure terminal**

Enters configuration mode.

Step 2 switch(config)# **logging logfile messages 3**

Configures logging of information for errors or events above with a severity level 3 or above to the default log file named messages.

Step 3 switch(config)# **logging logfile ManagerLog 3**

Configures logging of information for errors or events with a severity level 3 or above to a file named ManagerLog using the default size of 10,485,760 bytes.

Step 4 switch(config)# **logging logfile ManagerLog 3 size 3000000**

Configures logging information for errors or events with a severity level 3 or above to a file named ManagerLog. By configuring a size, you are restricting the file size to 3,000,000 bytes.

Step 5 switch(config)# **no logging logfile**

Disables logging messages to the logfile.

You can rename the log file using the **logging logfile** command.

The location of the log file cannot be changed. You can use the **show logging logfile** and clear logging logfile commands to view and delete the contents of this file. You can use the **dir log:** command to view logging file statistics. You can use the **delete log:** command to remove the log file.

You can copy the logfile to a different location using the **copy log:** command using additional copy syntax.

Configuring System Message Logging to Remote Logging Destinations

To configure system message logging to a remote logging destination, follow these steps:

Procedure

Step 1 switch# **configure terminal**

Enters configuration mode.

Step 2 switch(config)# **logging server** *name* [*severity-level*] [**port** *number*] [**secure** [**trustpoint client-identity** *name*]] [**facility** *facility-name*]

Configures system message logging to a remote destination at the specified hostname, IPv4, or IPv6 address. Specify the minimum severity of forwarded messages with the *severity-level* parameter. Use the **port** option to override the default destination port number. Use the **secure** option to use TCP, use the secure destination port, and encrypt the connection to the remote logging server using TLS. For TLS mutual authentication to succeed, identity certificates signed by trusted CAs must be installed using **crypto** commands. By default, certificates from all trust points are sequentially tried until authentication succeeds. Optionally, the certificates used for authentication may be restricted to a single trust point by specifying the **trustpoint client-identity** option. Use the **facility** option to specify a different logging category.

Step 3 switch(config)# **syslog priority** 1 **msg** "test message"

(Optional) Logs a test message to all system message logging destinations. This may be used to verify that logging to remote destinations is working.

Step 4 switch(config)# **no logging server** *name*

Removes the specified server as a destination for system message logs.

Configuring the Origin ID for System Messages

To specify the hostname, IP address, or a text string in the system messages that are sent to remote syslog servers, follow these steps:

Procedure

Step 1 switch# **configure**

Enters configuration mode.

Step 2 switch(config)# **logging origin-id** {**hostname** | **ip** *address* | **string** *word*}

Specifies the hostname, IP address, or a text string in the system messages that are sent to remote syslog servers.

Configuring System Message Logging Servers

You can configure a maximum of three system message logging servers. To send log messages to a UNIX system message logging server, you must configure the system message logging daemon on a UNIX server. Log in as a privileged user, and follow these steps:

Procedure

Step 1 Add the following line to the /etc/syslog.conf file.

local1.debug /var/log/ myfile .log

Note Be sure to add five tab characters between **local1.debug** and **/var/log/***myfile***.log**. Refer to entries in the /etc/syslog.conf file for further examples.

The switch sends messages according to the specified facility types and severity levels. The **local1** keyword specifies the UNIX logging facility used. The messages from the switch are generated by user processes. The **debug** keyword specifies the severity level of the condition being logged. You can set UNIX systems to receive all messages from the switch.

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

$ touch /var/log/ myfile .log

$ chmod 666 /var/log/ myfile .log

Step 3 Make sure the system message logging daemon reads the new changes by entering this command:

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

Configuring System Message Logging Distribution

To enable fabric distribution for system message logging server configurations, follow these steps:

Procedure

Step 1 switch# **configure terminal**

Enters configuration mode.

Step 2 switch(config)# **logging distribute**

Enables the system message logging server configuration to be distributed to all switches in the fabric, acquires a lock, and stores all future configuration changes in the pending database.

Step 3 switch(config)# **no logging distribute**

Disables (default) system message logging server configuration distribution to all switches in the fabric.

Committing Changes

To commit the system message logging server configuration changes, follow these steps:

Procedure

Step 1 switch# **configure terminal**

Enters configuration mode.

Step 2 switch(config)# **logging commit**

Distributes the configuration changes to all switches in the fabric, releases the lock, and overwrites the effective database with the changes made to the pending database.

Discarding Changes

To discard the system message logging server configuration changes, follow these steps:

Procedure

Step 1 switch# **configure terminal**

Enters configuration mode.

Step 2 switch(config)# **logging abort**

Discards the system message logging server configuration changes in the pending database and releases the fabric lock.

Fabric Lock Override

To use administrative privileges and release a locked system message logging session, use the **clear logging session** command.

```
switch# clear logging session
```

Displaying System Message Logging Information

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

Command	Purpose
show logging	Displays current system message logging.
show logging nvram	Displays NVRM log contents.

Command	Purpose
show logging logfile	Displays the log file.
show logging level	Displays logging facility.
show logging info	Displays logging information.
show logging last 2	Displays last few lines of a log file.
show logging module	Displays switching module logging status.
show logging monitor	Displays monitor logging status.
show logging server	Displays server information.

For detailed information about the fields in the output from these commands, refer to the *Cisco MDS 9000 Family Command Reference* .

Use the **show logging** command to display the current system message logging configuration . See Examples Current System Message Logging, on page 15 to Remote Logging Server Information, on page 20.

Note When using the **show logging** command, output is displayed only when the configured logging levels for the switch are different from the default levels.

Current System Message Logging

The following example displays the current system message logging settings and contents of the onboard log file:

```
switch# show logging

Logging console:                 enabled (Severity: critical)
Logging monitor:                 enabled (Severity: debugging)
Logging linecard:                enabled (Severity: debugging)
Logging server:                  enabled
{172.20.102.34}
        server severity:         debugging
        server facility:         local7
{10.77.202.88}
        server severity:         debugging
        server facility:         local7
{10.77.202.149}
        server severity:         debugging
        server facility:         local7
Logging logfile:                 enabled
        Name - messages: Severity - debugging Size - 4194304
Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
kern                    6                       6
user                    3                       3
mail                    3                       3
daemon                  7                       7
auth                    0                       7
syslog                  3                       3
```

```
lpr                     3                       3
news                    3                       3
uucp                    3                       3
cron                    3                       3
authpriv                3                       7
ftp                     3                       3
local0                  3                       3
local1                  3                       3
local2                  3                       3
local3                  3                       3
local4                  3                       3
local5                  3                       3
local6                  3                       3
local7                  3                       3
vsan                    2                       2
fspf                    3                       3
fcdomain                2                       2
module                  5                       5
sysmgr                  3                       3
zone                    2                       2
vni                     2                       2
ipconf                  2                       2
ipfc                    2                       2
xbar                    3                       3
fcns                    2                       2
fcs                     2                       2
acl                     2                       2
tlport                  2                       2
port                    5                       5
flogi                   2                       2
port_channel            5                       5
wwn                     3                       3
fcc                     2                       2
qos                     3                       3
vrrp_cfg                2                       2
ntp                     2                       2
platform                5                       5
vrrp_eng                2                       2
callhome                2                       2
mcast                   2                       2
rdl                     2                       2
rscn                    2                       2
bootvar                 5                       2
securityd               2                       2
vhbad                   2                       2
rib                     2                       2
vshd                    5                       5
0(emergencies)          1(alerts)       2(critical)
3(errors)               4(warnings)     5(notifications)
6(information)          7(debugging)
Feb 14 09:50:57 switchname %TTYD-6-TTYD_MISC: TTYD TTYD started
Feb 14 09:50:58 switchname %DAEMON-6-SYSTEM_MSG: precision = 8 usec
...
```

Use the **show logging nvram** command to view the log messages saved in NVRAM. Only log messages with a severity level of critical and below (levels 0, 1, and 2) are saved in NVRAM.

NVRM Log Contents

The following example displays the NVRM log contents:

```
switch# show logging nvram

Jul 16 20:36:46 switchname %KERN-2-SYSTEM_MSG: unable to alloc and fill in a
new mtsbuf (pid=2209, ret_val = -105)
Jul 16 20:36:46 switchname %KERN-2-SYSTEM_MSG: unable to alloc and fill in a
new mtsbuf (pid=2199, ret_val = -105)
Jul 16 20:36:46 switchname %KERN-2-SYSTEM_MSG: unable to alloc and fill in a
new mtsbuf (pid=2213, ret_val = -105)
Jul 16 20:36:46 switchname %KERN-2-SYSTEM_MSG: unable to alloc and fill in a
new mtsbuf (pid=2213, ret_val = -105)
...
```

Log File

The following example displays the onboard log file:

```
switch# show logging logfile

Jul 16 21:06:50 %DAEMON-3-SYSTEM_MSG: Un-parsable frequency in /mnt/pss/ntp.drift
Jul 16 21:06:56 %DAEMON-3-SYSTEM_MSG: snmpd:snmp_open_debug_cfg: no snmp_saved_dbg_uri ;
Jul 16 21:06:58 switchname %PORT-5-IF_UP: Interface mgmt0 is up
Jul 16 21:06:58 switchname %MODULE-5-ACTIVE_SUP_OK: Supervisor 5 is active
...
```

Console Logging Status

The following example displays the console logging status:

```
switch# show logging console

Logging console:                enabled (Severity: notifications)
```

Logging Facility

The following example displays the logging level of each switch facility:

```
switch# show logging level

Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
kern                    6                       6
user                    3                       3
mail                    3                       3
daemon                  7                       7
auth                    0                       7
syslog                  3                       3
lpr                     3                       3
news                    3                       3
uucp                    3                       3
cron                    3                       3
authpriv                3                       7
ftp                     3                       3
local0                  3                       3
local1                  3                       3
local2                  3                       3
```

```
local3                  3                       3
local4                  3                       3
local5                  3                       3
local6                  3                       3
local7                  3                       3
vsan                    2                       2
fspf                    3                       3
fcdomain                2                       2
module                  5                       5
sysmgr                  3                       3
zone                    2                       2
vni                     2                       2
ipconf                  2                       2
ipfc                    2                       2
xbar                    3                       3
fcns                    2                       2
fcs                     2                       2
acl                     2                       2
tlport                  2                       2
port                    5                       5
flogi                   2                       2
port_channel            5                       5
wwn                     3                       3
fcc                     2                       2
qos                     3                       3
vrrp_cfg                2                       2
ntp                     2                       2
platform                5                       5
vrrp_eng                2                       2
callhome                2                       2
mcast                   2                       2
rdl                     2                       2
rscn                    2                       2
bootvar                 5                       2
securityd               2                       2
vhbad                   2                       2
rib                     2                       2
vshd                    5                       5
0(emergencies)          1(alerts)       2(critical)
3(errors)               4(warnings)     5(notifications)
6(information)          7(debugging)
```

Logging Information

The following example displays the current system message logging settings:

```
switch# show logging info

Logging console:                enabled (Severity: critical)
Logging monitor:                enabled (Severity: debugging)
Logging linecard:               enabled (Severity: debugging)
Logging server:                 enabled
{192.168.1.34}
        server severity:        debugging
        server facility:        local7
{192.168.1.88}
        server severity:        debugging
        server facility:        local7
{192.168.1.149}
        server severity:        debugging
        server facility:        local7
```

```
Logging logfile:                enabled
        Name - messages: Severity - debugging Size - 4194304
Facility        Default Severity        Current Session Severity
--------        ----------------        ------------------------
kern                    6                       6
user                    3                       3
mail                    3                       3
daemon                  7                       7
auth                    0                       7
syslog                  3                       3
lpr                     3                       3
news                    3                       3
uucp                    3                       3
cron                    3                       3
authpriv                3                       7
ftp                     3                       3
local0                  3                       3
local1                  3                       3
local2                  3                       3
local3                  3                       3
local4                  3                       3
local5                  3                       3
local6                  3                       3
local7                  3                       3
vsan                    2                       2
fspf                    3                       3
fcdomain                2                       2
module                  5                       5
sysmgr                  3                       3
zone                    2                       2
vni                     2                       2
ipconf                  2                       2
ipfc                    2                       2
xbar                    3                       3
fcns                    2                       2
fcs                     2                       2
acl                     2                       2
tlport                  2                       2
port                    5                       5
flogi                   2                       2
port_channel            5                       5
wwn                     3                       3
fcc                     2                       2
qos                     3                       3
vrrp_cfg                2                       2
ntp                     2                       2
platform                5                       5
vrrp_eng                2                       2
callhome                2                       2
mcast                   2                       2
rdl                     2                       2
rscn                    2                       2
bootvar                 5                       2
securityd               2                       2
vhbad                   2                       2
rib                     2                       2
vshd                    5                       5
0(emergencies)          1(alerts)       2(critical)
3(errors)               4(warnings)     5(notifications)
6(information)          7(debugging)
```

Last Few Lines of a Log File

The following example displays the last few lines of a log file:

```
switch# show logging last 2

Nov 8 16:48:04 switchname %LOG_VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console from pts/1
 (171.71.58.56)
Nov 8 17:44:09 switchname %LOG_VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console from pts/0
 (171.71.58.72)
```

Switching Module Logging Status

The following example displays switching module logging status:

```
switch# show logging module


Logging linecard:                enabled (Severity: debugging)
```

Monitor Logging Status

The following example displays the monitor logging status:

```
switch# show logging monitor

Logging monitor:                 enabled (Severity: information)
```

Remote Logging Server Information

The following example displays the configured remote logging server information:

```
switch# show logging server
Logging server:                  enabled
{192.168.113.1}
        server severity:         notifications
        server facility:         local7
        server VRF:              default
        server port:             55552
        server transport:        secure
{192.168.106.50}
        server severity:         notifications
        server facility:         local7
        server VRF:              default
        server port:             55551
        server transport:        secure
{192.168.229.220}
        server severity:         notifications
        server facility:         local7
        server VRF:              default
        server port:             55552
```

Additional References

For additional information related to implementing system message logging, see the following section:

MIBs

MIBs	MIBs Link
• CISCO-SYSLOG-EXT-MIB • CISCO-SYSLOG-MIB	To locate and download MIBs, go to the following URL: http://www.cisco.com/en/US/products/ps5989/prod_technical_reference_list.html