



Configuring System Message Logging

This chapter describes how to configure system message logging on the Catalyst 6500 series switches.



Note

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 6500 Series Switch Command Reference* publication.



Note

For more information on system messages, refer to the *System Message Guide—Catalyst 6500 Series, Catalyst 4000 Family, Catalyst 2948G, and Catalyst 2980G Switches*.

This chapter consists of these sections:

- [Understanding How System Message Logging Works, page 27-1](#)
- [System Log Message Format, page 27-3](#)
- [Default System Message Logging Configuration, page 27-4](#)
- [Configuring System Message Logging on the Switch, page 27-5](#)

Understanding How System Message Logging Works

The system message logging software can save messages in a log file or direct the messages to other devices. The system message logging facility has these features:

- Provides you with logging information for monitoring and troubleshooting
- Allows you to select the types of logging information captured
- Allows you to select the destination of captured logging information

By default, the switch logs normal but significant system messages to its internal buffer and sends these messages to the system console. You can specify which system messages should be saved based on the type of facility (see [Table 27-1](#)) and the severity level (see [Table 27-2](#)). Messages are time stamped to enhance real-time debugging and management.

You can access logged system messages 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 that can store up to 500 messages. You can monitor system messages remotely by accessing the switch through Telnet or the console port, or by viewing the logs on a syslog server.

In the event of a system failure, the system `syslog-dump` feature allows you to write system messages in the `syslog` buffer to a Flash file, capturing pertinent `syslog` information before the system fails. If the system `core-dump` feature is enabled, the `syslog` is dumped before the core.

**Note**

When the switch first initializes, the network is not connected until the initialization completes. Therefore, messages that are redirected to a `syslog` server are delayed up to 90 seconds.

Table 27-1 describes the facility types that are supported by the system message logs.

Table 27-1 System Message Log Facility Types

Facility Name	Definition
all	All facilities
acl	ACL facility
cdp	Cisco Discovery Protocol
cops	Common Open Policy Server
dtp	Dynamic Trunking Protocol
dvlan	Dynamic VLAN
earl	Enhanced Address Recognition Logic
fileSYS	File System
gvrp	GARP VLAN Registration Protocol
ip	Internet Protocol
kernel	Kernel
ld	ASLB facility
mcast	Multicast
mgmt	Management
mls	Multilayer Switching
pagp	Port Aggregation Protocol
protfilt	Protocol Filter
pruning	VTP pruning
privatevlan	Private VLAN facility
qos	Quality of Service
radius	Remote Access Dial-In User Service
rsvp	ReSerVation Protocol
security	Security
snmp	Simple Network Management Protocol
spantree	Spanning Tree Protocol
sys	System
tac	Terminal Access Controller
tcp	Transmission Control Protocol

Table 27-1 System Message Log Facility Types (continued)

Facility Name	Definition
telnet	Terminal Emulation Protocol
tftp	Trivial File Transfer Protocol
udld	User Datagram Protocol
vmps	VLAN Membership Policy Server
vtp	VLAN Trunking Protocol

Table 27-2 describes the severity levels that are supported by the system message logs.

Table 27-2 Severity Level Definitions

Severity Level	Description
0—emergencies	System unusable
1—alerts	Immediate action required
2—critical	Critical condition
3—errors	Error conditions
4—warnings	Warning conditions
5—notifications	Normal bug significant condition
6—informational	Informational messages
7—debugging	Debugging messages

System Log Message Format

System log messages begin with a percent sign (%) and can contain up to 80 characters. Messages are displayed in the following format:

mm/dd/yyyy:hh/mm/ss:facility-severity-MNEMONIC:description

Table 27-3 describes the elements of syslog messages.

Table 27-3 System Log Message Elements

Element	Description
<i>mm/dd/yyyy:hh/mm/ss</i>	Date and time of the error or event. This information appears only if configured using the set logging timestamp enable command.
<i>facility</i>	Indicates the facility to which the message refers (for example, SNMP, SYS, etc.).
<i>severity</i>	Single-digit code from 0 to 7 that indicates the severity of the message.
<i>MNEMONIC</i>	Text string that uniquely describes the error message.
<i>description</i>	Text string containing detailed information about the event being reported.

This example shows typical switch system messages (at system startup):

```
1999 Apr 16 10:01:26 %MLS-5-MLSENABLED:IP Multilayer switching is enabled
1999 Apr 16 10:01:26 %MLS-5-NDEDISABLED:Netflow Data Export disabled
1999 Apr 16 10:01:26 %SYS-5-MOD_OK:Module 1 is online
1999 Apr 16 10:01:47 %SYS-5-MOD_OK:Module 3 is online
1999 Apr 16 10:01:42 %SYS-5-MOD_OK:Module 6 is online
1999 Apr 16 10:02:27 %PAGP-5-PORTTOSTP:Port 3/1 joined bridge port 3/1
1999 Apr 16 10:02:28 %PAGP-5-PORTTOSTP:Port 3/2 joined bridge port 3/2
```

Default System Message Logging Configuration

Table 27-4 describes the default system message logging configuration.

Table 27-4 Default System Message Logging Configuration

Configuration Parameter	Default Setting
System message logging to the console	Enabled
System message logging to Telnet sessions	Enabled
Logging buffer size	500 (default and maximum setting)
Logging history size	1
Logging history severity	Warnings (4)
Timestamp option	Enabled
Logging server	Disabled
Syslog server IP address	None configured
Server facility	LOCAL7
Server severity	Warnings (4)
Facility/severity level for system messages	sys/5 dtp/5 pagp/5 mgmt/5 mls/5 cdp/4 udld/4 <i>all other facilities/2</i>
System syslog dump	Disabled
System syslog-dump device and filename specifications	Flash device is slot0: File name is sysloginfo

Configuring System Message Logging on the Switch

These sections describe how to configure system message logging on the switch:

- [Enabling and Disabling Session Logging Settings, page 27-5](#)
- [Setting the System Message Logging Levels, page 27-6](#)
- [Enabling and Disabling the Logging Time Stamp Enable State, page 27-7](#)
- [Setting the Logging Buffer Size, page 27-7](#)
- [Limiting the Number of syslog Messages, page 27-7](#)
- [Configuring the syslog Daemon on a UNIX syslog Server, page 27-8](#)
- [Configuring syslog Servers, page 27-8](#)
- [Displaying the Logging Configuration, page 27-9](#)
- [Displaying System Messages, page 27-11](#)
- [Enabling and Disabling the System syslog Dump, page 27-11](#)
- [Specifying the System syslog Dump Flash Device and Filename, page 27-12](#)

Enabling and Disabling Session Logging Settings

By default, system logging messages are sent to console and Telnet sessions that are based on the default logging facility and severity values. If desired, you can disable logging to the console or logging to a given Telnet session.

When you disable or enable logging to console sessions, the enable state is applied to all future console sessions. For example, if you disable logging to the console, disconnect from the console port, and later reconnect, logging is still disabled for the console.

In contrast, when you disable or enable logging to a Telnet session, the enable state is applied only to that session. If you disable logging to a Telnet session, disconnect the session, and later reconnect, logging is enabled for the new session.



Note

If you enter the **set logging session** command while connected through the console port, the command has the same effect as entering the **set logging console** command. However, if you enter the **set logging console** command while connected through a Telnet session, the default console logging enable state is changed.

To enable or disable the logging state for console sessions, perform this task in privileged mode:

	Task	Command
Step 1	Enable or disable the default logging state for console sessions.	set logging console {enable disable}
Step 2	Verify the logging configuration.	show logging [noalias]

This example shows how to disable logging to the current and future console sessions:

```
Console> (enable) set logging console disable
System logging messages will not be sent to the console.
Console> (enable)
```

To enable or disable the logging state for the current Telnet session, perform this task in privileged mode:

	Task	Command
Step 1	Enable or disable the logging state for a Telnet session.	set logging session {enable disable}
Step 2	Verify the logging configuration.	show logging [noalias]

This example shows how to disable logging to the current Telnet session:

```
Console> (enable) set logging session disable
System logging messages will not be sent to the current login session.
Console> (enable)
```

Setting the System Message Logging Levels

You can set the severity level for each logging facility using the **set logging level** command. Enter the **all** keyword to specify all facilities. Enter the **default** keyword to make the specified severity level the default for the specified facilities. If you do not enter the **default** keyword, the specified severity level applies only to the current session.

To set the system message logging severity level setting for a logging facility, perform this task in privileged mode:

	Task	Command
Step 1	Set the severity level for logging facilities.	set logging level {all facility} severity [default]
Step 2	Verify the system message logging configuration.	show logging [noalias]

This example shows how to set the logging severity level to 5 for all facilities (for the current session only):

```
Console> (enable) set logging level all 5
All system logging facilities for this session set to severity 5(notifications)
Console> (enable)
```

This example shows how to set the default logging severity level to 3 for the **cdp** facility:

```
Console> (enable) set logging level cdp 3 default
System logging facility <cdp> set to severity 3(errors)
Console> (enable)
```

Enabling and Disabling the Logging Time Stamp Enable State

To enable or disable the logging time stamp, perform this task in privileged mode:

	Task	Command
Step 1	Enable or disable the logging time stamp state.	set logging timestamp {enable disable}
Step 2	Verify the logging time stamp state.	show logging [noalias]

This example shows how to enable the time stamp display on system logging messages:

```
Console> (enable) set logging timestamp enable
System logging messages timestamp will be enabled.
Console> (enable)
```

Setting the Logging Buffer Size

To set the number of messages to log to the logging buffer, perform this task in privileged mode:

	Task	Command
Step 1	Set the number of messages to log to the logging buffer.	set logging buffer <i>buffer_size</i>
Step 2	Verify the system message logging configuration.	show logging [noalias]

This example shows how to set the logging buffer size to 200 messages:

```
Console> (enable) set logging buffer 200
System logging buffer size set to <200>
Console> (enable)
```

Limiting the Number of syslog Messages

You can limit the number of syslog messages that are sent to the history table and the SNMP network management station based on severity. The default severity is set to warnings(4).

To limit the number of syslog messages, perform this task in privileged mode:

	Task	Command
Step 1	Limit the number of syslog messages.	set logging history severity <i>severity_level</i>
Step 2	Verify the system message logging configuration.	show logging

This example shows how to limit the number of syslog messages to messages with a severity level of notifications(5):

```
Console> (enable) set logging history severity 5
System logging history set to severity <5>
Console> (enable)
```

Configuring the syslog Daemon on a UNIX syslog Server

Before you can send system log messages to a UNIX syslog server, you must configure the syslog daemon on a UNIX server. Log in as root, and perform these steps:

Step 1 Add a line such as the following to the file `/etc/syslog.conf`:

```
user.debug                /var/log/myfile.log
```



Note There must be five tab characters between **user.debug** and `/var/log/myfile.log`. Refer to entries in the `/etc/syslog.conf` file for further examples.

The switch sends messages according to specified facility types and severity levels. The **user** keyword specifies the UNIX logging facility that is 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 that the syslog daemon reads the new changes by entering this command:

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

Configuring syslog Servers



Note Before you can send system log messages to a UNIX syslog server, you must configure the syslog daemon on the UNIX server as described in the “[Configuring the syslog Daemon on a UNIX syslog Server](#)” section on page 27-8.

To configure the switch to log messages to a syslog server, perform this task in privileged mode:

	Task	Command
Step 1	Specify the IP address of one or more syslog servers ¹ .	set logging server <i>ip_addr</i>
Step 2	Set the facility and severity levels for syslog server messages.	set logging server facility <i>server_facility_parameter</i> set logging server severity <i>server_severity_level</i>
Step 3	Enable system message logging to configured syslog servers.	set logging server enable
Step 4	Verify the configuration.	show logging [noalias]

1. You can configure a maximum of three syslog servers.

This example shows how to specify a syslog server, set the facility and severity levels, and enable logging to the server:

```
Console> (enable) set logging server 10.10.10.100
10.10.10.100 added to System logging server table.
Console> (enable) set logging server facility local5
System logging server facility set to <local5>
Console> (enable) set logging server severity 5
System logging server severity set to <5>
Console> (enable) set logging server enable
System logging messages will be sent to the configured syslog servers.
Console> (enable)
```

To delete a syslog server from the syslog server table, perform this task in privileged mode:

Task	Command
Delete a syslog server from the syslog server table.	clear logging server <i>ip_addr</i>

This example shows how to delete a syslog server from the syslog server table:

```
Console> (enable) clear logging server 10.10.10.100
System logging server 10.10.10.100 removed from system logging server table.
Console> (enable)
```

To disable logging to the syslog server, perform this task in privileged mode:

Task	Command
Disable system message logging to configured syslog servers.	set logging server disable

This example shows how to disable logging to syslog servers:

```
Console> (enable) set logging server disable
System logging messages will not be sent to the configured syslog servers.
Console> (enable)
```

Displaying the Logging Configuration

Enter the **show logging** command to display the current system message logging configuration. Enter the **noalias** keyword to display the IP addresses instead of the host names of the configured syslog servers.

To display the current system message logging configuration, perform this task:

Task	Command
Display the current system message logging configuration.	show logging [noalias]

This example shows how to display the current system message logging configuration:

```

Console> (enable) show logging
Logging buffered size:      500
      timestamp option:    enabled
Logging history size:      1
      severity:            notifications(5)
Logging console:           enabled
Logging server:            disabled
      server facility:     LOCAL7
      server severity:     warnings(4)
Current Logging Session:   enabled

```

Facility	Default Severity	Current Session Sever
-----	-----	-----
acl	5	5
cdp	4	4
cops	3	3
dtp	5	5
dvlan	2	2
earl	2	2
filesys	2	2
gvrp	2	2
ip	2	2
kernel	2	2
ld	3	3
mcast	2	2
mgmt	5	5
mls	5	5
pagp	5	5
protfilt	2	2
pruning	2	2
privatevlan	3	3
qos	3	3
radius	2	2
rsvp	3	3
security	2	2
snmp	2	2
spantree	2	2
sys	5	5
tac	2	2
tcp	2	2
telnet	2	2
tftp	2	2
udld	4	4
vmps	2	2
vtp	2	2
0 (emergencies)	1 (alerts)	2 (critical)
3 (errors)	4 (warnings)	5 (notifications)
6 (information)	7 (debugging)	

```

Console> (enable)

```

Displaying System Messages

Enter the **show logging buffer** command to display the messages in the switch logging buffer. If you do not specify *number_of_messages*, the default is to display the last 20 messages in the buffer (-20).

To display the messages in the switch logging buffer, perform one of these tasks:

Task	Command
Display the first <i>number_of_messages</i> messages in the buffer.	show logging buffer [<i>number_of_messages</i>]
Display the last <i>number_of_messages</i> messages in the buffer.	show logging buffer - [<i>number_of_messages</i>]

This example shows how to display the first five messages in the buffer:

```
Console> (enable) show logging buffer 5
1999 Apr 16 08:40:11 %SYS-5-MOD_OK:Module 1 is online
1999 Apr 16 08:40:14 %SYS-5-MOD_OK:Module 3 is online
1999 Apr 16 08:40:14 %SYS-5-MOD_OK:Module 2 is online
1999 Apr 16 08:41:15 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1
1999 Apr 16 08:41:15 %PAGP-5-PORTTOSTP:Port 2/2 joined bridge port 2/2
```

This example shows how to display the last five messages in the buffer:

```
Console> (enable) show logging buffer -5
%PAGP-5-PORTFROMSTP:Port 3/1 left bridge port 3/1
%SPANTREE-5-PORTDEL_SUCCESS:3/2 deleted from vlan 1 (PAgP_Group_Rx)
%PAGP-5-PORTFROMSTP:Port 3/2 left bridge port 3/2
%PAGP-5-PORTTOSTP:Port 3/1 joined bridge port 3/1-2
%PAGP-5-PORTTOSTP:Port 3/2 joined bridge port 3/1-2
Console> (enable)
```

Enabling and Disabling the System syslog Dump

If the system fails, a file containing the system messages in the syslog buffer (as displayed when entering the **show logging buffer** command) is produced.

To enable or disable the system syslog dump, perform this task in privileged mode (by default, the syslog dump is disabled):

	Task	Command
Step 1	Enable or disable the system syslog dump.	set system syslog-dump {enable disable}
Step 2	Verify the status of the system syslog dump.	show system

This example shows how to enable the system syslog dump:

```
Console> (enable) set system syslog-dump enable
(1) In the event of a system crash, this feature will
cause a syslog file to be written out.
(2) Selected syslog file is slot0:sysloginfo
(3) Please make sure the above device has been installed,
and ready to use.
Syslog-dump enabled
Console> (enable)
```

This example shows how to disable the system syslog dump:

```
Console> (enable) set system syslog-dump disable
Syslog-dump disabled
Console> (enable)
```

This example shows how to display the status of the system syslog dump:

```
Console> (enable) show system
PS1-Status PS2-Status
-----
ok          none

Fan-Status Temp-Alarm Sys-Status Uptime d,h:m:s Logout
-----
ok          off          ok          1,00:03:18  20 min
.
.
.
Core Dump           Core File
-----
disabled           slot0:crashinfo

Syslog Dump           Syslog File
-----
enabled            slot0:sysloginfo
Console> (enable)
```

Specifying the System syslog Dump Flash Device and Filename

You can change the Flash device and the filename when the syslog dump is enabled or disabled. If you only specify the Flash device, the filename is automatically set to sysloginfo. If you do not specify the Flash device or the filename, the previous filename for the system syslog dump is cleared and the default Flash device and filename (slot0:sysloginfo) are used.

To specify the Flash device and filename for the system syslog dump, perform this task in privileged mode:

	Task	Command
Step 1	Specify the Flash device and filename for the system syslog dump.	set system syslog-file [<i>device</i> : <i>filename</i>]
Step 2	Verify the Flash device and filename settings.	show system

This example shows how to set the Flash device for the system syslog dump:

```
Console> (enable) set system syslog-file bootflash:
Default filename sysloginfo added to the device bootflash:
System syslog-file set.
Console> (enable)
```

This example shows how to set the Flash device and the filename:

```
Console> (enable) set system syslog-file bootflash:sysmsgsl
System syslog-file set.
Console> (enable)
```

This example shows how to restore the Flash device and the filename to the default settings:

```
Console> (enable) set system syslog-file  
System syslog-file set to the default file.  
Console> (enable)
```

