



Configuring System Message Logging

This chapter describes how to configure system message logging on the Catalyst enterprise LAN switches.



Note

For complete syntax and usage information for the commands used in this chapter, refer to the *Command Reference—Catalyst 4000 Family, Catalyst 2948G, and Catalyst 2980G Switches*.

This chapter consists of these major sections:

- [Understanding How System Message Logging Works, page 34-1](#)
- [System Log Message Format, page 34-3](#)
- [Default System Message Logging Configuration, page 34-4](#)
- [Configuring System Message Logging, page 34-4](#)

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. With the system message logging facility, you can:

- Get logging information for monitoring and troubleshooting
- Select the types of logging information captured
- 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 34-1](#)) and the severity level (see [Table 34-2](#)). Messages are time-stamped to enhance real-time debugging and management.

You can access logged system messages using the switch 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 1024 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.



Note

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

[Table 34-1](#) describes the facility types supported by the system message logs.

Table 34-1 System Message Log Facilities

Facility Name	Definition
cdp	Cisco Discovery Protocol
dtp	Dynamic Trunking Protocol
drip	Dual Ring Protocol
dvlan	Dynamic VLAN
earl	Enhanced Address Recognition Logic
fddi	Fiber Distributed Data Interface
fileSYS	Flash file system
gvrp	GARP VLAN Registration Protocol
ip	IP permit list
kernel	Kernel
mgmt	Management messages
mcast	Multicast messages
pagp	Port Aggregation Protocol
protfilt	Protocol filtering
pruning	VTP pruning
qos	Quality of Service
radius	RADIUS authentication
rmon	Remote Monitoring
security	Port security
snmp	Simple Network Management Protocol
spantree	Spanning-Tree Protocol
sys	System
tac	TACACS+ authentication
tcp	Transmission Control Protocol
telnet	Terminal emulation protocol in the TCP/IP protocol stack
tftp	Trivial File Transfer Protocol
udld	UniDirectional Link Detection
vmps	VLAN Membership Policy Server
vtp	VLAN Trunking Protocol

Table 34-2 describes the severity levels supported by the system message logs.

Table 34-2 Definitions of System Message Log Severity Levels

Severity Level	Keyword	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 but significant conditions
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 34-3 describes the elements of syslog messages.

Table 34-3 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 you configure this with 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 34-4 describes the default system message logging configuration.

Table 34-4 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>

Configuring System Message Logging

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

- [Configuring Session Logging Settings, page 34-5](#)
- [Configuring the System Message Logging Levels, page 34-6](#)
- [Changing the Logging Timestamp Enable State, page 34-6](#)
- [Specifying the Logging Buffer Size, page 34-6](#)
- [Limiting the Number of syslog Messages, page 34-7](#)
- [Configuring the syslog Daemon on a UNIX syslog Server, page 34-7](#)
- [Configuring syslog Servers, page 34-8](#)
- [Displaying the Logging Configuration, page 34-9](#)
- [Displaying System Messages, page 34-10](#)

Configuring Session Logging Settings

By default, system logging messages are sent to console and Telnet sessions 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 change the logging enable state for console sessions, perform this task in privileged mode:

	Task	Command
Step 1	Change the default logging enable 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 change the logging enable state for the current Telnet session, perform this task in privileged mode:

	Task	Command
Step 1	Change the logging enable 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)
```

Configuring the System Message Logging Levels

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

To change 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 <i>facility</i> } <i>severity</i> [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)
```

Changing the Logging Timestamp Enable State

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

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

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

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

Specifying the Logging Buffer Size

To specify 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.

To configure the syslog daemon, follow these steps:

- Step 1 Log in to the UNIX server as root.
- Step 2 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 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 3 Create the log file by entering these commands at the UNIX shell prompt:

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

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 34-7.

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 as many as three syslog servers.	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 [<i>noalias</i>]

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 remove 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 remove 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

Use the **show logging** command to display the current system message logging configuration. Use 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 buffer size:          200
      timestamp option:      disabled
Logging history size:         1
      severity:              notifications(5)
Logging console:              enabled
Logging server:               enabled
{syslog.bigcorp.com}
      server facility:        LOCAL5
      server severity:        notifications(5)
```

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

Console> (enable)

Displaying System Messages

Use 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.

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)
```

