

Message Format

This chapter describes how messages from the Catalyst 5000, 4000, 2948G, 2926G, and 2926 series switches are formatted and how you can enable the System Message Log feature to send messages to the switch internal buffer and system console for display (and optionally, to a logging server on another system). Not all messages indicate problems; some messages are only informational, while others help diagnose problems with communications lines, internal hardware, or the system software.

Messages are listed by the facility (hardware device, protocol, or a module or system software) that produces the messages. Within each facility, messages are listed by the severity level, from highest to lowest. Each message is followed by an explanation and a recommended action. Messages appear only when the system remains operational.

This chapter contains the following sections:

- Message Structure, page 1-2
- System Message Log, page 1-5

Message Structure

Messages are structured as follows:

```
facility-severity-MNEMONIC:description
```

Messages from the System Message Log are structured the same, but include this date/time stamp at the beginning of the message:

```
mm/dd/yy:hh/mm/ss:facility-severity-MNEMONIC:description
```

where

```
mm/dd/yy:hh/mm/ss
```

is the date and time of the error/event.

Both message types contain this information:

- A *facility* code consists of two or more uppercase letters that indicate the reference facility to which the message refers. A facility can be a hardware device, a protocol, or a portion of the system software. See Table 1-1.

Table 1-1 Facility Codes

Code	Facility
CDP	Cisco Discovery Protocol
DRIP	Dual Ring Protocol
DTP	Dynamic Trunk Protocol
DVLAN	Dynamic VLAN ¹
EARL	Enhanced Address Recognition Logic
FDDI	Fiber Distributed Data Interface ²
FILESYS	Flash File System
IP	Internet Protocol
KERNEL	Kernel
MGMT	Management messages
MCAST	Multicast messages
MLS	Multilayer Switching

Table 1-1 Facility Codes (continued)

Code	Facility
PAGP	Port Aggregation Protocol
PROTFILT	Protocol Filtering
PRUNING	VLAN Trunk Protocol Pruning
RMON	Remote Monitoring
SECURITY	Port Security
SNMP	Simple Network Management Protocol
SPANTREE	Spanning-Tree Protocol
SYS	System
TAC	Terminal Access Controller Access Control System
TCP	Transmission Control Protocol ²
TELNET	Standard terminal emulation protocol in the TCP/IP ³ protocol stack ²
TFTP	Trivial File Transfer Protocol ²
VMPS	VLAN Membership Policy Server
VTP	VLAN Trunk Protocol

1 VLAN=virtual LAN

2 Not covered in this publication

3 TCP/IP=Transmission Control Protocol/Internet Protocol

- A *severity* level code is a single digit from 0 to 7 that reflects the severity of the condition. The lower the number, the more serious the situation. See Table 1-2.

Table 1-2 Message Severity Levels

Severity Level	Description
0 – emergency	System is unusable
1 – alert	Immediate action required
2 – critical	Critical condition
3 – error	Error condition
4 – warning	Warning condition
5 – notification	Normal but significant condition
6 – informational	Informational message only
7 – debugging	Message that appears during debugging only

- The *MNEMONIC* code uniquely identifies the error message. All mnemonics are all uppercase character strings.
- A *description* text string describes the condition. Sometimes it contains detailed information about the event, including terminal port numbers, network addresses, or addresses that correspond to locations in the system memory address space. Because these variable fields can change from message to message, they are represented by short strings in square brackets ([]). A decimal number, for example, is represented as [dec]. See Table 1-3.

Table 1-3 Representation of Variable Fields in Messages

Representation	Type of Information
[dec]	Decimal
[chars]	Character string
[hex]	Hexadecimal integer

The following is a sample system message; an explanation of the message follows:

```
06/17/1999,18:31:15:SYS-5-MOD_INSERT:Module 5 has been inserted  
where
```

06/17/1999,18:31:15 is the date and time of the error (this appears if set for system log messaging).

SYS is the facility type.

5 is the severity level, indicating that it is a normal but significant condition.

MOD_INSERT is the mnemonic code that uniquely identifies the message.

Module 5 has been inserted is the message text.

System Message Log

The System Message Log (syslog) software can save system 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 and the severity level. Messages can be 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. You can also save messages on UNIX servers that are configured properly. The syslog software reads the messages from the buffer and sends them to the specified destination.

With syslog, you can access system messages by logging in to the console through Telnet. This allows you to monitor system messages remotely from any workstation that supports the Telnet protocol.

System Message Log Procedures

This section describes the configurable options for the System Message Log.

Default System Message Log Configuration

The switches ship with the default configuration as shown in Table 1-4.

Table 1-4 Default System Message Logging Configuration

Configuration Parameters	Default Setting
System message logging to the console	Enabled
System message logging to Telnet sessions	Enabled
Logging server	Disabled
Syslog server IP address	None configured
Server facility	LOCAL7
Server severity	Warnings (4)
Logging buffer	500
Logging history size	1
Timestamp option	Disabled
Facility/severity level for system messages	sys/5 dtp/5 pagp/5 mgmt/5 mls/5 <i>all other facilities/2</i>

When you first log on to the switch console, enter the **show logging** command to display the default configuration.

Configuring System Message Logging

To change the default system message logging facility and severity levels, perform one of these tasks in privileged mode:

Task	Command
Set the default facility and severity level for system messages.	set logging level <i>facility severity</i>
Disable system message logging to the console.	set logging console disable

This example shows how to change the default system message logging facility and severity levels for the Cisco Discovery Protocol (CDP) to severity level 3:

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

This example shows how to disable system message logging to the console:

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

Configuring the syslog Daemon on UNIX syslog Server

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

Step 1 Add a line such as the following in 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.

System Message Log

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

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

Configuring syslog Servers

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 section “Configuring the syslog Daemon on UNIX syslog Server” section on page 1-7. To configure the switch to log messages to a syslog server, perform this task in privileged mode:

Task	Command
Step 1 Add a syslog server to the configuration ¹ .	set logging server <i>ip_addr</i>
Step 2 Enable system message logging to configured syslog servers.	set logging server enable
Step 3 Set the facility and severity level for syslog server messages.	set logging server facility <i>server_facility_parameter</i> set logging server severity <i>server_severity_level</i>

¹ You can configure a maximum of three syslog servers at any time.

This example shows how to add a new syslog server with an IP address of 171.69.192.205 to the system logging server table:

```
Console> (enable) set logging server 171.69.192.205  
171.69.192.205 added to the System logging server table.  
Console> (enable)
```

This example shows how to enable system message logging to a configured syslog server:

```
Console> (enable) set logging server enable  
System logging messages will be sent to the configured syslog servers.  
Console> (enable)
```

This example shows how to set the syslog server facility to local0:

```
Console> (enable) set logging server facility local0  
System logging server facility set to <local0>  
Console> (enable)
```

This example shows how to set the syslog server severity level to 4:

```
Console> (enable) set logging server severity 4  
System logging server severity set to <4>  
Console> (enable)
```

To remove a syslog server from the configuration, perform this task in privileged mode:

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

This example shows how to delete the syslog server 171.69.192.207 from the configuration:

```
Console> (enable) clear logging server 171.69.192.207  
System log server 171.69.192.207 removed from system log server table.  
Console> (enable)
```

System Message Log

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 system message logging to a configured syslog server:

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

Changing the Log Buffer Size

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

Task	Command
Change the buffer to limit the number of messages stored.	set logging buffer <i>buffer_size</i>

This example shows how to limit to 200 the number of messages stored in the buffer:

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

Changing the Logging Timestamp

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

Task	Command
Enable or disable the timestamp display on system logging messages.	set logging timestamp {enable disable}

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)
```

Configuring Telnet Login Sessions

By default, system messages are sent to Telnet sessions based on the default facility and severity values.

To configure the logging settings for Telnet sessions, perform one of these tasks in privileged mode:

Task	Command
• Change the facility and severity values for Telnet login sessions.	set logging level <i>facility severity</i>
• Disable system message logging to the current Telnet login session.	set logging session disable
• Disable system message logging to the console.	set logging console disable
• Reenable system message logging to the current Telnet login session.	set logging session enable
• Reenable system message logging to the console.	set logging console enable

System Message Log

This example shows how to change the facility and severity values for Telnet login sessions:

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

This example shows how to disable system message 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)
```

This example shows how to disable system message logging to the console session:

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

This example shows how to reenble system message logging to the current Telnet session:

```
Console> (enable) set logging session enable  
System logging messages will be sent to the current login session.  
Console> (enable)
```

This example shows how to reenble system message logging to the console session:

```
Console> (enable) set logging console enable  
System logging messages will be sent to the console.  
Console> (enable)
```

Displaying the System Logging Configuration

To display the current configuration for system messages, perform this task in privileged mode:

Task	Command
Display the current system message log configuration.	show logging

This example shows the results of a show logging command:

```

Console <enable> show logging

Logging buffer size:          500
        timestamp option:    enabled
Logging history size:         1
Logging console:              enabled
Logging server:               disabled
        server facility:     LOCAL7
        server severity:     warnings(4)
    
```

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

Console>

System Message Log

To verify the system message log configuration, enter the **show logging** command. If you are verifying the system message log configuration for the console and the syslog server is disabled, the first five lines of output look as follows:

```
Console (enable) show logging
Logging buffer size:      400
      timestamp:          enabled
Logging history size:     1
Logging console:          enabled
Logging server:           disabled
```

If you are verifying the system message log configuration for a Telnet login session, an additional line showing the current logging session is displayed, as follows:

```
Console <enable> show logging
Logging buffer size:      400
      timestamp:          enabled
Logging history size:     1
Logging console:          enabled
Logging server:           disabled
Current Logging Session:  enabled
```

Displaying System Messages

To display the first N system messages in the internal buffer of the switch, perform this task in privileged mode:

Task	Command
Display the first N messages in the buffer.	show logging buffer N

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

```
Console> (enable) show logging buffer 5
%PRUNING-4-NOTRUNK:trunk 100 not found(domain Lab_Network)
%PRUNING-4-NOTRUNK:trunk 100 not found(domain Lab_Network)
%MLS-5-ROUTERDEL:Route Processor 172.20.52.6 deleted - router excluded
from include list
%SYS-5-RTE_DEFGATEFROM:Default Gateway switching from 172.20.52.121
%SYS-5-RTE_DEFGATETO:Default Gateway switching to 172.20.52.125
Console> (enable)
```

To display the last *N* system messages in the internal buffer of the switch, perform this task in privileged mode:

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

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

```
Console> (enable) show logging buffer -5
%CDP-4-DUPLEXMISMATCH:Full/half duplex mismatch detected on port 10/1
%DTP-5-TRUNKPORTON:Port 10/1 has become dot1q trunk
%PAGP-5-PORTTOSTP:Port 10/1 joined bridge port 10/1
%SPANTREE-2-RX_1QPVIDERR: Rcvd pvid_inc BPDU on 1Q port 10/1 vlan 1.
%SPANTREE-2-TX_BLKPORTPVID: Block 10/1 on xmtting vlan 522 for inc peer
vlan.
Console> (enable)
```

System Message Log
