

Configuring System Message Logging

This chapter describes how to configure system message logging on the Catalyst 5000, 4000, 2948G, 2926G, and 2926 series switches.

Note For complete syntax and usage information for the commands used in this chapter, refer to the *Command Reference* for your switch.

This chapter consists of these sections:

- Understanding How System Message Logging Works on page 21-1
- System Log Message Format on page 21-3
- Default System Message Logging Configuration on page 21-3
- Configuring System Message Logging on page 21-4
- System Message Logging Examples on page 21-6

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 21-1) and the severity level (see Table 21-2). 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 21-1 describes the facility types supported by the system message logs.

Table 21-1 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 |
| ip | IP permit list |
| kernel | Kernel |
| mgmt | Management messages |
| mcast | Multicast messages |
| pagp | Port Aggregation Protocol |
| protfilt | Protocol filtering |
| pruning | VTP pruning |
| rmon | Remote Monitoring |
| snmp | Simple Network Management Protocol |
| spantree | Spanning-Tree Protocol |
| sys | System |
| tac | TACACS+ |
| tcp | Transmission Control Protocol |
| telnet | Terminal emulation protocol in the TCP/IP protocol stack |
| tftp | Trivial File Transfer Protocol |
| vmps | VLAN Membership Policy Server |
| vtp | VLAN Trunking Protocol |
| security | Port security |

Table 21-2 describes the severity levels supported by the system message logs.

Table 21-2 System Message Log Severity Level Definitions

| 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 condition |

Table 21-2 System Message Log Severity Level Definitions (continued)

| Severity Level | Keyword | Description |
|----------------|----------------------|------------------------|
| 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 21-3 describes the elements of syslog messages.

Table 21-3 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:

```
%SYS-5-MOD_OK:Module 1 is online
%SYS-5-MOD_OK:Module 2 is online
%SYS-5-MOD_OK:Module 3 is online
%DTP-5-TRUNKPORTON:Port 2/1 has become dot1q trunk
%PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1
```

Default System Message Logging Configuration

Table 21-4 describes the default system message logging configuration.

Table 21-4 Default System Message Logging Configuration

| Configuration Parameter | Default Setting |
|---|-----------------|
| System message logging to the console | Enabled |
| System message logging to Telnet sessions | Enabled |
| Logging server | Disabled |
| Syslog server IP address | None configured |
| Server facility | LOCAL7 |
| Server severity | Warnings (4) |
| Logging buffer | 500 |
| Logging history size | 1 |

Table 21-4 Default System Message Logging Configuration (continued)

| Configuration Parameter | Default Setting |
|---|--|
| 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> |

Configuring System Message Logging

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

| Task | Command |
|--|---|
| <ul style="list-style-type: none"> Set the default facility and severity level for system messages. | set logging level <i>facility severity</i> |
| <ul style="list-style-type: none"> Disable system message logging to the console. | set logging console disable |

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 the 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 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 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 21-4.

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 level <i>facility severity default</i> |

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

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> |

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 |

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 <i>facility</i> and <i>severity</i> 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 or set logging console disable |
| • Reenable system message logging to the current Telnet login session. | set logging session enable or set logging console enable |

Displaying System Messages

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 |

To display the first *N* system messages in the internal buffer of the Catalyst 5000 series switch, perform this task in privileged mode:

| Task | Command |
|--|-------------------------------------|
| Display the first <i>N</i> messages in the buffer. | show logging buffer <i>N</i> |

To display the last *N* system messages in the internal buffer of the Catalyst 5000 series 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> |

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

```
Console> (enable) show logging  
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 console:      enabled  
Logging server:       disabled  
Current Logging Session:  enabled
```

System Message Logging Examples

This section provides examples for entering the system message log commands to perform the following tasks:

- To enable system message logging to configured syslog servers, enter this command:

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

- To add a new syslog server at IP address 171.69.192.205 to the system logging server table, enter this command:

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

- To enable system logging messages to the current login session, enter this command:

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

- To change the default facility to **all** and severity to **1**, enter this command:

```
Console> (enable) set logging level all 1 default
System logging facility <all> set to severity 1(alerts).
```

- To display the new system message log configuration, enter this command and note the values in the Server/Default Severity and Current Session Severity columns:

```
Console> (enable) show logging
Logging console:          enabled
Logging server:          disabled
Current Logging Session:  enabled

Facility                Server/Default Severity  Current Session Severity
-----                -
cdp                     1                       1
mcast                   1                       1
dtp                     1                       1
dvlan                   1                       1
earl                    1                       1
fddi                    1                       1
ip                      1                       1
pruning                 1                       1
snmp                    1                       1
spantree                1                       1
sys                     1                       1
tac                     1                       1
tcp                     1                       1
telnet                  1                       1
tftp                    1                       1
vtp                     1                       1
vmps                    1                       1
kernel                  1                       1
filesys                 1                       1
drip                    1                       1
pagp                    1                       1
mgmt                    1                       1
mls                     1                       1
protfilt                1                       1
security                1                       1

0(emergencies)         1(alerts)                2(critical)
3(errors)               4(warnings)              5(notifications)
6(information)         7(debugging)

Console> (enable)
```

- To set the facility to **snmp** and the severity level to **3** for the current session, enter this command:

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

- To display the new system message log configuration, enter the following command, and note the new value for **snmp** under the Current Session Severity column (shown by the arrow):

```
Console> (enable) show logging

Logging console:          enabled
Logging server:          disabled
Current Logging Session:  enabled

Facility                Server/Default Severity  Current Session Severity
-----                -
cdp                     1                       1
mcast                   1                       1
dtp                     1                       1
```

System Message Logging Examples

```

dvlan          1          1
earl           1          1
fddi           1          1
ip             1          1
pruning        1          1
snmp           1          3
spantree       1          1
sys            1          1
tac            1          1
tcp            1          1
telnet         1          1
tftp           1          1
vtp            1          1
vmps           1          1
kernel         1          1
filesystems    1          1
drip           1          1
pagp           1          1
mgmt           1          1
mls            1          1
protfilt       1          1
security       1          1

0(emergencies) 1(alerts)      2(critical)
3(errors)      4(warnings)     5(notifications)
6(information) 7(debugging)
Console> (enable)
```

- To display the first four messages in the internal buffer, enter this command:

```

Console> (enable) show logging buffer 4
07/30/1998,12:59:24:SYS-5:Module 1 is online
07/30/1998,12:59:32:SYS-5:Module 9 is online
07/30/1998,12:59:35:SYS-5:Module 5 is online
07/30/1998,12:59:49:SYS-5:Module 2 is online
Console> (enable)
```

- To display the last four messages in the internal buffer, enter this command:

```

Console> (enable) show logging buffer -4
07/30/1998,15:44:19:PAGP-5:Port 1/1 joined bridge port 1/1.
07/30/1998,15:46:52:DTP-5:Port 1/1 has become isl trunk
07/30/1998,15:46:52:PAGP-5:Port 1/1 left bridge port 1/1.
07/30/1998,15:47:03:PAGP-5:Port 1/1 joined bridge port 1/1.
Console> (enable)
```