



Using the CSS Logging Features

This chapter describes how to enable logging, set up the log buffer, determine where to send the activity information, and display and interpret log messages. Information in this chapter applies to all CSS models, except where noted.

This chapter contains the following major sections:

- [Logging Overview](#)
- [Specifying Logging Buffer Size](#)
- [Configuring Logging for a Subsystem](#)
- [Specifying a Log File Destination](#)
- [Logging CLI Commands](#)
- [Showing Log Files](#)
- [Copying Log Files to an FTP or TFTP Server](#)
- [Interpreting sys.log Log Messages](#)
- [Interpreting Undeliverable Messages](#)
- [Frequently Queried Log Messages](#)

Logging Overview

The CSS generates log messages to assist you with debugging and monitoring operations. By default, the CSS saves boot and subsystem event messages to log files on its hard or Flash disk. The content of these files is recorded in ASCII text. You can also configure the CSS to send log messages to an active CSS session, e-mail address, or another host system.

The maximum size of a log file is 50 MB for hard disk-based systems, and 10 MB for Flash disk-based systems.

The boot log messages are the result of the boot process. The CSS saves these messages in the boot.log file.

The subsystem log messages are subsystem events that occur during the operation of the CSS. The CSS saves these messages in the sys.log file, created when the first loggable subsystem event occurs. The CSS determines which subsystem messages to log by its configured logging level. By default, the CSS logs events on all subsystems with a level of warning. The warning level designates that the CSS logs fatal, alert, critical, error, and warning messages for the subsystem.

You have the option to log subsystem messages at a different level than the default warning level. The level you specify instructs the CSS to log subsystem activity that occurs at that level and the activity greater than that level.

In addition to informational messages, the CSS also logs notice, warning, error, critical, alert, and fatal messages.

You can display or copy a log file using the **show log** or **copy log** command, respectively. For details on the **show log** command, see the [“Showing Log Files”](#) section. For details on the **copy log** command, see the [“Copying Log Files to an FTP or TFTP Server”](#) section. You need SuperUser privileges to use the **show log** command.

The CSS provides logging capabilities for debugging and system monitoring by generating the log files described in [Table 8-1](#).

Table 8-1 CSS Log File Descriptions

Log File	Log File Destination		Records
	Default Location	Alternate Location	
boot.log	Hard disk and console or Flash disk and console	None	Results of the boot process.
boot.bak	Hard disk and console or Flash disk and console	None	Backup of a boot log file. Each time you reboot the CSS, the software renames the current boot log file to boot.log.prev and starts a new boot log file. The CSS overwrites an existing backup boot log file when a boot log file is renamed.
sys.log	Hard disk or Flash disk	Console syslogd VTY1 VTY2	Log information for user-defined subsystem or CLI commands. By default, logging is enabled and logs subsystem all with level warning . The CSS creates sys.log to record this log information.

Table 8-1 CSS Log File Descriptions (continued)

Log File	Log File Destination		Records
	Default Location	Alternate Location	
sys.log.prev	Hard disk or Flash disk	Console syslogd VTY1 VTY2	Backup of a system log file. When a system log file reaches its maximum size (50 MB, for a hard disk-based CSS; 10 MB, for a Flash disk-based CSS), the software renames the system log file to sys.log.prev and starts a new system log file. The CSS overwrites an existing backup system log file when a system log file is renamed. When you reboot a CSS, the software continues to use the existing system log file until the file reaches its maximum size.

CSS Logging Quick Start Table

If you are familiar with the CSS logging functions, see [Table 8-2](#) for the commands and command options required to configure and enable logging.

You configure all logging commands from configuration mode except for the clear log command. The clear log command is available only in SuperUser mode at the root prompt (#).

Table 8-2 Configuring and Enabling Logging

Step	Logging Option	Example
1. Specify the disk buffer size.	<i>size</i> - Size of the disk buffer (0 to 64000)	logging buffer 1000
2. Select a CSS subsystem and determine which type of activity to log (default all) and level (default warning).	<p>subsystem - Valid subsystems:</p> <p>acl, all, app, boomerang, buffer, cdp, chassis, circuit, csdpeer, dhcp, dql, fac, flowagent, flowmgr, fp-driver, hfg, ipv4, keepalive, netman, netmgr, nql, ospf, pcm, portmapper, proximity, publish, radius, redundancy, replicate, rip, security, ssl-accel, slr, sntp, syssoft, urql, vlanmgr, vpm, vrrp, wcc</p> <p>level - Valid levels:</p> <p>fatal-0, alert-1, critical-2, error-3, warning-4, notice-5, info-6, debug-7</p>	logging subsystem rip level alert-1
3. Specify the destination (disk, host, line) where you wish to log subsystem activity.	<p>disk filename - New or existing filename in the log directory</p> <p>host ip or host - IP address of the syslog daemon on the host or a host name</p> <p>log line - CSS active session</p>	<p>logging disk stubs</p> <p>logging host 192.168.11.3</p> <p>logging host myhost.domain.com</p> <p>logging line vty1</p>

Table 8-2 Configuring and Enabling Logging (continued)

Step	Logging Option	Example
4. Optionally, enable the CSS to send log messages to an e-mail address and specify a level.	sendmail <i>email address</i> of mail recipient <i>IP address</i> or <i>hostname</i> of SMTP host level - Valid levels for the CSS: fatal-0, alert-1, critical-2, error-3, warning-4, notice-5, info-6, debug-7	logging sendmail us@arrowpoint.com 172.16.6.58 critical-2
5. Show the log file.	<i>filename</i> - Log file to display	show log stubs

Specifying Logging Buffer Size

The logging buffer size is the amount of information the CSS buffers in memory before outputting the information to disk. The larger you configure the buffer size, the less frequently the CSS outputs the contents to disk. Specifying a buffer size is required only if you specify logging to disk as the log file destination.

To set the disk buffering size, use the **logging buffer** command. Specify the buffer size from 0 to 64000 bytes. The default is 0, where the CSS sends the logging output directly to the log file.

To set the buffer size to 1000 bytes, enter:

```
(config)# logging buffer 1000
```

To send the logging output directly to the log file, enter:

```
(config)# no logging buffer
```

Configuring Logging for a Subsystem

This section describes how to select a CSS subsystem and log activity for the subsystem. This section includes the following topics:

- [Enabling and Disabling Logging for a Subsystem](#)
- [Configuring a Log Message for a Subsystem at a Logging Level](#)
- [Logging ACL Activity](#)
- [Sending Log Messages to an E-Mail Address](#)

Enabling and Disabling Logging for a Subsystem

Use the **logging subsystem** command to select a CSS subsystem and determine which type of activity to log. The level you specify instructs the CSS to log subsystem activity that occurs at that level and the activity greater than that level. For example, if you wish to log informational messages (info-6), the CSS also logs notice, warning, error, critical, alert, and fatal error levels.

To reset logging for a subsystem to the default logging level (warning-4), enter the **no** version of the logging command. For example:

```
(config)# no logging subsystem redundancy
```

The following example enables logging for the chassis subsystem with a critical-2 error level. The CSS logs all critical, alert, and fatal errors for the chassis.

```
(config)# logging subsystem chassis level critical-2
```

[Table 8-3](#) defines the CSS subsystems for which you can enable logging.

Table 8-3 Logging Subsystems

Subsystem	Definition
acl	Access control list (ACL)
all (default)	All CSS subsystems
app	Application Peering Protocol (APP)
boomerang	DNS Content Routing Agent (CRA)
buffer	Buffer manager

Table 8-3 Logging Subsystems (continued)

Subsystem	Definition
cdp	Cisco Discovery Protocol (CDP)
chassis	Chassis manager
circuit	Circuit manager
csdpeer	Content Server Database (CSD) peer
dhcp	Dynamic Host Configuration Protocol (DHCP)
dql	Domain Qualifier List (DQL)
fac	Flow Admission Control (FAC)
flowagent	Flow agent
flowmgr	Flow manager subsystem
fp-driver	Fathpath driver
hfg	Header Field Group (HFG)
ipv4	Internet Protocol version 4 (IPv4)
keepalive	Keepalive
natmgr	NAT manager
netman	Network management
nql	Network Qualifier List (NQL)
ospf	Open Shortest Path First (OSPF) protocol
pcm	Proximity CAPP Messaging (PCM)
portmapper	Port mapper
proximity	Proximity
publish	Publish
radius	Remote Authentication Dial-In User Service (RADIUS)
redundancy	CSS redundancy
replicate	Content replication
rip	Routing Information Protocol (RIP)
security	Security manager

Table 8-3 Logging Subsystems (continued)

Subsystem	Definition
ssl-accel	Secure Socket Layer (SSL) Acceleration
slr	Session Level Redundancy
sntp	Simple Network Time Protocol (SNTP)
syssoft	System software
urql	Uniform Resource Locator Qualifier List (URQL)
vlanmgr	VLAN manager
vpm	Virtual pipe manager
vrrp	Virtual Router Redundancy Protocol
wcc	Web conversation control

Table 8-4 defines the logging levels you can set for the specified CSS subsystem. The logging levels are listed in order of severity, with a fatal-0 level being the most severe errors and an info-6 level being the least severe error.

Table 8-4 Subsystem Logging Levels

Level	Definition
fatal-0	Fatal errors only.
alert-1	Alert errors, including fatal errors.
critical-2	Critical errors, including alert and fatal errors. The following trap events log at the critical level: link down, cold start, warm start, service down, service suspended.
error-3	General errors, including critical, alert, and fatal errors.
warning-4 (default)	Warning messages, including all lower levels (error, critical, alert, and fatal).
notice-5	Notice messages, including all trap events (except for events logged at critical) and all lower levels except for info and debug.

Table 8-4 Subsystem Logging Levels (continued)

Level	Definition
info-6	Informational messages, including all lower levels except for debug.
debug-7	<p>Debug messages, including all other error levels. The debug-7 log level may degrade the performance of the CSS. When you enter this option, the CSS prompts you with the following message:</p> <p>Logging at the debug level may degrade the CSS performance. Continue, [y/n]:</p> <p>Enter y to verify that you want to set the log level to debug-7. Enter n to cancel the executing of the debug-7 log level.</p>

Configuring a Log Message for a Subsystem at a Logging Level

Use the **cliLogMessage subsystem** command to define a log message for a subsystem at a particular logging level. The syntax for this global configuration mode command is:

```
cliLogMessage subsystem name "message" level level
```

The variables and options are as follows:

- **name** - The name of a CSS subsystem. Enter one of the subsystem names, as shown in [Table 8-3](#). To see a list of subsystems, enter:

```
cliLogMessage subsystem ?
```

- **level level** - The log level for the message. Enter one of the levels, from 0 to 7, as shown in [Table 8-4](#). To see a list of levels, enter:

```
cliLogMessage subsystem name "message" level ?
```

Logging ACL Activity

When you configure the CSS to log ACL activity, the CSS logs the event of the packet matching the clause and ACL. The CSS sends log information to the location you specified in the **logging** command.

Before you configure logging for a specific ACL clause, ensure global ACL logging is enabled. To globally enable ACL logging, use the **logging subsystem acl level debug-7** command in configuration mode.

To configure logging for an ACL clause:

1. Enter the ACL mode for which you want to enable logging.

```
(config)# acl 7  
(config-acl[7])#
```

2. Enable logging for:

- A new clause, by entering the **log** option at the end of the clause. For example:

```
(config-acl[7])# clause 1 deny udp any eq 3 destination any eq 3 log
```

- An existing clause, by using the **clause log enable** command:

```
(config-acl[7])# clause 1 log enable
```

To disable ACL logging for a specific clause, enter:

```
(config-acl[7])# clause 1 log disable
```

To globally disable logging for all ACL clauses, enter:

```
(config)# no logging subsystem acl
```

Sending Log Messages to an E-Mail Address

Use the **logging sendmail** command to send the log activity of a subsystem to an e-mail address. The syntax for this global configuration mode command is:

```
logging sendmail email_address ip_address level {domain}
```

The variables are as follows:

- *email_address* - The e-mail address for the recipient. Enter the e-mail address as an unquoted text string with a length of 1 to 30 characters.
- *IP_address* - The IP address for the SMTP host. Enter the IP address in dotted-decimal notation (for example, 192.168.11.1).
- *level* - The type of information to log. The valid levels are defined in [Table 8-4](#).
- *domain* - (Optional) The domain name for the SMTP host. Enter an unquoted text string with a maximum length of 64 characters (for example, arrowpoint.com). Do not insert an @ sign before the domain name. The CSS automatically prepends the @ sign to the domain name.

To turn off logging to an e-mail address, enter:

```
(config)# no logging sendmail email_address
```

Specifying a Log File Destination

To specify a destination where the CSS logs subsystem activity, use the **logging** command. You can specify the following locations for log files:

- **disk filename** - New or existing filename in the disk log directory
- **host ip** or **host** - IP address of the syslog daemon on the host or a host name
- **log line** - CSS active session

Logging to a CSS disk causes the performance of the CSS to degrade. If logging requires frequent writes to disk (that is, several hundred log messages per day), the most reliable configuration is to log to a hard disk and store all other system files on a Flash disk. Although Flash disks generally provide the most reliable way to store information over time, hard disks endure frequent writes to disk better than the Flash disks currently available.

To prevent excessive writes to the CSS disk, consider disabling logging to the `sys.log` file on disk (see the [“Disabling Logging to the `sys.log` File on the Disk”](#) section). You can continue sending CSS log information to the `sys.log` file at an alternate location. To do this, use either the **logging host** command to send log information to a syslog daemon on a host system (see the [“Specifying a Host for a Log File Destination”](#) section) or the **logging line** command to send (but not save) log information to an active CSS line (see the [“Specifying a Line for a Log File Destination”](#) section).

This section includes the following procedures:

- [Specifying a Log File on the Disk](#)
- [Disabling Logging to the `sys.log` File on the Disk](#)
- [Specifying a Host for a Log File Destination](#)
- [Specifying a Line for a Log File Destination](#)

Specifying a Log File on the Disk

Use the **logging disk** command to send log information to a specific file on the CSS disk. Specify a log filename. Enter a text string from 0 to 32 characters. The filename can be new or an existing name.

For example:

```
(config)# logging disk stubs
```

When you specify the **logging disk** command, the CSS:

- Stops writing default log information to the sys.log file
- Creates the filename you specify in the disk log directory
- Sends subsystem and level information to the log file specified

You can have only one active log file on the disk at a time. If you wish to send subsystem information to a different log file on the disk, reenter the logging disk command with a different filename.

**Caution**

Logging to a CSS disk causes the performance of the CSS to degrade.

To stop logging to the specified file and reenable logging to the sys.log file on the CSS, enter:

```
(config)# no logging disk
```

Disabling Logging to the sys.log File on the Disk

Use the **logging to-disk** command to disable logging to the sys.log file on the CSS disk (hard or Flash). Disabling logging to the sys.log file is useful when you want to prevent excessive writes to the CSS disk (for example, to the Flash disk) or to increase the performance of the CSS.

You can continue sending CSS log information to the sys.log file at an alternate location. To send log information to an alternate location, use either the **logging host** command to send log information to a syslog daemon on a host system (see the “[Specifying a Host for a Log File Destination](#)” section) or the **logging line** command to send (but not save) log information to an active CSS line (see the “[Specifying a Line for a Log File Destination](#)” section).

The options for the **logging to-disk** command are as follows:

- **logging to-disk disable** - Disables writing default log information to the CSS `sys.log` file on the CSS disk. The **logging to-disk disable** command affects the `sys.log` file only, and does not affect a disk log file specified through the **logging disk** command. You can still use the **logging disk filename** command to send log information to a specific filename on the CSS disk. To disable all logging to the CSS disk, first enter the **no logging disk** command and then enter the **logging to-disk disable** command. When you enter the **no logging disk** command, the CSS does not reenables logging to the `sys.log` file. You must specify the **logging to-disk enable** command to reactivate the `sys.log` file.
- **logging to-disk enable** - Resets logging back to disk and resumes writing default log information to the CSS `sys.log` file.

You are prompted to reboot the CSS after issuing the **logging to-disk disable** or **logging to-disk enable** commands for the command to take effect.

To disable logging to the CSS `sys.log` file on the CSS disk (Flash disk or hard disk), enter:

```
(config)# logging to-disk disable
```

To resume logging back to the CSS disk, enter:

```
(config)# logging to-disk enable
```

Specifying a Host for a Log File Destination

To send CSS log information to a syslog daemon running on the host system, use the **logging host** command. The syslog daemon receives and displays the CSS log messages on the host system.

The syntax for this configuration mode command is:

```
logging host ip_or_host facility number log-level number
```

The options and variables for this command are as follows:

- *ip_or_host* - Specifies the address of a syslog daemon on the host. Enter the IP address in dotted-decimal notation (for example, 192.168.11.1) or the mnemonic host name (for example, myhost.mydomain.com).
- **facility** *number* - Specifies the syslog daemon facility level. Facilities are considered service areas, such as printing, e-mail, or network. Enter a number from 0 to 7. For more information on the syslog daemon and facility levels, refer to your syslog daemon documentation.
- **log-level** *number* - Specifies the level of the CSS subsystem log messages to be sent to the syslog daemon on the host. The valid log levels for the CSS include: fatal-0, alert-1, critical-2, error-3, warning-4 (default), notice-5, info-6, debug-7. The logging levels are listed in order of severity, with a fatal-0 level being the most severe error and an info-6 level being the least severe error. Refer to [Table 8-4](#) for a definition of the different logging levels.

The **logging host log-level** *number* must be equal to or less than the log level you configure for the **logging subsystem** command (see the “[Configuring Logging for a Subsystem](#)” section). If the log-level value is less than the logging subsystem level, the CSS only sends the message level specified in the **log-level** option. If the log-level is greater than the logging subsystem level, the CSS only sends the level of messages specified in the **logging subsystem** command.

The CSS continues to send log information to the sys.log file on the CSS disk (hard or Flash disk) when the **logging host** command is entered. To disable logging to the sys.log file on the CSS disk, use the **logging to-disk disable** command (see the “[Disabling Logging to the sys.log File on the Disk](#)” section).

For example, to send log information to a host at IP address 192.168.11.1 with a facility level of 3 and a log-level of error-3:

```
(config)# logging host 192.168.11.1 facility 3 log-level error-3
```

To turn off logging to a host, enter:

```
(config)# no logging host
```

Specifying a Line for a Log File Destination

To send log information to an active CSS session, use the **logging line** command and specify a valid log line on the CSS. Enter the line as a case-sensitive text string with a maximum of 32 characters.

The CSS continues to send log information to the sys.log file on the CSS disk (hard or Flash disk) even when the **logging line** command is entered. To disable logging to the sys.log file on the CSS disk, use the **logging to-disk disable** command (see the [“Disabling Logging to the sys.log File on the Disk”](#) section).

To display a list of active CSS lines, enter the **logging line** command as shown. The asterisk (*) denotes your current session.

```
(config)# logging line ?

console      Login Name:  Location:local
*vty1        Login Name:  admin Location:10.0.3.35
```

To send subsystem information to your monitor, enter:

```
(config)# logging line vty1
```

To turn off logging, enter the **no logging line** command.

```
(config)# no logging line vty1
```

Logging CLI Commands

When you want to keep track of all CLI commands entered from the CSS, you can log them to the `sys.log` file. To log the CLI commands:

1. Set the logging level of the netman subsystem to info-6. Enter:

```
(config)# logging subsystem netman info-6
```

2. Enable logging of commands through the **logging commands enable** command. This command logs each CLI command to the `sys.log` file. Enter:

```
(config)# logging commands enable
```

To disable logging CLI commands to the `sys.log` file, enter:

```
(config)# no logging commands
```

Showing Log Files

Use the **show log** command to display the contents in a log or trap log file, a list of all log files, or the state of logging for CSS facilities. You need SuperUser privileges to use the **show log** command.

When you use the **show log** command to send the log activity to your current session, and you want to stop sending log activity, press any key on the terminal or workstation. The **show log** command performs the same function as the **logging line** command. You cannot run these commands at the same time.

This section covers:

- [Showing Log Activity](#)
- [Showing Log Lists](#)
- [Showing the Log State](#)

Showing Log Activity

Use the **show log** command and its options to send the log activity to your current session or to display the contents in a log or trap log file. You need SuperUser privileges to use the **show log** command.

The syntax for the **show log** command is:

```
show log {log_filename|traplog {tail lines} {line-numbers}}
```

The options and variables for this command are as follows:

- *log_filename* - Specifies the name of the log file. Enter an unquoted text string with no spaces. To see a list of log files with their creation dates, enter: **show log ?**
- **traplog** - (Optional) Displays all SNMP traps that have occurred. A trap log file is an ASCII file in the log directory containing generic and enterprise traps. By default, the following events generate level critical-2 messages:
 - Link Up
 - Link Down
 - Cold Start
 - Warm Start
 - Service Down
 - Service Suspended

All other SNMP traps generate level notice-5 messages.



Note When traps are disabled, the CSS still produces a log message for any event that would normally generate a trap.

- **tail lines** - (Optional) Displays the bottom and most recent portion of the log file. The CSS displays the log file, starting from the beginning of the file. The top of the file lists the older messages and the bottom lists the most recent messages. You can specify the number of lines to display (to a maximum of 1000 lines), starting at the end of the log file. Enter a number from 1 to 1000.
- **line-numbers** - (Optional) Includes the line numbers when displaying the contents of the log file.

To send the log activity to your current session, enter:

```
# show log
  Displaying Log events.
  Press any key to abort...
APR 14 16:28:09 5/1 2398 NETMAN-7: HTTPC:HTTPC_Open:
ERROR->connect <-1,0> <192.20.1.7> <80>
APR 14 16:28:15 5/1 2399 NETMAN-7: HTTPC:HTTPC_Open:
ERROR->connect <-1,0> <192.20.1.7> <80>
APR 14 16:28:21 5/1 2400 NETMAN-7: HTTPC:HTTPC_Open:
ERROR->connect <-1,0> <192.20.1.7> <80>
APR 14 16:28:27 5/1 2401 NETMAN-7: HTTPC:HTTPC_Open:
ERROR->connect <-1,0> <192.20.1.7> <80>
```

To display information in a specific log file, enter the **show log** command with a valid log filename. For example:

```
# show log stubs
SEP 22 09:59:18 5/1 918 NETMAN-7: SNMP:SET RSP (3803)
SEP 22 09:59:53 5/1 919 NETMAN-7: SNMP:SET (3804)
SEP 22 09:59:53 5/1 920 NETMAN-7: SNMP: 1
apLogHostIpAddress.[1.2.3.4] VT_IPADDRESS <1.2.3.4>
SEP 22 09:59:53 5/1 921 NETMAN-7: SNMP: 2
apLogHostIpAddress.[1.2.3.4] VT_IPADDRESS <1.2.3.4>
```

To view the content of the sys.log file, enter:

```
(config)# show log sys.log
```

To view the bottom and most recent portion of the file, use the **tail** option with the **show log** command. For example, to view the most recent 500 lines in the sys.log file, enter:

```
(config)# show log sys.log tail 500
```

Showing Log Lists

Use the **show log-list** command to display a list of all log files. For example:

```
(config)# show log-list
```

Showing the Log State

Use the **show log-state** command to display the state of logging for CSS facilities. For example:

```
(config)# show log-state
```

Table 8-5 describes the fields in the **show log-state** command output.

Table 8-5 Field Descriptions for the show log-state Command

Field	Description
Subsystems:	
acl	Access Control List (ACL)
app	Application Peering Protocol (APP)
boomerang	DNS Content Routing Agent (CRA)
buffer	Buffer manager
cdp	Cisco Discovery Protocol (CDP)
chassis	Chassis manager
circuit	Circuit manager
csdpeer	Content Server Database (CSD) peer
dhcp	Dynamic Host Configuration Protocol (DHCP)
dql	Domain Qualifier List (DQL)
fac	Flow Admission Control (FAC)
flowagent	Flow agent
flowmgr	Flow manager subsystem
fp-driver	Fathpath driver
hfg	Header Field Group (HFG)
ipv4	Internet Protocol version 4 (IPv4)
keepalive	Keepalive
natmgr	NAT manager
netman	Network management
nql	Network Qualifier List (NQL)

Table 8-5 Field Descriptions for the show log-state Command (continued)

Field	Description
ospf	Open Shortest Path First (OSPF)
pcm	Proximity CAPP Messaging (PCM)
portmapper	Port mapper
proximity	Proximity
publish	Publish
radius	Remote Authentication Dial-In User Service (RADIUS)
redundancy	CSS redundancy
replicate	Content replication
rip	Router Information Protocol (RIP)
security	Security manager
ssl-accel	Secure Socket Layer (SSL) Acceleration
slr	Session Level Redundancy
sntp	Simple Network Time Protocol (SNTP)
syssoft	System software
urql	Uniform Resource Locator Qualifier List (URQL)
vlanmgr	VLAN manager
vpm	Virtual pipe manager
vrrp	Virtual Router Redundancy Protocol
wcc	Web conversation control
acl	Access Control List (ACL)
all (default)	All CSS subsystems
app	Application Peering Protocol (APP)
Levels:	
debug	Log all errors and messages (Verbose)
info	Log informational messages, including errors at the notice level

Table 8-5 Field Descriptions for the `show log-state` Command (continued)

Field	Description
notice	Log notice messages, including errors at the warning level
warning	Log warning errors (default), including errors at the error level
error	Log errors, including errors at the critical level
critical	Log critical errors, including errors at the alert level
alert	Log alert errors, including errors at the fatal level
fatal	Log fatal errors only (Quiet)
File:	
Filename:	Name of the log file
Current size:	Current size of the log file
Log to Disk	Identifies whether logging to disk (Flash disk or hard disk) is Enabled or Disabled.

Copying Log Files to an FTP or TFTP Server

Use the `copy log` command to copy log files from the CSS to a File Transfer Protocol (FTP) or Trivial File Transfer Protocol (TFTP) server. The `copy log` command is available only in SuperUser mode.

This section includes the following sections:

- [Copying Log Files to an FTP Server](#)
- [Copying Log Files to a TFTP Server](#)

Copying Log Files to an FTP Server

Use the `copy log ftp` command to copy a log file to an FTP server. Before you copy a log file from the CSS to an FTP server, create an FTP record file containing the FTP server IP address, username, and password. Refer to [Chapter 3, Managing the CSS Software](#) for information on configuring an FTP record.

The syntax is:

```
copy log logfilename ftp ftp_record filename
```

The options and variables for this command are as follows:

- *logfilename* - Specifies the name of the log file on the CSS. Enter an unquoted text string with no spaces and a maximum of 32 characters. To see a list of log files, enter the **copy log ?** command.
- **ftp** - Copies a log file to an FTP server.
- *ftp_record* - Specifies the name of the FTP record file that contains the FTP server IP address, username, and password. Enter an unquoted text string with no spaces and a maximum of 16 characters. To create an FTP record, see [Chapter 3, Managing the CSS Software](#).
- *filename* - Specifies the name you want to assign to the file on the FTP server. Include the full path to the file. Enter an unquoted text string with no spaces and a maximum of 32 characters.

For example, to copy the *starlog* log file to an FTP server:

```
# copy log starlog ftp ftpserv1 starlogthurs
```

Copying Log Files to a TFTP Server

Use the **copy log tftp** command to copy a log file to a TFTP server.

The syntax is:

```
copy log log_filename [ftp ftp_record]tftp ip_or_host] filename
```

The options and variables for this command are as follows:

- *log_filename* - The name of the log file on the CSS. Enter an unquoted text string with no spaces and a maximum of 32 characters. To see a list of log files, enter the **copy log ?** command.
- **tftp** - Copies a log file to a TFTP server.
- *ip_or_host* - The IP address or host name of the TFTP server to receive the file. Enter an IP address in dotted-decimal notation (for example, 192.168.11.1) or in mnemonic host-name format (for example, myhost.mydomain.com). If you wish to use a host name, you must first set up a host table using the **host** command.

- *filename* - The name you want to assign to the file on the TFTP server. Include the full path to the file. Enter an unquoted text string with no spaces and a maximum of 32 characters.

For example, to copy the *starlog* log file to a TFTP server:

```
# copy log starlog tftp tftpserv1 starlogthurs
```

Interpreting sys.log Log Messages

The following example shows a sys.log message. This section describes the parts of a log message using this example.

```
FEB 16 14:01:13 5/1 2453 VLANMGR-7: Transmit sfm STP BPDU on bPort 1, egressLp 0x1f00 VlanLpSend() ret:0
```

A log message consists of the following components:

- The time stamp indicates when the log message event occurred. In this example, the time stamp is FEB 16 14:01:13.
- The physical interface indicates the *slot/port* (for example, 3/1) where the event occurred in the CSS.
- The counter records the incremental occurrence of each message. The count of this message is 2,453.
- The subsystem name and level is the CSS subsystem assigned to the message and the level of the message. Because this example is a subsystem message, the subsystem is the VLAN Manager and the log level is 7, which is a debug level (VLANMGR-7). See the “[Configuring Logging for a Subsystem](#)” section for a list of CSS subsystems.
- The log message indicating the event has occurred. The remaining string in the example is the event that occurred.

```
Transmit sfm STP BPDU on bPort 1, egressLp 0x1f00 VlanLpSend()  
ret:0
```

You can define a log message for a subsystem at a particular logging level through the **cliLogMessage subsystem** command. For more information, see the “[Configuring a Log Message for a Subsystem at a Logging Level](#)” section.

Interpreting Undeliverable Messages

Undeliverable messages, such as IMM, EVENT, and LOCAL, appear in the log when a queue on the CSS becomes full, overutilized, or needs to state a problem. The CSS supports EVENT and LOCAL messages.

Undeliverable messages consist of a logging header and a logging message, as shown in [Figure 8-1](#).

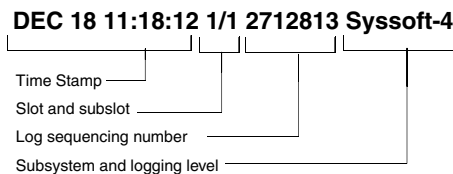
Figure 8-1 Undeliverable Message Format

Logging Header	Logging Message
DEC 18 11:18:12 1/1 2712813	Communications- QUEUE FULL- Ipv4arp: Internal Messages Dropped

The logging header ([Figure 8-2](#)) contains:

- A time stamp with the date and time
- The CSS slot and subslot number
- A logging sequence counter indicating that log messages were dropped due to excessive logging or CSS processor load
- The subsystem and its log level

Figure 8-2 Logging Header in a Log Message



The logging message that follows the logging header defines the error type (*Error Type*) and the destination (*Dest*), followed by a message (see [Figure 8-3](#)).

Figure 8-3 Logging Message

Logging Header	Logging Message
	Communications- <i>Error Type</i> - <i>Dest</i> : <i>Message ...</i>

The error type indicates one of the following:

- QUEUE FULL - The receiving queue has no room to accept messages
- QUEUE DELETED - The CSS was trying to place a message in a valid queue, the message was destroyed
- QUEUE INVALID - A destination message queue handle was not a valid object
- QUEUE UNKNOWN - The CSS was trying to determine the destination queue, the lookup failed.

The destination indicates one of the following:

- String decoded name of the destination message queue
- Hexadecimal value if the error type is QUEUE DELETED, QUEUE INVALID, or QUEUE UNKNOWN
- INTERNAL, a LOCAL message passed between the threads on the same processor

The message (*Message...*) in the logging message provides additional information concerning the problem. The log level for the undeliverable message determines how much information is in the logging message and how often the message occurs in the log. You can set the log level to Warning-4, Info-6, or Debug-7.

By default, the log level for undeliverable messages is Warning-4. These messages occur every two seconds per message queue that is experiencing the problem. The message in the logging messages provides only the following information:

```
Internal Messages Dropped.
```

When you change the log level to Info-6, the undeliverable message still occurs every two seconds per message queue that is experiencing the problem. However, the logging message displays a message similar to the following:

```
Internal Messages dropped 5 times since the previous log for a
total of 21 times since bootup.
```

This message provides additional information such as:

- How many times the internal messages were dropped since the previous logging of the message
- The total number of dropped messages since the CSS bootup

When you require more detailed information, set the log level to Debug-7. An undeliverable message appears in the log each time it occurs. The logging message displays a message similar to the following:

```
Message (IMM:Base Class-SYS_Event, Identifier 0) from 1/1 (other
CSS) failed to reach destination 'Ipv4Arp' on 1/1 (this CSS)
```

The fields in this message includes a message type, details based on the message type, source information, and destination information. See [Table 8-6](#) for descriptions of these fields.

```
Message (message_type:details) from Source_information failed to
reach destination Dest on Dest_info
```

Table 8-6 Message Fields in a Log Level Debug-7 Logging Message

Message Fields	Description and possible entries
message type (<i>message_type</i>)	<p>IMM - Message passed both as inter-processor or intra-processor messages.</p> <p>LOCAL - Message passed between the threads on the same processor and may be IMM in format.</p> <p>EVENT - Messages to be distributed to a registered set of recipients throughout the entire CSS.</p>
details (<i>details</i>)	<p>For a LOCAL message type, there is no detail.</p> <p>For an EVENT message type, the details can be one of the following:</p> <ul style="list-style-type: none"> • String decoded name of the event when the event is known: (Event: Ipv4ArpChangeEvent) • Hexadecimal encoded name of the event when the event is out of range: (Event: unknown type-0x00a00005) <p>For an IMM message type, the details include Base Class followed by one of the following:</p> <ul style="list-style-type: none"> • The string decoded name of the base task ID and an identifier that is the decimal instance in the class, for example: (IMM:Base Class-SYS_Event, Identifier 0) • Unknown and the hexadecimal value of the message type field, for example: (IMM:Base Class- Unknown, unknown type-0x00a00005)

Table 8-6 Message Fields in a Log Level Debug-7 Logging Message

Message Fields	Description and possible entries
Source information (<i>source_information</i>)	<p>The origin of the message. The information includes the slot and subslot numbers and whether they are on either “this CSS” or “the other CSS” in an Adaptive Session Redundancy (ASR) configuration. For example:</p> <pre>from 1/1 (this CSS)</pre> <p>A LOCAL message type also includes information for the local processor context in string format, for example:</p> <pre>from 1/1- 'EventAgent' (this CSS)</pre>
Destination (<i>Dest</i>) and Destination Information (<i>Dest_Info</i>)	<p>The destination is the same destination as the destination at the beginning of the logging message. The destination information is where the message is going. This information includes the slot and subslot numbers as they appears in the logging header. For example:</p> <pre>failed to reach destination Ipv4Arp on 1/1 (this CSS)</pre>

Frequently Queried Log Messages

Table 8-7 lists the frequently queried log messages for the Cisco 11500 series CSS. This table includes information on the possible cause and corrective action, if required. Log messages are divided by logging subsystem, with messages listed alphabetically.

Table 8-7 Cisco 11500 Series CSS Log Messages

Log Message (sys.log: Subsystem Name, Level, and Message)	Cause and Resolution
acl Subsystem	
<pre>ACL-7: ACL match 2:254 Discarding ACL-7: TCP SrcPort: 1043 DestPort: 21 ACL-7: Source: 172.20.57.2 ACL-7: Dest: 172.20.48.35</pre>	<p>Incoming traffic matches an ACL statement. The CSS examines, and then drops, the packet.</p> <p>The log message appears for a packet that has an ACL statement applied by the flow manager. This log message indicates that load balancing can take place.</p>
<pre>ACL-7: ACL rule match 2:254 Discarding packet, Log Enabled</pre>	<p>Incoming traffic matches an ACL statement. The CSS examines, and then drops, the packet.</p> <p>The log message appears for a packet that has an ACL statement applied by the IPV4 module. This log message indicates that the CSS may not set up flows for the packet (certain source or destination ports do not create a flow). This log message could also be related to issues with ICMP or RIP.</p>

Table 8-7 Cisco 11500 Series CSS Log Messages

Log Message (sys.log: Subsystem Name, Level, and Message)	Cause and Resolution
<p>chassis Subsystem</p> <p>CHMGR: Missing backup power supply.</p>	<p>The power supply lost AC power from the source. A CSS 11501 and CSS 11503 contains one power supply. The CSS 11506 contains up to three power supplies, but requires two functioning power supplies to guarantee service. If the following message appears first, then you can assume that the problem is with the AC power source, not the power supply.</p> <p>CHMGR: Cannot locate power supply: <i>PSnumber</i>.</p> <p>The <i>PSnumber</i> variable indicates which power supply cannot be found or has failed.</p> <p>To determine whether the CSS power supplies are working properly, both LEDs on the front of each power supply should be lit.</p>

Table 8-7 Cisco 11500 Series CSS Log Messages

Log Message (sys.log: Subsystem Name, Level, and Message)	Cause and Resolution
CHMGR: Cannot locate power supply: <i>PSnumber</i> .	<p>The CSS chassis cannot find the power supply. The CSS 11501 and CSS 11503 contain one power supply. The CSS 11506 contains up to three power supplies but requires two functioning power supplies to guarantee service. The <i>PSnumber</i> variable indicates which power supply cannot be found or has failed. If you know that the power source is supplied to the chassis and correctly flowing to it, then the problem may be the power supply.</p> <p>To determine whether the CSS power supplies are working properly, make sure that both LEDs on the front of each power supply are lit.</p>

Table 8-7 Cisco 11500 Series CSS Log Messages

Log Message (sys.log: Subsystem Name, Level, and Message)	Cause and Resolution																								
<p>circuit Subsystem</p> <pre>CIRCUIT-7: Circuit status message for circuit 1023 sent to CE 20202c01 cause code is 7</pre>	<p>Codes indicate the status of interfaces within VLANs. The logical port cause and command codes are as follows:</p> <table border="0"> <thead> <tr> <th data-bbox="747 475 821 500">Cause</th> <th data-bbox="1065 475 1130 500">Code</th> </tr> </thead> <tbody> <tr> <td>CM_CIRCUIT_CREATED</td> <td>1</td> </tr> <tr> <td>CM_IP_REGISTER</td> <td>2</td> </tr> <tr> <td>CM_IP_NOT_REGISTER</td> <td>3</td> </tr> <tr> <td>CM_IP_MODIFIED</td> <td>4</td> </tr> <tr> <td>CM_LP_STATE_CHG</td> <td>5</td> </tr> <tr> <td>CM_CIRCUIT_REMOVED</td> <td>6</td> </tr> <tr> <td>CM_LP_ADDED</td> <td>7</td> </tr> <tr> <td>CM_LP_REMOVED</td> <td>8</td> </tr> <tr> <td>CM_LP_MODIFIED</td> <td>9</td> </tr> <tr> <td>CM_LP_FAILOVER</td> <td>10</td> </tr> <tr> <td>CM_CIRCUIT_DOWN</td> <td>11</td> </tr> </tbody> </table> <p>This log message indicates that a port has been added to a VLAN. This log message can occur when the association to a VLAN changes as the port transitions from an up to a down state.</p> <p>Use the show circuit command to list the VLANs (refer to Chapter 5, Configuring Interfaces and Circuits). Check the status of the ports of the VLAN or determine whether the VLAN is active.</p>	Cause	Code	CM_CIRCUIT_CREATED	1	CM_IP_REGISTER	2	CM_IP_NOT_REGISTER	3	CM_IP_MODIFIED	4	CM_LP_STATE_CHG	5	CM_CIRCUIT_REMOVED	6	CM_LP_ADDED	7	CM_LP_REMOVED	8	CM_LP_MODIFIED	9	CM_LP_FAILOVER	10	CM_CIRCUIT_DOWN	11
Cause	Code																								
CM_CIRCUIT_CREATED	1																								
CM_IP_REGISTER	2																								
CM_IP_NOT_REGISTER	3																								
CM_IP_MODIFIED	4																								
CM_LP_STATE_CHG	5																								
CM_CIRCUIT_REMOVED	6																								
CM_LP_ADDED	7																								
CM_LP_REMOVED	8																								
CM_LP_MODIFIED	9																								
CM_LP_FAILOVER	10																								
CM_CIRCUIT_DOWN	11																								

Table 8-7 Cisco 11500 Series CSS Log Messages

Log Message (sys.log: Subsystem Name, Level, and Message)	Cause and Resolution
csdpeer Subsystem	
<pre>CSDPEER-7: LR Send list too small !!!</pre>	<p>The number of domain names sent by the peer exceeds the size of the CSS list. You can configure this parameter through the (config) dns-peer command (see the <i>Cisco Content Services Switch Advanced Configuration Guide</i>). We recommend that you configure the receive and send slots with the same value. The default slot value is 255.</p>
flowmgr Subsystem	
<pre>FLOWMGR-4: Flow manager received an illegal message with code 10</pre>	<p>One of the Ethernet ports received a high number of malformed packets, resulting in an overflow of the fastpath. In this case, the flow manager received a badly formatted control message from the fastpath. This problem may be due to intermittent hardware, which results in the fastpath corrupting the packets, or the problem is related to the fastpath receiving streams of malformed packets and leaking some of those packets to the flow manager.</p> <p>Use the show ether-errors command to display information for a port that is experiencing many errors. Try disconnecting the port or changing ports and determine whether the errors stop.</p>
<pre>FLOWMGR-4: Flow manager received an illegal message with code 255</pre>	<p>One of the CSS Ethernet ports encountered a significant number of errors and a few malformed packets reached the flow manager.</p>

Table 8-7 Cisco 11500 Series CSS Log Messages

Log Message (sys.log: Subsystem Name, Level, and Message)	Cause and Resolution
FLOWMGR-4: Flow manager received an illegal message with code 194	The flow manager received an illegal message from the fastpath. This log message may occur due to hardware problems or a port receiving an excessive number of malformed packets. Use the show mibii or show ether-errors command to look for errors on one of the CSS ports.
<pre> FLOWMGR-6: FM_Tcp: Handling generic FMTCP flow Re-Transmit ERROR FLOWMGR-6: FM_ReTransTimeout: Re-Transmit timeout ERROR FLOWMGR-6: FM_Tcp: Handling generic FMTCP flow Re-Transmit ERROR FLOWMGR-6: FM_ReTransTimeout: Re-Transmit timeout ERROR FLOWMGR-6: FM_Tcp: Handling generic FMTCP flow Re-Transmit ERROR </pre>	<p>If the CSS handles a content request for a Layer 5 rule that spans more than three TCP packets, after the CSS decides on the server to use, it sends the TCP packets in TCP slow start form. Here is an example of a five-TCP segment content request:</p> <pre> Segment 1 --> Segment 2 --> (wait for an ACK) <--- ACK Segment3 -> Segment4 -> Segment5 -> <-- Content </pre> <p>If the CSS does not receive an ACK from the server within three seconds, it will refuse any remaining packets and terminate the connection with a reset. At that point, the log message is generated.</p>

Table 8-7 Cisco 11500 Series CSS Log Messages

Log Message (sys.log: Subsystem Name, Level, and Message)	Cause and Resolution
<pre>FLOWMGR-6: \n FM_UtilGenericTcpFlowReject: Handling Generic Flow REJECT</pre>	<p>The CSS rejects a connection, either due to issues with the client side or the server side of the connection.</p> <p>When this log message occurs as a result of the client side connection, the issue could be due to a content request that spans more than the configured maximum (default is 6). Other reasons could include:</p> <ul style="list-style-type: none"> • A delayed ACK could not be sent to the client (at 200ms) • A delayed ACK is sent to the client, and the client responds back with a TCP SYN/FIN/RST handshake sequence. • The client side closes down unexpectedly. <p>When this log message occurs as a result of the server side connection, the issue could be due to the CSS sending the spanned content request to the server and did not get an acknowledgement from the server or received an unexpected response (for example, due to the flow being torn down to the client side).</p> <p>If this message appears frequently in the log, contact Cisco Systems TAC.</p>
<pre>FLOWMGR-7: Allocation for a vector-loaded flow, where theFlow = 840ef5b0</pre>	<p>This is an informational message. No further action is required.</p>

Table 8-7 Cisco 11500 Series CSS Log Messages

Log Message (sys.log: Subsystem Name, Level, and Message)	Cause and Resolution
FLOWMGR-7: Exceeded outflow SYN count	<p>For a Layer 5 rule, the CSS is trying to establish a connection with the backend server. The CSS sent four SYNs to the backend server and did not get a response.</p> <p>For the CSS to establish a connection with the backend server, the CSS must receive the following TCP/IP handshake:</p> <pre>SYN-> <-SYN/ACK ACK-> GET-></pre> <p>After receiving the GET message, the CSS opens the backend connection. At that point, the log message is generated.</p> <p>When several of these log messages occur, there might be a malfunctioning server. The server problem could be from keepalives, or from regular TCP HTTP traffic. Make sure the port 80 sockets are not full on the servers.</p>
<p>fp-driver</p> <p>FP_DRV-4: PrismImmFastPath::Send: Could not allocate an MCID. Remote message send aborted.</p>	<p>The CSS MIPS processor attempts to send a group message, but the processor cannot obtain an multicast ID (MCID) from the Multicast ID Module (MID). The MID keeps track of the reference count on a buffer when the CSS sends a packet to multiple locations. The fast path uses an MCID to reference count the buffer with a contained packet that is being flooded to all ports in a VLAN.</p>

Table 8-7 Cisco 11500 Series CSS Log Messages

Log Message (sys.log: Subsystem Name, Level, and Message)	Cause and Resolution
<p>FP_DRV-4: PrismImmFastPath::Send: Could not allocate an MCID. Remote message send aborted.</p> <p>(continued from previous page)</p>	<p>For MCIDs to be depleted in the CSS, there must be 1024 reference counted packets queued up in some combination of hardware queues and software queues.</p> <p>To fill up hardware queues, the CSS must receive a large number of packets, which it then chooses to flood out all ports.</p> <p>In the case of software queues, it might be possible for some task on the MIPS processor to deplete the MCID pool by sending a large number of messages to a group that contains both local and remote members. If the local member has a very large queue, the queue could fill up before running the recipient task, processing the messages, and freeing the buffers.</p> <p>Of the two potential causes, the most likely causes is the CSS receiving a large number of packets which it must flood out all ports.</p> <p>This log message typically occurs when the CSS loses a specific route and forwards the flow out the default gateway. The default gateway then forwards the flow back to the CSS because the routing table lists the CSS as the next hop. As a result, the packet is continuously routed out the default gateway and back to the CSS.</p>

Table 8-7 Cisco 11500 Series CSS Log Messages

Log Message (sys.log: Subsystem Name, Level, and Message)	Cause and Resolution
ipv4 Subsystem	
<pre>IPV4-4: Ipv4IfMgrCctUpdateMsg: IF config for circuit 1015 not found CIRCUIT-4: Error, Circuit 1015 does not exist.</pre>	<p>You deleted a circuit but the circuit is still referenced by an ACL or to another configuration parameter. Verify the CSS configuration and make the necessary modifications to remove references to the deleted circuit.</p>
<pre>IPV4-4: Ipv4ReceivePacket: out of mbufs</pre>	<p>An <i>mbuf</i> is a data structure in BSD UNIX-based IP stacks (such as the VxWorks stack) that is used for buffering. This log message indicates the CSS received a packet that was addressed to a CSS IP address, and when attempting to send the packet up the VxWorks IP stack, the CSS had no remaining buffers.</p> <p>Note These buffers are separate from those used for flow setup and forwarding purposes. They are used only when traffic is sent to the CSS itself, (for example, during a Telnet session).</p> <p>If you receive this message, contact Cisco Systems TAC.</p>

Table 8-7 Cisco 11500 Series CSS Log Messages

Log Message (sys.log: Subsystem Name, Level, and Message)	Cause and Resolution
IPV4-4: Ipv4SfmArpTx: unknown circuit in buffer (2001)	<p>An ARP TX task is running on the SFM, receiving packets from the SFM and transmitting them to the proper egress ports. This message includes the circuit number (2001, in this example). If the circuit number for this ARP was down or inactive while the ARP was still being queued in the SFM, the message would appear in the log. An action caused the circuit to be removed while data for the circuit was still in the buffer.</p> <p>Determine whether all physical interfaces in a circuit VLAN are going up and down, or a configuration change occurred on the VLAN at the time of the message.</p>
IPV4-4: Ipv4SfmForwRx: bad IP version received (0)	<p>The IPV4 receive task received a packet and the IP version is displayed in parentheses (). The CSS discards any packet that is not Ipv4 version 4. In this example, the IP version is 0. If you see many of these messages, the problem could be an improperly configured device or a DoS attack.</p>
IPV4-4: Ipv4SfmForwTx: No VC for buffer (0x00000000)	<p>The IPV4 transmit task has a buffer to transmit to the switch fabric processor, however the CSS still needs to create the Virtual Circuit to the fastpath. This message typically occurs if the CSS Ethernet port changes state.</p> <p>This is an informational message. No further action is required.</p>

Table 8-7 Cisco 11500 Series CSS Log Messages

Log Message (sys.log: Subsystem Name, Level, and Message)	Cause and Resolution
<pre>IPV4-4 Ipv4SfmForwTx: unknown logical port in buffer <0x05c01f00></pre>	<p>A link became unavailable while an ARP or other IPV4 packets were in transit. When this occurred, the CSS chose a logical port to transmit from, formatted the packets, and then attempted to transmit the packets. At the point when the CSS attempted to transmit packets, the logical port was no longer available.</p> <p>This is an informational message. No further action is required.</p>
<pre>IPV4-4: Ipv4ApIoctl: unknown command: 1074031872</pre>	<p>This is an informational message. No further action is required.</p>
<pre>IPV4-4: Ipv4SfmForwRx: buffer length (872) less than IP length (1004)</pre>	<p>IP packets have been corrupted and the IP header Total Length value does not match with the actual length of the packet. In this case, the SP receives less total bytes than expected from the IP header length. This message may be related to hardware problems or errors on the line (corrupted packets). Use the show mibii or show ether-errors command to look for errors on one of the CSS ports.</p>

Table 8-7 Cisco 11500 Series CSS Log Messages

Log Message (sys.log: Subsystem Name, Level, and Message)	Cause and Resolution
<pre>IPV4-4: (RIP) VIP Redundancy callback on unregistered address 0.0.0.0 range 0</pre>	<p>The CSS is running VIP redundancy and is using the global Routing Information Protocol (RIP) to advertise VIPs on the CSS to other routers (configured through the rip advertise command). In this case, RIP sends the redundancy manager in the CSS the VIP and the range, and requests to be informed of any changes in the VIP redundancy status.</p> <p>If the redundancy manager monitors a change in VIP redundancy status, it contacts RIP with the VIP address and the range. To ensure the proper advertisement of the VIPs, RIP verifies the VIP address and range. This log message occurs when RIP is unable to find the VIP address received in the callback message from the redundancy manager.</p> <p>Check the IP address specified in the rip advertise command and verify that the VIPs are configured properly for VIP and virtual interface redundancy.</p>
<pre>IPV4-0: Ipv4SfmProcessArpFrame: ARP packet with unknown ingress port 0x0fc01f00</pre>	<p>A CSS Ethernet port became unavailable while an ARP packet is in transit from the fastpath to the IPV4 destination. As a result, the ARP packet is dropped.</p> <p>This is an informational message. No further action is required.</p>

Table 8-7 Cisco 11500 Series CSS Log Messages

Log Message (sys.log: Subsystem Name, Level, and Message)	Cause and Resolution
<pre>IPV4-4: Ipv4SfmCmDeleteFlow: -1 response from VccRemoveVc, egress 0x09c01f00</pre>	<p>A CSS Ethernet port became unavailable. As a result, the IPV4 module was unable to delete a Virtual Circuit established through the switch fabric to the fastpath.</p> <p>This is an informational message. No further action is required.</p>
<pre>IPV4-4: Ipv4SfmProcessArpFrame: bad ARP packet received</pre>	<p>The CSS detects that it has received an invalid ARP packet. The following messages can appear in the log to clarify why the CSS logs the receipt of an invalid ARP packet.</p> <pre>IPV4-4: ffff53ff01ff ff0077fa6503 0806 IPV4-4: HW type: 0x0000 Proto type: 0x0000 IPV4-4: HLEN 0x00 PLEN 0x00 OPTPA-TSI-CSS1# 0x0000 IPV4-4: Sender HA 000000000000 IPV4-4: Sender IP 0.0.0.0 IPV4-4: Target HA 000000000000 IPV4-4: Target IP 0.0.0.0</pre> <p>The first line in the log message identifies the destination MAC address of the packet, the source address of the packet, and the type of IP packet. In the example above, the destination MAC address is ff-ff-53-ff-01-ff and the source MAC address is ff-00-77-e7-65-03. In addition, 0806 equals ETHERTYPE_ARP.</p> <p>The second line in the message identifies the hardware type and protocol type. In this example, the CSS logs the messages because both the hardware type and protocol type are 0000. The CSS views this value as an indication of an invalid packet.</p>

Table 8-7 Cisco 11500 Series CSS Log Messages

Log Message (sys.log: Subsystem Name, Level, and Message)	Cause and Resolution
<pre>IPV4-4: Duplicate IP address detected: 192.168.163.129 00-08-e2-10-38-54 IPV4-4: Incoming CE 0x3001f04, incoming (0 based) SLP 0xc</pre>	<p>A duplicate IP address has been detected by the CSS. Typically, two level 4 IPV4 messages appear to provide assistance in finding the duplicate IP address that was detected by the CSS.</p> <p>The first message states that the CSS received a packet with a source IP address that is also configured on the CSS. The message identifies the duplicate source IP address and its corresponding MAC address as an aid to locate the device with the duplicate IP address.</p> <p>The second message is intended to assist you in locating the port on the CSS that has received the duplicate IP address. Use the flow statistics command to locate the interface on the CSS. The flow statistics command should correspond the CE value listed in the log message with a port.</p>
keepalive Subsystem	
<pre>KAL-7: kal_ServiceNotify: kalIndex = 24 kalSvcEvent=3 KAL-7: kal_ServiceNotify: kalIndex = 31 kalSvcEvent=4 KAL-7: kal_ServiceNotify: kalIndex = 49 kalSvcEvent=5</pre>	<p>The CSS is configured with HTTP keepalives (HEAD or GET) and the servers transition between states. The service event (kalSvcEvent) values are as follows:</p> <ul style="list-style-type: none"> • 3 = Alive • 4 = Dying • 5 = Dead <p>Check the status of the server.</p>

Table 8-7 Cisco 11500 Series CSS Log Messages

Log Message (sys.log: Subsystem Name, Level, and Message)	Cause and Resolution
<p>netman Subsystem</p> <p>NETMAN-1: TRAP:Authentication:Generated by: 192.168.36.252</p>	<p>The CSS is configured to transmit SNMP trap messages and a user attempts to access the CSS with an incorrect SNMP community string. In this example, the CSS sends a trap to the configured SNMP trap receiver stating that a client with IP address 192.168.36.252 is trying to access the CSS with an incorrect community string.</p> <p>This log message also appears when a user attempts to access the CSS using SNMP and SNMP is not configured on the CSS. Refer to Chapter 12, Configuring Simple Network Management Protocol (SNMP) for configuration information.</p>
<p>NETMAN-2: Sshd:do_authenticated:ERROR-> TSM Rejects connection</p>	<p>Remote access is being initiated to the CSS CLI. If the CSS security manager rejects the log in, the session terminates.</p> <p>The security manager can reject the log in when:</p> <ul style="list-style-type: none"> • The maximum number of concurrent security manager users had been exceeded (128 concurrent users). • The CSS could not re-register (if you had a session that just ended and the flow cleanup was not performed, and you attempted to re-register too soon). • The CSS ran out of memory and could not allocate a control block.

Table 8-7 Cisco 11500 Series CSS Log Messages

Log Message (sys.log: Subsystem Name, Level, and Message)	Cause and Resolution
<pre>NETMAN-2: Generic:LINK DOWN for 13/1 CIRCUIT-6: Port 13/1 is down for circuit VLAN1 NETMAN-2: Generic:LINK DOWN for 13/2 CIRCUIT-6: Port 13/2 is down for circuit VLAN1 NETMAN-2: Generic:LINK DOWN for 13/3 CIRCUIT-6: Port 13/3 is down for circuit VLAN1 NETMAN-2: Generic:LINK DOWN for 13/4 CIRCUIT-6: Port 13/4 is down for circuit VLAN1 SYSSOFT-3: ONDM: Timeout downloading image to EPIF 0 from the switch. SYSSOFT-3: ONDM: Timeout downloading image to EPIF 0 from the switch.</pre>	<p>EPIF 0 belongs to the first four ports on a FEM. This log message usually relates to a problem with the SFM not getting the code to the FEM or the FEM not reading the SFM properly.</p> <p>In this case, there is a communications problem between the SP 9/2 and the FEM.</p> <pre>JAN 5 00:31:43 arrowpoint1.com 9/2 385390 SYSSOFT-3: ONDM: Timeout downloading image to EPIF 0 from the switch. JAN 5 00:31:45 arrowpoint1.com 9/2 385407 SYSSOFT-3: ONDM: Timeout downloading image to EPIF 0 from the switch.</pre> <p>Reseat the SFM in slot 9, then reseat the FEM in slot 13 that is controlled by the SFM. Cycle power to the CSS.</p>
<pre>NETMAN-2: Enterprise:Service Transition:ServerA -> down NETMAN-5: Enterprise:Service Transition:ServerA -> alive</pre>	<p>This is an information message when the service has changed state. Check the status of the server based on the keepalive parameters.</p>
<pre>NETMAN-4: SNMPAPI:SNMPAPI_Set:SET failure</pre>	<p>A user on the CLI, connected to the CSS either through the console or by Telnet, has entered an incorrect command. A Telnet or console session displays this message, stating that the command was incorrect.</p>
<pre>NETMAN-5: Enterprise: Login Failure:vty2 10.6.3.171 Mandy</pre>	<p>SNMP Enterprise login failure traps are enabled and an invalid username and password have been entered. Refer to Chapter 12, Configuring Simple Network Management Protocol (SNMP) for details on SNMP and the CSS.</p>

Table 8-7 Cisco 11500 Series CSS Log Messages

Log Message (sys.log: Subsystem Name, Level, and Message)	Cause and Resolution
NETMAN-5: Generic:SNMP Authentication > Failure from x.x.x.x	A user is trying to use SNMP to poll the CSS, but has entered the wrong community string. Refer to Chapter 12, Configuring Simple Network Management Protocol (SNMP) for details on specifying a community string.
NETMAN-5: Enterprise:Service > Transition:nexthop00001 -> down	The next hop IP address can not be reached by the CSS. When you configure a static route, an internal service is automatically created by the CSS. When the service is up, the static route is included in the routing table. If the service is unavailable, the service is removed from the routing table. Make sure that all of the routes included in the CSS routing table are available. Some routes may have transitioned between states.
NETMAN-5: Generic:LINK UP for 3/1 SYSSOFT-7: NP55_connection.c 512: Connection already open or reserved SYSSOFT-3: NP55 Driver: Connection already open or reserved SYSSOFT-2: VccAddVc:open conn failed w/ stat = -1; iVc 320; eVc 290 FLOWMGR-7: FM_GetIpv4Vc: Warning VCC_FP_IPV4_DC failed	The flow manager tried to reallocate a Virtual Circuit that was already established. These messages occur when the port is coming up. They do not represent a problem. The messages are most noticeable at the end of boot time if you connected through the console.
NETMAN-7: clm_ProcessStdAction:ERROR->A ction<clms_dir>not found NETMAN-7: CLM:ERROR from clm_DispatchActionRoutine()	An invalid CLI command was entered. In this example, a user entered the dir command in debug mode and specified an invalid directory. For example: (debug) # dir d:

Table 8-7 Cisco 11500 Series CSS Log Messages

Log Message (sys.log: Subsystem Name, Level, and Message)	Cause and Resolution
<pre>NETMAN-7: SNMP:UNKNOWN RSP (493512 NETMAN-7: SNMP:(493512) Index = 1 <NO_SUCH_NAME></pre>	<p>A valid SNMP agent (community string matched) is attempting to set an invalid object and the CSS does not recognize the object.</p>
<pre>NETMAN-7: TSM:tsm_SendToCLA:ERROR->Write</pre>	<p>This security manager message is associated with line data moving through the stack after a line has been disconnected (Telnet application disconnect). This message is at DEBUG level for developer information purposes only.</p>
<pre>NETMAN-7: ASUPPORT:as_SyncTask:ERROR->No registered reciever for MT:5/1.0 W</pre>	<p>This is an informational message. No further action is required.</p>

Table 8-7 Cisco 11500 Series CSS Log Messages

Log Message (sys.log: Subsystem Name, Level, and Message)	Cause and Resolution
portmapper Subsystem	
PORTMAPPER-5: PortUnmap no Port mapping found.	A source group is running out of portmappers. Use the portmap command to increase the portmappers on the source group so that the message does not appear, and users or services do not see a performance or network address translation problem.
publish Subsystem	
PUBLISH-1: Unable to allocate tree memory <4150000>	<p>The CSS is looking for a segment of memory that is approximately 4150000 bytes and it cannot locate an available block of memory. In some cases, this message may be caused by a replication misconfiguration. Review the configuration and verify that it reflects what was intended. Verify that files are being replicated properly.</p> <p>If this message is seen with significantly smaller memory requests, the system memory may not sufficient in size to meet the requirements of the configuration. To isolate the issue, monitor the available memory under non-replication conditions to determine a baseline and then repeat this process while replicating to isolate this issue.</p> <p>Use the show system-resources command to view information about the installed and free memory in the CSS. To make additional memory available, reboot the CSS.</p>

Table 8-7 Cisco 11500 Series CSS Log Messages

Log Message (sys.log: Subsystem Name, Level, and Message)	Cause and Resolution
radius Subsystem	
<pre>RADIUS-7: Auth Primary RADIUS-7: The id is 63 RADIUS-7: Return Auth Primary RADIUS-7: RADIUS no memory available</pre>	<p>The RADIUS server does not have the correct attributes set up for the CSS. Refer to Chapter 11, Configuring CSS Remote Access Methods for background information on setting up an ACS radius server.</p>
<pre>RADIUS-4: RADIUS Authentication failed with reason code 2</pre>	<p>In this message, the different codes include:</p> <pre>#define PW_ACCESS_REQUEST 1 #define PW_ACCESS_ACCEPT 2 #define PW_ACCESS_REJECT 3 #define PW_ACCOUNTING_REQUEST 4 #define PW_ACCOUNTING_RESPONSE 5 #define PW_ACCOUNTING_STATUS 6 #define PW_ACCESS_CHALLENGE 11</pre> <p>In the example above, code 2 indicates that the CSS received the Accept response from the RADIUS server but may have rejected the Accept response, perhaps due to an invalid username or password.</p> <p>This log message only appears when logging debug messages (debug-7) for the radius subsystem.</p>

Table 8-7 Cisco 11500 Series CSS Log Messages

Log Message (sys.log: Subsystem Name, Level, and Message)	Cause and Resolution
sntp Subsystem	
SNTP-6: Sntp Server has incorrect mode 29	This message indicates potential issues with the SNTP server. Ensure that the SNTP server is transmitting time updates as “server” to the CSS. SNTP server updates are the only SNTP server updates supported by the CSS.
syssoft Subsystem	
SYSSOFT-2: VccAddVc:open conn failed w/ stat = -1; iVc 320; eVc 290	This message occurs when a port transitions from an up to a down state. Check autonegotiation, for a defective cable, or for malfunctioning hardware.
SYSSOFT-3: ONDM: Could not open file <wsscm.sys> SYSSOFT-3: ONDM: Could not download Sub-module 8/1. SYSSOFT-3: ONDM: Could not open file <wssfm.sys> SYSSOFT-3: ONDM: Could not download Sub-module 6/2. SYSSOFT-3: ONDM: Could not download Sub-module 6/1. SYSSOFT-3: ONDM: Could not download Sub-module 5/2 SYSSOFT-3: ONDM: Could not download Sub-module 5/1. SYSSOFT-3: ONDM:No Sfm proxy for Slot 2. SYSSOFT-3: ONDM:No Sfm proxy for Slot 1.	The CSS could not find the image file to load on the disk. There is something wrong with the disk or the file was deleted from the directory. Contact Cisco Systems TAC.
SYSSOFT-4: SYS:SysImmBind:Bind Collision TSM:5/1.1 W	This is an informational message. No further action is required.

Table 8-7 Cisco 11500 Series CSS Log Messages

Log Message (sys.log: Subsystem Name, Level, and Message)	Cause and Resolution
<pre>SYSSOFT-4: Invalid Target(0x03087a01) for Chassis Type, Message being dropped.</pre>	<p>The CSS attempts to request the sending of a message to a slot and subslot that does not exist in the chassis. The log message indicates the incorrect address in hexadecimal and the message has been dropped. This message most likely occurs when you issue a command to slot 4 and subslot 1 on a CSS 11503.</p> <p>No corrective action is required.</p>
<pre>SYSSOFT-4: Event not deliverable, msgq id =0x8cc48980, event id = 29, event name = BridgeMacAddrEvent</pre>	<p>The CSS was unable to deliver a certain process because a queue was full. Every message signifies that a event has been dropped because the queue full condition. This message appears when the fastpath (network processor) performs a source MAC address lookup and cannot find an entry. The fastpath then sends a MAC address learn message to the SCM. If the SCM receives too many messages before it has time to process them, the messages fill the queue.</p>

Table 8-7 Cisco 11500 Series CSS Log Messages

Log Message (sys.log: Subsystem Name, Level, and Message)	Cause and Resolution
<pre>SYSSOFT-4: Event not deliverable, msgq id = 0x865c2110, event id = 4, event name = Ipv4RouteChangeEvent</pre>	<p>The CSS was unable to deliver a certain process because a queue was full. Every message signifies that a event has been dropped because the queue full condition. This message happens whenever a route change is detected. The RIP process, the OSPF process, the caretaker processes (one for each SFM, which try to keep the SFM and SCM route tables in sync), the static route process, and the ARP process register for this event.</p> <p>Look for any routes transitioning state, locally attached stations or servers going up and down, or a large number of ARP requests being performed.</p>
<pre>SYSSOFT-7: MPOOL:mpoolAutoAlloc:WARN->Ov errun on MPOOL 3 321</pre>	<p>This message typically appears at boot up as an informational message to let you know that additional CSS memory is being allocated. No further action is required.</p>

Table 8-7 Cisco 11500 Series CSS Log Messages

Log Message (sys.log: Subsystem Name, Level, and Message)	Cause and Resolution
vlanmgr Subsystem	
<pre>VLANMGR-4: DeleteMacAddr() called with VlanID = 0 for MacAddr 0- 0- 0- 0- 0- 0</pre>	<p>The VLAN Manager is being asked to delete a MAC address entry from the forwarding table with a VLAN ID and MAC address of all zeros.</p>
vpm Subsystem	
<pre>VPM removed Vc 8000b00 based on failure of port 3401f00.<010></pre>	<p>The CSS is reclaiming the resources used by a specific Ethernet port because the port is unavailable. The CSS reclaims resources when a port is unresponsive to an internal check, or when a circuit is unavailable. No addressing information is available for that Ethernet port. Use the show interface command to display information for the Ethernet ports and determine which port is the problem.</p>
wcc Subsystem	
<pre>WCC-7: Route Change for IP Address (x.x.x.x)</pre>	<p>This is an informational message, stating that an ARP came in on a different port.</p>

Where to Go Next

[Chapter 9, Configuring Flow and Port Mapping Parameters](#) provides information on how to configure TCP and UDP flow parameters for the CSS, such as configuring connections for TCP or UDP ports, configuring flow resource reclamation, and configuring CSS port mapping

■ Where to Go Next