

CHAPTER 6

Monitoring System Processes and Logs

This chapter provides details on monitoring the health of the switch. It includes the following sections:

- [Displaying System Processes, page 6-1](#)
- [Displaying System Status, page 6-2](#)
- [Core and Log Files, page 6-3](#)
- [Clearing the Core Directory, page 6-4](#)
- [Default Settings, page 6-8](#)

Displaying System Processes

To obtain general information about all processes using Device Manager, follow these steps:

Step 1 Choose **Admin > Running Processes**.

You see the Running Processes dialog box (see [Figure 6-1](#)).

Send documentation comments to fm-docfeedback@cisco.com

Figure 6-1 Running Processes Dialog Box

ProcessId	Name	MemAllocated (B)	CPU Time (us)
1	init	16620	94376300
2	keventd	0	1150
3	ksoftirqd_CPU0	0	1943880227
4	kswapd	0	2
5	bdflush	0	3
6	kupdated	0	8570879
1376	kjournald	0	1443394
1383	kjournald	0	583809
1578	portmap	17000	1081
1587	httpd	746040	91808014
1594	rpc.nfsd	22304	31492455
1596	rpc.mountd	23008	31660425
1598	sysmgr	4031464	721314311
1796	mping-thread	0	68
1797	mping-thread	0	35
1879	sdip-mts-thread	0	9106777
2617	xinetd	100340	26575
2618	tftpd	5820	7658
2619	syslogd	259488	888109476
2620	sdwrapd	170412	37699
2622	platform	1431168	713545891
2626	usd_mts_kthread	0	3
2633	kfu_fsm-app-137	0	18
2634	kfu_mts-app-137	0	6
2650	bel_mts_kthread	0	23
2654	redun_kthread	0	21
2655	redun_timer_kth	0	2
2659	ls-notify-mts-t	0	40517005

142 row(s)

Refresh Help Close

Where:

- ProcessId = Process ID
- Name = Name of the process
- MemAllocated = Sum of all the dynamically allocated memory that this process has received from the system, including memory that may have been returned
- CPU Time (ms) = CPU time the process has used, in microseconds

Step 2 Click **Close** to close the dialog box.

Displaying System Status

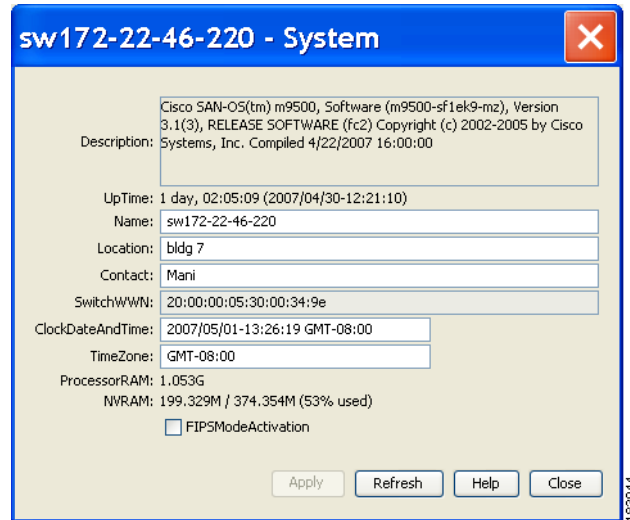
To display system status from Device Manager, follow these steps:

Step 1 Choose **Physical > System**.

You see the System dialog box (see [Figure 6-2](#)).

Send documentation comments to fm-docfeedback@cisco.com

Figure 6-2 System Dialog Box



Step 2 Click **Close** to close the dialog box.

Core and Log Files

This section contains the following topics:

- [Displaying Core Status, page 6-3](#)
- [Clearing the Core Directory, page 6-4](#)

Displaying Core Status



Note

Be sure SSH2 is enabled on this switch.

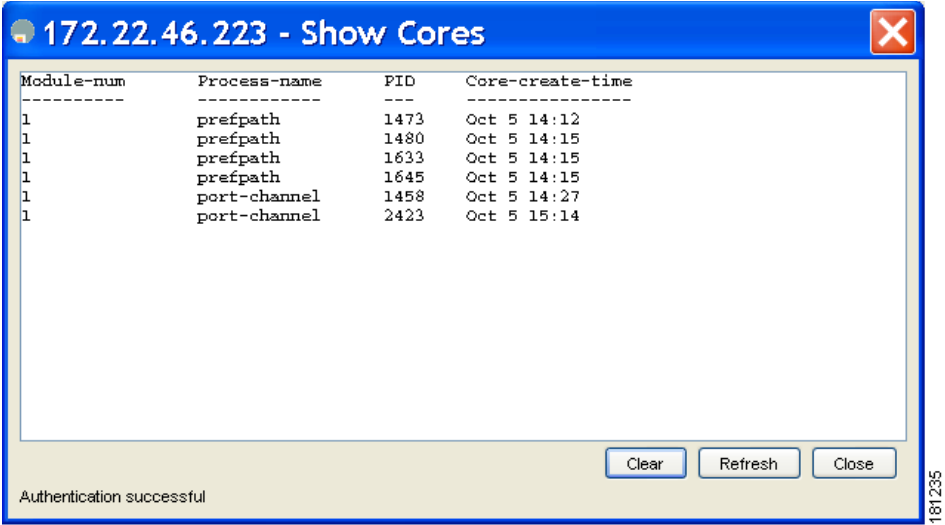
To display cores on a switch using Device Manager, follow these steps:

Step 1 Choose **Admin > Show Cores**.

You see the Show Cores dialog box (use [Figure 6-3](#)).

Send documentation comments to fm-docfeedback@cisco.com

Figure 6-3 Show Cores Dialog Box



Where Module-num shows the slot number on which the core was generated. In this example, the fspf core was generated on the active supervisor module (slot 5), fcc was generated on the standby supervisor module (slot 6), and acltcam and fib were generated on the switching module (slot 8).

Step 2 Click **Close** to close the dialog box.

Clearing the Core Directory



Note

Be sure SSH2 is enabled on this switch.

To clear the cores on a switch using Device Manager, follow these steps

Step 1 Click **Clear** to clear the cores.

The software keeps the **clear** last few cores command to clean out the core directory. The software per service and per slot and clears all the core files and other cores present on the active supervisor module.

```
switch# clear cores
```

Step 2 Click **Close** to close the dialog box.

First and Last Core

The first and last core feature uses the limited system resource and retains the most important core files. Generally, the first core and the most recently generated core have the information for debugging and, the first and last core feature tries to retain the first and the last core information.

Send documentation comments to fm-docfeedback@cisco.com

If the core files are generated from an active supervisor module, the number of core files for the service is defined in the service.conf file. There is no upper limit on the total number of core files in the active supervisor module.

Online System Health Management

The Online Health Management System (OHMS) (system health) is a hardware fault detection and recovery feature. It ensures the general health of switching, services, and supervisor modules in any switch in the Cisco MDS 9000 Family.

This section includes the following topics:

- [About OHMS, page 6-5](#)
- [Performing Internal Loopback Tests, page 6-7](#)
- [Performing External Loopback Tests, page 6-8](#)

About OHMS

The OHMS monitors system hardware in the following ways:

- The OHMS component running on the active supervisor maintains control over all other OHMS components running on the other modules in the switch.
- The system health application running in the standby supervisor module only monitors the standby supervisor module, if that module is available in the HA standby mode.

The OHMS application launches a daemon process in all modules and runs multiple tests on each module to test individual module components. The tests run at preconfigured intervals, cover all major fault points, and isolate any failing component in the MDS switch. The OHMS running on the active supervisor maintains control over all other OHMS components running on all other modules in the switch.

On detecting a fault, the system health application attempts the following recovery actions:

- Performs additional testing to isolate the faulty component.
- Attempts to reconfigure the component by retrieving its configuration information from persistent storage.
- If unable to recover, sends Call Home notifications, system messages and exception logs; and shuts down and discontinues testing the failed module or component (such as an interface).
- Sends Call Home and system messages and exception logs as soon as it detects a failure.
- Shuts down the failing module or component (such as an interface).
- Isolates failed ports from further testing.
- Reports the failure to the appropriate software component.
- Switches to the standby supervisor module, if an error is detected on the active supervisor module and a standby supervisor module exists in the Cisco MDS switch. After the switchover, the new active supervisor module restarts the active supervisor tests.
- Reloads the switch if a standby supervisor module does not exist in the switch.
- Provides CLI support to view, test, and obtain test run statistics or change the system health test configuration on the switch.

Send documentation comments to fm-docfeedback@cisco.com

- Performs tests to focus on the problem area.

Each module is configured to run the test relevant to that module. You can change the default parameters of the test in each module as required.

System Health Initiation

By default, the system health feature is enabled in each switch in the Cisco MDS 9000 Family.

Loopback Test Configuration Frequency

Loopback tests are designed to identify hardware errors in the data path in the module(s) and the control path in the supervisors. One loopback frame is sent to each module at a preconfigured frequency—it passes through each configured interface and returns to the supervisor module.

The loopback tests can be run at frequencies ranging from 5 seconds (default) to 255 seconds. If you do not configure the loopback frequency value, the default frequency of 5 seconds is used for all modules in the switch. Loopback test frequencies can be altered for each module.

Loopback Test Configuration Frame Length

Loopback tests are designed to identify hardware errors in the data path in the module(s) and the control path in the supervisors. One loopback frame is sent to each module at a preconfigured size—it passes through each configured interface and returns to the supervisor module.

The loopback tests can be run with frame sizes ranging from 0 bytes to 128 bytes. If you do not configure the loopback frame length value, the switch generates random frame lengths for all modules in the switch (auto mode). Loopback test frame lengths can be altered for each module.

Hardware Failure Action

The failure-action command controls the Cisco NX-OS software from taking any action if a hardware failure is determined while running the tests.

By default, this feature is enabled in all switches in the Cisco MDS 9000 Family—action is taken if a failure is determined and the failed component is isolated from further testing.

Failure action is controlled at individual test levels (per module), at the module level (for all tests), or for the entire switch.

Test Run Requirements

Enabling a test does not guarantee that the test will run.

Tests on a specific interface or module only run if you enable system health for all of the following items:

- The entire switch
- The required module
- The required interface

Send documentation comments to fm-docfeedback@cisco.com

**Tip**

The test will not run if system health is disabled in any combination. If system health is disabled to run tests, the test status shows up as disabled.

**Tip**

If the specific module or interface is enabled to run tests, but is not running the tests due to system health being disabled, then tests show up as enabled (not running).

Tests for a Specified Module

The system health feature in the NX-OS software performs tests in the following areas:

- Active supervisor's in-band connectivity to the fabric.
- Standby supervisor's arbiter availability.
- Bootflash connectivity and accessibility on all modules.
- EOBC connectivity and accessibility on all modules.
- Data path integrity for each interface on all modules.
- Management port's connectivity.
- User-driven test for external connectivity verification, port is shut down during the test (Fibre Channel ports only).
- User-driven test for internal connectivity verification (Fibre Channel and iSCSI ports).

Clearing Previous Error Reports

You can clear the error history for Fibre Channel interfaces, iSCSI interfaces, an entire module, or one particular test for an entire module. By clearing the history, you are directing the software to retest all failed components that were previously excluded from tests.

If you previously enabled the failure-action option for a period of time (for example, one week) to prevent OHMS from taking any action when a failure is encountered and after that week you are now ready to start receiving these errors again, then you must clear the system health error status for each test.

**Tip**

The management port test cannot be run on a standby supervisor module.

Performing Internal Loopback Tests

You can run manual loopback tests to identify hardware errors in the data path in the switching or services modules, and the control path in the supervisor modules. Internal loopback tests send and receive FC2 frames to and from the same ports and provide the round-trip time taken in microseconds. These tests are available for Fibre Channel, IPS, and iSCSI interfaces.

Choose **Interface > Diagnostics > Internal** to perform an internal loopback test from Device Manager.

Send documentation comments to fm-docfeedback@cisco.com

Performing External Loopback Tests

You can run manual loopback tests to identify hardware errors in the data path in the switching or services modules, and the control path in the supervisor modules. External loopback tests send and receive FC2 frames to and from the same port or between two ports.

You need to connect a cable (or a plug) to loop the Rx port to the Tx port before running the test. If you are testing to and from the same port, you need a special loop cable. If you are testing to and from different ports, you can use a regular cable. This test is only available for Fibre Channel interfaces.

Choose **Interface > Diagnostics > External** to perform an external loopback test from Device Manager.

On-Board Failure Logging

The Generation 2 Fibre Channel switching modules provide the facility to log failure data to persistent storage, which can be retrieved and displayed for analysis. This on-board failure logging (OBFL) feature stores failure and environmental information in nonvolatile memory on the module. The information will help in post-mortem analysis of failed cards.

About OBFL

OBFL data is stored in the existing CompactFlash on the module. OBFL uses the persistent logging (PLOG) facility available in the module firmware to store data in the CompactFlash. It also provides the mechanism to retrieve the stored data.

The data stored by the OBFL facility includes the following:

- Time of initial power-on
- Slot number of the card in the chassis
- Initial temperature of the card
- Firmware, BIOS, FPGA, and ASIC versions
- Serial number of the card
- Stack trace for crashes
- CPU hog information
- Memory leak information
- Software error messages
- Hardware exception logs
- Environmental history
- OBFL specific history information
- ASIC interrupt and error statistics history
- ASIC register dumps

Default Settings

[Table 6-1](#) lists the default system health and log settings.

Send documentation comments to fm-docfeedback@cisco.com

Table 6-1 **Default System Health and Log Settings**

Parameters	Default
Kernel core generation	One module
System health	Enabled
Loopback frequency	5 seconds
Failure action	Enabled

Send documentation comments to fm-docfeedback@cisco.com