



Troubleshooting Overview

This chapter introduces the basic concepts, methodology, and general troubleshooting guidelines for problems that may occur when configuring and using the Cisco MDS 9000 Family of multilayer directors and fabric switches.

This chapter includes the following sections:

- [Overview of the Troubleshooting Process, page 1-1](#)
- [Overview of Best Practices, page 1-2](#)
- [Troubleshooting Basics, page 1-2](#)
- [Primary Troubleshooting Flowchart, page 1-8](#)
- [System Messages, page 1-8](#)
- [System Messages, page 1-8](#)
- [Troubleshooting with Logs, page 1-12](#)
- [Contacting Customer Support, page 1-14](#)

Overview of the Troubleshooting Process

To troubleshoot your fabric environment, follow these general steps:

-
- | | |
|---------------|--|
| Step 1 | Gather information that defines the specific symptoms. |
| Step 2 | Identify all potential problems that could be causing the symptoms. |
| Step 3 | Systematically eliminate each potential problem (from most likely to least likely) until the symptoms disappear. |
-

To identify the possible problems, you need to use a variety of tools and understand the overall storage environment. For this reason, this guide describes a number of general troubleshooting tools in [Appendix B, “Troubleshooting Tools and Methodology,”](#) including those that are specific to the Cisco MDS 9000 Family. This chapter also provides a plan for investigating storage issues. See other chapters in this book for detailed explanations of specific issues.

Send documentation comments to mdsfeedback-doc@cisco.com

Overview of Best Practices

Best practices are the recommended steps you should take to ensure the proper operation of your fabric. Each chapter includes a section on best practices for the covered Cisco SAN-OS features. We recommend the following general best practices for most SAN fabrics:

- Maintain a consistent Cisco SAN-OS release across all your Cisco MDS switches.
- Refer to the release notes for your Cisco SAN-OS release for the latest features, limitations, and caveats.
- Enable system message logging. See the [“System Messages” section on page 1-8](#).
- Troubleshoot any new configuration changes after implementing the change.
- Use Fabric Manager and Device Manager to proactively manage your fabric and detect possible problems before they become critical.

Troubleshooting Basics

This section provides a series of questions that may be useful when troubleshooting a problem with a Cisco MDS 9000 Family switch or connected devices. Use the answers to these questions to plan a course of action and to determine the scope of the problem. For example, if a host can only access some, but not all, of the logical unit numbers (LUNs) on an existing subsystem, then fabric-specific issues (such as FSPF, ISLs, or FCNS) do not need to be investigated. The fabric components can therefore be eliminated from possible causes of the problem.

This section contains the following topics:

- [Troubleshooting Guidelines, page 1-2](#)
- [Gathering Information Using Common Fabric Manager Tools and CLI Commands, page 1-3](#)
- [Verifying Basic Connectivity, page 1-4](#)
- [Verifying SAN Element Registration, page 1-5](#)
- [Fibre Channel End-to-End Connectivity, page 1-5](#)

Troubleshooting Guidelines

The two most common symptoms of problems occurring in a storage network are:

- A host not accessing its allocated storage
- An application not responding after attempting to access the allocated storage

By answering the questions in the following subsections, you can determine the paths you need to follow and the components that you should investigate further. These questions are independent of host, switch, or subsystem vendor.

Answer the following questions to determine the status of your installation:

- Is this a newly installed system or an existing installation? (It could be a new SAN, host, or subsystem, or new LUNs exported to an existing host.)
- Has the host ever been able to see its storage?
- Does the host recognize any LUNs in the subsystem?

Send documentation comments to mdsfeedback-doc@cisco.com

- Are you trying to solve an existing application problem (too slow, too high latency, excessively long response time) or did the problem show up recently?
- What changed in the configuration or in the overall infrastructure immediately before the applications started to have problems?

To discover a SAN problem, use the following general SAN troubleshooting steps:

-
- | | |
|---------------|--|
| Step 1 | Gather information on problems in your fabric. See the “ Gathering Information Using Common Fabric Manager Tools and CLI Commands ” section on page 1-3. |
| Step 2 | Verify physical connectivity between your switches and end devices. See the “ Verifying Basic Connectivity ” section on page 1-4. |
| Step 3 | Verify registration to your fabric for all SAN elements. See the “ Verifying SAN Element Registration ” section on page 1-5. |
| Step 4 | Verify the configuration for your end devices (storage subsystems and servers). |
| Step 5 | Verify end-to-end connectivity and fabric configuration. See the “ Fibre Channel End-to-End Connectivity ” section on page 1-5. |
-

Gathering Information Using Common Fabric Manager Tools and CLI Commands

This section highlights the Fabric Manager tools and CLI commands that are commonly used to troubleshoot problems within your fabric. These tools and commands are a subset of what you may use to troubleshoot your specific problem. Each chapter may include tools and commands specific to the symptoms and possible problems.

Common Fabric Manager Tools

Use the following navigation paths in Fabric Manager or Device Manager to access common troubleshooting information:

- Overview of switch status—In Fabric Manager, click the **Switch Health Analysis** icon.
- End-to-end connectivity—In Fabric Manager, click the **End-to-End Connectivity Analysis** icon.
- Fabric configuration— In Fabric Manager, click the **Fabric Configuration Analysis** icon.
- Module status—In Device Manager, choose **Physical > Modules**.
- Cisco SAN-OS version—In Device Manager, choose **Physical > System**.
- View logs—In Device Manager, choose **Logs > FM Server** or **Logs > Switch Resident**.
- View Fabric Manager events—In Fabric Manager, click the **Events** tab in the map pane.
- Interface status—In Fabric Manager, choose **Switches > Interfaces** and select the port type you are interested in.
- View name server information— In Device Manager, choose **FC > Name Server**.
- View FLOGI information—In Fabric Manager, choose **Switches > Interfaces > FC Physical > FLOGI**.
- Analyze the results of merging zones – In Fabric Manager, choose **Zone > Merge Analysis**.

Send documentation comments to mdsfeedback-doc@cisco.com

Fabric Manager and Device Manager also provide the following tools to proactively monitor your fabric:

- ISL performance—In Fabric Manager, click the **ISL Performance** icon.
- Network monitoring—In Device Manager, click the **Summary** tab.
- Performance monitoring—In Fabric Manager, choose **Performance > Start Collection**.

Common CLI Commands

Issue the following commands and examine the outputs:

- **show module**
- **show version**
- **show running-config**
- **show logging log**
- **show interfaces brief**
- **show fcns**
- **show flogi**
- **show hardware internal errors**
- **show zoneset active**
- **show accounting log**



Note

To issue commands with the **internal** keyword, you must have an account that is a member of the network-admin group.

Verifying Basic Connectivity

Answer the following questions to verify basic connectivity between your end devices:

- Are you using the correct fiber (SM or MM)?
- Did you check for a broken fiber?
- Is the Fibre Channel port LED on the connected module green, and do the LEDs on any host bus adapter (HBA)/storage subsystem ports indicate normal functionality?
- Is there a LUN masking policy applied on the storage subsystem? If yes, is the server allowed to see the LUNs exported by the storage array?
- Is there a LUN masking policy configured on the host? Did you enable the server to see all the LUNs it can access?
- If LUN masking software is used, is the host's pWWN listed in the LUN masking database?
- Is the subsystem configured for an N port?

Examine the FLOGI database on the two switches that are directly connected to the host HBA and subsystem ports. Also, verify that both ports (attached to MDS-A and MDS-B) are members of the same VSAN. If both devices are listed in the FCNS database then ISLs are not an issue.

In Fabric Manager, choose **Tools > Ping** or **Tools > Traceroute** (or use the **fcping** or **fctrace** CLI commands) to verify connectivity. See the [“FC Ping and FC Traceroute” section on page B-4](#).

Send documentation comments to mdsfeedback-doc@cisco.com

Verifying SAN Element Registration

Answer the following questions to verify that your end devices are registered to the fabric:

- Are the HBAs and subsystem ports successfully registered with the fabric name server?
 - In Device Manager, choose **FC > Name Server**.
 - In the CLI, use the **show fcns** commands.
- Does the correct pWWN for the HBAs and the storage subsystem ports show up on the correct port in the FLOGI database?
 - In Fabric Manager, choose **Switches > Interfaces > FC Physical > FLOGI**.
 - In the CLI, use the **show flogi** commands.
- Are the HBA and storage subsystem on the same VSAN?
 - In Fabric Manager, choose **End Devices** and verify the VSAN IDs are identical.
 - From the CLI, use the **show vsan membership** command.
- Does any single zone contain both devices?
 - In Fabric Manager, choose the **Zone > Edit Full Zone Database** and select the active zone set (in bold) for the VSAN that contains the end devices. Verify that both devices are members of the same zone.
 - From the CLI, use the **show zoneset active** command.

Fibre Channel End-to-End Connectivity

Answering the following questions will help to determine if end-to-end Fibre Channel connectivity exists from a host or subsystem perspective:

- Does the host list the subsystem's port WWN (pWWN) or FC ID in its logs?
- Does the subsystem list the host's pWWN or FC ID in its logs or LUN masking database?
- Can the host complete a port login (PLOGI) to the storage subsystem?
- Is there any SCSI exchange that takes place between the server and the disk array?
- Is the HBA configured for N port?

You can use the HBA configuration utilities or the host system logs to determine if the subsystem pWWN or FC ID is listed as a device. This can validate that FSPF is working correctly.

Fabric Issues

Answering the following questions will help to determine the status of the fabric configuration:

- Are both the HBA and the subsystem port successfully registered with the fabric name server?
- Does the correct pWWN for the server HBA and the storage subsystem port show up on the correct port in the FLOGI database? In other words, is the device plugged into the correct port?
- Does any single zone contain both devices? The zone members can be WWNs or FC IDs.
- Is the zone correctly configured and part of the active configuration or zone set within the same VSAN?

Send documentation comments to mdsfeedback-doc@cisco.com

- Do the ISLs show any VSAN isolation?
- Do the host and storage belong to the same VSAN?
- Are any parameters, such as FSPF, static domain assignment, VSAN, or zoning, mismatched in the configuration of the different switches in the fabric?

Port Issues

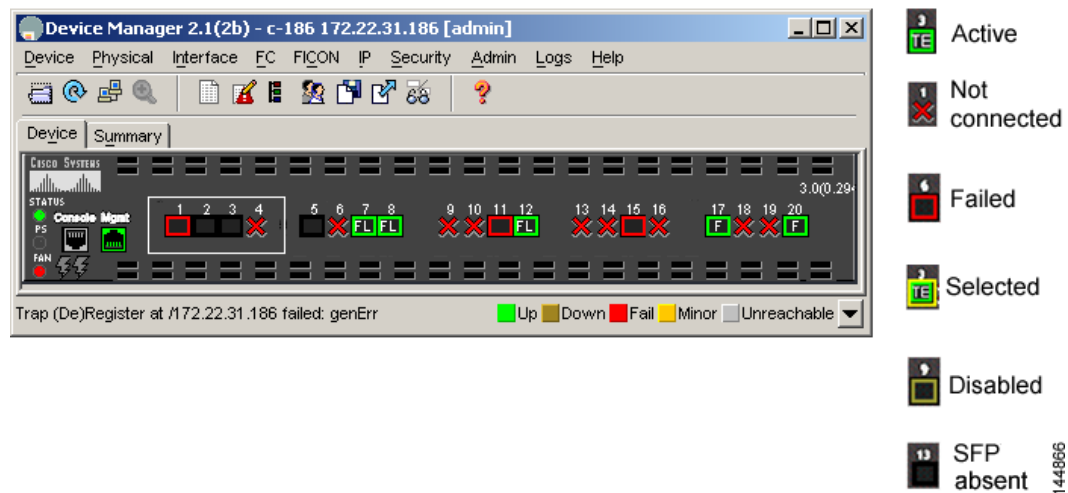
Initial tasks to perform while investigating port connectivity issues include:

- Verify correct media: copper or optical; single-mode (SM) or multimode (MM).
- Is the media broken or damaged?
- Is the LED on the switch green?
- Is the active LED on the HBA for the connected device on?

Basic port monitoring using Device Manager begins with the visual display in the Device View. (See [Figure 1-1](#).) Port display descriptions include:

- Green box: A successful fabric login has occurred; the connection is active.
- Red X: A small form-factor pluggable (SFP) transceiver is present but there is no connection. This could indicate a disconnected or faulty cable, or no active device connection.
- Red box: An SFP is present but fabric login (FLOGI) has failed. Typically there is a mismatch in port or fabric parameters with the neighboring device. For example, a port parameter mismatch would occur if a node device were connected to a port configured as an E port. An example of a fabric parameter mismatch would be differing timeout values.
- Yellow box: In Device Manager, a port has been selected.
- Gray box: The port is administratively disabled.
- Black box: An SFP is not present.

Figure 1-1 *Device Manager: Device View*



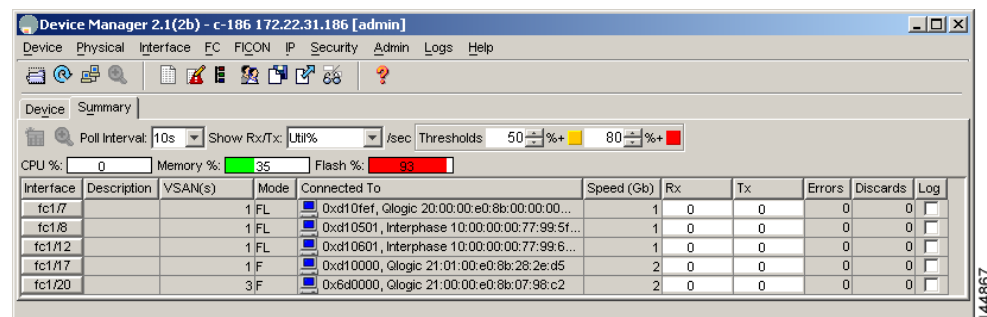
Send documentation comments to mdsfeedback-doc@cisco.com

Device Manager: Summary View

In Device Manager, selecting the Summary View expands the information available for port monitoring. (See [Figure 1-2](#).) The display includes:

- VSAN assignment
- For N ports, the port World Wide Name (pWWN) and Fibre Channel ID (FC ID) of the connected device
- For ISLs, the IP address of the connected switch
- Speed
- Frames transmitted and received
- Percentage utilization for the CPU, dynamic memory, and Flash memory

Figure 1-2 Device Manager: Summary View



Device Manager: Port Selection

To drill down for additional port information, use the Device View or Summary View. Select and double-click any port. The initial display shows administrative settings for Mode, Speed, and Status, plus current operational status, failure cause, and date of the last configuration change.

Additional tabs include:

- Rx BB Credit—Configure and view buffer-to-buffer credits (BB_credits).
- Other—View PortChannel ID, WWN, and maximum transmission unit (MTU), and configure maximum receive buffer size.
- FLOGI—View FC ID, pWWN, nWWN, BB_credits, and class of service for N port connections.
- ELP—View pWWN, nWWN, BB_credits, and supported classes of service for ISLs.
- Trunk Config—View and configure trunk mode and allowed VSANs.
- Trunk Failure—View the failure cause for ISLs.
- Physical—Configure beaconing; view SFP information.
- Capability—View current port capability for hold-down timers, BB credits, maximum receive buffer size.

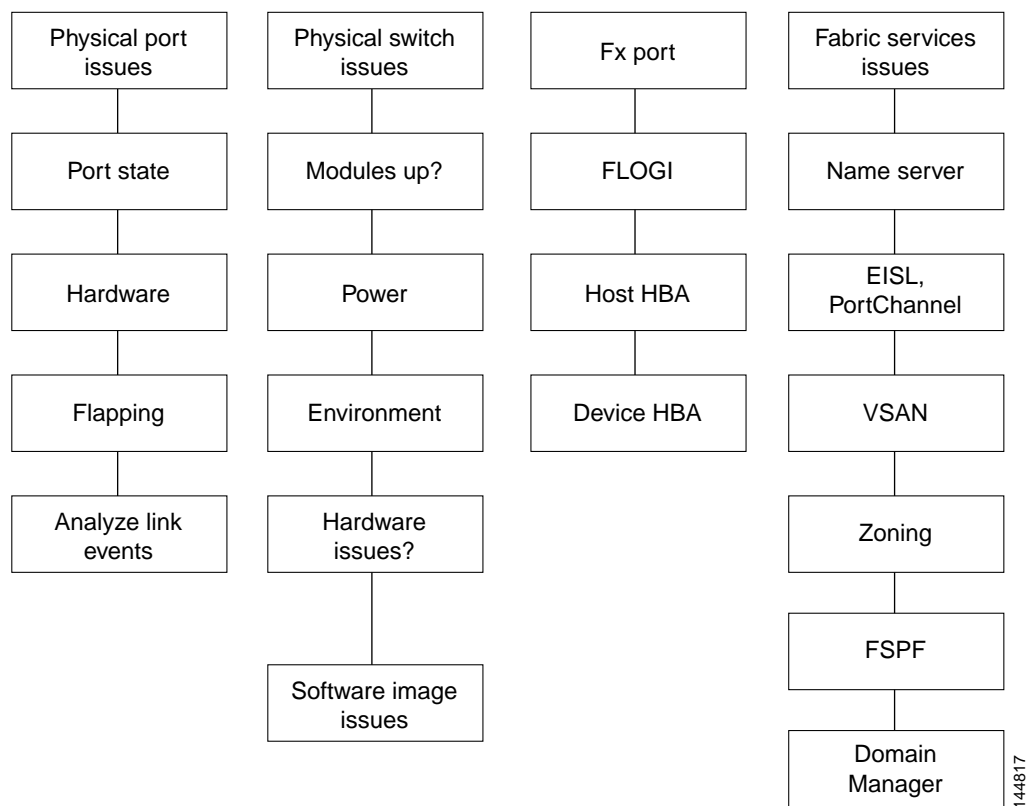
[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

Primary Troubleshooting Flowchart

The flowchart in [Figure 1-3](#) shows the overall troubleshooting process. Begin any troubleshooting investigation by checking one of the following four areas:

- Physical port issues
- Physical switch issues
- Fx port issues
- Fabric services

Figure 1-3 Troubleshooting Process Flowchart



System Messages

The system software sends these syslog (system) messages to the console (and, optionally, to a logging server on another system) during operation. Not all messages indicate a problem with your system. Some messages are purely informational, while others might help diagnose problems with links, internal hardware, or the system software.

This section contains the following topics:

- [System Message Text, page 1-9](#)
- [Syslog Server Implementation, page 1-10](#)

Send documentation comments to mdsfeedback-doc@cisco.com

- [Implementing Syslog with Fabric Manager, page 1-10](#)
- [Implementing Syslog with the CLI, page 1-11](#)

System Message Text

Message-text is a text string that describes the condition. This portion of the message might contain detailed information about the event, including terminal port numbers, network addresses, or addresses that correspond to locations in the system memory address space. Because the information in these variable fields changes from message to message, it is represented here by short strings enclosed in square brackets ([]). A decimal number, for example, is represented as [dec].

```
PORT-3-IF_UNSUPPORTED_TRANSCEIVER: Transceiver for interface [chars] is not supported.
```

Use this string to find the matching system message in the *Cisco MDS 9000 Family System Messages Reference*.

Send documentation comments to mdsfeedback-doc@cisco.com

Each system message is followed by an explanation and recommended action. The action may be as simple as “No action required.” It may involve a fix or a recommendation to contact technical support as shown in the following example:

Error Message PORT-3-IF_UNSUPPORTED_TRANSCEIVER: Transceiver for interface [chars] is not supported.

Explanation Transceiver (SFP) is not from an authorized vendor.

Recommended Action Enter the **show interface transceiver** CLI command or similar Fabric Manager/Device Manager command to determine the transceiver being used. Please contact your customer support representative for a list of authorized transceiver vendors.

Syslog Server Implementation

The syslog facility allows the Cisco MDS 9000 Family platform to send a copy of the message log to a host for more permanent storage. This can be useful if the logs need to be examined over a long period of time or when the Cisco MDS switch is not accessible.

This example will demonstrate how to configure a Cisco MDS switch to utilize the syslog facility on a Solaris platform. Although a Solaris host is being used, syslog configuration on all UNIX and Linux systems is very similar.

Syslog uses the concept of a facility to determine how it should be handled on the syslog server (the Solaris system in this example), and the message severity. Therefore, different message severities can be handled differently by the syslog server. They could be logged to different files or e-mailed to a particular user. Specifying a severity determines that all messages of that level and greater severity (lower number) will be acted upon.



Note

The Cisco MDS messages should be logged to a different file from the standard syslog file so that they cannot be confused with other non-Cisco syslog messages. The logfile should not be located on the / file system, to prevent log messages from filling up the / file system.

Syslog Client: switch1

Syslog Server: 172.22.36.211 (Solaris)

Syslog facility: local1

Syslog severity: notifications (level 5, the default)

File to log MDS messages to: /var/adm/MDS_logs

Implementing Syslog with Fabric Manager

To configure system message logging servers, follow these steps:

- Step 1** In Fabric Manager, choose **Switches > Events > Syslog** and click the **Servers** tab in the Information pane.
In Device Manager, choose **Logs > Syslog > Setup** and click the **Servers** tab in the Syslog dialog box.
- Step 2** Click **Create Row** in Fabric Manager or **Create** in Device Manager to add a new syslog server.
- Step 3** Enter the name or IP address in dotted decimal notation (for example, 192.168.2.12) of the syslog server in the Name or IP Address field.

Send documentation comments to mdsfeedback-doc@cisco.com

- Step 4** Set the message severity threshold by clicking the **MsgSeverity** radio button and set the facility by clicking the **Facility** radio button.
- Step 5** Click **Apply Changes** in Fabric Manager or click **Create** in Device Manager to save and apply your changes.
- Step 6** If CFS is enabled in Fabric Manager for the syslog feature, click **CFS** and commit these changes to propagate the configuration through the fabric.

Device Manager allows you to view event logs on your local PC as well as those on the switch. For a permanent record of all events that occur on the switch, you should store these messages off the switch. To do this the Cisco MDS switch must be configured to send syslog messages to your local PC and a syslog server must be running on that PC to receive those messages. These messages can be categorized into four classes:

- Hardware—Line card or power supply problems
- Link incidents—FICON port condition changes
- Accounting—User change events
- Events—All other events



Note

You should avoid using PCs that have IP addresses randomly assigned to them by DHCP. The switch continues to use the old IP address unless you manually change it; however the Device Manager prompts you if it does detect this situation. UNIX workstations have a built-in syslog server. You must have root access (or run the Cisco syslog server as setuid to root) to stop the built-in syslog daemon and start the Cisco syslog server.

Implementing Syslog with the CLI

To configure a syslog server using the CLI, follow these steps:

- Step 1** Configure the Cisco MDS switch:

```
switch1# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch1(config)# logging server 172.22.36.211 6 facility local1
```

To display the configuration:

```
switch1# show logging server
Logging server: enabled
{172.22.36.211}
server severity: notifications
server facility: local1
```

- Step 2** Configure the syslog server:

- a. Modify `/etc/syslog.conf` to handle `local1` messages. For Solaris, there needs to be at least one tab between the `facility.severity` and the action (`/var/adm/MDS_logs`).

```
#Below is for the MDS 9000 logging
local1.notice /var/adm/MDS_logs
```

- b. Create the log file.

Send documentation comments to mdsfeedback-doc@cisco.com

```
#touch /var/adm/MDS_logs
```

c. Restart syslog.

```
# /etc/init.d/syslog stop
# /etc/init.d/syslog start
syslog service starting.
```

d. Verify syslog started.

```
# ps -ef |grep syslogd
root 23508 1 0 11:01:41 ? 0:00 /usr/sbin/syslogd
```

Step 3 Test the syslog server by creating an event on the Cisco MDS switch . In this case, port fc1/2 was bounced and the following was listed on the syslog server. Notice that the IP address of the switch is listed in brackets.

```
# tail -f /var/adm/MDS_logs
Sep 17 11:07:41 [172.22.36.142.2.2] : 2004 Sep 17 11:17:29 pacific:
%PORT-5-IF_DOWN_INITIALIZING: %$VSAN 1%$ Interface fc1/2 is down (Initializing)
Sep 17 11:07:49 [172.22.36.142.2.2] : 2004 Sep 17 11:17:36 pacific: %PORT-5-IF_UP:
%$VSAN 1%$ Interface fc1/2 is up in mode TE
Sep 17 11:07:51 [172.22.36.142.2.2] : 2004 Sep 17 11:17:39 pacific:
%VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console from pts/0
(dhcp-171-71-49-125.cisco.com)
```

Troubleshooting with Logs

Cisco SAN-OS generates many types of system messages on the switch and sends them to a syslog server. These messages can be viewed using Fabric Manager or the CLI to determine what events may have led up to the current problem condition you are facing.

This section contains the following topics:

- [Viewing Logs with Fabric Manager, page 1-12](#)
- [Viewing Logs with the CLI, page 1-13](#)
- [Viewing the Log from the Supervisor, page 1-13](#)

Viewing Logs with Fabric Manager

Fabric Manager and Device Manager present concise views of the generated system messages and other logged events:

- In Device Manager, click **Logs** to set up and view logs.
- In Fabric Manager, select the **Logs** tab at the bottom of the map pane to view log information.
- Learn to use Threshold Manager to alert you that critical statistics have exceeded a set threshold.

Send documentation comments to mdsfeedback-doc@cisco.com

Viewing Logs with the CLI

The following CLI commands are available to access and view logs on a switch:

```
Musky-9506# show logging ?
console Show console logging configuration
info Show logging configuration
last Show last few lines of logfile
level Show facility logging configuration
logfile Show contents of logfile
module Show module logging configuration
monitor Show monitor logging configuration
nvram Show NVRAM log
server Show server logging configuration
<cr> Carriage Return
```

Example 1-1 shows an example of the **show logging** CLI command output.

Example 1-1 *show logging Command*

```
Musky-9506# show logging server
Logging server: enabled
{10.91.51.204}
server severity: critical
server facility: user
```

Viewing the Log from the Supervisor

You can view system messages from Device Manager if Device Manager is running from the same workstation as the Fabric Manager Server. Choose **Logs > Events > current** to view the system messages on Device Manager. The columns in the events table are sortable. In addition, you can use the Find button to locate text within the table.

You can view switch-resident logs even if you have not set up your local syslog server or your local PC is not in the switch's syslog server list. Because of memory constraints, these logs will wrap when they reach a certain size. The switch syslog has two logs: an NVRAM log that holds a limited number of critical and greater messages and a nonpersistent log that contains notice or greater severity messages. Hardware messages are part of these logs.

Use the **show logging** CLI command to view the logs on the supervisor.

Viewing NVRAM logs

System messages that are priority 0, 1, or 2 are logged into NVRAM on the supervisor module. After a switch reboots, you can display these syslog messages in NVRAM using the **show logging nvram** CLI command. See [Example 1-2](#).

Example 1-2 *Show logging nvram*

```
switch# show logging nvram
2005 Sep 16 13:19:20 172.20.150.82 %PLATFORM-2-PS_OK: Power supply 2 ok (Serial
number )
2005 Sep 16 13:19:20 172.20.150.82 %PLATFORM-2-PS_FANOK: Fan in Power supply 2 ok
2005 Sep 16 13:19:20 172.20.150.82 %PLATFORM-2-FANMOD_FAN_OK: Fan module 1 (Front fan) ok
2005 Sep 16 13:19:20 172.20.150.82 %PLATFORM-2-FANMOD_FAN_OK: Fan module 2 (Rear fan) ok
2005 Sep 16 13:19:20 172.20.150.82 %PLATFORM-2-CHASSIS_CLKMODOK: Chassis clock module A ok
```

Send documentation comments to mdsfeedback-doc@cisco.com

```

2005 Sep 16 13:19:20 172.20.150.82 %PLATFORM-2-CHASSIS_CLKMODOK: Chassis clock module B ok
2005 Sep 16 13:19:20 172.20.150.82 %PLATFORM-2-CHASSIS_CLKSRC: Current chassis clock
source is clock-A
2005 Sep 16 13:19:36 172.20.150.82 %PLATFORM-2-PFM_STDBY_BIOS_STUCK: standby supervisor
bios failed
2005 Sep 16 13:20:19 172.20.150.82 %IMAGE_DNLD-SLOT13-2-IMG_DNLD_STARTED: Module image
download process. Please wait until completion...
2005 Sep 16 13:20:32 172.20.150.82 %IMAGE_DNLD-SLOT13-IMG_DNLD_COMPLETE: Module image
download process. Download successful.
2005 Sep 16 15:44:46 172.20.150.82 %PLATFORM-2-PFM_STDBY_BIOS_STUCK: standby supervisor
bios failed
2005 Sep 16 15:44:53 172.20.150.82 %PLATFORM-2-MOD_ALL_PWRDN_NOXBAR: All modules powered
down due to non-availability of xbar modules
2005 Sep 16 15:45:41 172.20.150.82 %PLATFORM-2-MOD_PWRUP_XBAR: Modules powered up due to
xbar availability
2005 Sep 18 15:12:07 172.20.150.82 %MODULE-2-MOD_FAIL: Initialization of module 14
(serial: JAB092501FC) failed

```

Contacting Customer Support

If you are unable to solve a problem after using the troubleshooting suggestions in this guide, contact a customer service representative for assistance and further instructions. Before you call, have the following information ready to help your service provider assist you as quickly as possible:

- Date you received the switch
- Chassis serial number (located on a label on the right side of the rear panel of the chassis)
- Type of software and release number
- Maintenance agreement or warranty information
- Brief description of the problem
- Brief explanation of the steps you have already taken to isolate and resolve the problem

After you have collected this information, see the [“Obtaining Technical Assistance”](#) section on page xxv.

For more information on steps to take before calling Technical Support, see the [“Before Contacting Technical Support”](#) section on page A-1.