CHAPTER 32

Network Monitoring

The primary purpose of Fabric Manager is to manage the network. In particular, SAN discovery and network monitoring are two of its key network management capabilities.

This chapter contains the following sections:

SAN Discovery and Topology Mapping

Fabric Manager provides extensive SAN discovery, topology mapping, and information viewing capabilities. Fabric Manager collects information on the fabric topology through SNMP queries to the switches connected to it. Fabric Manager recreates a fabric topology, presents it to the user in a customizable map, and provides inventory and configuration information in multiple viewing options.

Device Discovery

Once Fabric Manager is invoked, a SAN discovery process begins. Using information polled from a seed Cisco MDS 9000 Family switch, including Name Server registrations, Fibre Channel Generic Services (FC-GS), Fabric Shortest Path First (FSPF), and SCSI-3, Fabric Manager automatically discovers all devices and interconnects on one or more fabrics. All available switches, host bus adapters (HBAs), and storage devices are discovered. The Cisco MDS 9000 Family switches use Fabric-Device Management Interface (FMDI) to retrieve HBA model, serial number and firmware version, and host operating-system type and version discovery without host agents. Fabric Manager gathers this information through SNMP queries to each switch. The device information discovered includes device names, software revision levels, vendor, ISLs, PortChannels, and VSANs.

Topology Mapping

Fabric Manager is built upon a topology representation of the fabric. Fabric Manager provides an accurate view of multiple fabrics in a single window by displaying topology maps based on device discovery information. The user may modify the topology map icon layout with an easy-to-use, drag-and-drop interface. The topology map visualizes device interconnections, highlights configuration

information such as zones, VSANs, and ISLs exceeding utilization thresholds. The topology map also provides a visual context for launching command-line interface (CLI) sessions, configuring PortChannels, and opening device managers.

Using the Topology Map

The Fabric Manager topology map can be customized to provide a view into the fabric that varies from showing all switches, end devices, and links, to showing only the core switches with single bold lines for any multiple links between switches. Use the icons along the left side of the topology map to control these views or right-click anywhere in the topology map to access the map controls.

You can zoom in or out on the topology map to see an overview of the SAN or focus on an area of importance. You can also open an overview window that shows the entire fabric. From this window, you can right-click and draw a box around the area you want to view in the main topology map view.

Another way to limit the scope of the topology display is to select a fabric or VSAN from the Logical Domains pane. The topology map displays only that fabric or VSAN.

Moving the mouse pointer over a link or switch provides a simple summary of that SAN component, along with a status indication. Right-clicking on the component brings up a pop-up menu. You can view the component in detail or access configuration or test features for that component.

Double-click a link to bring link status and configuration information to the information pane. Double-click a switch to bring up Device Manager for that switch.

Saving a Customized Topology Map Layout

Changes made to the topology map can be saved so that the customized view is available any time you open the Fabric Manager client for that fabric.

To save the customized layout in Fabric Manager, follow these steps:

Step 1 Choose **File > Preferences** to open the Fabric Manager preferences dialog box.

Step 2 Click the **Map** tab and check the **Automatically Save Layout** check box to save any changes to the topology map.

Step 3 Click **Apply** to save this change, or click **Close** to discard any unsaved changes and close the dialog box.

Using Enclosures with Fabric Manager Topology Maps

Because not all devices are capable of responding to FC-GS-3 requests, different ports of a single server or storage subsystem may be displayed as individual end devices on the topology map. See the "Modifying Device Grouping" section on page 3-15 to group these ports into a single enclosure for Fabric Manager.

The Alias->Enclosure button displays in the Information pane for hosts and storage elements. This button acts as a shortcut to naming enclosures. To use this shortcut, you highlight each row in the host or storage table that you want grouped in an enclosure and then click **Alias -> Enclosure**. This automatically sets the enclosure names of each selected row with the first token of the alias.

Mapping Multiple Fabrics

To log into multiple fabrics, the same username and password must be used. The information for both fabrics is displayed, with no need to select a seed switch. To see details of a fabric, click the tab for that fabric at the bottom of the Fabric pane, or double-click the fabric's cloud icon.

When you quit the Fabric Manager client, you can have Fabric Manager Server continuously monitor that fabric. Alternatively, you can use Fabric Manager client to select a fabric to monitor.

To continuously monitor a fabric in Fabric Manager, follow these steps:

Step 1 Choose **Server > Admin**. You see the Server Admin dialog box with a list of fabrics.

Step 2 Check the **Continuously Monitor** check box next to the fabric(s) you want Fabric Manager Server to monitor.

Step 3 Click **Apply**.

The Continuously Monitor feature requires the purchase of the Fabric Manager Server license package. If you have not purchased and installed this package, you see a pop-up window informing you that you are about to enable a demo license for this feature. Click **Yes** to enable the demo license.

Note When you are finished checking out the demo, you can "check in" the feature by clicking the **Check In FM** button as described in the "Fabric Manager Server Licensing" section on page 9-13.

Step 4 Click **Close** to close the Server Admin dialog box.

Inventory Management

The Information pane in Fabric Manager shows inventory, configuration, and status information for all switches, links, and hosts in the fabric. Inventory management includes vendor name and model, and software or firmware versions. Select a fabric or VSAN from the Logical Domains pane, and then select the **Summary** tab in the Information pane to get a count of the number of VSANS, switches, hosts, and storage elements in the fabric. See the "Using Fabric Manager Client" section on page 3-3 for more information on the Fabric Manager user interface.

Using the Inventory Tab from Fabric Manager Web Services

If you have configured Fabric Manager Web Services, you can launch this application and access the Inventory tab to see a summary of the fabrics managed by the Fabric Manager Server. The Inventory tab shows an inventory of the selected SAN, fabric, or switch.

- Summary—Shows all VSANs, switches, and ports in the selected SAN or fabric.
- VSANs— Shows all VSANs in the selected SAN or fabric.
- Switches—Shows all attributes (such as IP address, vendor, and model) for all switches in the selected SAN, fabric, or VSAN.
- Licenses—Shows details about the licenses in use in the fabric.
- Modules—Shows all line cards, fans, and power supplies for all switches in the selected SAN, fabric, or VSAN.

- End Devices—Shows the host and storage ports.
- ISLs—Shows all the Inter-Switch Links for the selected SAN, fabric, or VSAN.
- Zones—Shows all the active zone members (including those in inter-VSAN zones) for the selected SAN, fabric, or VSAN.

See Chapter 5, "Fabric Manager Web Services" for more information on how to configure and use Fabric Manager Web Services.

Configuring System Message Logging

The system message logging software saves messages in a log file or directs the messages to other devices. This feature provides you with the following capabilities:

- Provides logging information for monitoring and troubleshooting.
- Allows you to select the types of captured logging information.
- Allows you to select the destination of the captured logging information.

By default, the switch logs normal but significant system messages to a log file and sends these messages to the system console. You can specify which system messages should be saved based on the type of facility and the severity level. See the "Syslog Server Logging Facilities and Severity Levels" section on page 32-4. Messages are time-stamped to enhance real-time debugging and management.

The switch software saves system messages in a file that can be configured to save up to 4 MB. You can monitor system messages by clicking the **Events** tab on Fabric Manager or by choosing **Logs > Events > Current** on Device Manager. You can also monitor system messages remotely by accessing the switch through Telnet, SSH, or the console port, or by viewing the logs on a syslog server.

Note When the switch first initializes, the network is not connected until initialization completes. Therefore, messages are not redirected to a syslog server for a few seconds.

Syslog Server Logging Facilities and Severity Levels

All syslog messages have a logging facility and a level. The logging facility can be thought of as *where* and the level can be thought of as *what*.

The single syslog daemon (syslogd) sends the information based on the configured facility option. If no facility is specified, local7 is the default outgoing facility.

The outgoing logging facilities are listed in Table 32-1 for both Cisco MDS SAN-OS and Cisco FabricWare.

Table 32-1 Outgoing Logging Facilities

Facility Keyword	Description	Standard or Cisco MDS Specific
auth	Authorization system	Standard
authpriv	Authorization (private) system	Standard
cron	Cron or at facility	Standard
daemon	System daemons	Standard
ftp	File Transfer Protocol	Standard

Table 32-1 Outgoing Logging Facilities (continued)

Facility Keyword	Description	Standard or Cisco MDS Specific
kernel	Kernel	Standard
local0 to local7	Locally defined messages	Standard (local7 is the default)
lpr	Line printer system	Standard
mail	Mail system	Standard
news	USENET news	Standard
syslog	Internal syslog messages	Standard
user	User process	Standard
uucp	UNIX-to-UNIX Copy Program	Standard

Table 32-2 describes some samples of internal facilities supported by the system message logs for Cisco MDS SAN-OS.

Table 32-2 Internal Logging Facilities for Cisco MDS SAN-OS

Facility Keyword	Description	Standard or Cisco MDS Specific
acl	ACL manager	Cisco MDS 9000 Family specific
all	All facilities	Cisco MDS 9000 Family specific
auth	Authorization system	Standard
authpriv	Authorization (private) system	Standard
bootvar	Bootvar	Cisco MDS 9000 Family specific
callhome	Call Home	Cisco MDS 9000 Family specific
cron	Cron or at facility	Standard
daemon	System daemons	Standard
fcc	FCC	Cisco MDS 9000 Family specific
fcdomain	fcdomain	Cisco MDS 9000 Family specific
fcns	Name server	Cisco MDS 9000 Family specific
fcs	FCS	Cisco MDS 9000 Family specific
flogi	FLOGI	Cisco MDS 9000 Family specific
fspf	FSPF	Cisco MDS 9000 Family specific
ftp	File Transfer Protocol	Standard
ipconf	IP configuration	Cisco MDS 9000 Family specific
ipfc	PFC	Cisco MDS 9000 Family specific
kernel	Kernel	Standard
local0 to local7	Locally defined messages	Standard
lpr	Line printer system	Standard
mail	Mail system	Standard
mcast	Multicast	Cisco MDS 9000 Family specific
module	Switching module	Cisco MDS 9000 Family specific

Table 32-2 Internal Logging Facilities for Cisco MDS SAN-OS (continued)

Facility Keyword	Description	Standard or Cisco MDS Specific
news	USENET news	Standard
ntp	NTP	Cisco MDS 9000 Family specific
platform	Platform manager	Cisco MDS 9000 Family specific
port	Port	Cisco MDS 9000 Family specific
port-channel	PortChannel	Cisco MDS 9000 Family specific
qos	QoS	Cisco MDS 9000 Family specific
rdl	RDL	Cisco MDS 9000 Family specific
rib	RIB	Cisco MDS 9000 Family specific
rscn	RSCN	Cisco MDS 9000 Family specific
securityd	Security	Cisco MDS 9000 Family specific
syslog	Internal system messages	Standard
sysmgr	System manager	Cisco MDS 9000 Family specific
tlport	TL port	Cisco MDS 9000 Family specific
user	User process	Standard
uucp	UNIX-to-UNIX Copy Program	Standard
vhbad	Virtual host base adapter daemon	Cisco MDS 9000 Family specific
vni	Virtual network interface	Cisco MDS 9000 Family specific
vrrp_cfg	VRRP configuration	Cisco MDS 9000 Family specific
vrrp_eng	VRRP engine	Cisco MDS 9000 Family specific
vsan	VSAN system messages	Cisco MDS 9000 Family specific
vshd	vshd	Cisco MDS 9000 Family specific
wwn	WWN manager	Cisco MDS 9000 Family specific
xbar	Xbar system messages	Cisco MDS 9000 Family specific
zone	Zone server	Cisco MDS 9000 Family specific

Table 32-3 describes some samples of internal facilities supported by the system message logs for Cisco FabricWare.

Table 32-3 Internal Logging Facilities for Cisco FabricWare

Facility Keyword	Description	Standard or Cisco MDS Specific
all	All facilities	Cisco MDS 9000 Family specific
auth	Authorization system	Standard
fcdomain	fcdomain	Cisco MDS 9000 Family specific
fcns	Name server	Cisco MDS 9000 Family specific
fcs	FCS	Cisco MDS 9000 Family specific
fspf	FSPF	Cisco MDS 9000 Family specific
ipconf	IP configuration	Cisco MDS 9000 Family specific

Table 32-3 Internal Logging Facilities for Cisco FabricWare (continued)

Facility Keyword	Description	Standard or Cisco MDS Specific
module	Switching module	Cisco MDS 9000 Family specific
ntp	NTP	Cisco MDS 9000 Family specific
port	Port	Cisco MDS 9000 Family specific
sysmgr	System manager	Cisco MDS 9000 Family specific
user	User process	Standard
zone	Zone server	Cisco MDS 9000 Family specific

Table 32-4 describes the severity levels supported by the system message logs for both Cisco MDS SAN-OS and Cisco FabricWare.

Table 32-4 Error Message Severity Levels

Level Keyword	Level	Description	System Message Definition
emergency	0	System unusable	LOG_EMERG
alert	1	Immediate action needed	LOG_ALERT
critical	2	Critical conditions	LOG_CRIT
error	3	Error conditions	LOG_ERR
warning	4	Warning conditions	LOG_WARNING
notify	5	Normal but significant condition	LOG_NOTICE
info	6	Informational messages only	LOG_INFO
debug	7	Debugging messages	LOG_DEBUG

Note Refer to the *Cisco MDS 9000 Family System Messages Reference* for details on the error log message format.

Configuring Message Logging

System logging messages are sent to Fabric Manager or Device Manager based on the default (or configured) logging facility and severity values. You can enable logging to the console, terminal sessions, log file, or line cards using Fabric Manager or Device Manager.

When logging is enabled for a console session (default), you can configure the severity levels of messages that appear on the console. The default severity for console logging is critical.

Note Most tabs in the Information pane for features using CFS are dimmed until you click the CFS tab. The CFS tab shows which switches have CFS enabled and shows the master switch for this feature. Once the CFS tab is click, the other tabs in the Information pane that use CFS are activated.

Tip The current critical (default) logging level is maintained if the console baud speed is 9600 baud (default). All attempts to change the console logging level generate an error message. To increase the logging level (above critical), you must change the console baud speed to 38400 baud

Logging messages may be saved to a log file. You can configure the name of this file and restrict its size as required. The default log file name is messages. The file name can have up to 80 characters and the file size ranges from 4096 bytes to 4194304 bytes. The configured log file is saved in the /var/log/external directory. The location of the log file cannot be changed.

By default, logging is enabled at the debug level for all line cards. You can enable or disable logging for each line card at a specified level.

To enable or disable message logging for these features, follow these steps:

Step 1 In Fabric Manager, choose **Switches > Events > Syslog** and click the **Switch Logging** tab in the Information pane.

In Device Manager, choose **Logs > Syslog > Setup** and click the **Switch Logging** tab in the Syslog dialog box.

Step 2 Check the check boxes for where you want message logging to occur.

Step 3 Choose the message severity threshold from the **MsgSeverity** drop-down box for each switch in Fabric Manager, or click the appropriate message severity level radio button in Device Manager.

Step 4 Click **Apply Changes** on Fabric Manager, or **Apply** on Device Manager to save and apply your changes.

Configuring a Syslog Server

You can configure a maximum of three syslog servers. One of these syslog servers should be Fabric Manager if you want to view system messages from the Event tab in Fabric Manager.

To configure syslog 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** on Fabric Manager, or **Create** on 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.

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** on Fabric Manager, or click **Create** on Device Manager to save and apply your changes.

Step 6 If CFS is enabled on 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 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.

Verifying Syslog Servers from Fabric Manager Web Services

To verify the syslog servers remotely from Fabric Manager Web Services, follow these steps:

Step 1 Point your browser at the Fabric Manager Web Services server. See the "Launching and Using Fabric Manager Web Services" section on page 5-7.

Step 2 Choose **Admin > Events** to view the syslog server information for each switch. The columns in the table are sortable.

Viewing Logs from Fabric Manager Web Services

To view system messages remotely from Fabric Manager Web Services, follow these steps:

Step 1 Point your browser at the Fabric Manager Web Services server. See the "Launching and Using Fabric Manager Web Services" section on page 5-7.

Step 2 Choose **Events > Details** to view the system messages. The columns in the events table are sortable. In addition, you can use the Filter button to limit the scope of messages within the table.

Viewing Logs from Device Manager

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. Due to 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.

Health and Event Monitoring

Fabric Manager works with the Cisco MDS 9000 Family switches to show the health and status of the fabric and switches. Information about the fabric and its components is gathered from multiple sources, including Online System Health Management, Call Home, system messages, and SNMP notifications. This information is then made available from multiple menus on Fabric Manager or Device Manager.

Fabric Manager Events Tab

The Fabric Manager Events tab, available from the topology window, displays the events Fabric Manager received from sources within the fabric. These sources include SNMP events, RMON events, system messages, and system health messages. The Events tab shows a table of events, including the event name, the source and time of the event, a severity level, and a description of the event. The table is sortable by any of these column headings.

Event Information in Fabric Manager Web Services Reports

The Fabric Manager web services client displays collections of information gathered by the Performance Manager. This information includes events sent to the Fabric Manager Server from the fabric. To open these reports, choose **Performance Manager > Reports**. This opens the web client in a web browser and displays a summary of all fabrics monitored by the Fabric Manager Server. Choose a fabric and then click the **Events** tab to see a summary or detailed report of the events that have occurred in the selected fabric. The summary view shows how many switches, ISLs, hosts, or storage elements are down on the fabric and how many warnings have been logged for that SAN entity. The detailed view shows a list of all events that have been logged from the fabric and can be filtered by severity, time period, or type.

Events in Device Manager

Device Manager displays the events when you choose **Logs > Events**. Device Manager can display the current list of events or an older list of events that has been stored on the Fabric Manager host. The event table shows details on each event, including time, source, severity, and a brief description of the event.