CHAPTER 1

Getting Started with Cisco Fabric Manager

The Cisco Fabric Manager is a set of two network management tools that supports Secure Simple Network Management Protocol version 3 (SNMPv3) and legacy versions. It provides a graphical user interface (GUI) that displays real-time views of your network fabric, and lets you manage the configuration of Cisco MDS 9000 Family devices and third-party switches. The Cisco Fabric Manager tools are:

- Fabric Manager
- Device Manager

The Fabric Manager displays a map of your network fabric, including Cisco MDS 9000 Family switches, third-party switches, hosts, and storage devices. The Device Manager presents two views of a switch. Device View displays a graphic representation of the switch configuration and provides access to statistics and configuration information for a single switch. Summary View displays a summary of xEPorts (Inter-Switch Links), Fx Ports (fabric ports), and Nx Ports (attached hosts and storage) on the switch, as well as FC and IP neighbor devices.

The Cisco Fabric Manager is an alternative to the command-line interface (CLI) for most switch configuration commands. For information on using the CLI to configure a Cisco MDS 9000 Family switch, refer to the *Cisco 9000 Family Configuration Guide* or the *Cisco 9000 Family Command Reference*.

To learn more about Fabric Manager and Device Manager, read the following topics:

To install Fabric Manager and Device Manager on your system, refer to:

Storage Management Solutions Architecture

Management services required for the storage environment can be divided into five "layers," with the bottom layer being closest to the physical storage network equipment, and the top layer managing the interface between applications and storage resources.

Of these five layers of storage network management, Cisco Fabric Manager provides tools for device (element) management and fabric management. In general, the Device Manager is most useful for device management (a single switch), while Fabric Manager is more efficient for performing fabric management operations involving multiple switches.

Tools for "upper-layer" management tasks can be provided by Cisco or by third-party storage and network management applications. The following summarizes the goals and function of each layer of storage network management:

- Device management provides tools to configure and manage a device within a system or a fabric. You use device management tools to perform tasks on one device at a time, such as initial device configuration, setting and monitoring thresholds, and managing device system images or firmware.
- Fabric management provides a system-oriented view of a fabric and its devices. Fabric management applications provide fabric discovery, fabric monitoring, reporting, and fabric configuration.
- Resource management provides tools for managing resources such as fabric bandwidth, connected paths, disks, I/O operations per second (IOPS), CPU, and memory. You can use Fabric Manager to perform some of these tasks.
- Data management provides tools for ensuring the integrity, availability, and performance of data. Data management services include redundant array of independent disks (RAID) schemes, data replication practices, backup or recovery requirements, and data migration.
- Application management provides tools for managing the overall system consisting of devices, fabric, resources, and data from the application. Application management integrates all these components with the applications that use the storage network.

Managing Cisco MDS 9000 Switches

The Cisco MDS 9000 Family of switches can be accessed and configured in many different ways, and support standard management protocols. The different protocols that are supported in order to access, monitor, and configure the Cisco MDS 9000 Family of switches are described in Table 1-1.

Table 1-1 Supported Management Protocols

Management Protocol	Purpose
Telnet/SSH	Provides remote access to the CLI for a Cisco MDS 9000 switch.
FTP/SFTP/TFTP	Copies configuration and software images between devices.

Table 1-1 Supported Management Protocols

Management Protocol	Purpose
SNMPv1, v2c, and v3	Includes over 50 distinct Management Information Bases (MIBs). Cisco MDS 9000 Family switches support SNMP version 1, 2, and 3 and RMON V1 and V2. RMON provides advanced alarm and event management, including setting thresholds and sending notifications based on changes in device or network behavior. By default, the Cisco Fabric Manager communicates with Cisco MDS 9000 Family switches using SNMPv3, which provides secure authentication using encrypted user names and passwords. SNMPv3 also provides the option to encrypt all management traffic.
HTTP	HTTP is only used for the distribution and installation of the Cisco Fabric Manager software. It is *not* used for communication between the Cisco Fabric Manager and Cisco MDS 9000 Family switches.
ANSI T11 FC-GS3	FC-GS3 in the definition of the management servers defines the Fabric Configuration Server (FCS), which is a standard mechanism to collect information about platforms (end devices) and interconnecting elements (switches) building the fabric. The Cisco MDS 9000 uses the information provided by FCS on top of the information contained in the Name Server database and in the Fibre Channel Shortest Path First (FSPF) topology database to build a detailed topology view, and collect information for all the devices building the fabric.

In-Band Management and Out-of-Band Management

Cisco Fabric Manager requires an out-of-band (Ethernet) connection to at least one Cisco MDS 9000 Family switch. The interface referred to as the out-of-band management connection is a 10/100 Mbps Ethernet interface on the supervisor module, labeled mgmt0. The mgmt0 interface can be connected to a management network to access the switch through IP over Ethernet. You must connect to at least one Cisco MDS 9000 Family switch in the fabric, through its Ethernet management port. You can then use this connection to manage the other switches using in-band (Fibre Channel) connectivity. Otherwise, you need to connect the mgmt0 port on each switch to your Ethernet network.

Each supervisor module has its own Ethernet connection; however, the two Ethernet connections in a redundant supervisor system operate in active or standby mode. The active supervisor module also hosts the active mgmt0 connection. When a failover event occurs to the standby supervisor module, the IP address and media access control (MAC) address of the active Ethernet connection are moved to the standby Ethernet connection.

You can also manage switches on a Fibre Channel network using an in-band IP connection (using IP over Fibre Channel - IPFC). The Cisco MDS 9000 Family supports RFC 2625 IP over Fibre Channel (IPFC), which defines an encapsulation method to transport IP over a Fibre Channel network.

IPFC encapsulates IP packets into Fibre Channel frames so that management information can cross the Fibre Channel network without requiring a dedicated Ethernet connection to each switch. IP addresses are resolved to the Fibre Channel address through Address Resolution Protocol (ARP). This feature allows you to build a completely in-band management solution, in case of availability of servers mounting IP-enabled host bus adapters (HBAs).

Using the Local Console Port and the CLI

The first management interface you use to manage a Cisco MDS 9000 switch is the serial RJ-45 console connection on the supervisor module. This console connection provides access to the CLI and allows you to run the initial setup routine when you first turn on the switch.

You can use the CLI to perform many of the tasks you can perform using the Cisco Fabric Manager. However, complex tasks or tasks involving multiple switches may be easier to perform using the Cisco Fabric Manager. You need to use the CLI for the following tasks:

- Run the initial setup routine to complete the initial configuration required for establishing remote management connectivity
- Run **debug** and **show** commands for diagnostics and troubleshooting
- Write or run automated configuration scripts

For information about using the CLI, refer to the *Cisco 9000 Family Configuration Guide* and the *Cisco 9000 Family Command Reference*.

When you connect to a Cisco MDS 9000 Family switch using the local console and start the switch for the first time, the system displays a setup routine that helps you perform the basic configuration required to manage and connect the switch to end nodes or other switches. The setup routine must be completed before you can connect to the switch or manage it using the Cisco Fabric Manager.

The setup routine prompts for the following configuration values:

- Administrator password—you have the option to create a new login account or overwrite a pre-existing account password.
- SNMPv3 user name and authentication password. SNMP community string.
- Switch name - This is your switch prompt.
- IP address for the switch's management interface - The management interface can be an out-of-band Ethernet interface or an in-band Fibre Channel interface.
- Subnet mask for the switch's management interface.
- The following IP addresses: destination prefix, destination prefix subnet mask, and next hop IP address, if you want to enable IP routing. Also, provide the IP address of the default network. Otherwise, provide an IP address of the default gateway.
- DNS IP address (optional).
- Default domain name (optional).
- SSH service on the switch-if you wish to enable this service, then select the type of SSH key (dsa/rsa/rsa1) and number of key bits (768 to 2048).
- NTP server IP address (optional).

In addition to these settings, each Cisco MDS 9000 Family switch is configured with the following default values:

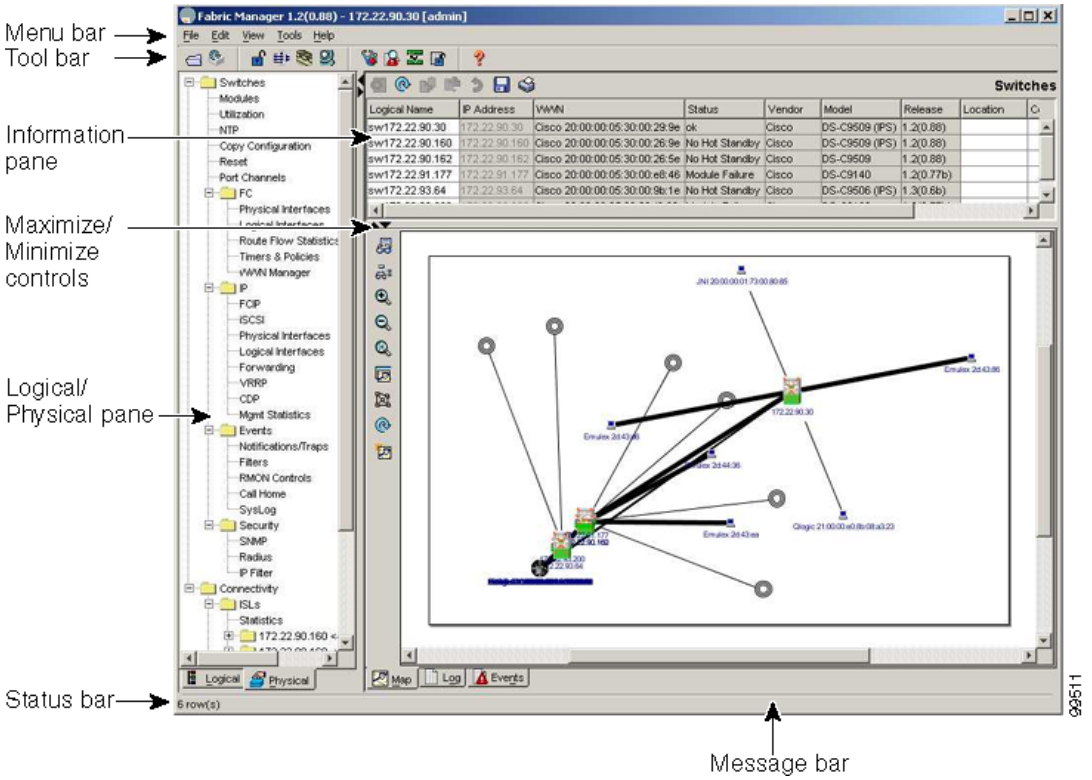
- VSAN membership—All ports are in VSAN 1
- Switch port speed and type—Autosense

Discovering and Viewing the Network Fabric

Cisco Fabric Manager collects information on the fabric topology, sends SNMP queries to the SNMP agent running on the switch to which Fabric Manager is connected. The switch replies after having discovered all devices connected to the fabric by using the information coming from its FSPF technology database and the Name Server database, and collected using the Fabric Configuration Server's request/response mechanisms defined by the FC-GS3 standard. When you start the Fabric Manager, you enter the IP address (or host name) of a "seed" switch.

After you start Fabric Manager and discovery completes, you see the Fabric Manager shown in Figure 1-1. It provides a view of your network fabric, including all discovered switches, hosts, and storage devices.

Figure 1-1 Fabric Manager



You use the Fabric Manager to discover and view your fabric topology and to manage zones and zone sets. It is also convenient to use the Fabric Manager to manage other kinds of configuration involving more than one switch, such as VSANs and Port Channels. The following are some of the main fabric management tasks that you can perform using Fabric Manager:

- Managing zones and zone sets
- Managing VSANs
- Managing Port Channels
- Controlling management access with users and roles

Table 2-2shows the various icons you may see in the Fabric Manager Map pane, and describes what they represent.

Controlling Administrator Access with Users and Roles

Cisco MDS 9000 Family switches support role-based management access whether using the CLI or the Cisco Fabric Manager. This lets you assign specific management privileges to particular roles and then assign one or more users to each role.

Cisco Fabric Manager uses SNMPv3 to establish role-based management access. After completing the setup routine, a single role, user name, and password are established. The role assigned to this user allows the highest level of privileges, which includes creating new users and roles. Use the Cisco Fabric Manager to create roles and users, and to assign passwords as required for secure management access in your network.

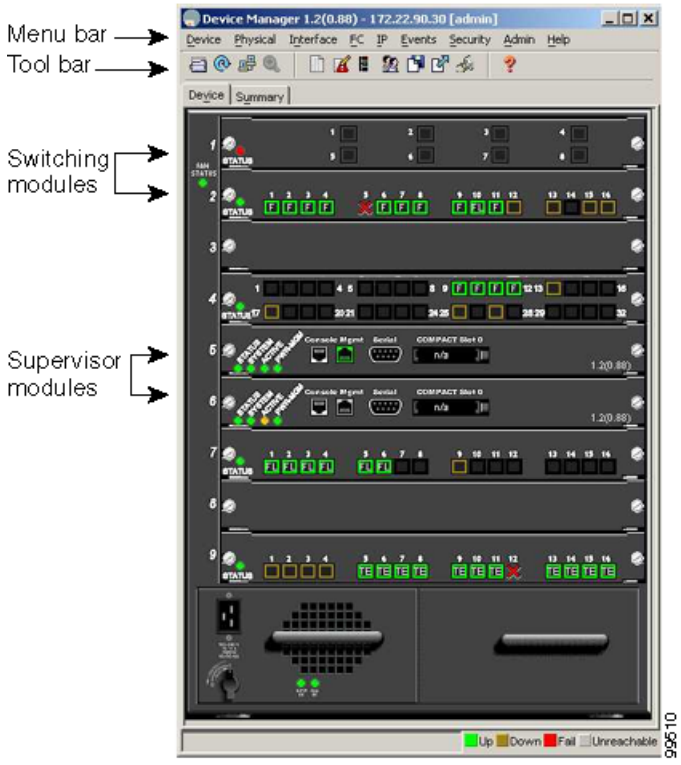
To enable RADIUS authentication of CLI users or to establish SNMP users and roles, see Chapter 5, "Managing Administrator Access."

Performing Device Management

Most tasks that you can perform with Device Manager can also be performed for multiple switches using the Fabric Manager. However, Device Manager may be more convenient to use when you are working with a single switch. Also, the Device Manager provides more detailed information for verifying or troubleshooting device-specific configuration than what is available from the Fabric Manager.

When you start the Device Manager, you see the Device View, shown in Figure 1-2.

Figure 1-2 Device Manager's Device View



The Device View provides a graphic representation of a Cisco MDS 9000 switch, including the installed switching modules, services modules, supervisor modules, and the status of each port within each module. You can use the Device View to perform any switch-level configuration tasks including the following:

- Manage ports, Port Channels, and trunking
- Manage SNMPv3 security access to switches
- Manage CLI security access to switches
- Manage alarms, events, and notifications
- Save and copy configuration files and software images
- View hardware configuration
- View chassis, module, and port status and statistics

Summary View provides a way of monitoring all of the ports on the switch, categorized by operative modes (Fx-Ports and E-Ports).

When you click the Summary tab on the Device Manager window, you see the Summary View, which provides summary information about the interfaces on a single switch.

Accessing Cisco Fabric Manager

Before you can access the Cisco Fabric Manager, you must complete the following tasks:

- A supervisor module must be installed on each switch that you want to manage.
- The supervisor module must be configured with the following values using the setup routine or the CLI:
  - IP address assigned to the mgmt0 interface
  - SNMPv3 user name and password, maintaining the same password for all the switches in the fabric (for information about managing SNMP security with the Fabric Manager, see Chapter 5, “Managing Administrator Access”).

Procedures you need to access the Cisco Fabric Manager include:

- Connecting to a Supervisor Module, page 1-8
- Launching Views, page 1-9
- Troubleshooting Installation and Access, page 1-10

Connecting to a Supervisor Module

The Cisco Fabric Manager software executables reside on each supervisor module of each Cisco MDS 9000 Family switch in your network. The supervisor module provides an HTTP server that responds to browser requests and distributes the software to Windows or UNIX network management stations.

To install the software for the first time, or if you want to update or reinstall the software, access the supervisor module with a web browser. When you click the Install buttons on the web page that is displayed, the software running on your workstation is verified to make sure you are running the most current version of the software. If it is not current, the most recent version is downloaded and installed on your workstation.

To download and install the software on your workstation, follow these steps:

Step 1 Enter the IP address or host name of the supervisor module in the address or location field of your browser.

When you connect to the server for the first time, it checks to see if you have the correct Sun Java Virtual Machine version installed on your workstation. If not, a link is provided to the appropriate web page on Sun Microsystem's website so you can install it.

The supervisor module HTTP server displays the window.

Step 2 Click the link to the Sun Java Virtual Machine software (if required) and install the software.

Using the instructions provided by the Sun Microsystems website to reconnect to the supervisor module by reentering the IP address or host name in the Location or Address field of your browser.

Step 3 Click either installation link (**Install Fabric Manager** or **Install Device Manager**).

You see a prompt asking for permission to install the Java applets on your workstation.

Step 4 Click **Start** to begin installing the software.

The Java Web Start application is automatically downloaded and installed on your workstation. Once the installation is complete, you can start the Cisco Fabric Manager directly from the Fabric Manager icon or the Device Manager icon on your desktop, or from the options on the Windows Start menu.

Launching Views

To launch the Fabric Manager (Fabric View) or Fabric Device Manager (Device View and Summary View), follow these steps:

Step 1 Double-click the **Fabric Manager** icon or the **Device Manager** icon on your desktop or select the option from the Windows Start menu.

You see the login screen.

Step 2 Enter the IP address or device name in the Device Name(s) field, or select an IP address from the list of previously accessed devices, accessible through the drop-down arrow to the right of the Device Name(s) field.

Step 3 Check the SNMPv3 check box to select SNMP version 3.

Note The default authentication digest used for storing user names and passwords is MD5. In case you selected SHA instead, the relative checkbox in the Fabric Manager initial login screen should be checked.

Step 4 Enter a user name and password.

Step 5 Enter the Privacy Password used for encrypting management traffic if the SNMPv3 Privacy option is enabled.

The Privacy option causes all management traffic to be encrypted while, with SNMPv3, user names and passwords are always encrypted.

To enable the Privacy option, see Chapter 5, "Managing Administrator Access."

Step 6 Click **Open**.

You see either the Fabric Manager (Figure 2-1 on page 2-3) or the Device Manager (Figure 2-2 on page 2-17).

Troubleshooting Installation and Access

The following two issues may be useful when troubleshooting Fabric Manager installation and access.

Configuring an OUI

After upgrading from Cisco MDS SAN-OS version 1.0(x) to version 1.1(x) or 1.2(1a), you may notice that Fabric Manager does not display information correctly, or that an error message appears in the Fabric Manager error log. The error message looks similar to the following example:

```
20:00:00:0d:29:2c:a0:80 and 20:01:00:0d:29:2c:a0:81 share the same IP
Address /9.11.203.90 Ignoring 20:01:00:0d:29:2c:a0:81:this may be due
to an unknown MDS OUI
```

This error does not impact the availability or the functionality of the switch and/or fabric. It occurs when two WWNs in different VSANs on the same fabric have the same IP address. To fix this issue, you will need to specify an Organizationally Unique Identifier (OUI) that Fabric Manager can use to differentiate the WWNs.

To specify an OUI, follow these steps:

Step 1 Using a text editor, open the file $HOME/.cisco_mds9000/site_ouis.txt. (On a Windows system, the default pathname for this file is D:\Documents and Settings*username*\.cisco_mds9000\site_ouis.txt.)

If this file is not already present on your system, create it.

Step 2 On a line by itself, add the hexadecimal equivalent of the address shown in the error message. For the address in the example error message above, you would type the value "0x000d29" in your site_ouis.txt file.

Step 3 Save the file and exit.

Step 4 Restart Fabric Manager.

Using a Proxy Server

If your network uses a proxy server for HTTP requests, make sure the Java Web Start Application Manager is properly configured with the IP address of your proxy server. To configure a proxy server in the Java Web Start Application Manager, follow these steps:

Step 1 Double-click the Java Web Start application manager icon on your Windows desktop, or Chose **Program Files > Java Web Start**.

Step 2 Select **File > Preferences** from the Java WebStart Application Manager.

Step 3 Click the **Manual** radio button and enter the IP address of the proxy server in the HTTP Proxy field.

Step 4 Enter the HTTP port number used by your proxy service in the HTTP Port field.

Step 5 Click **OK**.

Note For general problems installing or using the Fabric Manager software, refer to the *Release Notes for the Cisco MDS 9000 Family.*