



CHAPTER 1

Preparing for Installing Cisco DCNM-SAN Client

This chapter describes about the prerequisites for installing DCNM-SAN components and contains the following sections:

- [Information About Cisco MDS 9000 Switch Management and DCNM-SAN, page 1-1](#)
- [Prerequisites for Installing DCNM-SAN, page 1-5](#)

Information About Cisco MDS 9000 Switch Management and DCNM-SAN

The Cisco DCNM-SAN is a set of network management tools that supports Secure Simple Network Management Protocol version 3 (SNMPv3). It provides a graphical user interface (GUI) that displays real-time views of your network fabrics, and lets you manage the configuration of Cisco MDS 9000 Family devices and third-party switches. The Cisco DCNM-SAN provides an alternative to the command-line interface (CLI) for most switch configuration commands.

In addition to complete configuration and status monitoring capabilities for Cisco MDS 9000 switches, DCNM-SAN provides powerful Fibre Channel troubleshooting tools. These in-depth health and configuration analysis capabilities leverage unique MDS 9000 switch capabilities: Fibre Channel Ping and Traceroute.

This section includes the following topics:

- [Cisco MDS 9000 Switch Management, page 1-1](#)
- [Storage Management Solutions Architecture, page 1-2](#)
- [In-Band Management and Out-of-Band Management, page 1-3](#)
- [Cisco DCNM-SAN, page 1-4](#)

Cisco MDS 9000 Switch Management

The Cisco MDS 9000 Family of switches can be accessed and configured in many different ways and supports standard management protocols. [Table 1-1](#) lists the management protocols that DCNM-SAN supports to access, monitor, and configure the Cisco MDS 9000 Family of switches.

Send document comments to dcnm-docfeedback@cisco.com

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, SCP	Copies configuration and software images between devices.
SNMPv1, v2c, and v3	Includes over 80 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 DCNM-SAN 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/HTTPS	Includes HTTP and HTTPS for web browsers to communicate with DCNM-SAN Web Services and for the distribution and installation of the Cisco DCNM-SAN software. It is not used for communication between the Cisco DCNM-SAN Server and Cisco MDS 9000 Family switches.
XML/CIM over HTTP/HTTPS	Includes CIM server support for designing storage area network management applications to run on Cisco SAN-OS and NX-OS.
ANSI T11 FC-GS-3	Provides Fibre Channel-Generic Services (FC-GS-3) in the defining management servers in the Fabric Configuration Server (FCS). DCNM-SAN 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.

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 DCNM-SAN provides tools for device (element) management and fabric management. In general, the Device Manager is most useful for device management (a single switch), while DCNM-SAN is more efficient for performing fabric management operations involving multiple switches.

Send document comments to dcnm-docfeedback@cisco.com

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 view of an entire 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 DCNM-SAN 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. Data management capabilities are provided by third-party tools.
- 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. Application management capabilities are provided by third-party tools.

In-Band Management and Out-of-Band Management

Cisco DCNM-SAN requires an out-of-band (Ethernet) connection to at least one Cisco MDS 9000 Family switch. You need either mgmt0 or IP over Fibre Channel (IPFC) to manage the fabric.

mgmt0

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.

IPFC

You can also manage switches on a Fibre Channel network using an in-band IP connection. The Cisco MDS 9000 Family supports RFC 2625 IP over Fibre Channel, 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. This feature allows you to build a completely in-band management solution.

Send document comments to dcnm-docfeedback@cisco.com

Cisco DCNM-SAN

The Cisco DCNM-SAN provides 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 MDS 9000 Family NX-OS Fundamentals Configuration Guide* or the *Cisco MDS 9020 Switch Configuration Guide* and *Cisco MDS 9000 Family Command Reference Guide*.

In addition to complete configuration and status monitoring capabilities for Cisco MDS 9000 switches, DCNM-SAN provides powerful Fibre Channel troubleshooting tools. These in-depth health and configuration analysis capabilities leverage unique MDS 9000 switch capabilities: Fibre Channel Ping and Traceroute.

The Cisco DCNM-SAN includes these management applications:

- DCNM-SAN (client and server)
- Device Manager
- Performance Manager
- DCNM-SAN Web Server

DCNM-SAN Server

The DCNM-SAN Server component must be started before running DCNM-SAN. On a Windows PC, the DCNM-SAN Server is installed as a service. This service can then be administered using the Windows Services in the Control Panel. DCNM-SAN Server is responsible for discovery of the physical and logical fabric, and for listening for SNMP traps, syslog messages, and Performance Manager threshold events.

DCNM-SAN Client

The DCNM-SAN Client component displays a map of your network fabrics, including Cisco MDS 9000 Family switches, third-party switches, hosts, and storage devices. The DCNM-SAN Client provides multiple menus for accessing the features of the DCNM-SAN Server.

Device Manager

Starting from Cisco MDS NX-OS Release 5.2(1), DCNM-SAN will automatically install Device Manager. The Device Manager provides two views of a single switch:

- Device View displays a graphic representation of the switch configuration and provides access to statistics and configuration information.
- Summary View displays a summary of xE ports (Inter-Switch Links), Fx ports (fabric ports), and Nx ports (attached hosts and storage) on the switch, as well as Fibre Channel and IP neighbor devices. Summary or detailed statistics can be charted, printed, or saved to a file in tab-delimited format.

Performance Manager

Performance Manager presents detailed traffic analysis by capturing data with SNMP. This data is compiled into various graphs and charts that can be viewed with any web browser.

Send document comments to dcnm-docfeedback@cisco.com

DCNM Web Client

The DCNM Web Client allows operators to monitor and obtain reports for MDS events, performance, and inventory from a remote location using a web browser.

Prerequisites for Installing DCNM-SAN

This section includes the following topics:

- [Initial Setup Routine, page 1-5](#)
- [Preparing to Configure the Switch, page 1-5](#)
- [Default Login, page 1-6](#)
- [Setup Options, page 1-6](#)
- [Assigning Setup Information, page 1-7](#)
- [Enter the switch name: switch_name, page 1-9](#)
- [Starting a Switch in the Cisco MDS 9000 Family, page 1-15](#)
- [Accessing the Switch, page 1-16](#)

Initial Setup Routine

The first time you access a switch in the Cisco MDS 9000 Family, it runs a setup program that prompts you for the IP address and other configuration information necessary for the switch to communicate over the supervisor module Ethernet interface. This information is required to configure and manage the switch. The IP address can only be configured from the CLI. All Cisco MDS 9000 Family switches have the network administrator as a default user (admin). You cannot change the default user at any time. You must explicitly configure a strong password for any switch in the Cisco MDS 9000 Family. The setup scenario differs based on the subnet to which you are adding the new switch:

- Out-of-band management—This feature provides a connection to the network through a supervisor module front panel Ethernet port.
- In-band management—This feature provides IP over Fibre Channel (IPFC) to manage the switches. The in-band management feature is transparent to the network management system (NMS).

The first time that you access a switch in the Cisco MDS 9000 Family using the CLI, it runs a setup program that prompts you for the IP address and other configuration information necessary for the switch to communicate over the supervisor module Ethernet interface. This information is required to configure and manage the switch.



Note

The IP address can only be configured from the CLI. When you power up the switch for the first time, assign the IP address. After you perform this step, the Cisco MDS 9000 Family DCNM-SAN can reach the switch through the management port.

Preparing to Configure the Switch

Before you configure a switch in the Cisco MDS 9000 Family for the first time, you need the following information:

Send document comments to dcnm-docfeedback@cisco.com

- Administrator password, including:
 - Creating a password for the administrator (required).
 - Creating an additional login account and password (optional).
- IP address for the switch management interface—The management interface can be an out-of-band Ethernet interface or an in-band Fibre Channel interface (recommended).
- Subnet mask for the switch's management interface (optional).
- IP addresses, including:
 - 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 (optional).
 - Otherwise, provide an IP address of the default gateway (optional).
- SSH service on the switch—To enable this optional service, select the type of SSH key (dsa/rsa/rsa1) and number of key bits (768 to 2048).
- DNS IP address (optional).
- Default domain name (optional).
- NTP server IP address (optional).
- SNMP community string (optional).
- Switch name—This is your switch prompt (optional).



Note

Be sure to configure the IP route, the IP default network address, and the IP default gateway address to enable SNMP access. If IP routing is enabled, the switch uses the IP route and the default network IP address. If IP routing is disabled, the switch uses the default gateway IP address.



Note

You should verify that the DCNM-SAN Server hostname entry exists on the DNS server, unless the DCNM-SAN Server is configured to bind to a specific interface during installation.

Default Login

All Cisco MDS 9000 Family switches have the network administrator as a default user (admin). You cannot change the default user at any time (see the *Cisco DCNM for SAN Security Configuration Guide*).

You have an option to enforce secure password for any switch in the Cisco MDS 9000 Family. If a password is trivial (short, easy-to-decipher), your password configuration is rejected. Be sure to configure a secure password (see the *Cisco DCNM for SAN Security Configuration Guide*). If you configure and subsequently forget this new password, you have the option to recover this password (see the *Cisco DCNM for SAN Security Configuration Guide*).

Setup Options

The setup scenario differs based on the subnet to which you are adding the new switch. You must configure a Cisco MDS 9000 Family switch with an IP address to enable management connections from outside of the switch.

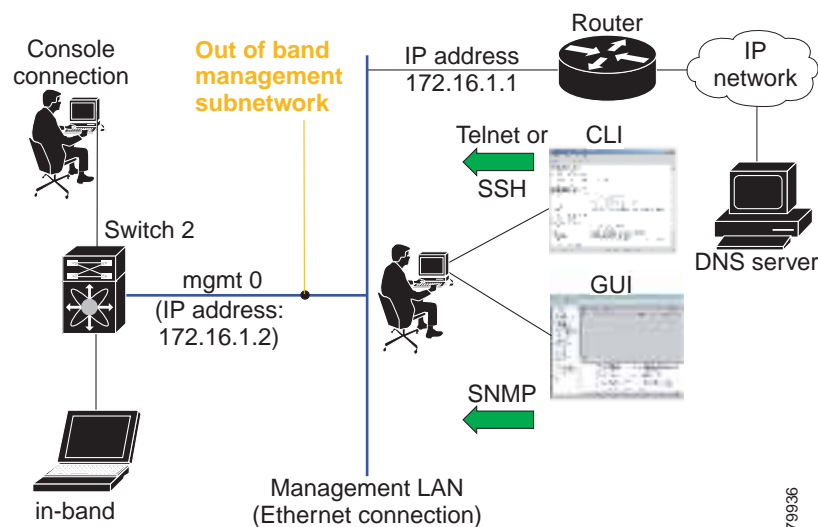
Send document comments to dcnm-docfeedback@cisco.com

**Note**

Some concepts such as out-of-band management and in-band management are briefly explained here. These concepts are explained in more detail in subsequent chapters.

- Out-of-band management—This feature provides a connection to the network through a supervisor module front panel Ethernet port (see [Figure 1-1](#)).
- In-band management—This feature provides IP over Fibre Channel (IPFC) to manage the switches. The in-band management feature is transparent to the network management system (NMS). Instead of conventional Ethernet physical media, switches in the Cisco MDS 9000 Family use IPFC as the transport mechanism. see *Cisco DCNM for SAN IP Services Configuration Guide*.

Figure 1-1 Management Access to Switches



79936

Assigning Setup Information

This section describes how to initially configure the switch for both out-of-band and in-band management.

**Note**

Press **Ctrl-C** at any prompt to skip the remaining configuration options and proceed with what is configured until that point. Entering a new password for the administrator is a requirement and cannot be skipped.

Send document comments to dcnm-docfeedback@cisco.com

**Tip**

If you do not wish to answer a previously configured question, or if you wish to skip answers to any questions, press **Enter**. If a default answer is not available (for example, switch name), the switch uses what was previously configured and skips to the next question.

Configuring Out-of-Band Management

**Note**

You can configure both in-band and out-of-band configuration together by entering **Yes** in both [Step 11c](#) and [Step 11d](#) in the following procedure.

To configure the switch for first time out-of-band access, follow these steps:

Step 1 Power on the switch. Switches in the Cisco MDS 9000 Family boot automatically.

Do you want to enforce secure password standard (Yes/No)?

Step 2 Enter **Yes** to enforce secure password.

a. Enter the administrator password

Enter the password for admin: **2008asdf*1kjh17**

b. Confirm the administrator password.

Confirm the password for admin: **2008asdf*1kjh17**

**Tip**

If a password is trivial (short, easy to decipher), your password configuration is rejected. Be sure to configure a secure password as shown in the sample configuration. Passwords are case-sensitive. You must explicitly configure a password that meets the requirements listed in the *Cisco DCNM for SAN Security Configuration Guide*.

Step 3 Enter **yes** to enter the setup mode.

**Note**

This setup utility will guide you through the basic configuration of the system. Setup configures only enough connectivity for management of the system.

Please register Cisco MDS 9000 Family devices promptly with your supplier. Failure to register may affect response times for initial service calls. MDS devices must be registered to receive entitled support services.

Press Enter anytime you want to skip any dialog. Use ctrl-c at anytime to skip away remaining dialogs.

Would you like to enter the basic configuration dialog (yes/no): **yes**

The setup utility guides you through the basic configuration process. Press **Ctrl-C** at any prompt to end the configuration process.

Step 4 Enter the new password for the administrator (admin is the default).

Enter the password for admin: **admin**

Step 5 Enter **yes** (no is the default) to create additional accounts.

Send document comments to dcnm-docfeedback@cisco.com

Create another login account (yes/no) [n]: **yes**

While configuring your initial setup, you can create an additional user account (in the network-admin role) besides the administrator's account. See the *Cisco DCNM for SAN Security Configuration Guide* for information on default roles and permissions.



Note User login IDs must contain non-numeric characters.

- a. Enter the user login ID [administrator].

Enter the user login ID: *user_name*

- b. Enter the user password.

Enter the password for user_name: *user-password*

- c. Confirm the user password for

Confirm the password for user_name: *user-password*

- Step 6** Enter **yes** (no is the default) to create an SNMPv3 account.

Configure read-only SNMP community string (yes/no) [n]: **yes**

- a. Enter the user name (admin is the default).

SNMPv3 user name [admin]: **admin**

- b. Enter the SNMPv3 password (minimum of eight characters). The default is **admin123**.

SNMPv3 user authentication password: *admin_pass*

- Step 7** Enter **yes** (no is the default) to configure the read-only or read-write SNMP community string.

Configure read-write SNMP community string (yes/no) [n]: **yes**

- a. Enter the SNMP community string.

SNMP community string: *snmp_community*

- Step 8** Enter a name for the switch.

Enter the switch name: *switch_name*

- Step 9** Enter **yes** (yes is the default) to configure out-of-band management.

Continue with Out-of-band (mgmt0) management configuration? [yes/no]: **yes**

- a. Enter the mgmt0 IP address.

Mgmt0 IPv4 address: *ip_address*

- b. Enter the mgmt0 subnet mask.

Mgmt0 IPv4 netmask: *subnet_mask*

- Step 10** Enter **yes** (yes is the default) to configure the default gateway (recommended).

Configure the default-gateway: (yes/no) [y]: **yes**

- a. Enter the default gateway IP address.

IPv4 address of the default gateway: *default_gateway*

Send document comments to dcnm-docfeedback@cisco.com

- Step 11** Enter **yes** (**no** is the default) to configure advanced IP options such as in-band management, static routes, default network, DNS, and domain name.

Configure Advanced IP options (yes/no)? [n]: **yes**

- a. Enter **no** (no is the default) at the in-band management configuration prompt.

Continue with in-band (VSAN1) management configuration? (yes/no) [no]: **no**

- b. Enter **yes** (no is the default) to enable IP routing capabilities.

Enable the ip routing? (yes/no) [n]: **yes**

- c. Enter **yes** (no is the default) to configure a static route (recommended).

Configure static route: (yes/no) [n]: **yes**

Enter the destination prefix.

Destination prefix: *dest_prefix*

Type the destination prefix mask.

Destination prefix mask: *dest_mask*

Type the next hop IP address.

Next hop ip address: *next_hop_address*



Note

Be sure to configure the IP route, the default network IP address, and the default gateway IP address to enable SNMP access. If IP routing is enabled, the switch uses the IP route and the default network IP address. If IP routing is disabled, the switch uses the default gateway IP address.

- d. Enter **yes** (no is the default) to configure the default network (recommended).

Configure the default network: (yes/no) [n]: **yes**

Enter the default network IP address.



Note

The default network IP address is the destination prefix provided in [Step 11c](#).

Default network IP address [dest_prefix]: *dest_prefix*

- e. Enter **yes** (no is the default) to configure the DNS IP address.

Configure the DNS IPv4 address? (yes/no) [n]: **yes**

Enter the DNS IP address.

DNS IPv4 address: *name_server*

- f. Enter **yes** (default is no) to configure the default domain name.

Configure the default domain name? (yes/no) [n]: **yes**

Enter the default domain name.

Default domain name: *domain_name*

- Step 12** Enter **yes** (no is the default) to enable Telnet service.

Send document comments to dcnm-docfeedback@cisco.com

Enable the telnet server? (yes/no) [n]: **yes**

Step 13 Enter **yes** (no is the default) to enable the SSH service.

Enabled SSH server? (yes/no) [n]: **yes**

Step 14 Enter the SSH key type.

Type the SSH key you would like to generate (dsa/rsa)? **dsa**

Step 15 Enter the number of key bits within the specified range.

Enter the number of key bits? (768 to 2048): **768**

Step 16 Enter **yes** (no is the default) to configure the NTP server.

Configure NTP server? (yes/no) [n]: **yes**

Configure clock? (yes/no) [n] :**yes**

Configure clock? (yes/no) [n] :**yes**

Configure timezone? (yes/no) [n] :**yes**

Configure summertime? (yes/no) [n] :**yes**

Configure the ntp server? (yes/no) [n] : **yes**

a. Enter the NTP server IP address.

NTP server IP address: *ntp_server_IP_address*

Step 17 Enter **noshut** (shut is the default) to configure the default switch port interface to the shut state.

Configure default switchport interface state (shut/noshut) [shut]: **noshut**

Step 18 Enter **on** (on is the default) to configure the switch port trunk mode.

Configure default switchport trunk mode (on/off/auto) [on]: **on**

Step 19 Enter **no** (no is the default) to configure switchport port mode F.

Configure default switchport port mode F (yes/no) [n] : **no**

Step 20 Enter **permit** (deny is the default) to deny a default zone policy configuration.

Configure default zone policy (permit/deny) [deny]: **permit**

Permits traffic flow to all members of the default zone.

Step 21 Enter **yes** (no is the default) to disable a full zone set distribution (see the *Cisco DCNM for SAN Fabric Configuration Guide*). Disables the switch-wide default for the full zone set distribution feature.

Enable full zoneset distribution (yes/no) [n]: **yes**

You see the new configuration. Review and edit the configuration that you have just entered.

Step 22 Enter **no** (no is the default) if you are satisfied with the configuration.

The following configuration will be applied:

```
username admin password admin_pass role network-admin
username user_name password user_pass role network-admin
snmp-server community snmp_community ro
switchname switch
interface mgmt0
    ip address ip_address subnet_mask
    no shutdown
ip routing
ip route dest_prefix dest_mask dest_address
ip default-network dest_prefix
ip default-gateway default_gateway
ip name-server name_server
```

Send document comments to dcnm-docfeedback@cisco.com

```
ip domain-name domain_name
telnet server enable
ssh key dsa 768 force
ssh server enable
ntp server ipaddr ntp_server
system default switchport shutdown
system default switchport trunk mode on
system default port-channel auto-create
zone default-zone permit vsan 1-4093
zoneset distribute full vsan 1-4093
```

Would you like to edit the configuration? (yes/no) [n]: **no**

Step 23 Enter **yes** (yes is default) to use and save this configuration:

Use this configuration and save it? (yes/no) [y]: **yes**



Caution

If you do not save the configuration at this point, none of your changes are updated the next time the switch is rebooted. Type **yes** to save the new configuration. This ensures that the kickstart and system images are also automatically configured.

Configuring In-Band Management

The in-band management logical interface is VSAN 1. This management interface uses the Fibre Channel infrastructure to transport IP traffic. An interface for VSAN 1 is created on every switch in the fabric. Each switch should have its VSAN 1 interface configured with an IP address in the same subnetwork. A default route that points to the switch providing access to the IP network should be configured on every switch in the Fibre Channel fabric (see *Cisco Fabric Manager Fabric Configuration Guide*)



Note

You can configure both in-band and out-of-band configuration together by entering **Yes** in both [Step 9c](#) and [Step 9d](#) in the following procedure.

To configure a switch for first time in-band access, follow these steps:

Step 1 Power on the switch. Switches in the Cisco MDS 9000 Family boot automatically.

Step 2 Enter the new password for the administrator.

Enter the password for admin: **2004asdf*1kjh18**



Tip

If a password is trivial (short, easy-to-decipher), your password configuration is rejected. Be sure to configure a strong password as shown in the sample configuration. Passwords are case-sensitive. You must explicitly configure a password that meets the requirements listed in the *User Accounts* section in *Cisco DCNM for SAN Security Configuration Guide*.

Step 3 Enter **yes** to enter the setup mode.

This setup utility will guide you through the basic configuration of the system. Setup configures only enough connectivity for management of the system.

Send document comments to dcnm-docfeedback@cisco.com

Please register Cisco MDS 9000 Family devices promptly with your supplier. Failure to register may affect response times for initial service calls. MDS devices must be registered to receive entitled support services.

Press Enter incase you want to skip any dialog. Use ctrl-c at anytime to skip away remaining dialogs.

Would you like to enter the basic configuration dialog (yes/no): **yes**

The setup utility guides you through the basic configuration process. Press **Ctrl-C** at any prompt to end the configuration process.

Step 4 Enter **no** (no is the default) if you do not wish to create additional accounts.

Create another login account (yes/no) [no]: **no**

Step 5 Configure the read-only or read-write SNMP community string.

a. Enter **no** (no is the default) to avoid configuring the read-only SNMP community string.

Configure read-only SNMP community string (yes/no) [n]: **no**

Step 6 Enter a name for the switch.



Note The switch name is limited to 32 alphanumeric characters. The default is **switch**.

Enter the switch name: *switch_name*

Step 7 Enter **no** (yes is the default) at the configuration prompt to configure out-of-band management.

Continue with Out-of-band (mgmt0) management configuration? [yes/no]: **no**

Step 8 Enter **yes** (yes is the default) to configure the default gateway.

Configure the default-gateway: (yes/no) [y]: **yes**

a. Enter the default gateway IP address.

IP address of the default gateway: *default_gateway*

Step 9 Enter **yes** (no is the default) to configure advanced IP options such as in-band management, static routes, default network, DNS, and domain name.

Configure Advanced IP options (yes/no)? [n]: **yes**

a. Enter **yes** (no is the default) at the in-band management configuration prompt.

Continue with in-band (VSAN1) management configuration? (yes/no) [no]: **yes**

Enter the VSAN 1 IP address.

VSAN1 IP address: *ip_address*

Enter the subnet mask.

VSAN1 IP net mask: *subnet_mask*

b. Enter **no** (yes is the default) to enable IP routing capabilities.

Enable ip routing capabilities? (yes/no) [y]: **no**

c. Enter **no** (yes is the default) to configure a static route.

Configure static route: (yes/no) [y]: **no**

Send document comments to dcnm-docfeedback@cisco.com

- d. Enter **no** (yes is the default) to configure the default network.

Configure the default-network: (yes/no) [y]: **no**

- e. Enter **no** (yes is the default) to configure the DNS IP address.

Configure the DNS IP address? (yes/no) [y]: **no**

- f. Enter **no** (no is the default) to skip the default domain name configuration.

Configure the default domain name? (yes/no) [n]: **no**

- Step 10** Enter **no** (yes is the default) to disable Telnet service.

Enable the telnet service? (yes/no) [y]: **no**

- Step 11** Enter **yes** (no is the default) to enable the SSH service.

Enabled SSH service? (yes/no) [n]: **yes**

- Step 12** Enter the SSH key type (see the *Cisco DCNM for SAN Security Configuration Guide*) that you would like to generate.

Type the SSH key you would like to generate (dsa/rsa/rsal)? **rsa**

- Step 13** Enter the number of key bits within the specified range.

Enter the number of key bits? (768 to 1024): **1024**

- Step 14** Enter **no** (no is the default) to configure the NTP server.

Configure NTP server? (yes/no) [n]: **no**

- Step 15** Enter **shut** (shut is the default) to configure the default switch port interface to the shut state.

Configure default switchport interface state (shut/noshut) [shut]: **shut**



Note The management Ethernet interface is not shut down at this point—only the Fibre Channel, iSCSI, FCIP, and Gigabit Ethernet interfaces are shut down.

- Step 16** Enter **auto** (off is the default) to configure the switch port trunk mode.

Configure default switchport trunk mode (on/off/auto) [off]: **auto**

- Step 17** Enter **deny** (deny is the default) to deny a default zone policy configuration.

Configure default zone policy (permit/deny) [deny]: **deny**

Denies traffic flow to all members of the default zone.

- Step 18** Enter **no** (no is the default) to disable a full zone set distribution.

Enable full zoneset distribution (yes/no) [n]: **no**

Disables the switch-wide default for the full zone set distribution feature.

You see the new configuration. Review and edit the configuration that you have just entered.

- Step 19** Enter **no** (no is the default) if you are satisfied with the configuration.

The following configuration will be applied:

```
username admin password admin_pass role network-admin
snmp-server community snmp_community rw
switchname switch
interface vsan1
ip address ip_address subnet_mask
```

Send document comments to dcnm-docfeedback@cisco.com

```
no shutdown
ip default-gateway default_gateway
no telnet server enable
ssh key rsa 1024 force
ssh server enable
no system default switchport shutdown
system default switchport trunk mode auto
no zone default-zone permit vsan 1-4093
no zoneset distribute full vsan 1-4093
```

Would you like to edit the configuration? (yes/no) [n]: **no**

Step 20 Enter **yes** (yes is default) to use and save this configuration.

Use this configuration and save it? (yes/no) [y]: **yes**



Caution

If you do not save the configuration at this point, none of your changes are updated the next time the switch is rebooted. Type **yes** to save the new configuration. This ensures that the kickstart and system images are also automatically configured.

Using the setup Command

To make changes to the initial configuration at a later time, you can issue the **setup** command in EXEC mode.

```
switch# setup
---- Basic System Configuration Dialog ----
This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.
*Note: setup always assumes a predefined defaults irrespective
of the current system configuration when invoked from CLI.

Press Enter incase you want to skip any dialog. Use ctrl-c at anytime
to skip away remaining dialogs.
```

Would you like to enter the basic configuration dialog (yes/no): **yes**

The setup utility guides you through the basic configuration process.

Starting a Switch in the Cisco MDS 9000 Family

The following procedure is a review of the tasks you should have completed during hardware installation, including starting up the switch. These tasks must be completed before you can configure the switch.



Note

You must use the CLI for initial switch start up.

Before you can configure a switch, follow these steps:

Step 1 Verify the following physical connections for the new Cisco MDS 9000 Family switch:

Send document comments to dcnm-docfeedback@cisco.com

- The console port is physically connected to a computer terminal (or terminal server).
- The management 10/100 Ethernet port (mgmt0) is connected to an external hub, switch, or router.

Refer to the *Cisco MDS 9000 Family Hardware Installation Guide* (for the required product) for more information.



Tip

Save the host ID information for future use (for example, to enable licensed features). The host ID information is provided in the Proof of Purchase document that accompanies the switch.

- Step 2** Verify that the default console port parameters are identical to those of the computer terminal (or terminal server) attached to the switch console port:
- 9600 baud
 - 8 data bits
 - 1 stop bit
 - No parity
- Step 3** Power on the switch. The switch boots automatically and the switch# prompt appears in your terminal window.

Accessing the Switch

After initial configuration, you can access the switch in one of the three ways:

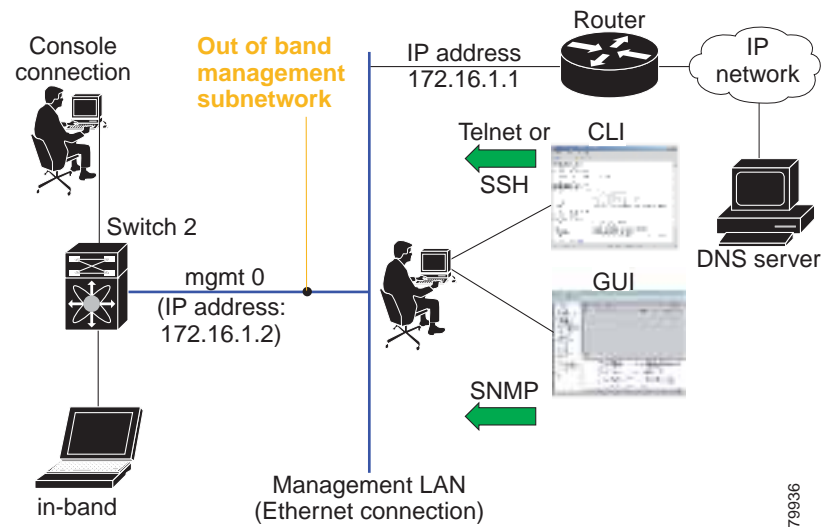
- Serial console access—You can use a serial port connection to access the CLI.
- In-band IP (IPFC) access—You can use Telnet or SSH to access a switch in the Cisco MDS 9000 Family or use SNMP to connect to a Cisco MDS 9000 DCNM-SAN application.
- Out-of-band (10/100BASE-T Ethernet) access—You can use Telnet or SSH to access a switch in the Cisco MDS 9000 Family or use SNMP to connect to a Cisco MDS 9000 DCNM-SAN application.

After initial configuration, you can access the switch in one of three ways (see [Figure 1-2](#)):

- Serial console access—You can use a serial port connection to access the CLI.
- In-band IP (IPFC) access—You can use Telnet or SSH to access a switch in the Cisco MDS 9000 Family or use Cisco MDS 9000 DCNM-SAN to access the switch.
- Out-of-band (10/100BASE-T Ethernet) access—You can use Telnet or SSH to access a switch in the Cisco MDS 9000 Family or use Cisco MDS 9000 DCNM-SAN to access the switch.

Send document comments to dcnm-docfeedback@cisco.com

Figure 1-2 Switch Access Options



79936

Where Do You Go Next?

After reviewing the default configuration, you can change it or perform other configuration or management tasks. The initial setup can only be performed at the CLI. However, you can continue to configure other software features, or access the switch after initial configuration by using either the CLI or the Device Manager and DCNM-SAN applications.

Send document comments to dcnm-docfeedback@cisco.com