CHAPTER 12

Initial Configuration

Most of the initial switch configuration procedures can only be performed using the CLI. Refer to the *Cisco MDS 9000 Family CLI Configuration Guide* for this information. This chapter includes the following sections:

Note The Cisco Fabric Switch for IBM BladeCenter does not use admin as the default user. Rather, the default user is USERID because there is no console access to the switch. You cannot delete the user USERID on this switch. The password for this default user is PASSW0RD, where the "0" is a zero. You can change this password; however, a write erase operation restores the default password. There is no initial setup menu.

Also note that you should not bring up the loader> prompt; the only way to fix this condition is to RMA the switch.

The following commands are not allowed on the Cisco Fabric Switch for IBM BladeCenter: **write erase boot** and **init system**; nor can you boot variables manually.

(see the "Overwriting a Generated Key-Pair" section on page 32-17)Assigning a Switch Name

Each switch in the fabric requires a unique name. You can assign names to easily identify the switch by its physical location, its SAN association, or the organization to which it is deployed. The assigned name is displayed in the command-line prompt. The switch name is limited to 20 alphanumeric characters.

To change the name of a switch using Fabric Manager, follow these steps:

Step 1 Expand **SAN** in the Logical Domains pane, select a fabric or a VSAN from the Logical Domains pane.

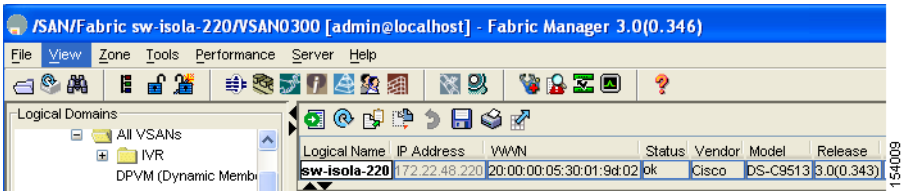
Step 2 Expand **Switches** in the Physical Attributes pane.

You see a list of switches in the Information pane.

Step 3 Double-click the Logical Name of the switch you want to change in the Information pane.

You see the name highlighted with a blinking cursor next to it.

Figure 12-1 Changing the Logical Name of a Switch



Step 4 Type the new name of the switch (see Figure 12-1).

Step 5 Click the **Apply Changes** icon.

Step 6 Right-click the Fabric pane map and choose **Refresh** to see your changes.

Verifying the Module Status

Before you begin configuring the switch, you need to ensure that the modules in the chassis are functioning as designed.

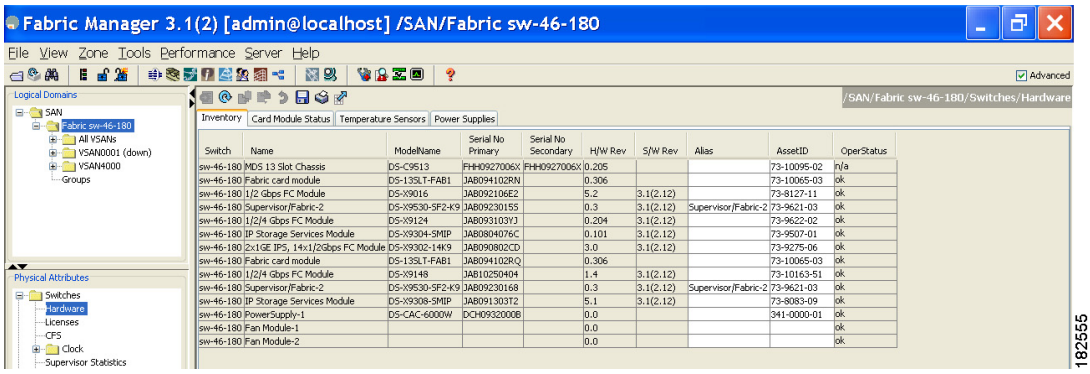
To verify the status of a module at any time, follow these steps:

Step 1 Expand **SAN** in the Logical Domains pane, then select a fabric or a VSAN from the Logical Domains pane.

Step 2 Expand **Switches** and choose **Hardware** in the Physical Attributes pane.

You see the contents of the **Inventory** tab in the Information pane shown in Figure 12-2.

Figure 12-2 Inventory of a Selected Module



Step 3 Click the **Card Module Status** tab.

You see the status in the Oper Status column of each module in each switch of the SAN, fabric, or VSAN you selected.

If the status is OK or active, you can continue with your configuration (see Chapter 1, "Managing Modules").

Configuring Date, Time, and Time Zone

Switches in the Cisco MDS 9000 Family use Universal Coordinated Time (UTC), which is the same as Greenwich Mean Time (GMT).

To change the default time on the switch with Fabric Manager, follow these steps:

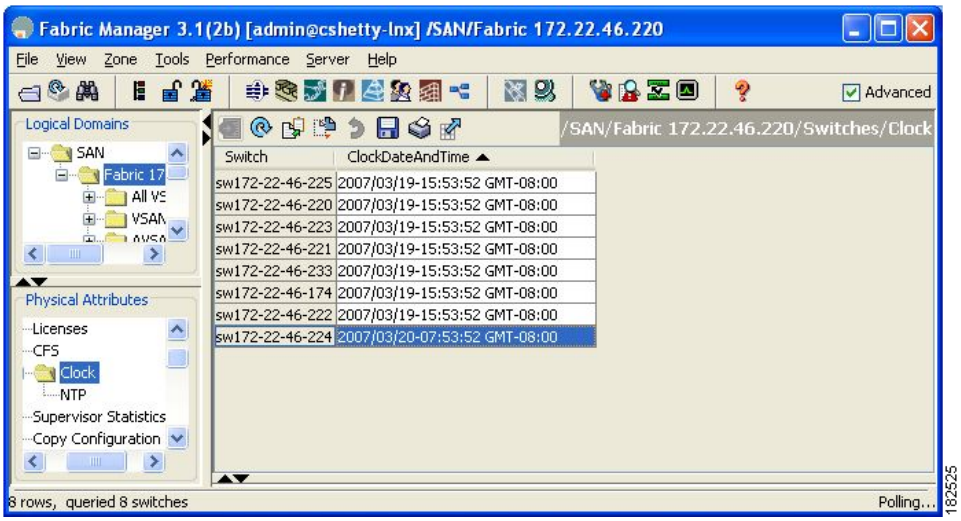
Step 1 Expand **SAN**, then select a fabric or a VSAN in the Logical Domains pane.

You see a list of switches in the Information pane.

Step 2 Expand **Switches and select Clock** in the Physical Attributes pane.

You see the clock information in the Information pane shown in Figure 12-3.

Figure 12-3 Clock Date and Time for Selected Switch



Step 3 Double-click the time in the ClockDateAndTime field for the switch to change.

Step 4 Enter the date, time, and time zone in the format *YYYY/MM/DD-hh:mm:ss* ZONE,

Where:

- *YYYY* is the year (2002)
- *MM* is the month (08)
- *DD* is the date (23)
- *hh* represents hours in military format (15 for 3 p.m.)
- *mm* is minutes (58)
- *ss* is seconds (09)

- ZONE is GMT + or - number of hours

Note If you do not enter a time zone, GMT is used as the default.

Step 5 Click the **Apply Changes** icon.

Note The date and **time** changes are saved across system resets.

Note CFS does not support daylight savings time because a single fabric can span multiple time zones; every switch must be configured individually.

If you want to configure daylight savings time on multiple switches simultaneously, see the RUN CLI command feature in the *Cisco MDS 9000 Family Fabric Manager Configuration Guide*.

NTP Configuration

A Network Time Protocol (NTP) server provides a precise time source (radio clock or atomic clock) to synchronize the system clocks of network devices. NTP is transported over User Datagram Protocol UDP/IP. All NTP communications use Universal Time Coordinated (UTC). An NTP server receives its time from a reference time source, such as a radio clock or atomic clock, attached to the time. NTP distributes this time across the network.

This section includes the following sections:

About NTP

In a large enterprise network, having one time standard for all network devices is critical for management reporting and event logging functions when trying to correlate interacting events logged across multiple devices. Many enterprise customers with extremely mission-critical networks maintain their own stratum-1 NTP source.

Time synchronization happens when several frames are exchanged between clients and servers. The switches in client mode know the address of one or more NTP servers. The servers act as the time source and receive client synchronization requests.

By configuring an IP address as a peer, the switch will obtain and provide time as required. The peer is capable of providing time on its own and is capable of having a server configured. If both these instances point to different time servers, your NTP service is more reliable. Thus, even if the active server link is lost, you can still maintain the right time due to the presence of the peer.

Tip If an active server fails, a configured peer helps in providing the NTP time. Provide a direct NTP server association and configure a peer to ensure backup support if the active server fails.

If you only configure a peer, the most accurate peer takes on the role of the NTP server and the other peer(s) acts as a peer(s). Both machines end at the right time if they have the right time source or if they point to the right NTP source.

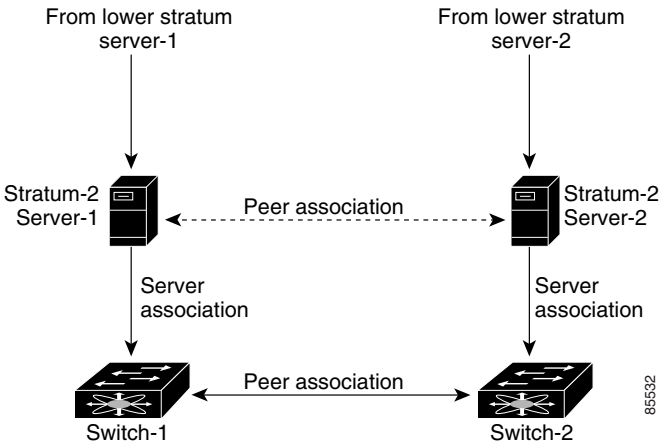
NTP Configuration Guidelines

The following guidelines apply to all NTP configurations:

- You should have a peer association with another switch only when you are sure that your clock is reliable (which means that you are a client of a reliable NTP server).
- A peer configured alone takes on the role of a server and should be used as backup. If you have two servers, then you can have several switches point to one server, and the remaining switches to the other server. Then you would configure peer association between these two sets. This forces the clock to be more reliable.
- If you only have one server, it's better for all the switches to have a client association with that server.

Not even a server down time will affect well-configured switches in the network. Figure 12-4 displays a network with two NTP stratum 2 servers and two switches.

Figure 12-4 NTP Peer and Server Association



In this configuration, the switches were configured as follows:

- Stratum 2 Server 1
  - IPv4 address–10.10.10.10
  - Stratum–2 Server-2
  - IPv4 address–10.10.10.9

- Switch 1 IPv4 address–10.10.10.1
- Switch 1 NTP configuration
  - **NTP server 10.10.10.10**
  - **NTP peer 10.10.10.2**
- Switch 2 IPv4 address–10.10.10.2
- Switch 2 NTP configuration
  - **NTP server 10.10.10.9**
  - **NTP peer 10.10.10.1**

Configuring NTP

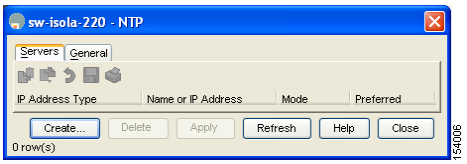
You can configure NTP using either IPv4 addresses, IPv6 addresses, or DNS names.

To create an NTP server or peer, follow these steps:

Step 1 In the Fabric Manager Physical pane, expand **Switches** then select **System**, or from Device Manager, choose **Admin > NTP**.

In Fabric Manager, you see the System information pane. In Device Manager, you see the NTP dialog box (see Figure 12-5).

Figure 12-5 Device Manager NTP Dialog Box



Step 2 Click the **NTP Peer** tab.

You see a list of NTP peers and servers for that switch.

Step 3 Click **Create**.

You see the Create NTP Peer dialog box.

Step 4 Enter the peer address in the Peer Address field.

Step 5 Choose the mode (**peer** or **server**).

Step 6 Check the **Preferred** check box if you want this peer to be a Preferred Peer.

Step 7 Click **Create** to create the peer or server, or click **Close** to close the dialog box without creating the peer or server.

The new peer or server is listed on the Peer tab.

Edit an NTP Server or Peer Configuration

To edit an NTP server or peer, follow these steps.

Step 1 In the Fabric Manager Physical Attributes pane, expand **Switches** then select **System**, or from Device Manager, choose **Admin > NTP**.

In Fabric Manager, you see the System information pane. In Device Manager, you see the NTP dialog box.

Step 2 Click the **NTP Peer** tab.

You see a list of NTP peers and servers for that switch.

Step 3 Change the peer address by double-clicking the IP address in the Peer Address column, and changing the numbers. Alternatively, you can triple click the IP address and type in a new address.

Step 4 Change the switch mode from **peer** to **server** by clicking the Mode column next to the address of the switch.

You see a drop-down list. Select the mode (**peer** or **server**) you want for the switch.

Step 5 Change the peer status of the switch to Preferred Peer by checking the **PrefPeer** check box next to the address of the switch. To remove this status, uncheck the check box.

Step 6 Click **Apply** to apply your changes to the switch, or click **Close** to close the dialog box without saving your changes.

Delete an NTP Server or Peer

To delete an NTP server or peer, follow these steps.

Step 1 In the Fabric Manager Physical pane, expand **Switches** and choose **System**, or from Device Manager, choose **Admin > NTP**.

In Fabric Manager, you see the System information pane. In Device Manager, you see the NTP dialog box.

Step 2 Click the **NTP Peer** tab.

You see a list of NTP peers and servers for that switch.

Step 3 Delete a server or peer by clicking the IP address in the Peer Address column. The Delete button is enabled.

Step 4 Click **Delete** to delete the peer or server, or click **Close** to close the dialog box without deleting the peer.

NTP CFS Distribution

You can enable NTP fabric distribution for all Cisco MDS switches in the fabric. When you perform NTP configurations, and distribution is enabled, the entire server/peer configuration is distributed to all the switches in the fabric.

You automatically acquire a fabric-wide lock when you issue the first configuration command after you enabled distribution in a switch. The NTP application uses the effective and pending database model to store or commit the commands based on your configuration.

See to Chapter 13, "Using the CFS Infrastructure," for more information on the CFS application.

This section includes the following sections:

Configure NTP with CFS

To configure NTP with CFS using Fabric Manager, follow these steps:

Step 1 Expand **Switches,** expand **Clock** then select **NTP** in the Physical Attributes pane.

You see the feature configuration in the Information pane.

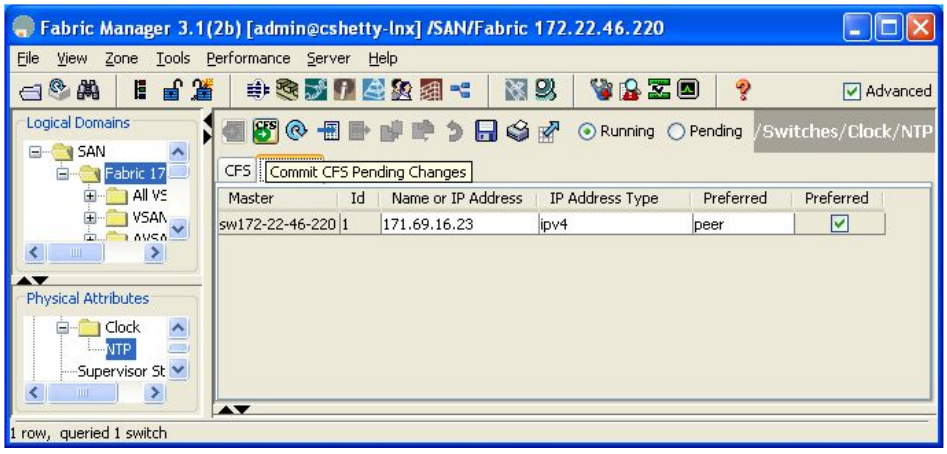
Step 2 Click the **CFS** tab in the Information pane.

You see the CFS configuration and status for each switch.

Step 3 Click a switch value in the Global column, **enable** or **disable**.

A drop-down menu appears (see Figure 12-6).

Figure 12-6 Enabling or Disabling NTP with CFS for a Switch



Step 4 Choose **enable.**

Step 5 Repeat steps 3 and 4 for all switches in the fabric.

Note A warning displays if you do not enable CFS for all switches in the fabric for this feature.

Step 6 Check the **Master** check box for the switch that you want to act as the merge master for this feature.

Step 7 Click the switch value in the Config Action column. A drop-down menu appears.

Step 8 Select **Commit**.

Step 9 Click the **Servers tab in** the Information pane. You see the configuration for this feature based on the master switch.

Step 10 Modify the Master configuration as needed. For example, right-click the value in the Master column and select **Create Row** to create a server for NTP.

a. Set the ID, and the Name or IP Address for the NTP server.

b. Choose a **Mode** radio button and, optionally, check the **Preferred** check box.

c. Click **Create** to add the server.
Fabric Manager sends the request to the master switch. Click the **CFS** tab and check the Last Results column for the new entry. It has a "pending" status.

Step 11 From the **CFS** tab, set the Config Action column to **commit** to distribute the feature change through the fabric. Fabric Manager only changes the status to “running” when **commit**, **clear,** or **abort** is selected and applied.

Note Fabric Manager will not change the status to “pending” if **enable** is selected, because the “pending” status does not apply until the first actual change is made.

Step 12 Click the **Apply Changes** icon to commit the configuration changes for that feature and distribute the changes through CFS, or click **Undo Changes** to discard the changes for that feature.

Committing NTP Configuration Changes

When you commit the NTP configuration changes, the effective database is overwritten by the configuration changes in the pending database and all the switches in the fabric receive the same configuration. When you commit the NTP configuration changes without implementing the session feature, the NTP configurations are distributed to all the switches in the fabric.

Discarding NTP Configuration Changes

After making the configuration changes, you can choose to discard the changes or to commit them. In either case, the lock is released.

Releasing Fabric Session Lock

If you have performed an NTP fabric task and have forgotten to release the lock by either committing or discarding the changes, an administrator can release the lock from any switch in the fabric. If the administrator performs this task, your changes to the pending database are discarded and the fabric lock is released.

Tip The changes are only available in the volatile directory and are subject to being discarded if the switch is restarted.

Database Merge Guidelines

When merging two fabrics, follow these guidelines:

- Be aware that the merge is a union of the existing and the received database in each switch in the fabric.
- Do not configure an IP address as a server on one switch and as a peer on another switch. The merge can fail if this configuration exists.
- Verify that the union of the databases does not exceed the maximum limit of 64.

See to the "CFS Merge Support" section on page 13-9 for detailed concepts.

Management Interface Configuration

The management interface on the switch allows multiple simultaneous Telnet or SNMP sessions. You can remotely configure the switch through the management interface (mgmt0), but first you must configure some IP parameters so that the switch is reachable. You can manually configure the management interface from the CLI. You can configure the mgmt 0 interface with either IPv4 address parameters or an IPv6 address.

On director class switches, a single IP address is used to manage the switch. The active supervisor module's mgmt0 interface uses this IP address. The mgmt0 interface on the standby supervisor module remains in an inactive state and cannot be accessed until a switchover happens. After a switchover, the mgmt0 interface on the standby supervisor module becomes active and assumes the same IP address as the previously active supervisor module.

The management port (mgmt0) is autosensing and operates in full duplex mode at a speed of 10/100/1000 Mbps (1000 Mbps is only available on the Supervisor-2 module). Autosensing supports both the speed and the duplex mode. On a Supervisor-1 module, the default speed is 100 Mbps and the default duplex mode is auto. On a Supervisor-2 module, the default speed is auto and the default duplex mode is auto.

You can set the management interface in the Fabric Manager Preferences screen to use SNMP over TCP. The advantages of this setting are an increased buffer size and faster transfer rate. If your fabric has a long timeout period, it may prevent you from using SNMP (which may have a relatively shorter timeout period). If so, change this setting to **false** and restart Fabric Manager Server. UDP is used instead.

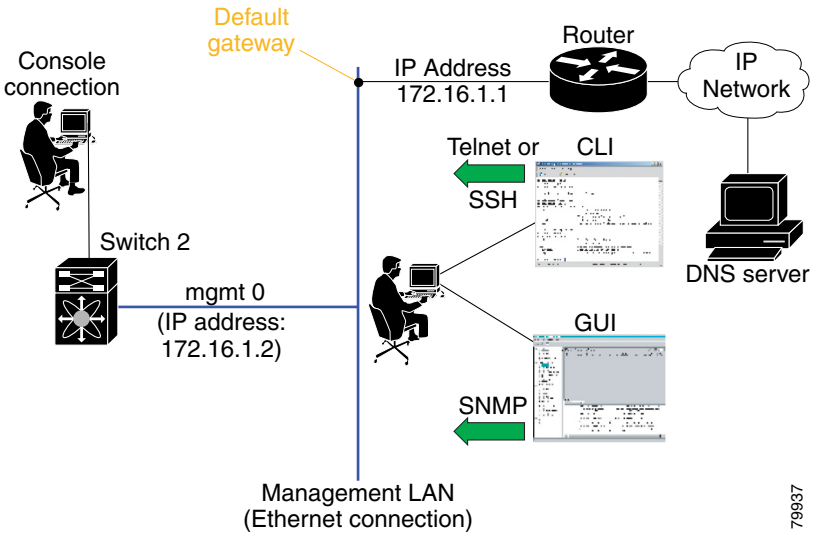
Note If it is set to false, the same choice must be set in FabricManager.

Note Before you begin to configure the management interface manually, obtain the switch's IPv4 address and IPv4 subnet mask or the IPv6 address. Also make sure the console cable is connected to the console port.

Default Gateway Configuration

The supervisor module sends IP packets with unresolved destination IPv4 addresses to the default gateway (see Figure 12-7).

Figure 12-7 Default Gateway



Telnet Server Connection

The Telnet server is enabled by default on all switches in the Cisco MDS 9000 Family. If you require a secure SSH connection, you need to disable the default Telnet connection and then enable the SSH connection (see the "Generating the SSH Server Key Pair" section on page 37-16).

Note For information on connecting a terminal to the supervisor module console port, refer to the *Cisco MDS 9200 Series Hardware Installation Guide* or the *Cisco MDS 9500 Series Hardware Installation Guide*.

Tip A maximum of 16 sessions are allowed in any switch in the Cisco MDS 9500 Series or the Cisco MDS 9200 Series.

Make sure the terminal is connected to the switch and that the switch and terminal are both powered on.

Disabling a Telnet Connection

To disable Telnet connections to the switch using Device Manager, follow these steps:

Step 1 Select **Device** > **Preferences**.

Step 2 Check the **Use Secure Shell instead of Telnet** check box.

Step 3 Click **Apply**.

Telnet is disabled and SSH is enabled on the switch.

Configuring CDP

The Cisco Discovery Protocol (CDP) is an advertisement protocol used by Cisco devices to advertise itself to other Cisco devices in the same network. CDP runs on the data link layer and is independent of Layer 3 protocols. Cisco devices that receive the CDP packets cache the information to make it is accessible through the CLI and SNMP.

CDP is supported on the management Ethernet interface on the supervisor module and the Gigabit Ethernet interfaces on the IPS and MPS-14/2 modules. The CDP daemon is restartable and switchable. The running and startup configurations are available across restarts and switchovers.

CDP version 1 (v1) and version 2 (v2) are supported in Cisco MDS 9000 Family switches. CDP packets with any other version number are silently discarded when received.

When the interface link is established, CDP is enabled by default and three CDP packets are sent at one-second intervals. Following this, the CDP frames are sent at the globally configured refresh interval.

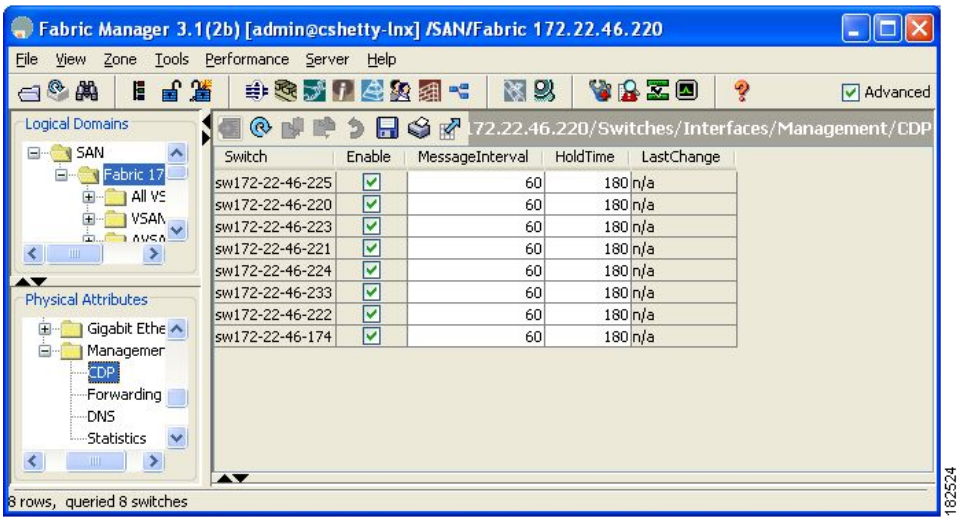
To globally disable CDP using Fabric Manager, follow these steps:

Step 1 Select a switch in the Logical Domains pane.

Step 2 Expand **Switches**, expand **Interfaces**, expand **Management**, and then select **CDP** in the Physical Attributes pane.

You see the CDP information in the Information pane shown in Figure 12-8.

Figure 12-8 Cisco Discovery Protocol



Step 3 Deselect the **Enable** check box.

Step 4 Click the **Apply Changes** icon.

To disable CDP using Device Manager, follow these steps:

Step 1 Click **IP > CDP**.

You see the CDP dialog box as shown in Figure 12-8.

Step 2 Deselect the **Enable** check box.

Step 3 Click the **Apply Changes** icon.

To globally configure the message interval for the CDP protocol using Device Manager, follow these steps:

Step 1 Click **IP > CDP**.

You see the CDP dialog box as shown in Figure 12-8.

Step 2 Set the message interval time in seconds (5-254).

Step 3 Click the **Apply icon**.

To globally configure the hold time advertised in CDP packets using Device Manager, follow these steps:

Step 1 Click **IP > CDP**.

You see the CDP dialog box as shown in Figure 12-8.

Step 2 Set the hold time in seconds (10-255).

Step 3 Click **Apply**.