Prerequisites

This chapter provides release-specific prerequisites information for your deployment of *Cisco Data Center Network Manager*.

General Prerequisites

This section includes the following topics:

Before you begin

Before you can install Cisco DCNM, ensure that the Cisco DCNM system meets the following prerequisites:

- Before installing Cisco DCNM, ensure that the host name is mapped with the IP address in the hosts file under the following location:
  - Microsoft Windows–`C:\WINDOWS\system32\drivers\etc\hosts`
  - Linux–`/etc/hosts`

Note If Oracle RAC is chosen as the database for Cisco DCNM, ensure that the database host IP addresses and virtual IP addresses are added to the hosts file with their host-names.

- For RHEL, the maximum shared memory size must be 256 MB or more. To configure the maximum shared memory to 256 MB, use the following command:

  sysctl -w kernel.shmmax=268435456

This setting, kernel.shmmax=268435456, should be saved in the `/etc/sysctl.conf` file. If this setting is not present or if it is less than 268435456, the Cisco DCNM server will fail after the server system is rebooted. For more information, visit the following URL:

http://www.postgresql.org/docs/8.3/interactive/kernel-resources.html

The server system must be registered with the DNS servers. The server hosting DCNM application must be dedicated to run DCNM alone and must not be shared with any other applications which utilizes memory and system resources.

- While using Remote PostgreSQL Database server, ensure that the Cisco DCNM Host IP addresses are added to the `pg_hba.conf` file present in the PostgreSQL installation directory. After the entries are added, restart the database.
- Users installing Cisco DCNM must have full administrator privileges to create user accounts and start services. Users should also have access to all ports. For more information, see Running Cisco DCNM Behind a Firewall.
- When you connect to the server for the first time, Cisco DCNM checks to see if you have the correct Sun Java Virtual Machine version installed on your local workstation. Cisco DCNM desktop clients look for version 1.8(x) during installation. If required, install the Sun Java Virtual Machine software.

Note When launching the Cisco DCNM installer, the *console* command option is not supported.

Note Using the Cisco DCNM installer in GUI mode requires that you must log in to the remote server using VNC or XWindows. Using Telnet or SSH to install Cisco DCNM in GUI mode is not possible.

Before you can use Cisco DCNM to manage network switches, you must complete the following tasks:

- Install a supervisor module on each switch that you want to manage.
- Configure the supervisor module with the following values using the setup routine or the CLI:
  - IP address assigned to the mgmt0 interface
  - SNMP credentials (v3 user name and password or v1/v2 communities), maintaining the same user name and password for all the switches in the fabric.

Initial Setup Routine

The first time that you access a Cisco NXOS-based switch for MDS or Nexus, 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. All Cisco Nexus or Cisco MDS 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 Nexus or Cisco MDS. 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).

Note IP address for a Cisco Nexus switch or a Cisco MDS switch can be set via CLI or USB key or POAP.

Preparing to Configure the Switch

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

- 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 Cisco DCNM-SAN Server host name entry exists on the DNS server, unless the Cisco DCNM-SAN Server is configured to bind to a specific interface during installation.

Default Login

All Cisco Nexus and 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 Security Configuration Guide, Cisco DCNM for SAN).

You have an option to enforce a 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 Security Configuration Guide, Cisco DCNM for SAN). If you configure and subsequently forget this new password, you have the option to recover this password (see the Security Configuration Guide, Cisco DCNM for SAN).

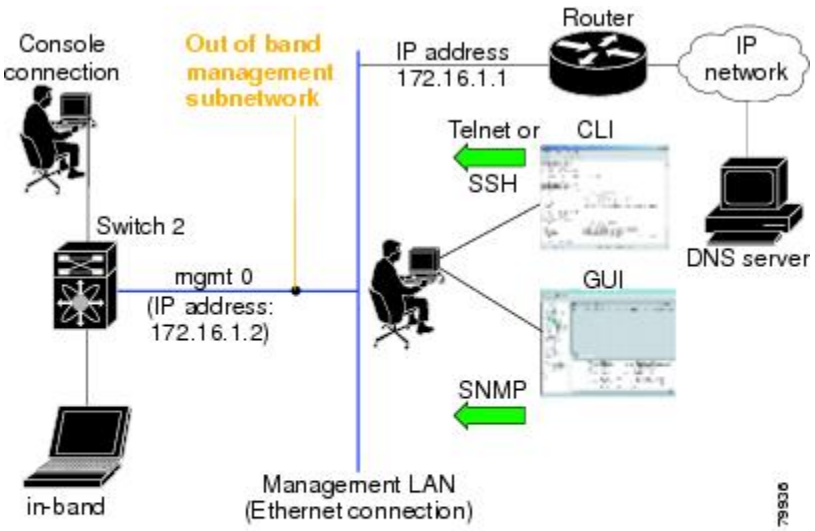
Note Adhere to the following password requirements. If you do not comply with the requirements, the DCNM application might not function properly:

- It must be at least 8 characters long and contain at least one alphabet and one numeral.
- It can contain a combination of alphabets, numerals, and special characters.
- Do not use any of these special characters in the DCNM password for any deployment mode: <SPACE> & $ % ‘ “ ^ = < > ; :

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 or a Cisco Nexus switch with an IP address to enable management connections from outside of the switch (see Figure 1: Management Access to Switches, on page 5).

Figure 1: Management Access to Switches



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.

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

You can configure both in-band and out-of-band configuration together by entering **Yes** in both in the following procedure.

Procedure

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

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

Step 2 Enter Yes to enforce a secure password.

a) Enter the administrator password.

```
Enter the password for admin: 2008asdf*lkjh17
```

Note The password can contain a combination of alphabets, numeric, and special characters. Do not use any of these special characters in the DCNM password for any deployment mode: <SPACE> & $ % ‘ “ ^ = < > ; :

b) Confirm the administrator password.

```
Confirm the password for admin: 2008asdf*lkjh17
```

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.

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

Note This setup utility guides 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.

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

While configuring your initial setup, you can create an additional user account (in the network administrator role) in addition to the administrator’s account. See the Security Configuration Guide, Cisco DCNM for SAN 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
```

The password can contain a combination of alphabets, numeric, and special characters. Do not use any of these special characters in the DCNM password for any deployment mode: <SPACE> & $ % ‘ “ ^ = < > ; :

c) Confirm the user password.

```
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 username (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
```

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
```

Enter the destination prefix mask.

```
Destination prefix mask: dest_mask
```

Enter 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 .

```
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.

```
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
```

This step 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 Fabric Configuration Guide, Cisco DCNM for SAN). 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
  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. Enter **yes** to save the new configuration to ensure 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 that is configured with an IP address in the same subnetwork. A default route that points to the switch that provides access to the IP network should be configured on every switch in the Fibre Channel fabric (see Fabric Configuration Guide, Cisco DCNM for SAN).

Note You can configure both in-band and out-of-band configuration together by entering in the following procedure.

Procedure

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*lkjh18
```

The password can contain a combination of alphabets, numeric, and special characters. The password can contain a combination of alphabets, numeric, and special characters. Do not use any of these special characters in the DCNM password for any deployment mode: <SPACE> & $ % ‘ “ ^ = < > ; :

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.
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 more 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
```

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 Security Configuration Guide, Cisco DCNM for SAN) that you want to generate.

```
Type the SSH key you would like to generate (dsa/rsa/rsa1)? 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
```

This step 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
```

This step 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 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
    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. Enter **yes** to save the new configuration. To ensure 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 enter 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.

Procedure

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

- 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.

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:

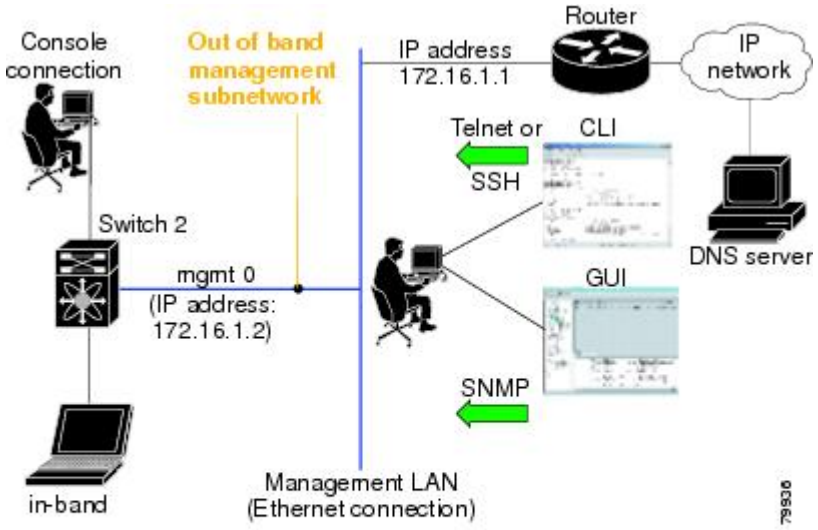
- Serial console access—You can use a serial port connection to access the CLI.
- In-band IP (IPFC) access—You can use Telnet or SSH to access a switch in the Cisco MDS 9000 Family or use SNMP to connect to a Cisco DCNM-SAN application.
- Out-of-band (10/100BASE-T Ethernet) access—You can use Telnet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

After initial configuration, you can access the switch in one of three ways (see Figure 2: Switch Access Options, on page 14):

- 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 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 DCNM-SAN to access the switch.

Figure 2: Switch Access Options



Prerequisites for Installing DCNM on Windows

- During the initial installation, disable all security andpost antivirus tools that are running on your Windows server.
- Do not run any other management applications on the Cisco DCNM server or the Cisco DCNM database server.
- Before installing Cisco DCNM, ensure that the hostname is mapped with the IP address in the hosts file under the location **C:\WINDOWS\system32\drivers\etc\hosts**.
- On Windows, remote Cisco DCNM installations or upgrades must be done through the console using VNC or through the Remote Desktop Client (RDC) in console mode (ensuring RDC is used with the **/Console** option). This process is important if the default PostgreSQL database is used with Cisco DCNM, because this database requires the local console for all installations and upgrades.
- Telnet Client application is not installed by default on Microsoft Windows Vista. To install Telnet Client, choose **Start > Programs > Control Panel > Click Turn Windows features on or off** (if you have UAC turned on, provide permissions to continue). Check **Telnet Client** check box and click **Ok**.

- You can run CiscoWorks on the same PC as Cisco DCNM although the Java requirements are different. When installing the later Java version for Cisco DCNM, make sure that it does not overwrite the earlier Java version that is required for CiscoWorks. Both versions of Java can coexist on your PC.
- Ensure that you use the same Operating System for all the nodes in the Federation setup.
- In the Federation setup, ensure that the server time is synchronized across all the nodes of the Federation setup. The servers will not be able to communicate if the time is not synchronized. We recommend that you use NTP server to synchronize time across all the nodes.
- Ensure that you uninstall the Windows Defender application, and restart Windows 2016 server before installing Cisco DCNM on Windows 2016 server.

Prerequisites for Installing DCNM on Linux

- For RHEL, the maximum shared memory size must be 256 MB or more. To configure the maximum shared memory to 256 MB, use the following command: **sysctl -w kernel.shmmax=268435456**. Save the **kernel.shmmax=268435456** value in the **/etc/sysctl.conf** file. If this value is not correct, the Cisco DCNM server fails after the server system reboots. For more information, visit the following URL: http://www.postgresql.org/docs/8.4/interactive/kernel-resources.html

Note Ensure that you've installed Visual C++ Redistributable Packages for Visual Studio 2013 64 bit before installing or upgrading to Cisco DCNM Release 11.4(1).

- The server system must be registered with the DNS servers.
- No other programs must be running on the server.
- Ensure that you select English as the preferred language during RHEL installation.
- Ensure that you use the same Operating System for all the nodes in the Federation setup.
- In the Federation setup, ensure that the server time is synchronized across all the nodes of the Federation setup. The servers will not be able to communicate if the time is not synchronized. We recommend that you use NTP server to synchronize time across all the nodes.
- After you upgrade from Cisco DCNM Release 11.2(1) on Linux Standalone server, ensure that you clear the browser cache and Java console cache before you launch the Web UI and download the SAN Client. The Java console remembers the previous version of the SAN client data. If you do not clear Java console cache, you will not be able to use the latest downloaded SAN Client.
- Along with Postgres SQL database backup, take a backup of **server.properties** file also to restore the DCNM server during disaster recovery.

Antivirus exclusion

Scanning the Cisco DCNM includes the scanning of the database files. This process will hamper the performance on the DCNM while operation. While scanning the Cisco DCNM on Linux RHEL server, exclude the directory `/usr/local/cisco/dcm/db and /var/lib/dcnm`.

For more information, refer to https://wiki.postgresql.org.

Note We recommend you to stop Anti-Virus scanning while installing DCNM because the port being used or blocked might cause failures. After the installation, you can enable or install Anti-Virus application with specific guidelines to avoid DCNM directories as part of the scan.

Oracle Database for DCNM Servers

This section details about the database required for the installation of DCNM server.

Note This section is not applicable for Cisco DCNM Native HA installation.

Cisco DCNM supports the following databases:

- Oracle Database 11g
- Oracle Database 12c
- Oracle RAC 11g, and 12c

You can change from the local database to an external Oracle database, if required.

Note Cisco DCNM is configured with AL32UTF8 character set.

The Cisco DCNM Database size is not limited and increases based on the number of nodes and ports that the DCNM manages with Performance Manager Collections enabled. You cannot restrict the database size. Cisco recommends that you use Oracle SE or Enterprise edition, instead of Oracle XE, due to table space limitations.

This section contains the following:

Oracle SQLPlus Command-Line Tool

The Oracle database procedures in this section require the use of the SQL*Plus command-line tool. The SQL*Plus executable is typically installed in the bin directory under the Oracle home directory.

Linux Environment Variables

If you are using Linux, before you use the SQL*Plus command-line tool, ensure that the ORACLE_HOME and ORACLE_SID environment variables are set to correct values.

For example, if you are using Oracle 11g on Linux, the following commands set the environment variables to the default Oracle home directory and SID if you are using a bash shell:

```
export ORACLE_HOME=<usr_home_directory>/app/oracle/product/11.2.0/
(or identify the Oracle home on the Oracle installed server)
export ORACLE_SID=XE
```

init.ora File

The init.ora file specifies startup parameters. The default name and location of the file is platform specific, as shown in the following table.

Table 1: Name and Default Location of init.ora File

Oracle Version	Operating System	Location of init.ora File
12c	Microsoft Windows	C:\app\Administrator\virtual\product\12.2.0\dbhome_1\srvm\admin\init.ora
	Linux	/usr/lib/oracle/orcl/app/oracle/product/12.2.0/db_1/srvm/initORCL.ora
11g	Microsoft Windows	C:\app\Administrator\product\11.1.0\db_1\dbs\initORCL.ora
	Linux	/usr/lib/oracle/orcl/app/oracle/product/11.1.0/db_1/dbs/initORCL.ora

Backing up the Oracle Database

Copy the oracle backup/restore script from the Cisco DCNM server directory `DCNM_SERVER_Install/dcm/dcnm/bin`.

For Linux, the script name is backup-remote-oracledb.sh/restore-remote-oracledb.sh and edit the DB_HOME variable to point to the Oracle installation.

For Windows, the script name is **backup-remote-oracledb.bat/restore-remote-oracledb.bat** and edit *DB_HOME* variable to point to the Oracle installation.

Use the following path for Oracle DBHOME:

- On Linux– `/usr/lib/oracle/xe/app/oracle/product/10.2.0/server`

  Replace `/usr/lib/oracle` with the Oracle installation path.

- On windows– `C:\oraclexe\app\oracle\product\10.2.0\server`

  Replace `C:\oraclexe` with the Oracle installation path.

Preparing the Oracle Database

You can prepare an Oracle database.

Procedure

Step 1 Increase the number of sessions and processes to 150 each. For more information, see the Increasing the Number of Sessions and Processes to 150 Each, on page 19.

Step 2 Increase the number of open cursors to 1000. For more information, see the Increasing the Number of Open Cursors to 1000, on page 19.

Logging Into Oracle

You can log into the Oracle database by using the SQL*Plus command-line tool.

Before you begin

Ensure that you know the database administrator username and password.

Procedure

Step 1 Run the SQL*Plus executable.

A command prompt appears.

Step 2 Enter the **connect** command.

The Username prompt appears.

Step 3 Enter the database administrator username.

The Password prompt appears.

Step 4 Enter the password for the username that you specified.

For example, if the Oracle administrator username is system and the password is oracle, you would log in as follows:

Example:

```
Username: sys as sysdba
Password: oracle
```

What to do next

For more information about using SQL*Plus, see the documentation for the Oracle database version that you are using.

Increasing the SYSTEM Tablespace

You can increase the SYSTEM tablespace.

Procedure

Step 1 Use the SQL*Plus command-line tool to log in to the Oracle database. For more information, see the Oracle SQLPlus Command-Line Tool, on page 16.

Step 2 Enter the following command:

```
select file_name, bytes, autoextensible, maxbytes
from dba_data_files where tablespace_name='SYSTEM';
```

Step 3 Enter the following command:

```
alter database datafile filename autoextend on next 100m maxsize 2000m;
```

where *file_name* is the filename from the output of the **select** command in the previous step.

The SYSTEM tablespace is increased.

Step 4 Enter the **exit** command.

Increasing the Number of Sessions and Processes to 150 Each

For each DCNM instance configured in the same Oracle database, the number of cursors and processes must be increased to more than the 150 and 1000.

For example, if two DCNM standalone (non HA) instances are configured to use the same Oracle database, the cursors and process must be increased to 300 and 2000 approximately, depending on any performance degradation or SQL Exception errors occurred during normal operations of either of the DCNM instances.

Procedure

Step 1 Ensure that the `init.ora` file exists and that it contains the single line that is applicable for your Oracle database installation. If there are additional lines, remove them.

For more information, see the init.ora File, on page 17.

Step 2 Use the SQL*Plus command-line tool to log in to the Oracle database. For more information, see the Oracle SQLPlus Command-Line Tool, on page 16.

Step 3 Shut down the system by entering the **shutdown** command. If the command fails, use the **shutdown abort** command.

Step 4 Enter the following command:

```
startup pfile='init_file_name';
```

where *init_file_name* is the init.ora filename for your Oracle database installation. For more information, see the init.ora File, on page 17.

Step 5 Set the number of sessions to 150 by entering the following command:

```
alter system set sessions = 150 scope=spfile;
```

Step 6 Shut down the system by entering the **shutdown** command. If the command fails, use the **shutdown abort** command.

Step 7 Start up the system by entering the **startup** command.

Step 8 Verify that the number of sessions and processes is changed to 150 by entering the following command:

```
show parameter sessions
```

Step 9 Exit by entering the **exit** command.

Increasing the Number of Open Cursors to 1000

You can increase the number of open cursors to 1000.

Procedure

Step 1 Ensure that the init.ora file exists and that it contains the single line that is applicable for your Oracle database installation. If there are additional lines in the file, remove them.

For more information, see the init.ora File, on page 17.

Step 2 Use the SQL*Plus command-line tool to log in to the Oracle database. For more information, see the Oracle SQLPlus Command-Line Tool, on page 16.

Step 3 Shut down the system by entering the **shutdown** command. If the command fails, use the **shutdown abort** command.

Step 4 Enter the following command:

```
startup pfile='init_file_name'
```

where *init_file_name* is the init.ora filename for your Oracle database installation. For more information, see the init.ora File, on page 17.

Step 5 Set the number of open cursors to 1000 by entering the following command:

```
alter system set open_cursors = 1000 scope=spfile;
```

Step 6 Shut down the system by entering the **shutdown** command. If the command fails, use the **shutdown abort** command.

Step 7 Start up the system by entering the **startup** command.

Step 8 Verify that the number of open cursors is changed to 1000 by entering the following command:

```
show parameter open_cursors
```

Step 9 Exit by entering the **exit** command.

Creating an Oracle DB User using the Command Prompt

To create an Oracle DB user using the command prompt, follow these steps:

```
export ORACLE_SID=XE
export ORACLE_HOME=/usr/lib/oracle/xe/app/oracle/product/10.2.0/server
cd $ORACLE_HOME/bin
sqlplus
sys as sysdba
create user dcnmdbusername identified by dcnmdbuserpassword default tablespace users temporary
 tablespace temp;
grant connect, resource to dcnmdbusername;
grant create session to dcnmdbusername;
grant dba to dcnmdbusername;
```

Note Ensure you set the Oracle_SID and Oracle_Home and enter the values for the DB Username and password fields.

Note When a DBA account cannot be created, an account with DML/DDL/schema privilege is sufficient.

Connecting to an Oracle RAC with SCAN Feature Type DB

To connect to an Oracle RAC with SCAN Feature type DB, enter the following command:

```
# appmgr update -u jdbc:oracle:thin:@//[ip_addr]:1521/[service name] -n [username] -p
[password]
```

Database for Federation Setup

Cisco DCNM can be deployed as Cisco DCNM-SAN federation. For Cisco DCNM-SAN federation, the database URL (properties) must remain the same for all Cisco DCNM-SAN nodes in the federation.

Note Ensure that you do not provide multicast addresses to form the federation.

Remote Oracle Database Utility Scripts for Backup and Restore

Irrespective of the platform, Cisco DCNM is installed (Windows or Linux), the following scripts to backup and restore the remote Oracle database.

Utility scripts for Oracle database that is installed on Linux platform are;

1. backup-remote-oracledb.sh
2. restore-remote-oracledb.sh

Utility scripts for Oracle database that is installed on Windows platform are:

1. backup-remote-oracledb.bat
2. restore-remote-oracledb.bat

Cisco DCNM host is configured to run with a remote Oracle database. As part of housekeeping, you can copy DCNM utility scripts to a remote Oracle database and restore the DCNM database schema.

To run the utility scripts, you need the database administrator credentials. These scripts will prompt you for:

1. DCNM database password (the user name is already present)
2. Username/password of the admin user.

While entering the DBA user credentials, ensure that you do not to enter “sys” as sysdba" because in some versions of Oracle, the presence of space might cause the backup/restore to fail. Instead, user should provide valid user credentials that does not have a space in the user name, for example, system or sysdba. The admin credentials are not saved/cached and hence they do not leak sensitive credential information.

Note User scripts under **dcnm/bin** can be run only by administrator user.

Local PostgreSQL Database Utility Scripts for Backup and Restore

Utility scripts for Local PostgreSQL database that is installed in RHEL machine are:

1. backup-pgsql-dcnm-db.sh
2. restore-pgsql-dcnm-db.sh

Utility scripts for Local PG database that is installed in Windows machine are:

1. backup-pgsql-dcnm-db.bat
2. restore-pgsql-dcnm-db.bat