Cisco Data Center Network Manager for LAN

New and Changed Information

As of Cisco DCNM Release 5.2, Cisco Fabric Manager and Cisco Data Center Network Manager for LAN are merged into one unified product called Cisco Data Center Network Manager (DCNM) that can manage both LAN and SAN environments. As a part of this product merger, the name Cisco DCNM for SAN replaces the name Cisco Fabric Manager.

The following documentation changes support the merged Cisco DCNM product:

Cisco DCNM product documentation for Cisco DCNM Release 5.2 is retitled with the name Cisco DCNM for LAN.

Cisco Fabric Manager product documentation for Cisco DCNM Release 5.2 is retitled with the name Cisco DCNM for SAN.

Cisco DCNM for SAN product documentation is now published to the Data Center Network Manager listing page on Cisco.com:

http://www.cisco.com/en/US/products/ps9369/tsd_products_support_configure.html

This URL is also the listing page for Cisco DCNM for LAN product documentation.

Cisco Fabric Manager documentation for software releases earlier than Cisco DCNM Release 5.2, retains the name Cisco Fabric Manager and remains available at its current Cisco.com listing page:

http://www.cisco.com/en/US/products/ps10495/tsd_products_support_configure.html

You should continue to use the Cisco Fabric Manager documentation if you are using a release of Cisco Fabric Manager software that is earlier than Cisco DCNM Release 5.2.

The name DCNM-SAN is used in place of Cisco DCNM for SAN in the user interface of Cisco Data Center Network Manager; likewise, the name DCNM-LAN is used in place of Cisco DCNM for LAN in the user interface. To match the user interface, the product documentation also uses the names DCNM-SAN and DCNM-LAN.

The following new publications support both Cisco DCNM for LAN and DCNM for SAN, and address the new licensing model, the new installation process, and the new features of Cisco DCNM:

- *Cisco DCNM Installation and Licensing Guide, Release 5.x*
- *Cisco DCNM Release Notes, Release 5.x*

For a complete list of Cisco DCNM documentation, see the “Related Documentation” section in the Preface.

The following describes the release-specific information for each new and changed feature in the *Cisco DCNM Installation and Licensing Guide, Release 5.x.* The latest version of this document is available at the following Cisco website:
http://www.cisco.com/en/US/products/ps9369/tsd_products_support_series_home.html

To check for additional information about Cisco Data Center Network Manager for LAN (DCNM-LAN) or Cisco Data Center Network Manager for SAN (DCNM-SAN), see the *Cisco DCNM Release Notes, Release 5.x*.

Table 1 summarizes the new and changed features for the *Cisco DCNM Installation and Licensing Guide, Release 5.x*, and tells you where they are documented.

Table 1 New and Changed Features for Release 5.x

Feature	Description	Changed in Release	Where Documented
DCN M License on a Cisco Nexus 1010 Switch	Support to install a Cisco DCNM license on a Virtual Service Blade (VSB)	5.2(2a)	Chapter 1, "Installing and Administering Cisco DCNM VSB"
Windows 2008 Support	DCNM-SAN Supported Software	5.0(1)	Chapter 1, "Installing Cisco DCNM-SAN Management Software"
Server installation	Support was added for setting up a DCNM-LAN clustered-server environment. Support was added for secondary server DCNM-LAN installation.	5.0(2)	Chapter 1, "Deploying Cisco DCNM-LAN" Chapter 1, "Installing Cisco DCNM-LAN Servers" Chapter 1, "Licensing a Cisco DCNM-LAN Deployment" Chapter 1, "Upgrading Cisco DCNM-LAN Servers"
Secure client communications	Support was added for DCNM-LAN TLS encryption of client-server communications.	5.0(2)	Chapter 1, "Configuring Cisco DCNM-LAN Servers"
Install Manager	Support was added for DCNM-LAN Install Manager tool.	5.1	Chapter 1, "Installing Cisco DCNM-LAN Servers" Chapter 1, "Licensing a Cisco DCNM-LAN Deployment" Chapter 1, "Upgrading Cisco DCNM-LAN Servers" Chapter 1, "Uninstalling Cisco DCNM-LAN Servers"
Common Installer	Support was added to install DCNM-LAN and DCNM-SAN.	5.2(0)	Chapter 1, "Installing Cisco DCNM-SAN Management Software" Chapter 1, "Installing Cisco DCNM-LAN Servers"

Preface

This preface describes the audience, organization, and conventions of the *Cisco DCNM Installation and Licensing Guide, Release 5.x*. It also provides information on how to obtain related documentation.

This preface includes the following topics:

Audience

This publication is for experienced network administrators who plan to install Cisco Data Center Network Manager for SAN (DCNM-SAN) and/or Cisco Data Center Network Manager for LAN (DCNM-LAN) to configure, monitor, and maintain Cisco Nexus, Cisco MDS, and Cisco Unified Computing System products.

Document Organization

This document is organized into the following chapters:

Chapter	Description
Part 1 Cisco Data Center Network Manager for SAN	Proviudes installation information for DCNM-SAN.
Chapter 1, “Prerequisites for Installing DCNM-SAN”	Describes how to prepare for a Cisco DCNM-SAN installation.
Chapter 1, “Installing Cisco DCNM-SAN Management Software”	Describes how to install the Cisco DCNM-SAN management software.
Chapter 1, “Maintaining Cisco DCNM-SAN”	Describes how to maintain a Cisco DCNM-SAN installation.

Chapter	Description
Chapter 1, "Uninstalling Cisco MDS NX-OS and DCNM-SAN"	Describes how to uninstall the Cisco DCNM-SAN server software.
Part 1 Cisco Data Center Network Manager for LAN	Provides installation information for DCNM-LAN.
Chapter 1, "Deploying Cisco DCNM-LAN"	Provides an overview of how to begin using Cisco DCNM-LAN.
Chapter 1, "Preparing a Database for DCNM-LAN"	Describes how to prepare a database for a successful Cisco DCNM-LAN installation.
Chapter 1, "Installing Cisco DCNM-LAN Servers"	Describes how to install the Cisco DCNM-LAN server software.
Chapter 1, "Licensing a Cisco DCNM-LAN Deployment"	Describes Cisco DCNM-LAN licensing, how to acquire licenses, and how to install licenses.
Chapter 1, "Upgrading Cisco DCNM-LAN Servers"	Describes how to upgrade the Cisco DCNM-LAN server software.
Chapter 1, "Configuring Cisco DCNM-LAN Servers"	Describes how to configure Cisco DCNM-LAN servers.
Chapter 1, "Uninstalling Cisco DCNM-LAN Servers"	Describes how to uninstall the Cisco DCNM-LAN server software.
Chapter 1, "Troubleshooting the Cisco DCNM-LAN Server Installation"	Describes how to identify and resolve common issues with the installation of Cisco DCNM-LAN servers.

Document Conventions

This document uses the following conventions:

Note Means reader *take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

In this document, the following shortened names are used:

- Cisco Data Center Network Manager for SAN is also referred to as DCNM-SAN.
- Cisco Data Center Network Manager for LAN is also referred to as DCNM-LAN.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

Send document comments to dcnm-docfeedback@cisco.com

Introduction to Cisco Data Center Network Manager

Cisco Data Center Network Manager (DCNM) is a management system for the Cisco Unified Fabric. It enables you to provision, monitor, and troubleshoot the data center network infrastructure. It provides visibility and control of the unified data center so that you can optimize for the quality of service (QoS) required to meet service-level agreements.

Cisco DCNM increases overall data center infrastructure uptime and reliability, thereby improving business continuity. It provides a robust framework and comprehensive feature set that meets the routing, switching, and storage administration needs of data centers. Cisco DCNM streamlines the provisioning for the unified fabric and monitors the SAN and LAN components. Cisco DCNM provides a high level of visibility and control through a single web-based management console for Cisco Nexus, Cisco MDS, and Cisco Unified Computing System products.

Cisco DCNM also supports the installation of the Cisco DCNM for SAN and Cisco DCNM for LAN components with a single installer.

The following documentation changes support the merged Cisco DCNM product:

- Cisco DCNM product documentation for Cisco DCNM Release 5.2 is retitled with the name Cisco DCNM for LAN.
- Cisco Fabric Manager product documentation for Cisco DCNM Release 5.2 is retitled with the name Cisco DCNM for SAN.

All Cisco DCNM for SAN and Cisco DCNM for LAN product documentation is now published to the Data Center Network Manager listing page on Cisco.com:

http://www.cisco.com/en/US/products/ps9369/tsd_products_support_configure.html

Send document comments to dcnm-docfeedback@cisco.com

PART 1

Cisco Data Center Network Manager for SAN

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

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

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.

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.

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.

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 Fundamentsls 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.

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

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:

- 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*).

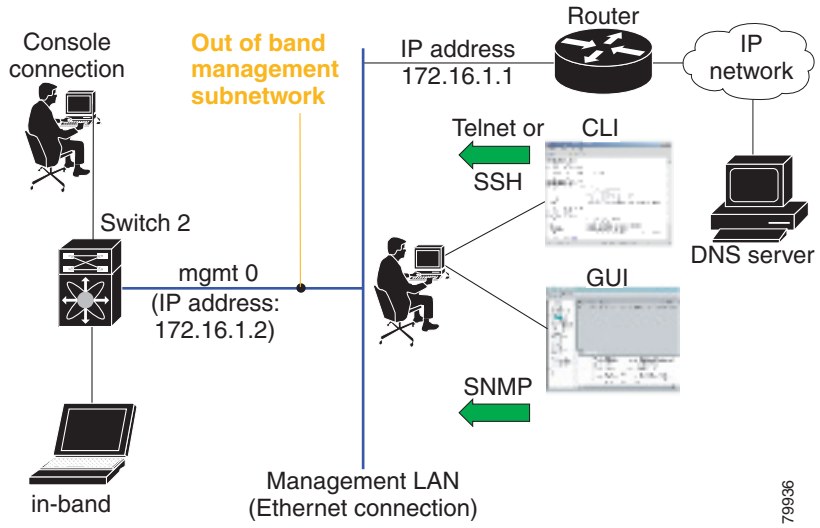
Setup Options

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.

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



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

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*lkjh17
```

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. 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.

```
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
```

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.

```
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
```

```
  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*lkjh18
```

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.
```

```
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
```

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/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
```

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
```

```
    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:

- 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

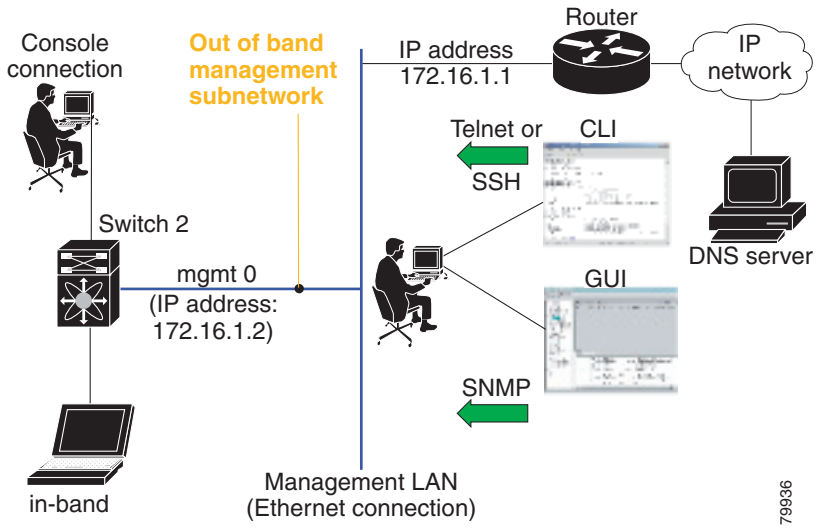
After initial configuration, you can access the switch in one of the three ways:

- 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.

Figure 1-2 Switch Access Options



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.

CHAPTER 1

Installing the Database for Cisco DCNM-SAN

This chapter describes about installing the database for Cisco DCNM for SAN (DCNM-SAN) and contains the following sections:

Information about the Database

Before you install DCNM-SAN, you must install a database. As of Cisco MDS NX-OS Release 4.1(1) and later, DCNM-SAN is packaged with PostgreSQL database. You can install PostgreSQL by using DCNM-SAN installer from Cisco.com. If the PostgreSQL database is present in your computer, the DCNM-SAN installer will upgrade it to the latest version.

Installing the Database

This section includes the following topics:

Restrictions

- If you are installing Cisco SAN-OS Release 3.1(2b) or later, you can also use Oracle Database 10g Express. Your other choice is PostgreSQL.
- If you are installing Cisco NX-OS Release 5.0(1a) or later, you can also use Oracle Database 10g Express, or Oracle Database 10g. Your other choice is PostgreSQL.
- Be sure to back up all of the rrd file in $INSTALL/pm/db before the upgrade.

- If you want to use Oracle Database 10g Express, you must install the database and create a user name and password before continuing with the DCNM-SAN installation.
- We recommend the Oracle Database 10g Express option for all users who are running Performance Manager on large fabrics (1000 or more end devices).

Directory Structure

Starting from Cisco MDS NX-OS Release 4.1(3a), the directory structure has changed to accommodate its future integration with Nexus 5000 products. By default, the DCNM-SAN components are installed on your computer's hard drive, in the C:\Program Files\ folder. The installation path is the root directory on your computer, such as C:\Program Files\Cisco Systems. DCNM-SAN and databases are installed in application directories, such as C:\Program Files\Cisco Systems\DCM\FM. Table 1-1 and Table 1-2 describe the directory structure for Windows, UNIX and Solaris operating systems.

Table 1-1 Directory Structure (Windows)

Directory	Description
C:\Program Files\Cisco Systems\	Home directory for Cisco products.
C:\Program Files\Cisco Systems\DCM\	Home directory for Cisco Data Center Management products.
C:\Program Files\Cisco Systems\DCM\FM	Home directory for DCNM-SAN and Device Manager.
C:\Program Files\Cisco Systems\DCM\JBOSS-4.2.2.GA	Home directory for JBoss (DCNM-SAN Server infrastructure).
C:\Program Files\Cisco Systems\DCM\DB	Home directory for database (Oracle and PostgreSQL).
C:\Program Files\Cisco Systems\DCM\JRE	Home directory for Java Runtime Environment.
C:\Program Files\Cisco Systems\DCM\JBOSS-4.2.2.GA\SERVER\FM	Home directory for DCNM-SAN Server.

Table 1-2 Directory Structure (Unix and Solaris)

Directory	Description
/usr/local/cisco	Home directory for Cisco products.
/usr/local/cisco/dcm/	Home directory for Cisco Data Center Management products.
/usr/local/cisco/dcm/fm	Home directory for DCNM-SAN and Device Manager.
/usr/local/cisco/dcm/jboss-4.2.2.GA	Home directory for JBoss (DCNM-SAN Server infrastructure).
/usr/local/cisco/dcm/db	Home directory for database (Oracle and PostgreSQL).
/usr/local/cisco/dcm/jboss-4.2.2.GA/server/fm	Home directory for DCNM-SAN Server.

Installing Oracle

To install the Oracle database, follow these steps:

Step 1 Click the following link to install Oracle Database 10g Express or Oracle Database 11g.

http://www.oracle.com/technology/software/products/database/xe/index.html

Note If you have another instance of Oracle already installed on a PC, we recommend that you do not install the Oracle database on the same PC. In such cases, DCNM-SAN can only use the PostgreSQL database.

Step 2 Run OracleXE.exe to install the Oracle database. Set the password for the system user. The database administrator uses the password to manage and administer Oracle Database 10g Express server, which is installed by the Oracle installer.

Step 3 Finish the installation and verify that both services (OracleServiceXE and OracleXETNSListener) are running from the Services window.

Step 4 Run the following script to

a. Change the default Oracle admin port to 8082, and

b. To create a database account. This example creates a new user 'scott' with a password 'tiger'. You need to keep this login credentials as it is required at a later point in the installation process.

```
C:\> cd c:\oraclexe\app\oracle\product\10.2.0\server\bin
C:\oraclexe\app\oracle\product\10.2.0\server\bin>sqlplus / as sysdba
SQL> exec dbms_xdb.sethttpport(8082);
SQL> GRANT CONNECT,RESOURCE,UNLIMITED TABLESPACE TO SCOTT IDENTIFIED BY
TIGER;
SQL> EXIT;
```

Note The Oracle Database 10g Express option is only supported on Microsoft Windows. It is not supported on UNIX systems.

Note For information about backing up the Oracle database, go to this location:
http://download.oracle.com/docs/cd/B25329_01/doc/admin.102/b25107/backrest.htm#i1004902.

You can also use the exp/imp utility at this location:
http://download.oracle.com/docs/cd/B25329_01/doc/admin.102/b25107/impexp.htm#BCEEDCIB.

If you are using the Oracle database, you need to install the Oracle JDBC (Java Database Connectivity) component for DCNM-SAN to connect to the database.

Increasing UDP Buffer Size

If the DCNM-SAN SNMP packet log shows an SNMP VarBind decode error, the UDP buffer size is low and the buffer size needs to be increased.

To increase the UDP buffer size, do the following:

Step 1 For Solaris, ensure that the UDP buffer size is at least 64 K.

```
ndd -set /dev/udp udp_recv_hiwat 65535
ndd -set /dev/udp udp_xmit_hiwat 65535
```

Step 2 Add the following setting in **/etc/system**, so that the buffer size will be in effect even after a reboot.

```
set ndd:udp_recv_hiwat=65535
set ndd:udp_xmit_hiwat=65535
```

Note Before starting the installation, make sure that you have logged in as a Superuser.

Backing up Database

The DCNM-SAN uses PostgresSQL Database as the default database. The DCNM-SAN backup utility uses PostgresSQL pg_dump utility to dump all of the database content to an ASCII dump file. Restore utility uses PostgresSQL to recreate data using the dump file.

The dump file represents a snapshot of the database at the time of backup.

To perform a backup of the DCNM-SAN database, enter these commands on Linux/Solaris. Assume INSTALLDIR is the top directory of DCNM-SAN installation.

```
cd $INSTALLDIR/bin
/pgbackup.sh 02252008.data
```

The backup file 02252008.data will be created in $INSTALLDIR/bin directory. If you want to create it in a standard backup director provide the full path name of the dump file.

To perform a backup of the DCNM-SAN database, enter these commands on Windows. Assume INSTALLDIR is the top directory of DCNM-SAN installation.

```
cd $INSTALLDIR/bin
/pgbackup.bat 02252008.data
```

The backup file 02252008.data will be created in $INSTALLDIR/bin directory. If you want to create it in a standard backup director provide the full path name of the dump file.

Note When PostgreSQL is chosen as the database, ensure that the Microsoft Windows user installing the software has administrative privileges and not the domain admin privileges. This is a prerequisite for successful installation.

For information about backing up the PostgreSQL database, run the pg_dump utility to have a good backup. For more information, go to this location:
http://www.postgresql.org/docs/8.1/static/app-pgdump.html.

Restoring Database

To restore DCNM-SAN database, you must have a good backup file, and you must stop the DCNM-SAN server before restoration. Run restore and enter these commands on Linux Solaris. Assume INSTALLDIR is the top directory of the DCNM-SAN installation.

```
cd $INSTALLDIR/bin
./FMServer.sh stop
./pgrestore.sh 02252008.data
./FMServer.sh start
```

To restore DCNM-SAN database, you must have a good backup file, and you must stop the DCNM-SAN server before restoration. Run restore and enter these commands on Windows. Assume INSTALLDIR is the top directory of the DCNM-SAN installation.

```
cd $INSTALLDIR/bin
./FMServer.bat stop
./pgrestore.bat 02252008.data
./FMServer.bat start
```

CHAPTER 1

Installing Cisco DCNM-SAN Management Software

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

Installing the Management Software

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

Note Before upgrading or uninstalling DCNM-SAN or Device Manager, make sure any instances of these applications have been shut down.

Installation options include:

- Upgrade—The installer detects your current version of DCNM-SAN and Device Manager, and it provides the option to upgrade. The default is to upgrade to the latest version of DCNM-SAN or Device Manager.
- Uninstall—If you are downgrading from Fabric Manager 2.x or later to Fabric Manager 1.3x or earlier, use the Uninstall batch file or shell script. Do not delete the MDS 9000 folder as this might prevent your installation from being upgraded in the future.

Note We recommend that you install the latest version of the DCNM-SAN applications. DCNM-SAN is backward-compatible with the Cisco MDS SAN-OS and Cisco FabricWare software running on the switches. When upgrading, upgrade the DCNM-SAN software first, and then upgrade the Cisco MDS SAN-OS or NX-OS or Cisco FabricWare software on the switch.

This section includes the following topics:

Prerequisites

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

- Users installing DCNM-SAN must have full administrator privileges to create user accounts and start services. Users should also have access to all ports. These are the ports used by DCNM-SAN Server and the PostgreSQL database: 1098, 1099, 4444, 4445, 8009, 8083, 8090, 8092, 8093, 514, 5432.
- Starting from Cisco MDS NX-OS Release 4.1(3a), DCNM-SAN is no longer packaged with a Cisco MDS 9000 Family switch.
- For switches running Cisco MDS 9000 FabricWare, you can download DCNM-SAN from Cisco.com. To download the software from Cisco.com, go to the following website: http://cisco.com/cgi-bin/tablebuild.pl/mds-fm
- When you connect to the server for the first time, DCNM-SAN checks to see if you have the correct Sun Java Virtual Machine version installed on your workstation. DCNM-SAN looks for version 1.6(x) during installation. If required, install the Sun Java Virtual Machine software.
- On Windows, remote DCNM-SAN installations or upgrades should 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 is very important if the default PostgreSQL database is used with DCNM-SAN, because this database requires the local console for all installations and upgrades.
- Before installing Cisco DCNM-SAN on a Windows Vista system, turn the User Account Control (UAC) off. To turn off UAC, select **Start > Control Panel > User Accounts > Turn User Account Control** on or off, clear the **Use User Account Control** (UAC) to help protect your computer check box, and then click OK. Click **Restart** Now to apply the change.
- Telnet Client application is not installed by default on Microsoft Windows Vista. To install Telnet Client, select **Start > Programs > Control Panel >** Click Turn Windows features on or off (if you have UAC turned on you will need to give it the permission to continue). Check the Telnet Client check box and then click **OK**.
- You can run CiscoWorks on the same PC as DCNM-SAN, even though the Java requirements are different. When installing the later Java version for DCNM-SAN, make sure it does not overwrite the earlier Java version required for CiscoWorks. Both versions of Java can coexist on your PC.

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

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

Before you can access the Cisco DCNM-SAN, 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
- Ensure you disable the default firewall on a Microsoft Windows 2008 64-bit machine before you install Cisco DCNM. To disable the firewall, use the following command:

```
netsh advfirewall set allprofiles state off
```

Cisco MDS SAN-OS Release 2.x, 3.x, and NX-OS Release 4.2(0) and later supports AAA authentication using RADIUS, TACACS, or local SNMP users.

The Cisco Device Manager software executable files reside on each supervisor module of each Cisco MDS 9000 Family switch running Cisco MDS SAN-OS or NX-OS software in your network. The supervisor module provides an HTTP server that responds to browser requests and distributes the software to Windows or UNIX network management stations. You can also find Cisco DCNM-SAN software on Cisco.com at the following website:

http://cisco.com/cgi-bin/tablebuild.pl/mds-fm

Supported Software

Note For the latest information on supported software, refer to the *Cisco DCNM Release Notes, Release 5.2*.

Cisco DCNM-SAN and Cisco Device Manager have been tested with the following software:

- Operating Systems
  - Windows Vista SP1 (Enterprise edition), Windows 2008 (32 bit and 64 bit), Windows 7
  - Red Hat Enterprise Linux Server Release 5.4 or later
  - Solaris (SPARC) 9 and 10

  Note You cannot install Cisco DCNM-SAN and DCNM-LAN Server on Windows 7 (32 bit and 64 bit) platform.

- Java
  - Sun JRE and JDK 1.6(x) is supported
  - Java Web Start 1.5 and 1.6

  Note Do not use Java 1.6 Update 13

- Browsers

  The following common web browsers that support Adobe Flash 10 are qualified to use with Cisco DCNM-LAN and DCN-SAN.

  - Internet Explorer

  - Firefox
  - Chrome
  - Safari
- Databases
  - Oracle Database 10g Express, Oracle Enterprise Edition 10g, Oracle Enterprise Edition 11g and 11g2 Enterprise Edition (Cisco recommends Oracle 11g2 Enterprise Edition for customers with large fabrics.)
  - PostgreSQL 8.1, 8.4 (Windows and Red Hat Enterprise Linux Server Release 5.4 or later)
  - PostgreSQL 8.1 (Solaris 9 and 10)
- Security
  - Cisco ACS 3.1 and 4.0
  - PIX Firewall
  - IP Tables
  - SSH v2
  - Global Enforce SNMP Privacy Encryption
  - HTTPS

Java Database Connectivity

Java database connectivity (JDBC) is the JavaSoft specification of a standard application programming interface (API) that allows Java programs to access database management systems.

A JDBC driver is a software component enabling a Java application to interact with a database. DCNM-SAN uses Oracle JDBC drivers ojdbc14.jar and ojdbc14.jar to access the Oracle database and store data.

You can download the recommended version (10.2.0.1.0) of the ojdbc14.jar file, from the following link:

http://www.oracle.com/technology/software/tech/java/sqlj_jdbc/htdocs/jdbc_10201.html

Alternatively, if you have access to the system where Oracle is installed in your environment, you can find the jar file in the Oracle installation directory under ORACLE_HOME\jdbc\lib\.

Minimum Hardware Requirements

For a PC running DCNM-SAN Server on large fabrics (1000 or more end devices), we recommend you use a Dual Core/Dual CPU high-speed system with 2 GB of RAM and 10 GB of free disk space.

Installing DCNM-SAN on Solaris

To install DCNM-SAN on Solaris, follow these steps:

Step 1 Copy the DCNM-SAN jar file dcnm-installer-k9.5.2.0.252.S2-solaris.bin from Cisco.com to a folder on the Solaris workstation.

Step 2 Change the filepermissions using the following command:

```
chmod 0700 dcnm-installer-k9.5.2.0.252.S2-solaris.bin
```

Step 3 Launch the installer using the following command:

```
./dcnm-installer-k9.5.2.0.252.S2-solaris.bin
```

Step 4 Follow the on-screen instructions provided in the DCNM-SAN management software setup wizard.

Installing DCNM-SAN on Windows

Starting from MDS NX-OS Release 4.1(3a) and later, DCNM-SAN has an express installation option. When you select this option, DCNM-SAN will be installed on your computer with a set of default user credentials. If the PostgreSQL database is not present on your computer, the installer will install PostgreSQL. If the PostgreSQL database is present, the installer will upgrade it to latest version. You may change the default credentials after the installation is complete.

This section includes the following topics:

Express Installation

To install (Express) DCNM-SAN on Windows, follow these steps:

Step 1 Click the **Install Management Software** link.

Step 2 Choose **Management Software > Cisco DCNM-SAN**.

Step 3 Click the **Installing DCNM** link.

Step 4 Click the **DCNM Installer** link.

You see the welcome message in the Cisco DCNM-SAN Installer window.

Figure 1-1 Management Software Setup Wizard

Step 5 Click **DCNM-SAN** and then click **Standalone**.

Step 6 Check the **Express (with Default Options)** check box, and then click **Next** to begin express installation.

Note DCNM-SAN express installation option uses *admin* as the user name and *password* as the user password. The user may change the password after the installation is complete.

Note DCNM-SAN express installation option installs the PostgreSQL database with *dcnmuser* as the user name and *password_1_2_3* as the user password. The user may change the password after the installation is complete.

You see the default credentials in the Cisco DCNM-SAN Installer window shown in Figure 1-2.

Figure 1-2 Default User Credentials

Step 7 Click **Install**.

Once the installation is finished, you see an installation completed message in the Cisco DCNM-SAN Installer window shown in Figure 1-3.

Figure 1-3 Install Complete

Note You can choose to launch DCNM-SAN or Device Manager by checking the Launch DCNM-SAN or Launch Device Manager check boxes. Icons for DCNM-SAN and Device Manager are automatically created on the desktop.

Step 8 Click **Finish** to close the Cisco DCNM-SAN Installer window.

Custom Installation

To install (Custom) DCNM-SAN on Windows, follow these steps:

Step 1 Click the **Install Management Software** link.

Step 2 Choose **Management Software > Cisco DCNM-SAN**.

Step 3 Click the **Installing DCNM** link.

Step 4 Click the **DCNM Installer** link.

You see the introduction message in the Cisco DCNM-SAN Installer window shown in Figure 1-4.

Figure 1-4 Introduction Screen

Step 5 Click the **Next** to begin the installation.

You see the Installation Help window as shown in Figure 1-5.

Figure 1-5 Introduction Help

Step 6 Click **Next**.

You see the Choose Installation Settings window as shown in Figure 1-6

Figure 1-6 Choose Installation Settings

Step 7 Check the DCNM-SAN checkbox and then click the radio button for either:

a. DCNM-SAN Server (Licensed) to install the server components for DCNM-SAN Server.

Add Server to an existing server federation to add the server to an already existing server federation.

SMIS to enable the SMIS option for the server.

b. DCNM-SAN Standalone to install the standalone version of DCNM-SAN.

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.

Note DCNM-SAN Standalone is a single application containing DCNM-SAN Client and a local version of DCNM-SAN Server bundled together. DCNM-SAN Standalone allows you to discover and monitor the immediate fabric.

Step 8 Select an installation folder on your workstation for DCNM-SAN.

On Windows, the default location is **C:\Program Files\Cisco Systems**. On a UNIX (Solaris or Linux) machine, the installation path name is **/usr/local/cisco/dcm** or **$HOME/dcm**, depending on the permissions of the user doing the installation.

Step 9 Click **Next**.

You see the Database Options dialog box shown in Figure 1-7.

Figure 1-7 Database Options Dialog Box

Step 10 Click the radio button for either Install PostgreSQL or Use existing DB to specify which database you want to use.

If you choose Install PostgreSQL, accept the defaults and enter a password. The PostgreSQL database will be installed.

Note If you choose to install PostgreSQL, you must disable any security software you are running, because PostgreSQL may not install certain folders or users.

Note Before you install PostgreSQL, remove the **cygwin/bin** from your environment variable path if Cygwin is running on your system.

Step 11 If you select Use existing DB, click the radio button for either PostgreSQL 8.1/8.2 or Oracle10/11g.

Step 12 Click **Next** in the Database Options dialog box.

You see the Local User Credentials dialog box shown in Figure 1-8.

Figure 1-8 Local User Credentials Dialog Box

Step 13 Enter a user name and password and click **Next**.

You see the Authentication Options dialog box shown in Figure 1-9.

Figure 1-9 Authentication Options Dialog Box

Step 14 Choose an authentication mode (Local, RADIUS or TACACS) and click **Next**.

Step 15 Click **Verify** to test your login.

You see the Configuration Options dialog box for DCNM-SAN Standalone shown in Figure 1-10.

Figure 1-10 Configuration Options Dialog Box for DCNM-SAN Standalone

Step 16 Check the Use HTTPS Web Server check box as desired.

Step 17 Click **Advanced Settings** to configure security settings.

Note You can change the DCNM-SAN Server port number to a port that is not used by any other application.

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.

Note If you check the **Use HTTPS Web Server** check box, the Web Server Port field is grayed out and the default port is 443.

Note If you select a specific IP address during installation and change the server host IP address, you must modify the following two files that are all located in the $INSTALL/conf directory. Change **server.bindaddrs** to the new IP address in the server.properties file and change **wrapper.app.parameter.4** to the new IP address in the FMServer.conf file.

Step 18 Check the Require SNMPv3 and Disable SNMPv2c check box for enhanced security and then click OK.

Step 19 Click **Next** in the Configuration Options dialog box.

You see the Pre-Installation Summary window as shown in Figure 1-11.

Figure 1-11 Pre-Installation Summary

Step 20 Click **Next**.

Once the installation is completed, you see an installation completed message in the Cisco DCNM-SAN Installer window shown in Figure 1-12.

Figure 1-12 Install Complete

Figure 1-13 Install Complete

Step 21 Click **Done** to close the Cisco DCNM-SAN Installer window.

On a UNIX (Solaris or Linux) machine, shell scripts are created in the install directory. The shell scripts that run the programs equivalent to the Windows services are FMServer.sh, all the server-side data and Performance Manager data are stored in the install directory.

DCNM-SAN Client cannot run without DCNM-SAN Server. The server component is downloaded and installed when you download and install DCNM-SAN. On a Windows machine you install the DCNM-SAN Server as a service. This service can then be administered using Services in the Microsoft Windows Control Panel. The default setting for the DCNM-SAN Server service is that the server is automatically started when the machine is rebooted. You can change this behavior by modifying the properties in Services.

Importing PM Statitics Data to DCNM-SAN

To manually import existing Performance Manager statistics data to DCNM-SAN, follow these steps:

Step 1 Stop the DCNM-SAN Server.

Step 2 Copy the existing RRD file (from a prior installation) to $INSTALLDIR/pm/db.

Step 3 Run the $INSTALLDIR/bin/pm.bat s.

Step 4 Restart the DCNM-SAN Server.

Step 5 Add the fabric to the Performance Manager collection using WebClient.

Creating DCNM-SAN Shortcut Manually

The DCNM-SAN shortcut on the desktop is available only when launching the application for the first time. The shortcut is not offered when you lauch DCNM-SAN from the DCNM download page.

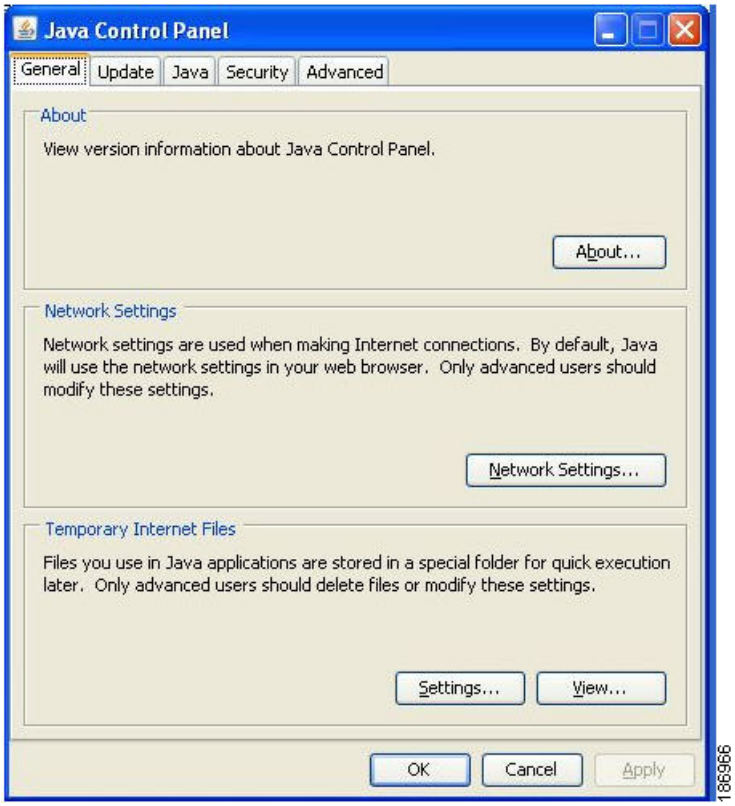
To create DCNM-SAN shortcut on the desktop, follow these steps:

Step 1 Navigate to **Control Panel> Java**.

Double-click Java.

The Java Control Panel displays as shown in the Figure 1-14.

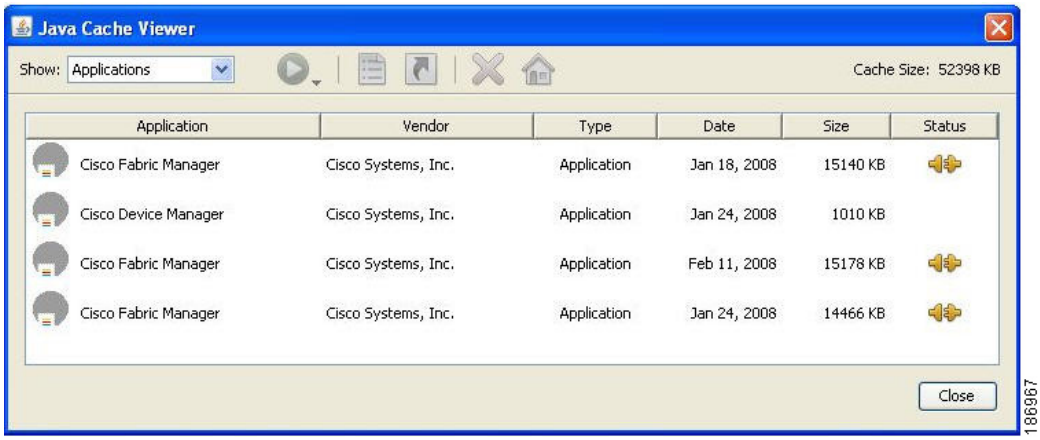
Figure 1-14 Java Control Panel Dialog Box



Step 2 In the **Temporary Internet Files** area, click **View**.

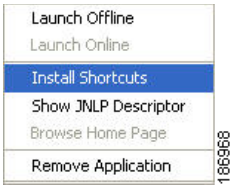
The **Java Cache Viewer** dialog box displays as shown in Figure 1-15.

Figure 1-15 Java Cache Viewer Dialog Box



Step 3 To recreate the shortcut, right-click on the application, and select **Install Shortcuts** from the shortcut menu, as shown in Figure 1-16.

Figure 1-16 Shortcut Menu



Upgrading DCNM-SAN

This section includes the following topics:

- Upgrading Fabric Manager in Cisco SAN-OS Releases Prior to 3.1(2b), page 1-17
- Upgrading Fabric Manager in Cisco SAN-OS Releases 3.1(2b) and Later to 3.2(1), page 1-17
- Upgrading Fabric Manager Server and Fabric Manager Standalone Version Using the Fabric Manager Update Installer, page 1-18

Upgrading Fabric Manager in Cisco SAN-OS Releases Prior to 3.1(2b)

When you install Cisco Fabric Manager 3.2(1), data is migrated from the Hypersonic HSQL database to either the PostgreSQL database or Oracle Database 10g Express during the installation. To install the PostgreSQL database on Windows, click the FM Installer link on the CD.

Note If you are upgrading a previous installation of DCNM-SAN Server, be sure the previous installation of the database is running. Do not uninstall the previous version. If the previous version is uninstalled, the database will not be migrated and your server settings will not be preserved. After you ensure that the previous installation is running, follow the steps listed in the "Installing the Management Software" section on page 1-1. Before beginning the upgrade, you must close DCNM-SAN and Device Manager.

Upgrading Fabric Manager in Cisco SAN-OS Releases 3.1(2b) and Later to 3.2(1)

When you install Cisco SAN-OS 3.2(1), data is migrated from the Hypersonic HSQL database to either the PostgreSQL database or Oracle Database 10g Express during the installation. Data is also migrated from Oracle to Oracle.

Note If you migrate the database from Oracle to Oracle, the schema is updated as required by Cisco SAN-OS 3.2(1).

To install the PostgreSQL database on Windows, click the FM Installer link on the CD. To install Oracle Database 10g Express, follow the instructions in the "Installing Oracle" section on page 1-3.

Upgrading the Management Software

If you log into a switch running Cisco MDS SAN-OS with Device Manager and that switch has a later version of the management software, you are prompted to install the later version. To upgrade the Cisco MDS DCNM-SAN software, follow the instructions described in the "Installing the Management Software" section on page 1-1. You can also upgrade Device Manager at any time by entering the IP address or host name of the supervisor module with the later version of software in the Address field of your browser. You will need a new CD to upgrade DCNM-SAN.

Note As of Cisco MDS SAN-OS Release 3.x, downgrades are not supported through the installer. To downgrade DCNM-SAN or Device Manager to an earlier release, you need to manually uninstall first and then reinstall the previous version of DCNM-SAN or Device Manager.

Upgrading DCNM-SAN Federated Server

To upgrade DCNM-SAN federated server on Linux and Solaris machines, follow these steps:

Step 1 Log on to the server node in the federation.

Step 2 Run **$INSTALLDIR/FMServer.sh stop** to stop the server node.

Step 3 Run the dcnm-installer-k9.5.2.0.252.S2.exe (java -Xmx512m -jar dcnm-installer-k9.5.2.0.252.S2.jar) on the first server node to upgrade the first server in the federation.

Step 4 Repeat steps 1 through step 3 on all the other servers nodes.

To upgrade DCNM-SAN federated server on a Windows machine, follow these steps:

Step 1 Log on to the server node in the federation.

Step 2 Stop the DCNM-SAN Server service. To stop the DCNM-SAN Server service, click **Start** > **Control Panel** > **Administrative Tools** > **Services**.

Step 3 Right-click Cisco DCNM-SAN Server services in the services window, and then click **Stop** to stop the services.

Step 4 Repeat step 1 through step 3 on all the server nodes.

Step 5 Run the **dcnm-installer-k9.5.2.0.252.S2.jar** (java -Xmx512m -dcnm-installer-k9.5.2.0.252.S2.jar) on the first server node to upgrade the first server.

Step 6 Repeat step 5 on all the other server nodes.

Upgrading Fabric Manager Server and Fabric Manager Standalone Version Using the Fabric Manager Update Installer

As of Release 3.3(1a), you can use the Cisco MDS 9000 Fabric Manager Update Installer to upgrade:

- Fabric Manager Server

- Fabric Manager Standalone

The Fabric Manager Update Installer is smaller in size than the Fabric Manager installer which makes it easier to download. The update Installer has limited capability to upgrade Fabric Manager Server or the Fabric Manager Standalone version and it does not have the capability to install a database or the Fabric Manager Server infrastructure (JBoss). Table 1-1 shows the recommended Fabric Manager upgrade paths.

Table 1-1 Fabric Manager Upgrade Path Using Update Installer

Current Version	Upgrading To	Upgrade Path
3.0(x)[1]	3.3(1a) or above	**1.** Upgrade to 3.1(x). **2.** Upgrade to 3.2(x). **3.** Upgrade to 3.3(x) or above by launching the update installer {**java –Xmx512m –jar jar_file_name**} and then follow the steps to upgrade Fabric Manager. **Note** Change the server port to 9099 if you are not upgrading from Release 3.2(2c) in Step 2.
3.1(x)[1]	3.3(1a) or above	**1.** Upgrade to 3.2(x). **2.** Upgrade to 3.3(x) or above by launching the update installer {**java –Xmx512m –jar jar_file_name**} and then follow the steps to upgrade Fabric Manager. **Note** Change the server port to 9099 if you are not upgrading from Release 3.2(2c) in Step 1.
3.2(x)	3.3(1a) or above	**1.** Upgrade to 3.3(x) or above by launching the update installer{**java –Xmx512m –jar jar_file_name**} and then follow the steps to upgrade Fabric Manager. **Note** Change the server port to 9099 if you are not upgrading from Release 3.2(2c).
3.3(x)	NX-OS 4.1(1b)	**1.** Upgrade to 4.1(x) or above by launching the update installer {**java –Xmx512m –jar jar_file_name**} and then follow the steps to upgrade Fabric Manager. **Note** Change the server port to 9099 if you are not upgrading from Release 3.4(x).

1. The gateway upgrade needs to be performed as the HSQL database data cannot be migrated to the new database.

⚠ You should not discover another fabric, re-discover the upgraded fabric or close the fabric when the upgrade is running.

Integrating Cisco DCNM-SAN with Other Management Tools

You can use DCNM-SAN, Device Manager, and Performance Manager with these management tools:

- **Cisco Traffic Analyzer**—Allows you to break down traffic by VSANs and protocols and to examine SCSI traffic at a logical unit number (LUN) level.
- **Cisco Protocol Analyzer**—Enables you to examine actual sequences of Fibre Channel frames easily using the Fibre Channel and SCSI decoders Cisco developed for Ethereal.
- **Cisco Port Analyzer Adapter 2**—Encapsulates SPAN traffic (both Fibre Channel control and data plane traffic) in an Ethernet header for transport to a Windows PC or workstation for analysis. Both the Cisco Traffic Analyzer and Cisco Protocol Analyzer require the PAA to transport MDS SPAN traffic to a Windows PC or workstation.

For more information on these tools and how they work together with the Cisco DCNM-SAN management applications, see *Cisco MDS 9000 Family NX-OS Troubleshooting Guide*.

Running DCNM-SAN Behind a Firewall

For Windows PCs running DCNM-SAN, Device Manager, and Performance Manager behind a firewall, certain ports need to be available.

By default, DCNM-SAN Client and Device Manager use the first available UDP port for sending and receiving SNMP responses. The UDP SNMP trap local ports are 1162 for DCNM-SAN, and 1163 or 1164 for Device Manager. DCNM-SAN Server also opens TCP RMI port 9099.

In Fabric Manager Release 2.1(2) or later, you can select the UDP port that Fabric Manager Client or Device Manager uses for SNMP responses by uncommenting the following statement:

- On a Windows desktop, uncomment the following in the FabricManager.bat or DeviceManager.bat file in the C:\Program Files\Cisco Systems\MDS9000\bin directory:

```
rem JVMARGS=%JVMARGS% -Dsnmp.localport=9001
```

- On a UNIX desktop, uncomment the following in the FabricManager.sh or DeviceManager.sh file in the $HOME/.cisco_mds9000/bin directory:

```
# JVMARGS=$JVMARGS -Dsnmp.localport=9001
```

In Fabric Manager Release 3.2(1) or later, Fabric Manager Client initiates communication with Fabric Manager Server on the port 9099 for Java Naming Directory and Interface (JNDI) lookup. Fabric Manager Server redirects the client to 1098 and JBoss directs the request to the appropriate service.

Fabric Manager Server proxy services uses a configurable TCP port (9198 by default) for SNMP communications between the Fabric Manager Client or Device Manager and Fabric Manager Server.

The Fabric Manager Server component requires two predictable TCP ports to be opened on the firewall for an incoming connection:

- server.port = 9099

- server.data.port = 9100

As long as these two ports are open, Fabric Manager Client can connect to the server. Other TCP ports connected to Fabric Manager Client are initiated by the server, which is behind the firewall.

The following table lists all ports used by DCNM-SAN applications:

Communication Type	Port(s) Used
Used by All Applications	
SSH	Port 22 (TCP)
Telnet	Port 23 (TCP)
HTTP	Port 80 (TCP)
TFTP	Port 69 (UDP)
SNMP	Port 161 (UDP)
Syslog	Port 514 (UDP)
Used by DCNM-SAN Server and Performance Manager	
SNMP_TRAP	Port 2162 (UDP)
SNMP	Picks a random free local port (UDP) or 9198 (TCP) if SNMP proxy is enabled. Can be changed in server.properties.
Java RMI	Ports 9099, 9100 (TCP)
Used by DCNM-SAN Client	
SNMP	Picks a random free local port (UDP) if SNMP proxy is enabled. Can be changed with the client -Dsnmp.localport option.
Java RMI	Picks a free local port between 19199 and 19399 (TCP). Can be changed with the client -Dclient.portStart and -Dclient.portEnd options. For example, -Dclient.portStart = 19199 -Dclient.portEnd = 19399.
Used by Device Manager	
SNMP_TRAP	Picks a free local port between 1163 and 1170 (UDP).
SNMP	Picks a random free local port (UDP) or 9198 (TCP) if SNMP proxy is enabled. Can be changed in **server.properties**.

Port(s) Used/Type	Service Descriptor	Service Name	Attribute Name	Description
1098 (TCP)	conf/jboss-service.xml	jboss:service=Naming	RMI Naming Service Port	This port is for JNDI based naming services. The client look up this port for JNDI binding objects and resources.
9099 (TCP)	conf/jboss-service.xml	jboss:service=Naming	Bootstrap JNP Port (FM changed 1099 to 9099)	This port is for JNDI based naming services. The client look up this port for JNDI binding objects and resources.

4444 (TCP)	conf/jboss-service.xml	jboss:service=invoker,type=jrmp	RMI /JRMP ObjectPort	The org.jboss.invocation.jrmp.server.JRMPInvoker class is an MBean service that provides the RMI/JRMP implementation of the Invoker interface. The JRMPInvoker exports itself as an RMI server so that when it is used as the Invoker in a remote client, the JRMPInvoker stub is sent to the client instead.
4445 (TCP)	conf/jboss-service.xml	jboss:service=invoker,type=pooled	Pooled Invoker	The org.jboss.invocation.pooled.server.PooledInvoker is an MBean service that provides RMI over a custom socket transport implementation of the Invoker interface. The PooledInvoker exports itself as an RMI server so that when it is used as the Invoker in a remote client, the PooledInvoker stub is sent to the client instead and invocations use the a custom socket protocol.
8009 (TCP)	deploy/jbossweb-tomcat41.sar/META-INF/jboss-service.xml	jboss.web:service=WebServer?	AJP Connector	The AJP Connector element represents a Connector component that communicates with a web connector via the AJP protocol. This is used for invisibly integrating JBoss Web into an existing or a new Apache server.
8083 (TCP)	conf/jboss-service.xml	jboss:service=WebService	RMI dynamic class loader port	The WebService MBean provides dynamic class loading for RMI access to the server EJBs. Used for web service
8092 (TCP)	deploy/jms/oil2-service.xml	jboss.mq:service=InvocationLayer?,type=OIL2	Optimized Invocation Layer for JMS	This port is used for JBossMQ services. JBossMQ is composed of several services working together to provide JMS API level services to client applications. Optimized Invocation Layer is a service used by JMS client.
8093 (TCP)	deploy/jms/uil2-service.xml	jboss.mq:service=InvocationLayer?,type=UIL2	Unified Invocation Layer for JMS	This port is used for JBossMQ services. JBossMQ is composed of several services working together to provide JMS API level services to client applications. Unified Invocation Layer is a service used by JMS client.
3873 (TCP)	Service end point for EJB3 aspect service	JBoss EJB3 Aspect Service Deployer	JBoss EJB3 Invoker	This port used by the client to communicate with EJB3(Enterprise JavaBean 3.0) services on JBoss Server.

DCNM-SAN Server Proxy Services

The DCNM-SAN Client and Device Manager use SNMP to communicate with the DCNM-SAN Server. In typical configurations, the DCNM-SAN Server may be installed behind a firewall. The SNMP proxy service available in Cisco Fabric Manager Release 2.1(1a) or later provides a TCP-based transport proxy for these SNMP requests. The SNMP proxy service allows you to block all UDP traffic at the firewall and configure DCNM-SAN Client to communicate over a configured TCP port.

DCNM-SAN uses the CLI for managing some features on the switches. These management tasks are used by DCNM-SAN and do not use the proxy services. Your firewall must remain open for CLI access for the following features:

- External and internal loopback test
- Flash files
- Create CLI user
- Security - ISCSI users
- Show image version
- Show tech
- Switch resident reports (syslog, accounting)
- Zone migration
- Show cores

If you are using the SNMP proxy service and another application on your server is using port 9198, you need to modify your workstation settings.

Note The MDS switch always checks the local SNMP users before the remote AAA users, unlike the CLI.

To modify a Windows workstation, follow these steps:

Step 1 Open Internet Explorer and select **Tools > Internet Options**.

You see the Internet Options dialog box.

Step 2 Select the **Connections** tab and click **LAN Settings**.

You see the LAN Settings dialog box.

Step 3 Check the **Use a Proxy Server for your LAN** check box and click **Advanced**.

Step 4 Add your server IP Address or local host under the Exceptions section.

Step 5 Click **OK** to save your changes.

CHAPTER 1

Maintaining Cisco DCNM-SAN

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

Upgrading Cisco DCNM-SAN

This section includes the following topics:

Upgrading Fabric Manager in Cisco SAN-OS Releases Prior to 3.1(2b)

When you install Cisco Fabric Manager 3.2(1), data is migrated from the Hypersonic HSQL database to either the PostgreSQL database or Oracle Database 10g Express during the installation. To install the PostgreSQL database on Windows, click the FM Installer link on the CD. To install Oracle Database 10g Express, follow the instructions in the "Installing Oracle" section on page 1-3.

Note If you are upgrading a previous installation of DCNM-SAN Server, be sure the previous installation of the database is running. Do not uninstall the previous version. If the previous version is uninstalled, the database will not be migrated and your server settings will not be preserved. After you ensure that the previous installation is running, follow the steps listed in the "Installing the Management Software" section on page 1-1. Before beginning the upgrade, you must close DCNM-SAN, Device Manager, and DCNM-LAN. For more information on DCNM-LAN, see Upgrading Cisco DCNM-LAN Servers, page 1-2.

Upgrading Fabric Manager in Cisco SAN-OS Releases 3.1(2b) and Later to 3.2(1)

When you install Cisco SAN-OS 3.2(1), data is migrated from the Hypersonic HSQL database to either the PostgreSQL database or Oracle Database 10g Express during the installation. Data is also migrated from Oracle to Oracle.

Note If you migrate the database from Oracle to Oracle, the schema is updated as required by Cisco SAN-OS 3.2(1).

To install the PostgreSQL database on Windows, click the FM Installer link on the CD. To install Oracle Database 10g Express, follow the instructions in the "Installing Oracle" section on page 1-3.

Upgrading the Management Software

If you log into a switch running Cisco MDS SAN-OS with Device Manager and that switch has a later version of the management software, you are prompted to install the later version. To upgrade the Cisco MDS DCNM-SAN software, follow the instructions described in the "Upgrading Cisco DCNM-SAN" section on page 1-1. You can also upgrade Device Manager at any time by entering the IP address or host name of the supervisor module with the later version of software in the Address field of your browser. You will need a new CD to upgrade DCNM-SAN.

Note As of Cisco MDS SAN-OS Release 3.x, downgrades are not supported through the installer. To downgrade DCNM-SAN or Device Manager to an earlier release, you need to manually uninstall first and then reinstall the previous version of DCNM-SAN or Device Manager.

Upgrading DCNM-SAN Federated Server

To upgrade DCNM-SAN federated server on Linux and Solaris machines, follow these steps:

Step 1 Log on to the server node in the federation.

Step 2 Run **$INSTALLDIR/FMServer.sh stop** to stop the server node.

Step 3 Run the **dcnm-installer-k9.5.2.0.252.S2.jar** (java -Xmx512m -jar dcnm-installer-k9.5.2.0.252.S2.jar) on the first server node to upgrade the first server in the federation.

Step 4 Repeat steps 1 through step 3 on all the other servers nodes.

To upgrade DCNM-SAN federated server on a Windows machine, follow these steps:

Step 1 Log on to the server node in the federation.

Step 2 Stop the DCNM-SAN Server service. To stop the DCNM-SAN Server service, click **Start** > **Control Panel** > **Administrative Tools** > **Services**.

Step 3 Right-click Cisco DCNM-SAN Server services in the services window, and then click **Stop** to stop the services.

Step 4 Repeat step 1 through step 3 on all the server nodes.

Step 5 Run the **dcnm-installer-k9.5.2.0.252.S2.jar** (java -Xmx512m -jar dcnm-installer-k9.5.2.0.252.S2.jar) on the first server node to upgrade the first server.

Step 6 Repeat step 5 on all the other server nodes.

Upgrading Fabric Manager Server and Fabric Manager Standalone Version Using the Fabric Manager Update Installer

As of Release 3.3(1a), you can use the Cisco MDS 9000 Fabric Manager Update Installer to upgrade:

- Fabric Manager Server
- Fabric Manager Standalone

The Fabric Manager Update Installer is smaller in size than the Fabric Manager installer which makes it easier to download. The update Installer has limited capability to upgrade Fabric Manager Server or the Fabric Manager Standalone version and it does not have the capability to install a database or the Fabric Manager Server infrastructure (JBoss). Table 1-1 shows the recommended Fabric Manager upgrade paths.

Table 1-1 Fabric Manager Upgrade Path Using Update Installer

Current Version	Upgrading To	Upgrade Path
3.0(x)[1]	3.3(1a) or above	**1.** Upgrade to 3.1(x). **2.** Upgrade to 3.2(x). **3.** Upgrade to 3.3(x) or above by launching the update installer {**java –Xmx512m –jar jar_file_name**} and then follow the steps to upgrade Fabric Manager. **Note** Change the server port to 9099 if you are not upgrading from Release 3.2(2c) in Step 2.
3.1(x)[1]	3.3(1a) or above	**1.** Upgrade to 3.2(x). **2.** Upgrade to 3.3(x) or above by launching the update installer {**java –Xmx512m –jar jar_file_name**} and then follow the steps to upgrade Fabric Manager. **Note** Change the server port to 9099 if you are not upgrading from Release 3.2(2c) in Step 1.

Table 1-1 Fabric Manager Upgrade Path Using Update Installer

Current Version	Upgrading To	Upgrade Path
3.2(x)	3.3(1a) or above	1. Upgrade to 3.3(x) or above by launching the update installer{**java –Xmx512m –jar jar_file_name**} and then follow the steps to upgrade Fabric Manager. **Note** Change the server port to 9099 if you are not upgrading from Release 3.2(2c).
3.3(x)	NX-OS 4.1(1b)	1. Upgrade to 4.1(x) or above by launching the update installer {**java –Xmx512m –jar jar_file_name**} and then follow the steps to upgrade Fabric Manager. **Note** Change the server port to 9099 if you are not upgrading from Release 3.4(x).

1. The gateway upgrade needs to be performed as the HSQL database data cannot be migrated to the new database.

You should not discover another fabric, re-discover the upgraded fabric or close the fabric when the upgrade is running.

Integrating Cisco DCNM-SAN with Other Management Tools

You can use DCNM-SAN, Device Manager, and Performance Manager with these management tools:

- **Cisco Traffic Analyzer**—Allows you to break down traffic by VSANs and protocols and to examine SCSI traffic at a logical unit number (LUN) level.
- **Cisco Protocol Analyzer**—Enables you to examine actual sequences of Fibre Channel frames easily using the Fibre Channel and SCSI decoders Cisco developed for Ethereal.
- **Cisco Port Analyzer Adapter 2**—Encapsulates SPAN traffic (both Fibre Channel control and data plane traffic) in an Ethernet header for transport to a Windows PC or workstation for analysis. Both the Cisco Traffic Analyzer and Cisco Protocol Analyzer require the PAA to transport MDS SPAN traffic to a Windows PC or workstation.

For more information on these tools and how they work together with the Cisco DCNM-SAN management applications, see *Cisco MDS 9000 Family NX-OS Troubleshooting Guide*.

Running DCNM-SAN Behind a Firewall

For Windows PCs running DCNM-SAN, Device Manager, and Performance Manager behind a firewall, certain ports need to be available.

By default, DCNM-SAN Client and Device Manager use the first available UDP port for sending and receiving SNMP responses. The UDP SNMP trap local ports are 1162 for DCNM-SAN, and 1163 or 1164 for Device Manager. DCNM-SAN Server also opens TCP RMI port 9099.

In Fabric Manager Release 2.1(2) or later, you can select the UDP port that Fabric Manager Client or Device Manager uses for SNMP responses by uncommenting the following statement:

- On a Windows desktop, uncomment the following in the FabricManager.bat or DeviceManager.bat file in the C:\Program Files\Cisco Systems\MDS9000\bin directory:

  ```
  rem JVMARGS=%JVMARGS% -Dsnmp.localport=9001
  ```

- On a UNIX desktop, uncomment the following in the FabricManager.sh or DeviceManager.sh file in the $HOME/.cisco_mds9000/bin directory:

  ```
  # JVMARGS=$JVMARGS -Dsnmp.localport=9001
  ```

In Fabric Manager Release 3.2(1) or later, Fabric Manager Client initiates communication with Fabric Manager Server on the port 9099 for Java Naming Directory and Interface (JNDI) lookup. Fabric Manager Server redirects the client to 1098 and JBoss directs the request to the appropriate service.

Fabric Manager Server proxy services uses a configurable TCP port (9198 by default) for SNMP communications between the Fabric Manager Client or Device Manager and Fabric Manager Server.

The Fabric Manager Server component requires two predictable TCP ports to be opened on the firewall for an incoming connection:

- server.port = 9099
- server.data.port = 9100

As long as these two ports are open, Fabric Manager Client can connect to the server. Other TCP ports connected to Fabric Manager Client are initiated by the server, which is behind the firewall.

The following table lists all ports used by DCNM-SAN applications:

Communication Type	Port(s) Used
Used by All Applications	
SSH	Port 22 (TCP)
Telnet	Port 23 (TCP)
HTTP	Port 80 (TCP)
TFTP	Port 69 (UDP)
SNMP	Port 161 (UDP)
Syslog	Port 514 (UDP)
Used by DCNM-SAN Server and Performance Manager	
SNMP_TRAP	Port 2162 (UDP)
SNMP	Picks a random free local port (UDP) or 9198 (TCP) if SNMP proxy is enabled. Can be changed in server.properties.
Java RMI	Ports 9099, 9100 (TCP)
Used by DCNM-SAN Client	
SNMP	Picks a random free local port (UDP) if SNMP proxy is enabled. Can be changed with the client -Dsnmp.localport option.
Java RMI	Picks a free local port between 19199 and 19399 (TCP). Can be changed with the client -Dclient.portStart and -Dclient.portEnd options. For example, -Dclient.portStart = 19199 -Dclient.portEnd = 19399.
Used by Device Manager	

Communication Type	Port(s) Used
SNMP_TRAP	Picks a free local port between 1163 and 1170 (UDP).
SNMP	Picks a random free local port (UDP) or 9198 (TCP) if SNMP proxy is enabled. Can be changed in **server.properties**.

Port(s) Used/Type	Service Descriptor	Service Name	Attribute Name	Description
1098 (TCP)	conf/jboss-service.xml	jboss:service=Naming	RMI Naming Service Port	This port is for JNDI based naming services. The client look up this port for JNDI binding objects and resources.
9099 (TCP)	conf/jboss-service.xml	jboss:service=Naming	Bootstrap JNP Port (FM changed 1099 to 9099)	This port is for JNDI based naming services. The client look up this port for JNDI binding objects and resources.
4444 (TCP)	conf/jboss-service.xml	jboss:service=invoker,type=jrmp	RMI /JRMP ObjectPort	The org.jboss.invocation.jrmp.server.JRMPInvoker class is an MBean service that provides the RMI/JRMP implementation of the Invoker interface. The JRMPInvoker exports itself as an RMI server so that when it is used as the Invoker in a remote client, the JRMPInvoker stub is sent to the client instead.
4445 (TCP)	conf/jboss-service.xml	jboss:service=invoker,type=pooled	Pooled Invoker	The org.jboss.invocation.pooled.server.PooledInvoker is an MBean service that provides RMI over a custom socket transport implementation of the Invoker interface. The PooledInvoker exports itself as an RMI server so that when it is used as the Invoker in a remote client, the PooledInvoker stub is sent to the client instead and invocations use the a custom socket protocol.
8009 (TCP)	deploy/jbossweb-tomcat41.sar/META-INF/jboss-service.xml	jboss.web:service=WebServer?	AJP Connector	The AJP Connector element represents a Connector component that communicates with a web connector via the AJP protocol. This is used for invisibly integrating JBoss Web into an existing or a new Apache server.
8083 (TCP)	conf/jboss-service.xml	jboss:service=WebService	RMI dynamic class loader port	The WebService MBean provides dynamic class loading for RMI access to the server EJBs. Used for web service

8092 (TCP)	deploy/jms/oil2-service.xml	jboss.mq:service=InvocationLayer?,type=OIL2	Optimized Invocation Layer for JMS	This port is used for JBossMQ services. JBossMQ is composed of several services working together to provide JMS API level services to client applications. Optimized Invocation Layer is a service used by JMS client.
8093 (TCP)	deploy/jms/uil2-service.xml	jboss.mq:service=InvocationLayer?,type=UIL2	Unified Invocation Layer for JMS	This port is used for JBossMQ services. JBossMQ is composed of several services working together to provide JMS API level services to client applications. Unified Invocation Layer is a service used by JMS client.
3873 (TCP)	Service end point for EJB3 aspect service	JBoss EJB3 Aspect Service Deployer	JBoss EJB3 Invoker	This port used by the client to communicate with EJB3(Enterprise JavaBean 3.0) services on JBoss Server.

DCNM-SAN Server Proxy Services

The DCNM-SAN Client and Device Manager use SNMP to communicate with the DCNM-SAN Server. In typical configurations, the DCNM-SAN Server may be installed behind a firewall. The SNMP proxy service available in Cisco Fabric Manager Release 2.1(1a) or later provides a TCP-based transport proxy for these SNMP requests. The SNMP proxy service allows you to block all UDP traffic at the firewall and configure DCNM-SAN Client to communicate over a configured TCP port.

DCNM-SAN uses the CLI for managing some features on the switches. These management tasks are used by DCNM-SAN and do not use the proxy services. Your firewall must remain open for CLI access for the following features:

- External and internal loopback test
- Flash files
- Create CLI user
- Security - ISCSI users
- Show image version
- Show tech
- Switch resident reports (syslog, accounting)
- Zone migration
- Show cores

If you are using the SNMP proxy service and another application on your server is using port 9198, you need to modify your workstation settings.

Note The MDS switch always checks the local SNMP users before the remote AAA users, unlike the CLI.

To modify a Windows workstation, follow these steps:

Step 1 Open Internet Explorer and select **Tools > Internet Options**.

You see the Internet Options dialog box.

Step 2 Select the **Connections** tab and click **LAN Settings**.

You see the LAN Settings dialog box.

Step 3 Check the **Use a Proxy Server for your LAN** check box and click **Advanced**.

Step 4 Add your server IP Address or local host under the Exceptions section.

Step 5 Click **OK** to save your changes.

CHAPTER 1

Uninstalling Cisco MDS NX-OS and DCNM-SAN

This chapter describes about installing Cisco DCNM-SAN components and contains the following section:

Uninstalling the Management Software

To uninstall the Cisco DCNM-SAN applications on a Microsoft Windows PC, follow these steps:

Detailed Steps

Step 1 Close all running instances of Cisco DCNM-SAN and Device Manager.

Step 2 Select **Start > Programs > Cisco DCNM Server > Uninstall_DCNM**.

Alternatively, you can run the following executable file:

```
INSTALL_DIR\dcm\dcnm\Uninstall_DCNM\Uninstall DCNM.exe
```

where the default *INSTALL_DIR* value is C:\Program Files\Cisco Systems.

Step 3 Click **Uninstall**.

Step 4 Click **Done**.

Note When you uninstall Cisco DCNM-SAN Server, only Cisco DCNM-SAN client is removed. Jboss and the database, either PostgreSQL or Oracle, are not removed because they might be shared with other applications such as Cisco DCNM-SAN.

Note If you have installed Cisco DCNM-SAN or Device Manager on Windows Vista, you may see the application shortcuts on your desktop even after uninstalling the application. To remove the shortcuts, you need to refresh the desktop.

Note If the DCNM-SAN Client fails to uninstall with an error message, you may need to remove the DCNM-SAN Client from cache using Java Cache Viewer. To remove DCNM-SAN Client from cache, select Start > Run and enter javaws -viewer. Select DCNM-SAN Client in the java cache viewer and click delete.

Note For older installations, delete the .cisco_mds9000 folder. Manually delete all desktop icons and program menu items.

On a Windows PC, this folder is created under the Documents and Settings folder (for example, d:\Documents and Settings\Administrator\.cisco_mds9000 if you had installed it as user Administrator). On a UNIX machine, the default installation folder is /usr/bin.

To uninstall the DCNM-SAN applications on a UNIX machine, use the Uninstall_DCNM script, as follows:

```
sh Uninstall_DCNM
```

You can find this script in your home folder or the folder that you specified when setting up the link folder during your installation of Cisco DCNM-SAN.

Note For all releases starting with Release 2.x, run the shell script $HOME/cisco_mds9000/Uninstall.sh or /usr/local/cisco_mds9000/uninstall.sh, depending on where DCNM-SAN was installed. You can find this script in your home folder or the folder that you specified when setting up the link folder during your installation of Cisco DCNM-SAN.

Note For all releases starting with Release 1.3(1), run the shell script $HOME/.cisco_mds9000/Uninstall.sh or /usr/local/.cisco_mds9000/uninstall.sh, depending on where DCNM-SAN was installed.
For earlier installations, delete the $HOME/.cisco_mds9000 folder.

Note To uninstall DCNM-SAN Federated Server, on a windows machine, run the batch file $TOPDIR/Uninstall.bat on each server node.

CHAPTER 1

Licensing Cisco MDS 9000 Family DCNM-SAN Software Features

This chapter describes licensing for Cisco Data Center Network Manager for SAN (DCNM-SAN).

This chapter contains the following section:

Information About Cisco MDS DCNM-SAN Software Licenses

Licenses are available for all switches in the Cisco MDS 9000 Family. Licensing allows you to access specified premium features on the switch after you install the appropriate license for that feature. You can also obtain licenses to activate ports on the Cisco MDS 9124 Fabric Switch, the Cisco MDS 9134 Fabric Switch, the Cisco Fabric Switch for HP c-Class BladeSystem, and the Cisco Fabric Switch for IBM BladeCenter.

Note DCNM-SAN can discover the Cisco MDS 9124 Fabric Switch, Cisco MDS 9134 Fabric Switch and Cisco Fabric Switch for HP c-Class BladeSystem that are running NX-OS Release 5.0 and earlier versions of software. Cisco NX-OS Release 5.2(1) is not supported on these fabric switches.

Cisco DCNM can be licensed for SAN and LAN environments separately or together. A significant change for Cisco DCNM-SAN, as compared to Cisco Fabric Manager, is that licenses are no longer hosted on a specific switch. Instead, the licenses are hosted on the Cisco DCNM-SAN server. All existing Cisco Fabric Manager licenses are grandfathered into this model (which means that they continue) so customers do not need to order or deploy any additional licenses to manage their existing Cisco MDS 9000 Family switches.

Starting from Cisco MDS NX-OS Release 5.2(1a), the DCNM-SAN uses FLEXnet licensing format. DCNM-SAN will continue to support permenant switch license formats. However the support will be limited to the licenses that are already checked out.

This section contains information related to licensing types, options, procedures, installation, and management for the Cisco MDS DCNM-SAN software.

This section contains the following topics:

Licensing Terminology

The following terms are used in this chapter:

- Licensed feature—Permission to use a particular feature through a license file, a hardware object, or a legal contract. This permission is limited to the number of users, number of instances, time span, and the implemented switch.
- Licensed application—A software feature that requires a license to be used.
- License enforcement—A mechanism that prevents a feature from being used without first obtaining a license.
- Node-locked license—A license that can only be used on a particular switch using the switch's unique host ID.
- Host IDs—A unique chassis serial number that is specific to each Cisco MDS switch.
- Proof of purchase—A document entitling its rightful owner to use licensed feature(s) on one Cisco MDS switch as described in that document. Also known as the claim certificate.
- Product Authorization Key (PAK)—The PAK allows you to obtain a license key from one of the sites listed in the proof of purchase document. After registering at the specified website, you will receive your license key file and installation instructions through e-mail.
- License key file—A switch-specific unique file that specifies the licensed features. Each file contains digital signatures to prevent tampering and modification. License keys are required to use a licensed feature. License keys are enforced within a specified time span.
- Counted license—The number of licenses issued for a single feature (for example, FCIP). You can increase counted licenses (incremental licenses) should a need arise in the future.
- Missing license—If the bootflash has been corrupted or a supervisor module replaced after a license has been installed, that license will show as "missing." The feature will still work, but the license count will be inaccurate. You should reinstall the license as soon as possible.

- Incremental license—An additional licensed feature that was not in the initial license file. License keys are incremental—if you purchase some features now and others later, the license file and the software detect the sum of all features for the specified switch.
- Port Activation license—A license that activates additional ports on any of the following:
  - Cisco MDS 9124 Multilayer Fabric Switch
  - Cisco MDS 9134 Multilayer Fabric Switch
  - Cisco Fabric Switch for HP c-Class BladeSystem
  - Cisco Fabric Switch for IBM BladeCenter
- Evaluation license—A temporary license. Evaluation licenses are time bound (valid for a specified number of days) and are not tied to a host ID (switch serial number).
- Permanent license—A license that is not time bound is called a permanent license.
- Grace period—The amount of time the features in a license package can continue functioning without a license.
- Support—If you purchased Cisco support through a Cisco reseller, contact the reseller directly. If you purchased support directly from Cisco Systems, contact Cisco Technical Support at this URL: http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

Licensing Model

Any feature not included in a license package is bundled with the Cisco MDS 9000 Family switches and is provided at no extra charge. We recommend that you do not download more licenses than can be used for a module or switch.

Starting from Cisco MDS NX-OS Release 5.2(1a), the DCNM-SAN uses FLEXnet licensing format to be consistant with DCNM-LAN licensing. DCNM-SAN will continue to support permenant switch license formats. However the support will be limited to the licenses that are already checked out.

Two types of Cisco DCNM-SAN licenses are available:

- Cisco DCNM-SAN Essentials Edition (comparable to Cisco Fabric Manager) is included at no charge with every Cisco MDS 9000 hardware purchase and can also be downloaded from http://www.cisco.com/do/dcnm.
- Cisco DCNM-SAN Advanced Edition (comparable to Cisco Fabric Manager Server) provides additional capabilities and is required to use the Virtual Machine Topology and Performance feature and the Performance Forecasting Charts feature.

The licensing model defined for the Cisco MDS product line has two options:

- Feature-based licenses allow features that are applicable to the entire switch. The cost varies based on a per-switch usage. Table 1-1 lists the feature-based license packages.
- Module-based licenses allow features that require additional hardware modules. The cost varies based on a per-module usage. An example is the 18/4-port MSM module using the FCIP feature.

Note Each module requires its own separate license. If you replace a module that requires a license with a module of the same type (such as replacing a Storage Services Node (SSN-16) with another SSN-16), the existing license will support the new module.

Note The Cisco MDS 9216i and the Cisco MDS 9222i switches enable SAN extension features on the two fixed IP services ports only. The features enabled on these ports are identical to the features enabled by the SAN extension over IP license on the 14/2-port Multiprotocol Services (MPS-14/2) module. If you install a module with IP ports in the empty slot on the Cisco MDS 9216i or the Cisco MDS 9222i switch, a separate SAN extension over IP license is required to enable related features, such as FCIP, on the IP ports of the additional module.

Table 1-1 Cisco DCNM Feature-Based Licenses

Feature	DCNM Essential Edition (Free)	DCNM Advanced Edition (Licensed)
FC/FCoE/FICON/iSCSI Topoplgy View	✓	✓
Fabric, Device, and Summary Views	✓	✓
Port, Switch, and fabric-level configuration	✓	✓
Event and security management	✓	✓
Configuration analysis tools	✓	✓
Network diagnostic and troubleshooting tools	✓	✓
Real-time performance monitoring	✓	✓
One command multi-switch CLI access	✓	✓
Device Manager	✓	✓
Template based provisioning	✓	✓
Gold Diagnostics	✓	✓
Heterogeneous storage array discovery		✓
Scale-out federation architecture		✓
SAN Host Path Redundancy Analysis		✓

Table 1-1 Cisco DCNM Feature-Based Licenses (continued)

Feature	DCNM Essential Edition (Free)	DCNM Advanced Edition (Licensed)
Automatic fabric failover		✓
VMware vCenter Plug-in		✓
Multiple fabric management		✓
Centralized management server with discovery		✓
Continuous health and event monitoring		✓
Historical performance monitoring and reporting		✓
Event forwarding		✓
DCNM proxy services		✓
Configuration backup, archive, and compare		✓
Roaming user profiles		✓
VMpath analytics		✓
Domain Dashboards		✓
Capacity Manager		✓
Event Snooze		✓
SMI-S[1]		✓

1. Minimum of one DCNM-SAN Advanced License is required for each fabric.

Note License packages for Cisco DMM (Cisco Data Mobility Manager) and Cisco SME (Cisco Storage Media Encryption) are documented in the *Cisco MDS Data Mobility Manager Configuration Guide*, and the *Cisco Storage Media Encryption Configuration Guide*.

Licensing High Availability

As with other Cisco MDS DCNM-SAN features, the licensing feature also maintains the following high availability standards for all switches in the Cisco MDS 9000 Family:

- Installing any license in any switch is a nondisruptive process.
- Installing a license automatically saves a copy of permanent licenses to the chassis.
- If you have enabled the grace period feature, enabling a licensed feature that does not have a license key starts a counter on the grace period. You then have 120 days to install the appropriate license keys, disable the use of that feature, or disable the grace period feature. If at the end of the 120-day grace period the device does not have a valid license key for the feature, the Cisco DCNM-SAN software automatically disables the feature and removes the configuration from the device.

Note Some licenses, for example, Cisco TrustSec, do not have a grace period.

Devices with dual supervisors have the following additional high availability features:

- The license software runs on both supervisor modules and provides failover protection.
- The license key file is mirrored on both supervisor modules. Even if both supervisor modules fail, the license file continues to function from the version that is available on the chassis.

License Installation

If you have purchased a new switch through either your reseller or through Cisco Systems, you can:

- Obtain a factory-installed license (only applies to new switch orders).
- Perform a manual license installation (applies to existing switches).

This section contains the following topics:

Obtaining a Factory-Installed License

You can obtain factory-installed licenses for a new switch.

Detailed Steps

To obtain a factory-installed license for a new Cisco MDS switch, follow these steps:

Step 1 Contact your reseller or Cisco representative and request this service.

Note If you purchased Cisco support through a Cisco reseller, contact the reseller directly. If you purchased support directly from Cisco Systems, contact Cisco Technical Support at this URL: http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

Your switch is shipped with the required licenses installed in the system. The proof of purchase document is sent along with the switch.

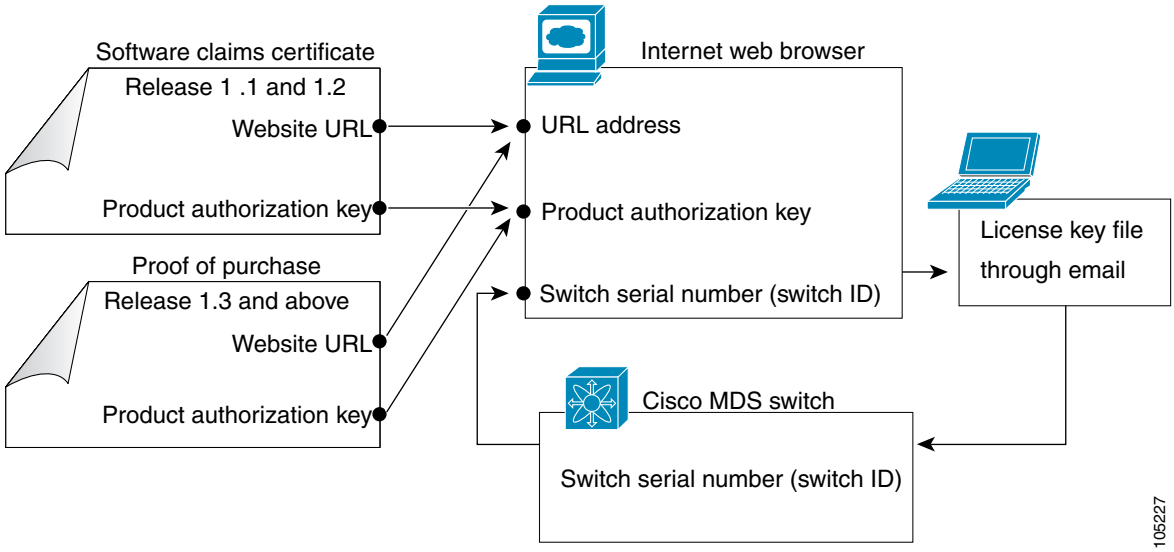
Step 2 Obtain the host ID from the proof of purchase document for future use.

Step 3 Start to use the switch and the licensed features.

Performing a Manual Installation

If you have existing switches or if you wish to install the licenses on your own, you must first obtain the license key file and then install that file in the switch (see Figure 1-1).

Figure 1-1 Obtaining a License Key File



Obtaining the Switch License Key File

Detailed Steps

To obtain new or updated license key files using Device Manager, follow these steps:

Step 1 From the menu bar, choose **Physical > Inventory**. You see the inventory for the switch. The host ID is referred to as the serial number.

Tip Prepend the serial number with VDH=. For example, if the serial number is `FOX064317SQ`, the full serial number is VDH=FOX064317SQ.

Step 2 Obtain either your claim certificate or your proof of purchase document. This document accompanies every Cisco MDS switch.

Step 3 Obtain the Product Authorization Key (PAK) from either the claim certificate or the proof of purchase document.

Step 4 Locate the website URL from either the claim certificate or the proof of purchase document.

Step 5 Access the specified URL that applies to your switch and enter the switch serial number and the PAK.

The license key file is sent to you by e-mail. The license key file is digitally signed to only authorize use on the requested switch. The requested features are also enabled once the Cisco DCNM-SAN software on the specified switch accesses the license key file.

Caution Install the license key file in the specified MDS switch without making any modifications.

A license is either permanent or it expires on a fixed date. If you do not have a license, the grace period for using that feature starts from the first time you start using a feature offered by that license.

Step 6 Use the **copy licenses** command in EXEC mode to save your license file to one of two locations—the bootflash: directory or the slot0: device.

Installing the Switch License Key File

The best way to install licenses on the switches in your fabric is to use the License Wizard provided in DCNM-SAN. You can also use Device Manager to install licenses on each switch individually.

Tip If you need to install multiple licenses in any switch in the Cisco MDS 9000 Family, be sure to provide unique file names for each license key file.

Note You do not need a license to access a switch with DCNM-SAN. See the "Licensing Model" section on page 1-3 for a list of features requiring licenses.

This section contains the following topics:

Installing Switch Licenses Using DCNM-SAN License Wizard

Detailed Steps

To install licenses using the DCNM-SAN License Wizard, follow these steps:

Step 1 Log into a switch in the fabric containing the switches for which you want to install licenses.

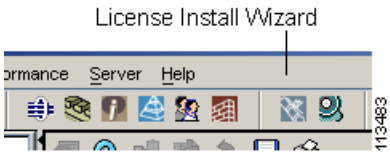
To install licenses on multiple switches, you do not need to log into each switch; however, the switches must be in the fabric you are viewing.

Step 2 Start the License Wizard by choosing **Tools > Install >License**. Or, you can select **Licenses** under **Switches** in the Physical Attributes pane.

You see the license information in the Information pane, one line per feature.

Step 3 Click the **Keys** tab, and then click the **License Install Wizard** icon in the toolbar.

Figure 1-2 License Install Wizard Icon



You see the initial screen of the License Wizard.

Step 4 If you have already obtained the license key files, click the corresponding radio button and proceed to Step 6.

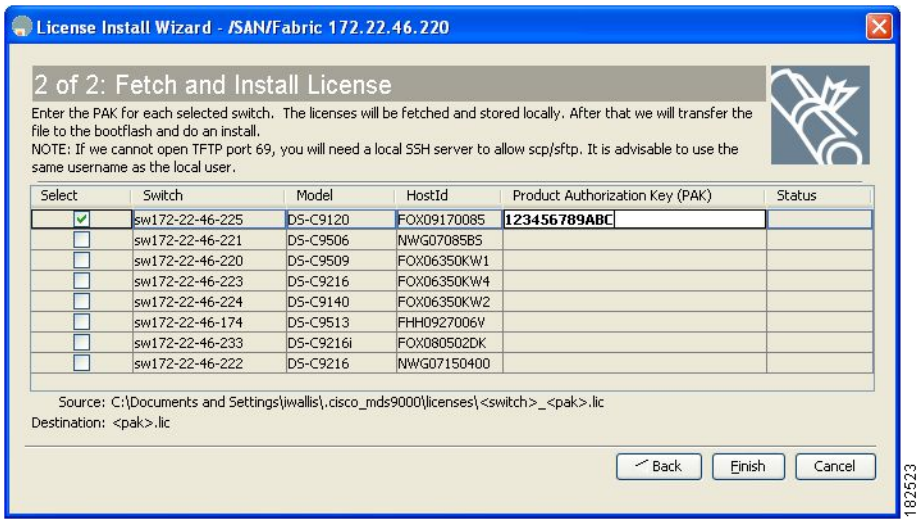
Step 5 Click **I have the Product Authorization Key (PAK)** if you have the authorization key.

Step 6 Select the vendor, from whom you purchased your switch, in the Vendor drop-down list.

The License Server URL changes depending on the vendor you select. If your URL is different, or if you select **Other** as the vendor, enter the correct license server URL.

Step 7 Click **Next** to continue to the next screen (see Figure 1-3).

Figure 1-3 License Install Wizard Dialog Box



Step 8 Select the switches for which you have PAKs or license key files.

When you check the check box for a switch, the PAK or license file name field for that switch becomes editable. The *serial number* for each switch is shown in the Host ID column.

Step 9 Enter the PAK or license file name for each switch you have selected in the appropriate column. If you have the license files on your PC, you can double-click in the License File Name text area to bring up a dialog box and browse for the license files.

You can install multiple licenses on the same switch using different PAKs. To do this, enter the PAKs separated by commas.

Step 10 Click **Finish** to transfer the licenses from the host to the switches.

DCNM-SAN accesses the appropriate license site and installs the licenses onto each switch. The status of each installation is displayed in the Status column, as follows:

- success—Install or uninstall operation completed successfully.
- inProgress—License install or uninstall operation is in progress.
- corruptedLicenseFile—License file content is invalid or corrupted.
- targetLicenseFileAlreadyExist—Target license file-name already exists.
- invalidLicenseFileName—License file does not exist.
- duplicateLicense—License file is already installed.
- generalLicensingFailure—General error from License Manager.
- none—No install operation is performed.
- licenseExpiryConflict—License exists with a different expiration date for the feature.
- invalidLicenseCount—License count is invalid for the feature.

Step 11 Click the **Close** button to close the wizard. To install more licenses at this point, you must close the wizard and launch it again.

Installing or Updating Switch Licenses Using Device Manager

Detailed Steps

To install a license on your switch using Device Manager, follow these steps:

Step 1 Select **Licenses** from the Admin menu.

You see the Licenses dialog box.

Step 2 Click the **Install** tab.

The HostId shows the "VDH=" portion of the serial number. The rest of the number is completed in Steps 3 through 5.

Step 3 Enter the uniform resource identifier (URI) from which the license file will be retrieved.

You should already have copied the license file provided by Cisco.com or by some other means (for example, through the CLI) to this location.

Step 4 Enter the target file name in the Target Filename field to specify where the license file will be installed.

Step 5 Click **Install** if you are installing, or **Update** if you are updating.

You see the status of the installation at the bottom of the dialog box, as follows:

- success—Install or uninstall operation completed successfully.
- inProgress—License install or uninstall operation is in progress.
- corruptedLicenseFile—License file content is invalid or corrupted.
- targetLicenseFileAlreadyExist—Target license file name already exists.
- invalidLicenseFileName—License file does not exist.
- duplicateLicense—License file is already installed.
- generalLicensingFailure—General error from License Manager.
- none—No install operation is performed.
- licenseExpiryConflict—License exists with a different expiration date for the feature.

- invalidLicenseCount—License count is invalid for the feature.
- notThisHost—License host ID in the license file does not match.
- licenseInGraceMore—Number of licenses in grace period is more than the number in the install license file.
- licenseFileNotFound—License file not found for the install, uninstall, or update operation.
- licenseFileMissing—A previously installed license file is found missing.
- invalidLicenseFileExtension—License file does not have a .lic extension.
- invalidURI—Invalid license file URI specified for install operation.
- noDemoLicenseSupport—Demo license not supported.
- invalidPlatform—Invalid platform.

Step 6 Repeat Steps 3 through 5 to install another license, or click **Close** to close the License Manager dialog box.

Viewing Fabric Licenses

Detailed Steps

To view the fabric licenses, follow thses steps:

Step 1 From the menu bar, choose **File > Open**.

Step 2 Click Refresh to refresh the table.

Note License state of the fabrics that are unmanaged is displayed as unknown.

Adding a License File to Cisco DCNM-SAN Server

Prerequisites

You must have network administrator privileges to complete the following proedure.

Before You Begin

Acquire the required licensing file.

Detailed Steps

To add a license file, follow these steps:

Step 1 Log into the Cisco DCNM-SAN server system.

Step 2 Download the license pack file that you received from Cisco into a directory on the server system.

Step 3 Copy the license file into INSTALL_DIR/dcm/licenses directory. On a Microsoft Windows system, the default INSTALL_DIR value is C:\Program Files\Cisco Systems.

Step 4 From the menu bar, choose **File > Open** and then click **License Files** tab.

Step 5 Click **Reload License Files** to reload the licences.

Assigning a License to a Swtich

Prerequisites

You must have network administrator privileges to complete the following proedure.

Before You Begin

You need to make sure that the switch that you want to assign a license is not managed. You can verify

Detailed Steps

To assign a license to a switch, follow thses steps:

Step 1 From the menu bar, choose **File > Open** and then click **License Assignment** tab.

Step 2 From the table, select the switch that you want to assign the license to.

Step 3 Click **Assign License**.

Unassigning Licensing to a Switch

Prerequisites

You must have network administrator privileges to complete the following proedure.

Before You Begin

You need to make sure that the switch that you want to assign a license is not managed. You can verify

Detailed Steps

To unassign a license to a switch, follow thses steps:

Step 1 From the menu bar, choose **File > Open** and then click **License Assignment** tab.

Step 2 From the table, select the switch that you want to unassign the license.

Step 3 Click **Unassign License**.

Identifying License Features in Use

When a Cisco MDS DCNM-SAN software feature is enabled, it can activate a license grace period.

To identify the features active for a specific license using DCNM-SAN, follow these steps:

Step 1 Select a switch from the Fabric pane, or select a group of switches (SAN, fabric, VSAN) from the Logical Domains pane.

Step 2 Select **Licenses** under **Switches in** the Physical Attributes pane.

You see the contents of the **Feature Usage** tab in the Information pane, with installed licenses listed in the Feature column.

Step 3 Click the **Usage** tab.

You see the features currently in use in the Application column.

.

Uninstalling Licenses

You can only uninstall a permanent license that is not in use. If you try to delete a permanent license that is currently being used, the software rejects the request and issues an error message. Uninstalling an unused license causes the grace period to come into effect. The grace period is counted from the first use of the feature without a license and is reset when a valid license file is installed.

Note Permanent licenses cannot be uninstalled if they are currently being used. Features turned on by permanent licenses must first be disabled, before that license is uninstalled.

Tip If you are using an evaluation license and would like to install a new permanent license, you can do so without service disruption and before the evaluation license expires. Removing a permanent license immediately triggers a grace period without service disruption.

Caution Disable related features before uninstalling a license. The delete procedure fails if the license is in use.

Detailed Steps

To uninstall a license, follow these steps:

Step 1 Log into the switch. If you are using DCNM-SAN to remove licenses from multiple switches, you do not need to log in to each switch; however, the switches must be in the fabric you are viewing.

Step 2 From the DCNM-SAN Physical Attributes pane, choose **Licenses** > **Switches**. You see the license information in the Information pane, one line per feature.

From Device Manager menu, choose **Admin > Licenses**. You see the Licenses dialog box.

Step 3 In DCNM-SAN, click the **Keys** tab. You see the list of License Key files. Click the name of the license you want to remove, and press the **Delete** keyboard key or click the **Delete Row** icon in the toolbar.

In Device Manager, click **Uninstall**, and enter the name of the License Key file you want to remove. Click **Apply** to remove the License Key file, and click **Close** to close the dialog box.

Note To delete a license, you must disable the features enabled by that license. The delete procedure fails if the license is in use, and an error message is displayed.

Updating Licenses

If your license is time bound, you must obtain and install an updated license. Contact technical support to request an updated license.

Note If you purchased Cisco support through a Cisco reseller, contact the reseller directly. If you purchased support directly from Cisco Systems, contact Cisco Technical Support at this URL: http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

Detailed Steps

To update a license, follow these steps:

Step 1 Obtain the updated license file using the procedure described in the "Obtaining the Switch License Key File" section on page 1-7.

Step 2 Save your running configuration to a remote server using the **copy** command.

Step 3 Verify the name of the file to be updated.

Step 4 Follow the procedure for updating a license described in the "Uninstalling Licenses" section on page 1-13.

Grace Period Alerts

Cisco DCNM-SAN gives you a 120-day grace period. This grace period starts or continues when you are evaluating a feature for which you have not installed a license.

Note There is no grace period for licenses purchased for the On-Demand Port Activation license feature.

The grace period stops if you disable a feature you are evaluating, but if you enable that feature again without a valid license, the grace period countdown continues where it left off.

The grace period operates across all features in a license package. License packages can contain several features. If you disable a feature during the grace period and there are other features in that license package that are still enabled, the countdown does not stop for that license package. To suspend the grace period countdown for a license package, you must disable every feature in that license package.

The Cisco DCNM-SAN license counter keeps track of all licenses on a switch. If you are evaluating a feature and the grace period has started, you will receive console messages, SNMP traps, system messages, and Call Home messages on a daily basis. The frequency of these messages become hourly during the last seven days of the grace period.

The following example uses the FICON feature. On January 30th, you enabled the FICON feature, using the 120-day grace period. You will receive grace period ending messages as:

- Daily alerts from January 30th to May 21st.
- Hourly alerts from May 22nd to May 30th.

On May 31st, the grace period ends, and the FICON feature is automatically disabled. You will not be allowed to use FICON until you purchase a valid license.

Note You cannot modify the frequency of the grace period messages.

Caution After the final seven days of the grace period, the feature is turned off and your network traffic may be disrupted. Any future upgrade will enforce license requirements and the 120-day grace period.

License Transfers Between Switches

A license is specific to the switch for which it is issued and is not valid on any other switch. If you need to transfer a license from one switch to another, contact your customer service representative.

Note Rehosting licenses is only supported for RMAs.

Note If you purchased Cisco support through a Cisco reseller, contact the reseller directly. If you purchased support directly from Cisco Systems, contact Cisco Technical Support at this URL: http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

Displaying License Information

You can use DCNM-SAN Client or Device Manager to display all license information configured on a switch.

This section contains the following topics:

Viewing License Information in DCNM-SAN Client

Detailed Steps

To view license information in DCNM-SAN, follow these steps:

Step 1 Select **Licenses** under **Switches** in the Physical Attributes pane. You see the license information in the Information pane, one line per feature.

Step 2 Click the **Feature Usage** tab to see the switch, the name of the feature package, the type of license installed, the number of licenses used (Installed Count), the expiration date, the grace period (if you do not have a license for a particular feature), and any errors (for example, if you have a missing license).

Step 3 Click the **Keys** tab to display the information about each of the License Key files installed on your switches.

Caution Once an expiration period has started, notifications appear in the DCNM-SAN's Events pane on a daily basis. During the last seven days of the expiration period, these messages are displayed hourly. After the final seven days of the expiration period, the feature is turned off and your network traffic may be disrupted.

Step 4 Click the **Usage** tab to see the applications using the feature package on each switch. Use this tab to determine which applications depend on each license installed.

Viewing License Information in Device Manager

Detailed Steps

To view license information in Device Manager, follow these steps:

Step 1 Select **Admin > Licenses** from the menu.

You see the Licenses dialog box.

Step 2 Click the **Features** tab to see the name of the feature package, the type of license, the expiration date, the grace period (if you do not have a license for a particular feature), and any errors, such as a missing license.

Step 3 Click the **Files** tab to display the information about each of the License Key files installed on your switch.

Step 4 Click the **Install** tab to install or update a license file.

Step 5 Click the **Usage** tab to which applications are using the features on the switch.

Viewing Licenses Using DCNM Web Client

Cisco DCNM Web Client supports viewing license use across the fabric from Fabric Manager Web Client. This view summarizes the licenses used on all switches in the fabric.

To view licenses using Cisco DCNM-SAN Web Client, choose **Inventory > Licenses**.

DCNM-SAN Server Licensing

When you install Cisco DCNM-SAN, the basic version of the Cisco DCNM-SAN Server (DCNM-SAN Server) is installed with it. To get the enhanced features, such as Performance Manager and remote client support you will need to buy and install the Cisco MDS 9000 Family DCNM-SAN Server license package.

However, trial use of these enhanced features is available. To enable the 120-day trial, you simply use the feature as you would if you had purchased the license. You see a dialog box explaining that this is a demo version, enabled for a limited time.

If you are evaluating Cisco DCNM-SAN Server features and want to stop the evaluation period for that feature, you can do that using Device Manager.

Detailed Steps

To stop the evaluation using Device Manager, follow these steps:

Step 1 Select **Admin > Licenses**.

You see the Licenses dialog box.

Step 2 Click the **Features** tab and select the feature to check in.

When you select the feature, you see a Check In FM button at the bottom of the dialog box.

Step 3 Click **Check In FM** to stop the demo period timer.

On-Demand Port Activation Licensing

This section describes how to use the on-demand port activation licensing feature on the Cisco MDS 9124 Fabric Switch, the Cisco MDS 9134 Fabric Switch, the Cisco Fabric Switch for HP c-Class BladeSystem, and the Cisco Fabric Switch for IBM BladeCenter.

This section contains the following topics:

Information About On-Demand Port Activation Licensing

You can expand your SAN connectivity as needed by enabling users to purchase and install additional port licenses. By default, all ports are eligible for license activation. On the Cisco MDS 9124 Fabric Switch, licenses are allocated sequentially. However, you can move or reassign licenses to any eligible port on the switch.

On the Cisco MDS 9134 Fabric Switch, the first 32 ports operate at 1 Gbps, 2 Gbps, or 4 Gbps. The switch has two ports that operate at 10 Gbps. Licenses are allocated sequentially. On the Cisco Fabric Switch for HP c-Class BladeSystem and the Cisco Fabric Switch for IBM BladeCenter, licenses for internal ports are allocated as the ports come up. Licenses for external ports are allocated sequentially.

This section contains the following topics:

Port-Naming Conventions

Table 1-2 describes the port-naming conventions for the four Cisco Fabric switches.

Table 1-2 Port-Naming Conventions for Cisco Fabric Switches

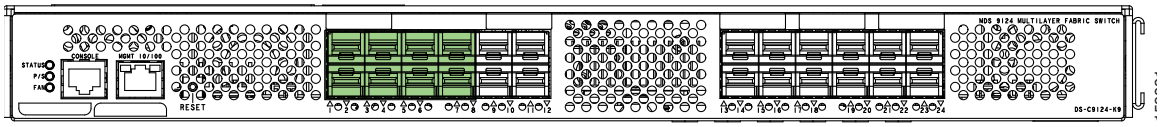
Cisco MDS 9124 Switch	Cisco MDS 9134 Switch	Cisco Fabric Switch for HP c-Class BladeSystem	Cisco Fabric Switch for IBM BladeCenter
fc1/1 through fc1/24	fc1/1 through fc1/34	Internal ports: bay1 through bay16	Internal ports: bay1 through bay14
		External ports: ext1 through ext8	External ports: ext0 and ext15 through ext19

Port Licensing

On the Cisco MDS 9124 Switch, the first eight ports are licensed by default. You are not required to perform any tasks beyond the default configuration unless you prefer to immediately activate additional ports, make ports ineligible, or move port licenses.

Figure 1-4 shows the ports that are licensed by default for the Cisco MDS 9124 Switch.

Figure 1-4 Cisco MDS 9124 Switch Default Port Licenses (fc1/1 - fc1/8)



If you need additional connectivity, you can activate additional ports in 8-port increments with each on-demand port activation license, up to a total of 24 ports.

On the Cisco MDS 9134 Switch, the first 24 ports that can operate at 1 Gbps, 2 Gbps, or 4 Gbps are licensed by default. If you need additional connectivity, you can activate the remaining eight ports with one on-demand port activation license. A separate 10G license file is required to activate the remaining two 10-Gbps ports.

Figure 1-5 shows the ports that are licensed by default for the Cisco MDS 9134 Switch.

Figure 1-5 Cisco MDS 9134 Switch Default Port Licenses (fc1/1 - fc1/24)

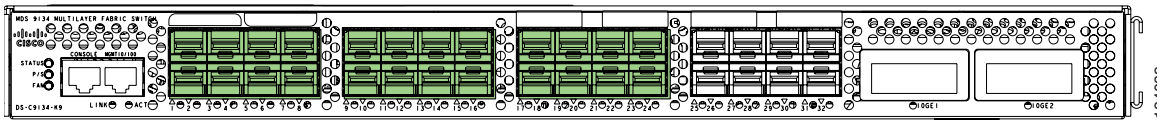
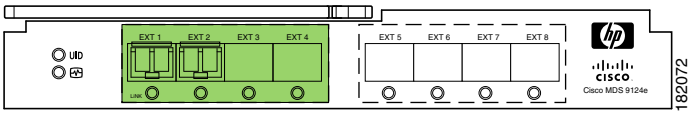


Figure 1-6 shows the external ports that are licensed by default for the Cisco Fabric Switch for HP c-Class BladeSystem.

Figure 1-6 Cisco Fabric Switch for HP c-Class BladeSystem Default Port Licenses (ext1 - ext4)

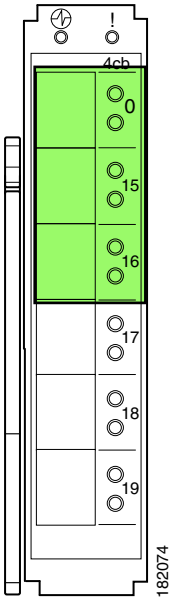


On the Cisco Fabric Switch for HP c-Class BladeSystem, any eight internal ports and the external ports (ext1 through ext4) are licensed by default. A single on-demand port activation license is required to use the remaining eight internal and four external ports.

On the Cisco Fabric Switch for IBM BladeCenter, any seven internal ports and the external ports(ext0, ext15 and ext16) are licensed by default. A single on-demand port activation license is required to use the remaining seven internal and three external ports.

Figure 1-7 shows the external ports that are licensed by default for the Cisco Fabric Switch for IBM BladeCenter.

Figure 1-7 Cisco Fabric Switch for IBM BladeCenter Default Port Licenses (ext0, ext15 - ext16)



If you do not prefer to accept the default behavior and would rather assign a license to a specific port, make the port ineligible to receive a license, or move licenses among ports, refer to the "Configuring Port Activation Licenses" section on page 1-20.

License Status Definitions

Table 1-3 defines the port activation license status terms.

Table 1-3 Port Activation License Status Definitions

Port Activation License Status	Definition
acquired	The port is licensed and active.

Table 1-3 Port Activation License Status Definitions (continued)

Port Activation License Status	Definition
eligible	The port is eligible to receive a license but does not yet have one.
ineligible	The port is not allowed to receive a license.

By default, when you install additional port license activation packages, the activation status of ports changes from "eligible" to "acquired." If you prefer to accept the default behavior, no further action is required.

Note You can uninstall licenses for ports not in use; however, you cannot uninstall default licenses.

Configuring Port Activation Licenses

This section contains the following topics:

Checking the Status of Licenses

Note The dialog boxes shown in Figures 11-5 and 11-6 apply only to the Cisco MDS 9124 Fabric Switch.

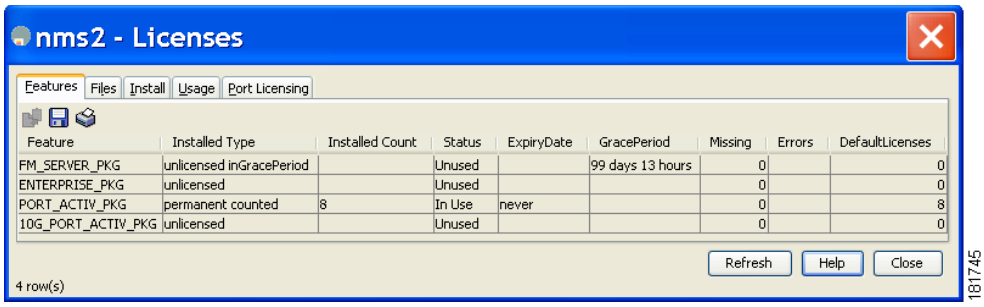
Detailed Steps

To check the number of licenses that are in use using Device Manager, follow these steps:

Step 1 From the menu bar, choose **Admin** > **Licenses**.

You see the Licenses dialog box as shown in Figure 1-8.

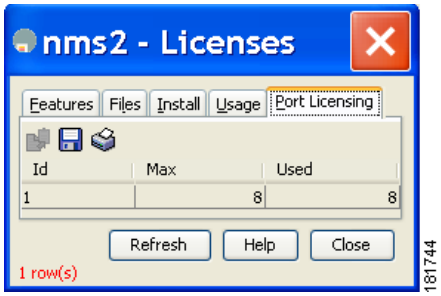
Figure 1-8 Licenses Dialog Box



Step 2 Click the **Port Licensing** tab.

You see the licenses that are in use as shown in Figure 1-9.

Figure 1-9 Licenses in Use



Step 3 Click **Close** to close the dialog box.

Making a Port Eligible for a License

By default, all ports are eligible to receive a license. However, if a port has already been made ineligible and you prefer to activate it, then you must make that port eligible by using the **port-license** command.

To make a port eligible to acquire a license, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# interface fc1/1` `switch(config-if)#`	Specifies the port interface that you want to make eligible for a license. **Note** The name of the port depends on the switch you are using. See "Port-Naming Conventions" section on page 1-18 for information on port names.

	Command	Purpose
Step 3	`switch(config-if)# port-license`	Makes the port eligible to acquire a license.
	`switch(config-if)# no port-license`	Removes a license from a port if it already has been assigned, and also makes the port ineligible to acquire a license. **Note** You can remove licenses only from ports that are not in an administrative shutdown state.

Note The dialog box shown in Figure 11-7 applies only to the Cisco MDS 9124 Fabric Switch.

Detailed Steps

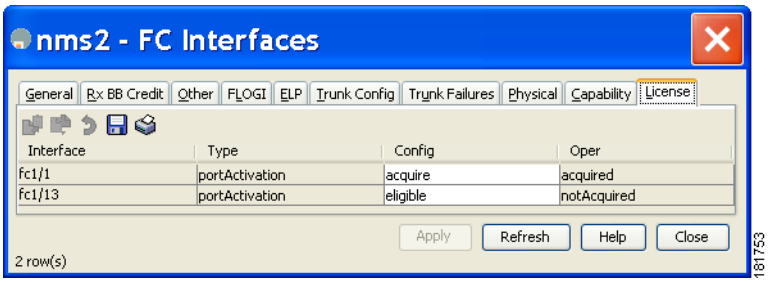
To make multiple ports eligible to acquire a license using Device Manager, follow these steps:

Step 1 From the menu bar, choose **Interface > FC All** and click the **License** tab or hold down the **Control** key, and then click each port that you want to make eligible.

Step 2 Right-click the selected ports, select **Configure,** and click the **License** tab.

You see the FC Interfaces dialog box as shown in Figure 1-10.

Figure 1-10 FC Interfaces Dialog Box



Step 3 Select **eligible** from the Config drop-down list for each port that you want to make eligible.

Step 4 Click **Apply** to save the changes.

Note The dialog box shown in Figure 11-8 applies only to the Cisco MDS 9124 Fabric Switch.

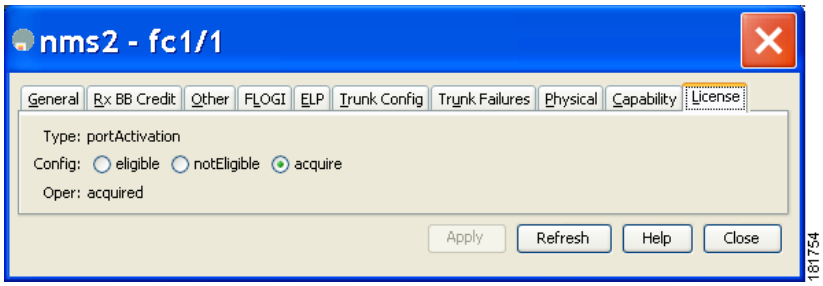
Detailed Steps

To make a single port eligible to acquire a license using Device Manager, follow these steps:

Step 1 Right-click a port, select **Configure,** and click the **License** tab.

You see the port licensing options for the selected port as shown in Figure 1-11.

Figure 1-11 License Tab for Selected Port



Step 2 Click the **eligible** radio button to make the port eligible.

Step 3 Click **Apply** to save the changes.

Acquiring a License for a Port

If you do not prefer to accept the default on-demand port license assignments, you will need to first acquire licenses for ports to which you want to move the license.

To acquire a license for a port, follow these steps:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# interface fc1/1` `switch(config-if)#`	Specifies the port interface for which you want to acquire a license. **Note** The name of the port depends on the switch you are using. See "Port-Naming Conventions" section on page 1-18 for information on port names.
Step 3	`switch(config-if)# port-license acquire`	Grants a license to a port or range of ports.
	`switch(config-if)# no port-license`	Removes a license from a port or range of ports.

Detailed Steps

To acquire licenses for multiple ports using Device Manager, follow these steps:

Step 1 Choose **Interface > FC All** and click the **License** tab or hold down the **Control** key, and then click each port for which you want to acquire a license.

Step 2 Right-click the selected ports, select **Configure,** and click the **License** tab.

You see the FC Interfaces dialog box as shown in Figure 1-10.

Step 3 Select **acquire** from the Config drop-down list for each port that you want to acquire a license.

Step 4 Click **Apply** to save the changes.

To acquire a license for a single port using Device Manager, follow these steps:

Step 1 Right-click a port, select **Configure,** and click the **License** tab.

You see the port licensing options for the selected port as shown in Figure 1-11.

Step 2 Click the **acquire** radio button to acquire a license for the port.

Step 3 Click **Apply** to save the changes.

Send document comments to dcnm-docfeedback@cisco.com

PART 1

Cisco Data Center Network Manager for LAN

CHAPTER 1

Deploying Cisco DCNM-LAN

This chapter describes how to deploy Cisco Data Center Network Manager for LAN (DCNM-LAN) deployment and general steps for deploying Cisco DCNM-LAN single-server or clustered-server environments.

This chapter includes the following sections:

Information About Deploying Cisco DCNM-LAN

This section includes the following topics:

Database Support

Cisco DCNM-LAN supports the following databases:

- PostgreSQL 8.1
- PostgreSQL 8.2
- PostgreSQL 8.3

- Oracle Database 10g
- Oracle Database 11g

If the Cisco DCNM installer does not find a previous installation of a supported database, it can install PostgreSQL 8.2 for you.

Cisco DCNM-SAN Support

Cisco DCNM supports installing the Cisco DCNM-LAN server on a server system that has an installation of Cisco DCNM-SAN; however, the Cisco DCNM-LAN release number and the Cisco DCNM-SAN release number must be the same.

Note The Cisco DCNM installer is the installer for both DCNM-SAN and DCNM-LAN. The installer also provides support for the initial installation of both DCNM-SAN and DCNM-LAN on a server.

If you install the Cisco DCNM-LAN server on a server system that already has an installation of Cisco DCNM-SAN, the Cisco DCNM installer detects the DCNM-SAN installation, which has the following effects on the installation:

- The installation folder is determined by the installer and cannot be configured.
- The database that the installer configures the Cisco DCNM-LAN server to use is the database that DCNM-SAN is configured to use. You cannot choose a database other than the database used by DCNM-SAN.
- The installer resolves port conflicts between the ports in use by DCNM-SAN and the default ports that the Cisco DCNM-LAN server uses.

Operating Systems

For information about the specific editions of supported server operating systems, see the *Cisco DCNM Release Notes, Release 5.x*, at the following location:

http://www.cisco.com/en/US/products/ps9369/tsd_products_support_series_home.html

You can install Cisco DCNM-LAN on a supported version of one of the following operating systems:

- Microsoft Windows Server

  If the server system runs the Microsoft Windows operating system, the Cisco DCNM-LAN server software runs as a service. By default, the Cisco DCNM-LAN server starts automatically when you boot up the server system.
- Red Hat Enterprise Linux

VMware Support

Cisco DCNM-LAN supports the installation of Cisco DCNM-LAN servers in VMware virtual machines that have a compatible Windows operating system or Linux operating system supported by Cisco DCNM-LAN. The following requirements apply:

- The VMware server software must be a supported version.

- The virtual machine in which you install a Cisco DCNM-LAN server must meet all server requirements.

For the latest information about supported VMware server software and other server requirements, see the *Cisco DCNM Release Notes, Release 5.x*, at the following location:

http://www.cisco.com/en/US/products/ps9369/tsd_products_support_series_home.html

Primary and Secondary Servers

The distinction of primary and secondary servers is only for the purposes of installing, upgrading, and licensing Cisco DCNM-LAN server software. Whether a server is a primary or secondary server does not affect the function of the Cisco DCNM-LAN server software.

In a single-server Cisco DCNM-LAN deployment, the server is a primary server.

In a clustered-server Cisco DCNM-LAN deployment, one server is a primary server and the remaining servers are secondary servers.

When you install, upgrade, or license the Cisco DCNM-LAN server software on the primary server, the installer records the configuration choices that you make in properties files. You use these properties files when you install, upgrade, or license each of the secondary servers in a server cluster.

We recommend that you choose one server in the cluster to be the primary server and always use that server as the primary server. This practice helps to avoid confusion during server maintenance and helps you ensure that you meet the server-cluster requirements, as described in the "Clustered-Server Cisco DCNM-LAN Requirements" section on page 1-5.

Master and Member Servers

In a Cisco DCNM-LAN server cluster, one server performs the master server role and the remaining servers are member servers. The server with the oldest start time is the master server; therefore, you can control which server is the master server by starting that server first. For information about how Cisco DCNM-LAN operates in a clustered-server environment, see the Cluster Administration feature in the *Cisco DCNM Fundamentals Guide, Release 5.x*.

To help simplify the management of your server cluster, we recommend that you use the primary Cisco DCNM server as the master server. To do so, start the primary server before you start any other server in the cluster.

Server Ports

A Cisco DCNM-LAN server must be able to receive the network traffic from Cisco DCNM-LAN clients on a number of ports. Any network gateway device that controls the traffic sent from a Cisco DCNM-LAN client to a Cisco DCNM-LAN server must permit the traffic sent to the ports that the Cisco DCNM-LAN server is configured to use.

Table 1-1 lists the default ports that services on a Cisco DCNM-LAN server listen to for client communications. One port is not configurable. You can configure the other ports. The server installer can resolve port conflicts automatically.

Table 1-1 Default TCP Ports for Client Communications

Service Name	Default Port	Configurable?
Secondary Server Bind	None	After installation—See the "Specifying a Secondary Server Bind Port" section on page 1-6.
RMI	1098	During installation
Naming Service	1099	During installation
SSL	3843	During installation
EJB	3873 (DCNM-LAN) 3973 (DCNM-SAN)	During installation
Server Bind 1	4445	During installation
Server Bind 2	4446	During installation
JMS	4457	During installation
Syslog (system message) Receiver	5445	During installation
AJP Connector	8009	During installation
Web Server	8080	During installation
Web Service	8083	During installation
RMI Object	14444	During installation

In a clustered-server deployment, the Cisco DCNM-LAN servers in the cluster listen for UDP messages that are multicast to the cluster partition name. The supported topologies for clustered-server deployments do not allow gateway devices between servers in the cluster; however, for reference purposes, Table 1-2 lists the default ports that a Cisco DCNM-LAN server listens to for server cluster communications. Some ports are not configurable. You can configure the other ports during the server installation. The installer software creates a default value for the three ports.

Table 1-2 Default Ports for Clustered-Server Communications

Service Name	Protocol	Default Port	Configurable?
High Availability Naming Service	TCP	1100	No
High Availability RMI Naming Service	TCP	1101	No
High Availability Naming Service	UDP	1102	No
Multicast port	UDP	Determined at installation	During installation
Multicast port	UDP	Determined at installation	During installation
Multicast port	UDP	Determined at installation	During installation

Prerequisites for Installing a Cisco DCNM-LAN Server

The Cisco DCNM-LAN server system has the following prerequisites:

- The server system must meet the server system requirements listed in the *Cisco DCNM Release Notes, Release 5.x*, available online at the following URL:

  http://www.cisco.com/en/US/products/ps9369/tsd_products_support_series_home.html
- The IP address of the server system should be statically assigned. The Cisco DCNM-LAN server binds to an IP address that you specify during installation. If the IP address of the server system changes after you install the Cisco DCNM-LAN server, Cisco DCNM-LAN clients are unable to connect to the Cisco DCNM-LAN server and you must stop and reinstall the Cisco DCNM-LAN server so that you can reconfigure the IP address.
- The server system must be registered with the DNS servers on your network.
- If you plan to use RADIUS or TACACS+ authentication of Cisco DCNM-LAN users, you must ensure that the authentication servers are configured to accept authentication requests from the Cisco DCNM-LAN server.
- If you plan to run the Cisco DCNM-LAN database on a different server than the Cisco DCNM-LAN server software, the servers must be in the same Ethernet network segment. You can interconnect the servers with a switch or hub. There can be no routing device between servers in a Cisco DCNM-LAN deployment.
- A Perl environment must already be installed on the server system. We recommend ActivePerl version 5.8.9.x. You can download ActivePerl for your server operating system from the following location:

  ftp://ftpeng.cisco.com/dcnm/perl/active-perl/ActivePerl-5.8.9.827/
- The path to the Perl executable must be defined in the server system PATH environment variable.
- For Red Hat Enterprise Linux (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-LAN server will fail after the server system is rebooted. For more information, see the following URL:

  http://www.postgresql.org/docs/8.3/interactive/kernel-resources.html
- Ensure that no other programs are running on the server system except for a compatible release of Cisco DCNM-SAN and the database software used by Cisco DCNM-SAN.
- Using the Cisco DCNM-LAN installer in GUI mode requires that you must login to the remote server using VNC or XWindows. Using telnet or SSH to install Cisco DCNM-LAN in GUI mode is not possible.
- Ensure you disable the default firewall on a Microsoft Windows 2008 64-bit machine before you install Cisco DCNM. To disable the firewall, use the following command:

  ```
  netsh advfirewall set allprofiles state off
  ```

Clustered-Server Cisco DCNM-LAN Requirements

This section includes the following topics:

Prerequisites for Deploying a Clustered-Server Cisco DCNM-LAN Environment

Before you begin to deploy a clustered-server Cisco DCNM-LAN environment, you must ensure that the server systems in the cluster meet the following requirements:

- The following items must be identical for all server systems in the cluster:
  - Operating system
  - Number of CPUs
  - CPU speed
  - Memory
- If you plan to install Cisco DCNM-LAN servers in VMware virtual machines, the following additional requirements must be met:
  - All servers in the cluster must be installed in a virtual machine. You cannot deploy a server cluster with a mix of virtual and physical server systems.
- All servers in the cluster must be in the same Ethernet network segment. If the Cisco DCNM-LAN database is remote to Cisco DCNM-LAN servers, the database server must be in the same Ethernet network segment as all Cisco DCNM-LAN servers. You can interconnect the servers with a switch or hub. There can be no routing device between servers in a Cisco DCNM-LAN deployment.
- If you plan to use RADIUS or TACACS+ authentication of Cisco DCNM-LAN users, you must ensure that the authentication servers are configured to accept authentication requests from all the Cisco DCNM-LAN servers in the cluster.
- You must enable the Network Time Protocol (NTP) on all servers in the cluster.

Clustered-Server Configuration Requirements

During the deployment of a clustered-server Cisco DCNM-LAN environment, you must ensure that the following requirements are met:

- All servers in the cluster must run an identical release of Cisco DCNM-LAN, such as Cisco DCNM Release 5.0(2).
- You must specify the following information identically on all servers:
  - Cluster partition name
  - Multicast addresses and ports
  - Cisco DCNM-LAN database path and credentials
  - Authentication settings

  This requirement is met by the secondary server installation process. For more information, see the "Secondary Server Installation" section on page 1-2.
- The archive directory specified during the installation of each server must refer to the same directory. The path to the directory can be different for each server. This shared directory must be an external shared directory and accessible by all DCNM-LAN servers with read/write privilege. For example, two Cisco DCNM-LAN servers installed on Microsoft Windows could use different paths, such as X:\DCNM\data and F:\data, but the two paths must refer to the same directory.

- If you acquire licenses for Cisco DCNM-LAN, all servers in the cluster must have the same Cisco DCNM-LAN license files installed.

  This requirement is met by the secondary server license installation process. For more information, see the "Secondary Server Licensing Installation" section on page 1-4.

- You must enable or disable secured client communications on all servers in the cluster.

Deploying a Single-Server Cisco DCNM-LAN Environment

You can deploy Cisco DCNM-LAN in a single-server environment. In a single-server environment, the primary Cisco DCNM-LAN server is the one server system that runs the Cisco DCNM-LAN server software. This procedure provides the general steps that you must take to deploy a single-server Cisco DCNM-LAN environment and links to more detailed procedures to help you with each general step.

BEFORE YOU BEGIN

The server system that will run the Cisco DCNM-LAN server must meet the system requirements for the Cisco DCNM-LAN server. For details about system requirements, see the *Cisco DCNM Release Notes, Release 5.x*.

DETAILED STEPS

Step 1 Ensure that the server system that you want to install the Cisco DCNM-LAN server on meets all the server system requirements.

For more information, see the "Prerequisites for Installing a Cisco DCNM-LAN Server" section on page 1-5.

Step 2 Download the Cisco DCNM-LAN server software.

For more information, see the "Downloading the Cisco DCNM-LAN Server Software" section on page 1-11.

Step 3 If your deployment will use a previously installed database, make sure that you have prepared the database:

- PostgreSQL—If the PostgreSQL server system will be remote to the single Cisco DCNM-LAN server, you must configure the PostgreSQL server to allow connections from the Cisco DCNM-LAN server. For more information, see the "Preparing a PostgreSQL Database" section on page 1-6.

  If you intend to install the Cisco DCNM-LAN server on the same server system as the PostgreSQL software, no further database preparation is required.

- Oracle—Cisco DCNM-LAN requires that several Oracle database configuration settings exceed their default settings. For more information, see the "Preparing an Oracle Database" section on page 1-2.

Step 4 Install the Cisco DCNM-LAN server software on the server system.

For more information, see the "Installing a Primary Cisco DCNM-LAN Server" section on page 1-2.

Step 5 (Optional) If you want to encrypt client-server communication, enable the Cisco DCNM-LAN server to use TLS with client-server communications.

For more information, see the "Enabling Encrypted Client-Server Communications" section on page 1-2.

Step 6 (Optional) If you want to allow the use of the Cisco DCNM-LAN client outside a firewall or other gateway device that the Cisco DCNM-LAN server is behind, do the following:

a. Configure the Cisco DCNM-LAN server with a specific secondary server bind port.

For more information, see the "Specifying a Secondary Server Bind Port" section on page 1-6.

b. Configure the firewall or gateway device to permit connections from the Cisco DCNM-LAN client to the ports used by the Cisco DCNM-LAN server, including the secondary server bind port that you specified.

For more information about the ports used by the Cisco DCNM-LAN server, see the "Server Ports" section on page 1-3.

Step 7 (Optional) If you did not start the Cisco DCNM-LAN server when you installed it, start the Cisco DCNM-LAN server now. For more information, see the *Cisco DCNM Fundamentals Guide, Release 5.x*.

Step 8 (Optional) If you want to use licensed Cisco DCNM-LAN features, follow these steps:

a. Acquire Cisco DCNM-LAN licenses. For more information, see the "Implementing Cisco DCNM-LAN Licenses" section on page 1-4.

Note If you did not record the Cisco DCNM-LAN instance ID number when you installed the Cisco DCNM-LAN server software, install the Cisco DCNM-LAN client before performing this step.

b. On the primary Cisco DCNM-LAN server system, install the license. For more information, see the "Installing Licenses on a Primary Cisco DCNM-LAN Server" section on page 1-4.

Step 9 Install the Cisco DCNM-LAN client. For more information, see the *Cisco DCNM Fundamentals Guide, Release 5.x*.

Step 10 Perform device discovery for one or more devices. For more information, see the *Cisco DCNM Fundamentals Guide, Release 5.x*.

Step 11 (Optional) If you installed a license, enable Cisco DCNM-LAN to use licensed features on specific devices by adding managed devices to the license. For more information, see the *Cisco DCNM Fundamentals Guide, Release 5.x*.

Step 12 Begin using Cisco DCNM-LAN to configure and monitor the managed devices. For more information about using Cisco DCNM-LAN, see the Cisco DCNM-LAN configuration guides, available at the following location:

http://www.cisco.com/en/US/products/ps9369/tsd_products_support_series_home.html

Deploying a Clustered-Server Cisco DCNM-LAN Environment

Beginning with Cisco DCNM-LAN Release 5.0, you can deploy Cisco DCNM-LAN in a clustered-server environment. A Cisco DCNM-LAN server cluster includes one primary server and between one and four secondary servers. This procedure provides the general steps that you must take to deploy a clustered-server Cisco DCNM-LAN environment and links to more detailed procedures to help you with each general step.

BEFORE YOU BEGIN

Every server system that will run the Cisco DCNM-LAN server software must meet the system requirements for the Cisco DCNM-LAN server. For details about system requirements, see the *Cisco DCNM Release Notes, Release 5.x*.

DETAILED STEPS

Step 1 Ensure that each server system that will be part of the Cisco DCNM-LAN server cluster meets all the server system requirements.

For more information, see the "Prerequisites for Installing a Cisco DCNM-LAN Server" section on page 1-5.

Step 2 Ensure that each server system meets the additional server requirements for a clustered-server deployment.

For more information, see the "Prerequisites for Deploying a Clustered-Server Cisco DCNM-LAN Environment" section on page 1-6.

Step 3 Download the Cisco DCNM-LAN server software.

For more information, see the "Downloading the Cisco DCNM-LAN Server Software" section on page 1-11.

Step 4 If your deployment will use a previously installed database, make sure that you have prepared the database as follows:

- PostgreSQL—You must configure the PostgreSQL server to allow connections from each remote server in the cluster. For more information, see the "Preparing a PostgreSQL Database" section on page 1-6.

  If you intend to install one of the Cisco DCNM-LAN servers on the same server system as the PostgreSQL software, you do not need to configure the PostgreSQL server to accept connections from the locally installed Cisco DCNM-LAN server.

  Note Cisco DCNM-LAN server installations using a remote PostgreSQL server will fail if the PostgreSQL server is not configured to accept remote connections from the Cisco DCNM-LAN server system.

- Oracle—Cisco DCNM-LAN requires that several Oracle database configuration settings exceed their default settings. For more information, see the "Preparing an Oracle Database" section on page 1-2.

Step 5 Set up a shared directory that all Cisco DCNM-LAN servers in the cluster can use to archive common data and files. The path to the directory can be different for each server. The DCNM-LAN shared directory must be an external shared directory and accessible by all DCNM-LAN servers with read/write privilege. For example, two Cisco DCNM-LAN servers installed on Microsoft Windows could use different paths, such as X:\DCNM\data and F:\data, but the two paths must refer to the same directory.

Step 6 On the primary server system, install the Cisco DCNM-LAN server software.

For more information, see the "Installing a Primary Cisco DCNM-LAN Server" section on page 1-2.

Step 7 If you installed the PostgreSQL server during the primary Cisco DCNM-LAN server, you must configure the PostgreSQL server to allow connections from each secondary Cisco DCNM-LAN server in the cluster, because these connections are remote to the PostgreSQL server system. For more information, see the "Preparing a PostgreSQL Database" section on page 1-6.

Note Cisco DCNM-LAN server installations using a remote PostgreSQL server will fail if the PostgreSQL server is not configured to accept remote connections from the Cisco DCNM-LAN server system.

Step 8 On each secondary server system, install the Cisco DCNM-LAN server software.

For more information, see the "Installing a Secondary Cisco DCNM-LAN Server" section on page 1-7.

Step 9 (Optional) If you want to use secure client communication, enable every Cisco DCNM-LAN server in the cluster to use TLS to encrypt client-server communications.

For more information, see the "Enabling Encrypted Client-Server Communications" section on page 1-2.

Step 10 (Optional) If you want to allow the use of the Cisco DCNM-LAN client outside a firewall or other gateway device that the Cisco DCNM-LAN server cluster is behind, do the following:

a. Configure each Cisco DCNM-LAN server in the cluster with the same, specific secondary server bind port.

For more information, see the "Specifying a Secondary Server Bind Port" section on page 1-6.

b. Configure the firewall or gateway device to permit connections from the Cisco DCNM-LAN client to the ports used by each Cisco DCNM-LAN server in the cluster, including the secondary server bind port that you specified.

For more information about the ports used by the Cisco DCNM-LAN server, see the "Server Ports" section on page 1-3.

Step 11 (Optional) If you have not started all the Cisco DCNM-LAN servers in the cluster, start each server system in the server cluster now. For more information about starting a Cisco DCNM-LAN server cluster, see the *Cisco DCNM Fundamentals Guide, Release 5.x*.

Step 12 (Optional) If you want to use licensed Cisco DCNM-LAN features, follow these steps:

a. Acquire Cisco DCNM-LAN licenses. For more information, see the "Implementing Cisco DCNM-LAN Licenses" section on page 1-4.

Note If you did not record the Cisco DCNM-LAN instance ID number when you installed the primary server, install the Cisco DCNM-LAN client before performing this step.

b. On the primary Cisco DCNM-LAN server system, install the license. For more information, see the "Installing Licenses on a Primary Cisco DCNM-LAN Server" section on page 1-4.

c. On each secondary server system, install the licenses. For more information, see the "Installing Licenses on a Secondary Cisco DCNM-LAN Server" section on page 1-6.

Step 13 Install the Cisco DCNM-LAN client. For more information, see the *Cisco DCNM Fundamentals Guide, Release 5.x*.

Step 14 Perform device discovery for one or more devices. For more information, see the *Cisco DCNM Fundamentals Guide, Release 5.x*.

Step 15 (Optional) If you installed a license, enable Cisco DCNM-LAN to use licensed features on specific devices by adding managed devices to the license. For more information, see the *Cisco DCNM Fundamentals Guide, Release 5.x*.

Step 16 Begin using Cisco DCNM-LAN to configure and monitor the managed devices. For more information about using Cisco DCNM-LAN, see the Cisco DCNM-LAN configuration guides, available at the following location:

http://www.cisco.com/en/US/products/ps9369/tsd_products_support_series_home.html

Downloading the Cisco DCNM-LAN Server Software

This section describes how to download the Cisco DCNM-LAN server software from Cisco.com. The file that you download is in tape archive (TAR) format. It contains the following files:

- dcnm-k9.*release*.exe—Installation file for the supported Microsoft Windows operating system.
- dcnm-k9.*release*.bin—Installation file for the supported Linux operating system.

BEFORE YOU BEGIN

Downloading the Cisco DCNM-LAN server software requires a Cisco.com user account. If you do not have a Cisco.com user account, go to http://www.cisco.com/ and create one before you attempt to download the software.

DETAILED STEPS

Step 1 Open a web browser and go to the following website:

http://www.cisco.com/

The Cisco web page opens.

Step 2 From the Support menu, choose **Download Software**.

The Download Software page appears.

Step 3 Under Select a Software Product Category, choose **Network Management**.

Step 4 If the Log In page appears now, enter your Cisco.com username and password, and then click **Log In**.

The Tools & Resources Download Software web page displays a tree of Cisco devices.

Step 5 From the tree, choose **Data Center Management > Cisco Data Center Network Manager**.

Step 6 If the Log In page appears now, enter your Cisco.com username and password, and then click **Log In**.

A tree of Cisco DCNM releases appears.

Step 7 From the tree, choose the Cisco DCNM release that you need.

To the right of the tree, the Download Now button appears beside the filename and information for the Cisco DCNM release that you chose.

Step 8 Click **Download Now**.

The Download Cart web page lists the Cisco DCNM release that you chose.

Step 9 Click **Proceed with Download**.

The browser lists a link to the software license agreement and the software download rules.

Step 10 Read the software license agreement and the rules, and then click **Agree**.

Step 11 Click **Non Java Download Option**.

A download list appears in a new browser window.

Step 12 Click the **Download** link that appears to the right of the Cisco DCNM release that you chose.

The download begins.

Step 13 After the download completes, extract the files from the downloaded TAR file by doing one of the following:

- For Microsoft Windows, use a file archive utility, such as WinZip, to extract the contents of the TAR file.
- For RHEL, use the following command to extract the contents of the TAR file:

```
tar -xvf dcnm-k9.release.tar
```

Downgrading the Cisco DCNM-LAN Server

The Cisco DCNM installer does not support downgrading to earlier releases.

DETAILED STEPS

Step 1 Uninstall the Cisco DCNM-LAN server that you want to downgrade from.

Step 2 Install and deploy the earlier release of the Cisco DCNM-LAN server that you want to downgrade to. For more information, see the applicable section, as follows:

- Deploying a Single-Server Cisco DCNM-LAN Environment, page 1-7
- Deploying a Clustered-Server Cisco DCNM-LAN Environment, page 1-8.

CHAPTER 1

Preparing a Database for DCNM-LAN

This chapter describes how to prepare a database for a successful Cisco Data Center Network Manager for LAN (DCNM-LAN) installation.

This chapter includes the following sections:

Information About Preparing a Database

A Cisco DCNM-LAN server installation can make use of an existing database if the database is a supported database; however, you might need to prepare the database.

This section includes the following topics:

Oracle Database Preparation

If you plan to use an Oracle database, Cisco DCNM-LAN requires that some Oracle database configuration settings exceed the Oracle default values. Table 1-1 and Table 1-2 list the specific requirements for each supported Oracle database.

Table 1-1 Oracle 10g Database Configuration Requirements

Oracle Setting	Oracle Default	Cisco DCNM-LAN Minimum Requirement
SYSTEM tablespace	1 GB	2 GB
Sessions	50	150
Processes	50	150
Open cursors	50	1000

Table 1-2 Oracle 11g Database Configuration Requirements

Oracle Setting	Oracle Default	Cisco DCNM-LAN Minimum Requirement
Sessions	50	150
Processes	50	150
Open cursors	300	1000

PostgreSQL Database Preparation

If you plan to use a PostgreSQL database that is remote to any Cisco DCNM-LAN server in your deployment, you must ensure that the PostgreSQL server software is configured to permit remote connections from Cisco DCNM-LAN server systems. The pg_hba.conf file in a PostgreSQL database installation controls whether remote connections are allowed. You must ensure that the records in the pg_hba.conf file permit connections from remote Cisco DCNM-LAN server systems prior to installing Cisco DCNM-LAN.

Note When PostgreSQL is chosen as the database, ensure that the Microsoft Windows user installing the software has administrative privileges and not the domain admin privileges. This is a prerequisite for successful installation.

For more information about the pg_hba.conf file, see the documentation for your PostgreSQL server or see the following location:

http://www.postgresql.org/docs/8.2/interactive/auth-pg-hba-conf.html

Preparing an Oracle Database

You can prepare an Oracle database for use by Cisco DCNM-LAN.

DETAILED STEPS

Step 1 (Oracle 10g only) Increase the SYSTEM tablespace to 2 GB from the default of 1 GB. For more information, see the "Increasing the SYSTEM Tablespace" section on page 1-4.

Step 2 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" section on page 1-5.

Step 3 Increase the number of open cursors to 1000. For more information, see the "Increasing the Number of Open Cursors to 1000" section on page 1-5.

Information About the Oracle SQL*Plus 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. In Microsoft Windows, the default location for the SQL*Plus executable is as follows:

C:\oraclexe\app\oracle\product\10.2.0\server\bin

In Linux, the default location for the SQL*Plus binary file is as follows:

/usr/lib/oracle/xe/app/oracle/product/10.2.0/server/bin

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 10g 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/lib/oracle/xe/app/oracle/product/10.2.0/server
export ORACLE_SID=XE
```

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.

DETAILED STEPS

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:

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

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

Information About the init.ora File

The init.ora file specifies startup parameters. The default name and location of the file is platform specific, as shown in Table 1-3.

Table 1-3 Name and Default Location of init.ora File

Oracle Version	Operating System	Content of init.ora File
10g	Microsoft Windows	C:\oraclexe\app\oracle\product\10.2.0\server\database\initXE.ora
	Linux	/usr/lib/oracle/xe/app/oracle/product/10.2.0/server/dbs\initXE.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

The init.ora file should contain only one line, which is the full path of the server parameter file, as shown in Table 1-4.

Table 1-4 Content of init.ora File

Oracle Version	Operating System	Content of init.ora File
10g	Microsoft Windows	SPFILE='C:\oraclexe\app\oracle\product\10.2.0\server\dbs\spfileXE.ora
	Linux	SPFILE='/usr/lib/oracle/xe/app/oracle/product/10.2.0/server/dbs/spfileXE.ora'
11g	Microsoft Windows	SPFILE='C:\oraclexe\app\oracle\product\11.1.0\server\dbs\spfileXE.ora
	Linux	SPFILE='/usr/lib/oracle/orcl/app/oracle/product/11.1.0/db_1/dbs/spfileXE.ora

Increasing the SYSTEM Tablespace

You can increase the SYSTEM tablespace.

DETAILED STEPS

Step 1 Use the SQL*Plus command-line tool to log in to the Oracle database. For more information, see the "Information About the Oracle SQL*Plus Command-Line Tool" section on page 1-3.

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 Step 2.

The SYSTEM tablespace is increased.

Step 4 Enter the **exit** command.

Increasing the Number of Sessions and Processes to 150 Each

You can increase the number of sessions and processes to 150 each.

DETAILED STEPS

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 "Information About the init.ora File" section on page 1-4.

Step 2 Use the SQL*Plus command-line tool to log in to the Oracle database. For more information, see the "Information About the Oracle SQL*Plus Command-Line Tool" section on page 1-3.

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 "Information About the init.ora File" section on page 1-4.

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

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

Step 6 Set the number of processes to 150 by entering the following command:

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

Step 7 Shut down the system by entering the **shutdown** command. If the command fails, use the **shutdown abort** command.

Step 8 Start up the system by entering the **startup** command.

Step 9 Verify that the number of sessions and processes is changed to 150 by entering the following command:

```
show parameter sessions
```

Step 10 Exit by entering the **exit** command.

Increasing the Number of Open Cursors to 1000

You can increase the number of open cursors to 1000.

DETAILED STEPS

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 "Information About the init.ora File" section on page 1-4.

Step 2 Use the SQL*Plus command-line tool to log in to the Oracle database. For more information, see the "Information About the Oracle SQL*Plus Command-Line Tool" section on page 1-3.

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 "Information About the init.ora File" section on page 1-4.

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.

Preparing a PostgreSQL Database

This procedure describes how to configure the PostgreSQL server to permit connections from Cisco DCNM-LAN server systems that are remote to the PostgreSQL server system.

For more information about the pg_hba.conf file, see the documentation for your PostgreSQL server or see the following location:

http://www.postgresql.org/docs/8.2/interactive/auth-pg-hba-conf.html

BEFORE YOU BEGIN

Ensure that the PostgreSQL server is a supported version of PostgreSQL. If you used the Cisco DCNM installer software to install the PostgreSQL server, the version of PostgreSQL is supported. For information about supported databases, see the *Cisco DCNM Release Notes, Release 5.x*.

Determine the IP address of the Cisco DCNM-LAN servers that are remote to the PostgreSQL database server system.

DETAILED STEPS

Step 1 Stop the PostgreSQL database service.

Step 2 Go to the data directory in the PostgreSQL server installation location. In Microsoft Windows, the default location of the data directory for PostgreSQL 8.2 is C:\Program Files\PostgreSQL\8.2\data.

Step 3 In the data directory, use a text editor to open the pg_hba.conf file.

Step 4 In the pg_hba.conf file, locate the connection records for IPv4 connections.

Step 5 For each Cisco DCNM-LAN server system that is remote to the PostgreSQL server system, add one record, as follows:

```
host all all IP-address/32 md5
```

where *IP-address* is the IPv4 address of the Cisco DCNM-LAN server system.

Tip If you want to allow all remote connections, add the following single record:

```
host all all 0.0.0.0/0 md5
```

Step 6 Save and close the pg_hba.conf file.

Step 7 Start the PostgreSQL database service.

Feature History for Preparing a Database

Table 1-5 lists the release history for this feature.

Table 1-5 Feature History for Preparing a Database

Feature Name	Releases	Feature Information
PostgreSQL remote connections	5.0(2)	Information about this requirement was added.
Oracle database configuration	5.0(2)	No change from Release 4.2.

CHAPTER 1

Installing Cisco DCNM-LAN Servers

This chapter describes how to install Cisco Data Center Network Manager for LAN (DCNM-LAN) server software on a server system where no previous Cisco DCNM-LAN server installation is present.

This chapter includes the following sections:

Note The Cisco DCNM installer is the installer for both DCNM-SAN and DCNM-LAN. The installer provides support for the initial installation of both DCNM-SAN and DCNM-LAN on a server.

Information About Cisco DCNM-LAN Server Installation

This section includes the following topics:

Primary Server Installation

You perform a primary server installation when you are installing the Cisco DCNM-LAN server software for either of the following two purposes:

- You are deploying a single-server Cisco DCNM-LAN environment.
- You are installing the first Cisco DCNM-LAN server in a clustered-server environment.

A primary server installation uses the Cisco DCNM installer wizard to collect information about how the Cisco DCNM-LAN server should be configured. After you have provided the installer the information that it needs, it installs the server software.

A primary server installation also creates the following files in the *INSTALL_DIR*/dcm/dcnm/config directory:

- installer.properties—For use during the installation of each secondary server in the server cluster that the primary server belongs to.

- re-installer.properties—For use during the reinstallation of any secondary server in the server cluster that the primary server belongs to.
- licenses-installer.properties—For use during the Cisco DCNM-LAN license installation with any secondary server in the server cluster that the primary server belongs to.

On a Microsoft Windows server system, the default *INSTALL_DIR* value is C:\Program Files\Cisco Systems. On a RHEL server system, the default *INSTALL_DIR* value is /usr/local/cisco.

Secondary Server Installation

You perform a secondary server installation when you are installing additional Cisco DCNM-LAN servers in a clustered-server environment. This type of installation can only be performed after you install the primary server in the cluster.

A secondary server installation is a silent installation. After you run the installer from a command prompt, the installer does not prompt you for information. Instead, a secondary server installation uses the information from the installer.properties file that was created when you installed the primary server in the cluster that the secondary server belongs to.

Using the installer.properties file from the primary server ensures that each secondary server is configured identically, as required by Cisco DCNM-LAN clustered-server deployments. For more information, see the "Clustered-Server Configuration Requirements" section on page 1-6.

Installing a Primary Cisco DCNM-LAN Server

This section describes how to install the Cisco DCNM-LAN server software on a primary server system of a clustered-server environment or as the only server in a single-server environment.

BEFORE YOU BEGIN

Note

- For a single-server deployment, you must have performed Step 1 through Step 3 in the "Deploying a Single-Server Cisco DCNM-LAN Environment" section on page 1-7.
- For a clustered-server deployment, you must have performed Step 1 through Step 5 in the "Deploying a Clustered-Server Cisco DCNM-LAN Environment" section on page 1-8.

If you want the Cisco DCNM-LAN server to use a previously installed database, ensure that the database is running. If the database is remote to the primary server system, ensure that the database is reachable from the primary server system.

Determine the full path to the archive directory that you want Cisco DCNM-LAN to use. If you are deploying a clustered-server Cisco DCNM-LAN environment, determine the full path from the primary server to the directory that you prepared for use by all servers in the cluster. The path to the archive directory does not need to be identical on each server; however, all servers in the cluster must use the same archive directory.

Disable antivirus and instruction detection software on the server system. In general, disable any security software or feature that might interfere with the installation of the Cisco DCNM-LAN server software. After you complete the installation, reenable the software or features.

DETAILED STEPS

Step 1 Log into the server with a user account that has the required privileges, as follows:

- For Microsoft Windows, the user account must be a member of the local administrators group.
- For RHEL, the user account must be root.

If you are installing Cisco DCNM-LAN on Microsoft Windows and using Remote Desktop Connection (RDC) to access the Cisco DCNM-LAN server system, start RDC from a command prompt and use the /console option, as follows:

```
C:\>mstsc /console /v:server
```

where *server* is the DNS name or IP address of the Cisco DCNM-LAN server system.

Step 2 Go to the directory where you downloaded the Cisco DCNM-LAN server software and run one of the following files:

- For Microsoft Windows, run the dcnm-k9.*release*.exe file.
- For RHEL, use the following **sh** command:

```
sh dcnm-k9.release.bin
```

Note For Microsoft Windows and RHEL, the *console* command option is not supported.

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

After the installer prepares the installation, the Introduction step appears in the Cisco DCNM installer window.

Step 3 Click **Next** when the Introduction step appears in the Cisco DCNM installer window after the installer prepares the installation.

Step 4 Click **Next** when the Please Read Before Continuing information appears in the Cisco DCNM installer window.

Step 5 Enter the following when the Choose Install Folder step appears in the Cisco DCNM installer window:

a. Check the DCNM-LAN checkbox.

b. (Optional) If you want to change the default installation folder, type or choose the desired installation folder.

c. Click **Next**.

The Database Options step appears in the Cisco DCNM installer window. You can use an existing PostgreSQL installation or an existing Oracle installation. If PostgreSQL is not installed on the server system, you can use the Cisco DCNM installer to add a PostgreSQL installation.

Note If the Cisco DCNM installer detects an installation of Cisco DCNM-SAN Release 4.2(1) and later releases on the server system, the only database option that is available is the database that DCNM-SAN is configured to use.

Step 6 If you want to install PostgreSQL, do the following:

a. Next to RDBMS, click **Install PostgreSQL**.

If your server system runs RHEL, the System User dialog box appears.

b. (RHEL only) In the System User dialog box, enter the username for the user account that should be used to run the PostgreSQL software. This user account should not have administrator or root privileges.

c. In the DB Admin User field, enter the username of a database administrator account. The installer creates the administrator account that you specify.

d. In the DB Admin Password field, enter the password for the database administrator username that you specified.

e. In the DCNM DB User field, enter the username that Cisco DCNM-LAN should use to access the database. The default username is dcnmuser. The installer will create the user account that you specify.

f. In the DCNM DB Password field, enter the password for the database user account that you specified.

g. In the Confirm DCNM DB Password field, reenter the password for the database user account that you specified.

h. (Optional) If you want to change the default PostgreSQL database installation folder, in the Install Location field, enter or choose the desired installation folder.

Step 7 If you want to use an existing relational database management system (RDBMS) installation, do the following:

a. Next to RDBMS, click one of the following:

- **Use existing PostgreSQL 8.1/8.2/8.3**
- **Use existing Oracle 10g/11g**

If the Cisco DCNM installer detected an existing RDBMS installation, the DB URL field shows the URL to the database.

Note If the Cisco DCNM installer detects an installation of Cisco DCNM-SAN Release 4.2(1) and later releases on the server system, the DB URL field shows the URL of the DCNM-SAN database and cannot be configured.

b. If the DB URL field does not have the correct URL to the database, enter the correct URL.

Note The database is not automatically created. You need to manually create the database. A valid database URL is required to create a database schema and connect to it.

c. In the DB Admin User field, enter the username of a database user account that has permissions to create the Cisco DCNM-LAN database schema and Cisco DCNM-LAN database user account.

d. In the DB Admin Password field, enter the password for the database administrator username that you specified.

e. In the DCNM DB User field, enter the username that Cisco DCNM-LAN should use to access the database.

The installer uses the Cisco DCNM-LAN admin user that you specified to create the Cisco DCNM-LAN database user account.

f. In the DCNM DB Password field, enter the password for the database user account that you specified.

g. In the Confirm DCNM DB Password field, reenter the password for the database user account that you specified.

Step 8 Click **Next**.

Step 9 If the Choose Database (PostgreSQL/Oracle) Root Folder step appears in the Cisco DCNM installer window, do the following:

a. Enter or choose the folder that contains the BIN directory for the existing RDBMS that you specified. The installer lists the default installation paths for the supported databases.

b. Click **Next**.

The Configuration Options step appears in the Cisco DCNM installer window.

Step 10 From the Server IP Address list, choose the IP address that you want to use for the Cisco DCNM-LAN server. The list shows only the IP addresses currently assigned to network interfaces on the server system.

Note The IP address of the server system should be statically assigned. The Cisco DCNM-LAN server binds to an IP address that you specify during installation. If the IP address of the Cisco DCNM-LAN server changes, Cisco DCNM-LAN clients are unable to connect to the Cisco DCNM-LAN server and you must reinstall the Cisco DCNM-LAN server so that you can reconfigure the IP address.

Step 11 If you want to change the port that the Cisco DCNM-LAN web server listens to, enter the new port number in the Web Server Port field. By default, the Cisco DCNM-LAN web server listens to TCP port 8080.

Note If you change the web server port number, it affects the URL that Cisco DCNM-LAN users use to download the Cisco DCNM-LAN client.

Step 12 If you want to change the port that the Cisco DCNM-LAN server accepts Cisco DCNM-LAN client connections on, enter the new port number in the Naming Service Port field in Advanced Settings. By default, the Cisco DCNM-LAN server accepts connections from Cisco DCNM-LAN clients on TCP port 1099.

Note If you change the Cisco DCNM-LAN server port number, it affects the port that Cisco DCNM-LAN users specify when they log into the Cisco DCNM-LAN client.

Step 13 (Optional) For the remaining service ports listed on the Configuration Options step, if you want to specify a different port number, follow these steps in **Advanced Settings**:

a. For each service port number that you want to change, enter the new port number in the field.

b. Click **Resolve Port Conflicts**.

If the Cisco DCNM installer detects that a port that you specified is already in use, it automatically assigns an unused port number to the service.

c. Click **OK** to save the Advanced Settings.

Step 14 Click **Next** to save the Configuration Options and the IP Multicast Addresses Configuration step appears in the Cisco DCNM installer window.

Step 15 (Optional) If you are installing the primary server for a Cisco DCNM-LAN server cluster, follow these steps:

a. In the Partition Name field, enter a unique name for a Cisco DCNM-LAN server cluster. The default partition name is the database host instance ID. The name can contain letters and numbers only.

b. (Optional) As needed, change the multicast IP addresses. You may need to change the multicast IP addresses if the addresses provided by the installer are already in use in the routing environment of the Cisco DCNM-LAN server cluster.

c. (Optional) As needed, change the multicast ports. You may need to change the multicast ports if the port numbers provided by the installer are already in use on the server system that you are installing Cisco DCNM-LAN on.

Step 16 Click **Next**.

The Choose Archive Folder step appears in the Cisco DCNM installer window.

Step 17 Do one of the following:

- If you are deploying a clustered-server Cisco DCNM-LAN environment, enter or choose the archive folder that you prepared for use by all the servers in the cluster.
- If you are deploying a single-server Cisco DCNM-LAN environment, you can accept the default archive folder or choose the desired archive folder.

Step 18 Click **Next**.

The Local User Credentials step appears in the Cisco DCNM installer window.

Step 19 In the Local Admin Username field, enter a name for a Cisco DCNM-LAN server user. The installer creates the Cisco DCNM-LAN server user and assign the Administrator role to it.

Step 20 In the Password field, enter a password for the user, and then in the Confirm Password field, reenter the password.

Note We recommend that you use a strong password. Common guidelines for strong passwords include a minimum password length of eight characters and at least one letter, one number, and one symbol. For example, the password Re1Ax@h0m3 has ten characters and contains uppercase and lowercase letters in addition to one symbol and three numbers.

Step 21 Click **Next**.

The Authentication Settings step appears in the Cisco DCNM installer window.

Choose the authentication method that the Cisco DCNM-LAN server should use to authenticate users who log into the Cisco DCNM-LAN client. You can choose one of the following:

- **Local**—Cisco DCNM-LAN client users are authenticated by the Cisco DCNM-LAN server user accounts only.
- **RADIUS**—Cisco DCNM-LAN client users are authenticated by a RADIUS server.
- **TACACS+**—Cisco DCNM-LAN client users are authenticated by a TACACS+ server.

For RADIUS or TACACS+, you can specify up to three servers.

Step 22 If you chose RADIUS or TACACS+, for each server that you want to specify, do the following:

a. In the server address field, enter the IPv4 address of the server in dotted-decimal format.

b. In the secret key field, type the shared secret of the server.

c. (Optional) If you want to ensure that Cisco DCNM-LAN can communicate with the server, click **Verify**.

Step 23 Click **Next**.

If you are using Microsoft Windows, the installer asks you to specify a shortcut to the application. If you are using RHEL, the installer asks you to specify a link folder.

Step 24 Choose the shortcut or link options that you want.

Step 25 (Optional) If you want the installer to create the shortcuts for all users who can log into the server system, check the **Create Icons for All Users** check box.

Step 26 Click **Next**.

The Pre-Installation Summary step appears in the Cisco DCNM installer window.

Step 27 Carefully review the summary of your choices. If you need to change anything, click **Previous** until the Cisco DCNM installer window displays the step that you need to change, and then return to the applicable preceding step.

Step 28 Click **Next** when you are ready to install the Cisco DCNM-LAN server software.

The installer installs the Cisco DCNM-LAN server software.

The Installing DCNM installer window appears.

Step 29 Choose whether you want to start the Cisco DCNM-LAN server now. If you start the Cisco DCNM-LAN server now, a splash screen appears while the server starts.

The Install Complete step appears in the Cisco DCNM installer window. The Cisco DCNM instance ID number is displayed.

Step 30 (Optional) If you plan to order licenses for Cisco DCNM-LAN, record the Cisco DCNM instance ID number. The licensing process requires that you enter that number.

Note You can begin using Cisco DCNM-LAN without a license but some features are not available unless you purchase and install a license and apply the license to managed devices that you want to use licensed features with.

Step 31 Click **Done**.

If you chose in Step 29 to start the Cisco DCNM-LAN server after installation, a splash screen appears while the server starts.

Step 32 (Optional) If you need to start the Cisco DCNM-LAN server, see the *Cisco DCNM Fundamentals Guide, Release 5.x*.

Step 33 (Optional) If you want to install a Cisco DCNM-LAN license, see Chapter 1, "Licensing a Cisco DCNM-LAN Deployment."

Installing a Secondary Cisco DCNM-LAN Server

Depending on the operating system of the secondary server, you can install the Cisco DCNM-LAN server using the CLI or the DCNM Install Manager tool. You can use the CLI or the DCNM Install Manager tool for a secondary server that runs RHEL. For a secondary server that runs Microsoft Windows, you install the Cisco DCNM-LAN server with the CLI.

This section includes the following topics:

- Installing with the CLI, page 1-8

- Installing with Install Manager, page 1-10

Installing with the CLI

This procedure describes how to install the Cisco DCNM-LAN server software on a secondary server system of a clustered-server environment. Secondary server installations use a silent installation method, which requires the use of a command line interface—for Microsoft Windows, a command prompt window, and for RHEL, a shell window.

The Cisco DCNM installer creates the DCNM_InstallLog.log file in the home directory of the user account that you use to install the secondary server. You can determine the success of the secondary server installation by monitoring the DCNM_InstallLog.log file.

BEFORE YOU BEGIN

Note You must have performed Step 1 through Step 8 in the "Deploying a Clustered-Server Cisco DCNM-LAN Environment" section on page 1-8.

The database that the primary Cisco DCNM-LAN server is configured to use must be running when you install a secondary server.

Determine the IP address of the secondary server.

Determine the full path from the secondary server to the archive directory that you have prepared for use by all servers in the cluster. The path to the archive directory does not need to be identical on each server; however, all servers in the cluster must use the same archive directory.

Note Disable antivirus and instruction detection software on the server system. In general, disable any security software or feature that might interfere with the installation of the Cisco DCNM-LAN server software. After you have completed the installation, reenable the software or features.

DETAILED STEPS

Step 1 From the primary server system, get a copy of the **installer.properties** file from the following location:

INSTALL_DIR/dcm/dcnm/config

On a Microsoft Windows server system, the default *INSTALL_DIR* value is C:\Program Files\Cisco Systems. On a RHEL server system, the default *INSTALL_DIR* value is /usr/local/cisco.

Step 2 Log into the secondary server with a user account that has the required privileges, as follows:

- For Microsoft Windows, the user account must be a member of the local administrators group.
- For RHEL, the user account must be root.

If you are installing Cisco DCNM-LAN on Microsoft Windows and using Remote Desktop Connection (RDC) to access the Cisco DCNM-LAN server system, start RDC from a command prompt and use the /console option, as follows:

```
C:\>mstsc /console /v:server
```

where *server* is the DNS name or IP address of the Cisco DCNM-LAN server system.

Step 3 Choose a directory and copy the following files to that directory:

- The installer.properties file that you copied from the primary Cisco DCNM-LAN server system.
- The Cisco DCNM-LAN server software that you downloaded.

Step 4 At a command prompt, change directories as needed to ensure that the working directory is the directory that contains the installer.properties file and the Cisco DCNM-LAN server software. On Microsoft Windows, use the **chdir** command without arguments to display the working directory. On RHEL, use the **pwd** command.

Step 5 Run the applicable command as follows:

- For Microsoft Windows:
  dcnm-k9.*release***.exe -i silent -f installer.properties**
  -DDCNM_IP_ADDRESS=*server_ip_address* **-DDATA_PATH=***configuration_archive_directory*
  [**-DUSER_INSTALL_DIR=***installation_directory*]
- For RHEL:
  sh dcnm-k9.*release***.bin -i silent -f installer.properties**
  -DDCNM_IP_ADDRESS=*server_ip_address* **-DDATA_PATH=***configuration_archive_directory*
  [**-DUSER_INSTALL_DIR=***installation_directory*]

For example, to install a secondary Cisco DCNM-LAN Release 5.0(2) server in the default installation directory on a Microsoft Windows server system that is assigned the IPv4 address 10.72.139.14 and that has the directory W:\DCNMdata prepared for the Cisco DCNM-LAN configuration archive, the installation command is as follows:

```
dcnm-k9.5.0.2.exe -i silent -f installer.properties -DDCNM_IP_ADDRESS=10.72.189.14
-DDATA_PATH=W:\DCNMdata
```

Table 1-1 describes the command syntax.

Table 1-1 Secondary Server Installation Command Syntax

Option	Description
-i silent	Specifies that the installation is silent.
-f installer.properties	Specifies the installer.properties file.
-DDCNM_IP_ADDRESS=*server_ip_address*	Specifies the IPv4 address of the secondary server on which you are installing the Cisco DCNM-LAN server software.
-DDATA_PATH= *configuration_archive_directory*	Specifies the full path to the archive directory that you prepared for use by all the servers in the cluster.
-DUSER_INSTALL_DIR= *installation_directory*	(Optional) Specifies the full path to a custom installation directory. If you do not include this option, the Cisco DCNM-LAN server is installed at the applicable default location: • For Microsoft Windows: C:\Program Files\Cisco Systems • For RHEL: /usr/local/cisco

Step 6 Monitor the DCNM_InstallLog.log file to determine the status of the installation. The Cisco DCNM installer writes the log file to the home directory of the current user account.

Step 7 (Optional) If you want to install a Cisco DCNM-LAN license, see Chapter 1, "Licensing a Cisco DCNM-LAN Deployment."

Installing with Install Manager

Cisco DCNM Install Manager is a GUI tool for servers running Linux. It is designed to assist in performing silent mode installation operations on secondary servers (remote nodes).

Note Cisco DCNM Install Manager does not support Windows servers.

Note Disable antivirus and instruction detection software on the server system. In general, disable any security software or feature that might interfere with the installation of the Cisco DCNM-LAN server software. After you have completed the installation, reenable the software or features.

DETAILED STEPS

Step 1 To access Install Manager, navigate to the **dcnm-install-manager.sh** file that is located in the bin folder where the DCNM-LAN server was installed.

The default bin folder location for servers running Linux is /usr/local/Cisco/dcm/dcnm/bin.

Step 2 Double click the **dcnm-install-manager.sh** file to launch Install Manager.

Step 3 In the DCNM Installer Folder drop-down list, choose the path that contains the binary executable file for DCNM-LAN server installation.

Step 4 Click the **New** icon in the toolbar near the top of the Install Manager GUI for every secondary server.

A new row in the list of Server Nodes is created every time that the New icon is clicked.

Note Click the **Delete** icon in the toolbar to delete a selected row in the list of Server Nodes. This action does not delete a secondary server from the clustered-server environment.

Step 5 For each secondary server represented by a row in the list of Server Nodes, enter the following:

- Server name or IP address in the Server Name/IP Address field.
- Protocol used for connectivity in the Protocol field.

  The protocol is either Telnet or SSH.
- User credentials (user ID and password) used for connecting to the secondary server in the User Credentials field.

  The user credentials are used for SSH connectivity to the server. Telnet connectivity to the server does not require user credentials.

  Alternatively, default user credentials can be set by entering the credentials in the Default Credentials section of the GUI. The default credentials are used when the User Credential field is blank.
- (Optional) Comments that might be useful to identify the secondary server in the Comments field.

The Last Action Status column in the list of Server Nodes includes the success or failure status of the last performed action. Clicking the **+** icon for the Last Action Status expands the display to show the entire log of actions performed on the server.

Step 6 In the list of Server Nodes, choose the secondary servers to perform the installation.

Step 7 In the toolbar, click the **Verify** icon to verify the connectivity to the selected secondary servers.

Correct any connectivity issues before continuing the installation.

Step 8 (Optional) In the DCNM Install Location field, enter the path on the secondary server for the installation of the DCNM-LAN server.

If the DCNM Install Location field is blank, the Install Manager uses the default path, /usr/local/Cisco/dcm, for the installation of the DCNM-LAN server.

Step 9 In the Data Path Location field, enter the path for the archival configuration data for the secondary servers.

The data path is the same for all the secondary servers and matches the data path of the primary server.

Step 10 In the toolbar, click the **Install** icon to begin the installation on the selected secondary servers.

Before starting the installation, the Install Manager does the following:

- Checks the connectivity to the server.
- Performs upgrade and reinstallation depending on the version already installed.

Step 11 Monitor the Last Action Status column to determine the status of the installation.

In addition, you may also review the DCNM_Installer_Manager.log file. This file, located at /root/.dcnm, contains the log for all the operations of the Install Manager.

If the installation operation fails on a secondary server, the installation log of the secondary server is automatically copied to /usr/local/Cisco/dcm/FailureLog_<SECONDARY_SERVER_IP_ADDRESS>.log on the primary server, where <SECONDARY_SERVER_IP_ADDRESS> is the IP address of the secondary server.

Step 12 (Optional) To install a Cisco DCNM-LAN license, see Chapter 1, "Licensing a Cisco DCNM-LAN Deployment."

Note The Install Manager is a standalone application. The settings specified are not saved and are not persistent. The settings are lost when the Install Manager GUI is closed.

Feature History for Installing Cisco DCNM-LAN Servers

Table 1-2 lists the release history for this feature.

Table 1-2 Feature History for Installing Cisco DCNM-LAN Servers

Feature Name	Releases	Feature Information
Multicast IP address configuration for clustered-server environments	5.0(2)	This feature was introduced.

Table 1-2 Feature History for Installing Cisco DCNM-LAN Servers (continued)

Feature Name	Releases	Feature Information
Secondary server installation	5.0(2)	This feature was introduced.
Install Manager	5.1	This feature was introduced.

CHAPTER 1

Licensing a Cisco DCNM-LAN Deployment

This chapter describes how to install licenses for Cisco Data Center Network Manager for LAN (DCNM-LAN).

This chapter includes the following sections:

Information About Licensing a Cisco DCNM-LAN Deployment

This section includes the following topics:

Cisco DCNM-LAN Licensing

When you install the Cisco DCNM-LAN server, you initially install the software without applying a license. Many of the features of Cisco DCNM-LAN do not require a license. If you try to use a feature that does require a license, Cisco DCNM-LAN displays a message that indicates that a license is required by that feature. To use licensed features, you must install the Cisco DCNM LAN Enterprise license.

To use licensed Cisco DCNM-LAN features with Cisco Nexus 7000 Series switches, you must purchase a DCNM LAN Enterprise license. To use licensed Cisco DCNM-LAN features with other supported Cisco Nexus Series switches, you can obtain a DCNM LAN Enterprise license at no cost.

Table 1-2 shows the Cisco DCNM-LAN features and requirements for a DCNM LAN Enterprise license. Table 1-1 shows the legend for the table of features and requirements.

Table 1-1 Table Legend

Symbol	Description
X	No license required. (Works without a license.)
$0	No cost license. (License for DCNM LAN is required, but has no fee.)
$$	Not free license. (License for DCNM LAN Enterprise is required with fee.)
N/A	Feature not applicable.

Table 1-2 Cisco DCNM-LAN Features and DCNM License Requirements

Cisco DCNM-LAN Feature	Cisco Nexus 7000	Cisco Nexus 5000 /Nexus 3000 /Nexus 2000	Cisco Nexus 4000	Cisco Nexus 1000
Port/Port Channel	X	X	X	X
Virtual Port Channel	$$	$0	N/A	N/A
FEX Port Pinning	N/A	X	N/A	N/A
LACP	X	X	X	X
VLAN 802.1q/PVLAN	X	X	X	X
STP (MST, RPVST)	X	X	X	X
ACL (MAC, IP, VLAN)	X	X	X	X
Traffic Storm Control	X	X	X	X
AAA	X	X	X	X
Environmental (hardware resource utilization with TCAM statistics)	X	X	X	X
Module Temperature	X	N/A	X	X
SPAN	X	X	X	X
Discovery and Inventory	X	X	X	X
L1 and L2 Topology Map	X	X	X	X

Table 1-2 Cisco DCNM-LAN Features and DCNM License Requirements

Cisco DCNM-LAN Feature	Cisco Nexus 7000	Cisco Nexus 5000 /Nexus 3000 /Nexus 2000	Cisco Nexus 4000	Cisco Nexus 1000
Fault Management	X	X	X	X
Traffic Statistics Reports	X	X	X	X
RBAC	X	X	X	X
Serial over LAN / Wake on LAN / Trunk Failover / Chassis Internal Network.g	N/A	N/A	X	X
Web Services and Java API	X	X	X	X
Virtual Device Context	$$	N/A	N/A	N/A
802.1X	$$	$0	$0	$0
GLBP, Object Tracking, Key Chain	$$	$0	$0	$0
HSRP	$$	$0	$0	$0
Cisco Integrated Security Features (DHCP Snooping, Dynamic ARP Inspection, IP Source Guard)	$$	$0	$0	$0
Port Security	$$	$0	$0	$0
Tunnel Interface	$$	$0	$0	$0
Configuration Change Control (arch, roll-back and diff)	$$	$0	$0	$0
OS Image Management	$$	$0	$0	N/A

For information about obtaining and installing a Cisco DCNM LAN Enterprise license, see the "Installing Licenses on a Primary Cisco DCNM-LAN Server" section on page 1-4.

Primary Server Licensing Installation

You perform a primary server license installation when you are installing Cisco DCNM-LAN licenses for either of the following two purposes:

- You are licensing a single-server Cisco DCNM-LAN environment.
- You are installing licenses on the primary Cisco DCNM-LAN server in a clustered-server environment.

A primary server license installation uses the Cisco DCNM installer wizard. After you have provided the license file location to the installer wizard, it installs the licenses on the primary server.

A primary server license installation also creates the licenses-installer.properties file in the *INSTALL_DIR*/dcm/dcnm/config directory. This file is for use during the secondary server license installation with all of the secondary servers that are in the server cluster that the primary server belongs to. On a Microsoft Windows server system, the default *INSTALL_DIR* value is C:\Program Files\Cisco Systems. On a RHEL server system, the default *INSTALL_DIR* value is /usr/local/cisco.

Secondary Server Licensing Installation

You perform a secondary server license installation when you are installing Cisco DCNM-LAN licenses on all secondary servers in a clustered-server environment.

Note If you license a clustered-server Cisco DCNM-LAN deployment, each server in the cluster must have the same license files installed. For more information, see the "Clustered-Server Configuration Requirements" section on page 1-6.

A secondary server license installation is a silent installation. The installer does not prompt you for information. You provide a path to the directory that contains the license files when you run the installer from a command prompt. You also specify the license-installer.properties file that was created when you installed the primary server in the cluster that the secondary server belongs to.

Implementing Cisco DCNM-LAN Licenses

You can obtain a Cisco DCNM LAN no charge license from the Cisco Technical Assistance Center (TAC).

Note You can obtain a Cisco DCNM LAN Enterprise License from your local Cisco partner or your local Cisco account team.

DETAILED STEPS

Step 1 Obtain the Cisco DCNM-LAN Instance ID number by doing one of the following:

- When you finish installing the primary Cisco DCNM-LAN server, record the number when it is displayed at the end of the Cisco DCNM-LAN installation process.
- When running the Cisco DCNM-LAN client, choose **Help > Show Cisco DCNM Instance ID** and record the number.

Step 2 Contact Cisco TAC and obtain one or more Cisco DCNM-LAN licenses. Present the Cisco DCNM-LAN Instance ID number and specify the number of devices that you want to license.

Cisco TAC will send you a license pack file that you can use for each installation that you ordered.

Installing Licenses on a Primary Cisco DCNM-LAN Server

You can install Cisco DCNM-LAN licenses on a primary Cisco DCNM-LAN server.

After you install licenses, you must specify which managed devices that the licenses apply to before you can use Cisco DCNM-LAN licensed features with those devices. For more information, see the *Cisco DCNM Fundamentals Guide, Release 5.x*.

Note Each server in a Cisco DCNM-LAN server cluster must have the same license files installed. For more information, see the "Clustered-Server Configuration Requirements" section on page 1-6.

BEFORE YOU BEGIN

Acquire the license file. For more information, see the "Implementing Cisco DCNM-LAN Licenses" section on page 1-4.

Ensure that there are no executable files in the folder where you plan to install the licenses file.

DETAILED STEPS

Step 1 Log into the primary Cisco DCNM-LAN server system.

Step 2 Download the license pack file that you received from TAC into a directory on the server system.

Caution Make sure that there are no other executable files in the directory where you download the license pack file. Having other files in the directory where you download the license pack file can disrupt the installation of the licenses.

Step 3 Go to the directory where you downloaded the Cisco DCNM-LAN server software and run one of the following files:

- For Microsoft Windows, run the dcnm-k9.*release*.exe file.
- For RHEL, use the following **sh** command:

  ```
  sh dcnm-k9.release.bin
  ```

Step 4 Click **Next** when the Introduction step appears in the Cisco DCNM installer window.

Step 5 Click **Next** when the Please Read Before Continuing information appears in the Cisco DCNM installer window.

Step 6 When the Choose Install Folder step appears in the Cisco DCNM installer window, do the following:

a. Check the **DCNM-LAN** checkbox.

b. Click **Next**.

A warning dialog box indicates that an existing installation of the Cisco DCNM-LAN server was found.

Step 7 Click **OK**.

The Reinstall step appears in the Cisco DCNM installer window.

Step 8 Choose **License Install** and click **Next**.

The Choose Cisco DCNM License Folder step appears in the Cisco DCNM installer window.

Step 9 In the Please Choose a Folder field, enter or choose the folder that contains the license file, and then click **Next**.

The Pre-Installation Summary step appears in the Cisco DCNM installer window. The License files(s) field shows the licenses that the Cisco DCNM installer found in the folder that you specified.

Step 10 Click **Next**.

The Install Complete step appears in the Cisco DCNM installer window.

Step 11 Click **Done**.

You can now specify the managed devices that you want to use licensed Cisco DCNM-LAN features with. For more information, see the *Cisco DCNM Fundamentals Guide, Release 5.x*.

Installing Licenses on a Secondary Cisco DCNM-LAN Server

Depending on the operating system of the secondary server of a clustered-server environment, you can install licenses using the CLI or the DCNM Install Manager tool. You can use the CLI or the DCNM Install Manager tool for a secondary server running RHEL. For a secondary server running Microsoft Windows, you install licenses with the CLI.

Installing Licenses with the CLI

This section describes how to install licenses on a secondary Cisco DCNM-LAN server system of a clustered-server environment. Secondary server license installations use a silent installation method, which requires the use of a command line interface—for Microsoft Windows, a command prompt window, and for RHEL, a shell window.

The Cisco DCNM installer creates the DCNM_InstallLog.log file in the home directory of the user account that you use to install licenses on the secondary server. You can determine the success of the secondary server license installation by monitoring the DCNM_InstallLog.log file.

Note Each server in a Cisco DCNM-LAN server cluster must have the same license files installed. For more information, see the "Clustered-Server Configuration Requirements" section on page 1-6.

BEFORE YOU BEGIN

You must have installed the licenses on the Cisco DCNM-LAN server software on the primary server system. The license-installer.properties file, required for secondary server license installation, is created during primary server license installation.

Note Disable antivirus and instruction detection software on the server system. In general, disable any security software or feature that might interfere with the installation of the Cisco DCNM-LAN server software. After you complete the installation, reenable the software or features.

DETAILED STEPS

Step 1 From the primary Cisco DCNM-LAN server system, get the following:

- A copy of the license-installer.properties file from the following location:

  INSTALL_DIR/dcm/dcnm/config

  On a Microsoft Windows server system, the default *INSTALL_DIR* value is C:\Program Files\Cisco Systems. On a RHEL server system, the default *INSTALL_DIR* value is /usr/local/cisco.

- A copy of the license pack file(s).

Step 2 Log into the secondary server with a user account that has the required privileges, as follows:

- For Microsoft Windows, the user account must be a member of the local administrators group.
- For RHEL, the user account must be root.

If you are installing Cisco DCNM-LAN on Microsoft Windows and using Remote Desktop Connection (RDC) to access the Cisco DCNM-LAN server system, start RDC from a command prompt and use the /console option, as follows:

```
C:\>mstsc /console /v:server
```

where *server* is the DNS name or IP address of the Cisco DCNM-LAN server system.

Step 3 Choose a directory and copy the following files to that directory:

- The license-installer.properties file that you copied from the primary Cisco DCNM-LAN server system.
- The Cisco DCNM-LAN server software that you downloaded.

Step 4 Choose a second directory and copy to that directory the license pack file(s) from the primary server system.

Caution Make sure that there are no other executable files in the directory that you copy the license pack file(s) to. Having other files in the directory where you download the license pack file can disrupt the installation of the licenses.

Step 5 At a command prompt, change directories as needed to ensure that the working directory is the directory that contains the license-installer.properties file and the Cisco DCNM-LAN server installer software. On Microsoft Windows, use the **chdir** command without arguments to display the working directory. On RHEL, use the **pwd** command.

Step 6 Run the applicable command as follows:

- For Microsoft Windows:
  dcnm-k9.*release***.exe -i silent -f license-installer.properties -DLICENSE_FOLDER=***license_directory***
- For RHEL:
  sh dcnm-k9.*release***.bin -i silent -f license-installer.properties -DLICENSE_FOLDER=***license_directory***

For example, to install licenses on a secondary Cisco DCNM-LAN Release 5.0(2) server on a Microsoft Windows server system that has license files in the directory C:\DCNMlic, the installation command is as follows:

```
dcnm-k9.5.0.2.exe -i silent -f license-installer.properties -DLICENSE_FOLDER=C:\DCNMlic
```

Table 1-3 describes the command syntax.

Table 1-3 Secondary Server License Installation Command Syntax

Option	Description
-i silent	Specifies that the installation is silent.
-f license-installer.properties	Specifies the license-installer.properties file.
-DLICENSE_FOLDER= *license_directory*	Specifies the full path to the directory that contains the Cisco DCNM-LAN license pack file(s) that you received from Cisco.

Step 7 Monitor the DCNM_InstallLog.log file to determine the status of the license installation. The Cisco DCNM installer writes the log file to the home directory of the current user account.

Installing Licenses with Install Manager

DCNM Install Manager is a GUI tool for servers running Linux. It is designed to assist in performing silent mode operations on secondary servers (remote nodes).

Note DCNM Install Manager does not support Windows servers.

Note Disable antivirus and instruction detection software on the server system. In general, disable any security software or feature that might interfere with the license install of the Cisco DCNM-LAN server software. After you complete the license install, reenable the software or features.

DETAILED STEPS

Step 1 To access Install Manager, navigate to the **dcnm-install-manager.sh** file that is located in the bin folder where the DCNM-LAN server was installed.

The default bin folder location for servers running Linux is /usr/local/Cisco/dcm/dcnm/bin.

Step 2 Double click the **dcnm-install-manager.sh** file to launch Install Manager.

Step 3 In the DCNM Installer Folder drop-down list, choose the path that contains the binary executable file for DCNM-LAN server installation.

Step 4 In the DCNM License Folder drop-down list, choose the path that contains the license file for the DCNM-LAN server.

Step 5 In the toolbar, click the **New** icon in the toolbar near the top of the Install Manager GUI for every secondary server.

A new row in the list of Server Nodes is created every time that the New icon is clicked.

Note Click the **Delete** icon in the toolbar to delete a selected row in the list of Server Nodes. This action does not delete a secondary server from the clustered-server environment.

Step 6 For each secondary server represented by a row in the list of Server Nodes, enter the following:

- Server name or IP address in the Server Name/IP Address field.
- Protocol used for connectivity in the Protocol field.

  The protocol is either Telnet or SSH.
- User credentials (user ID and password) used for connecting to the secondary server in the User Credentials field.

  The user credentials are used for SSH connectivity to the server. Telnet connectivity to the server does not require user credentials.

Alternatively, default user credentials can be set by entering the credentials in the Default Credentials section of the GUI. The default credentials are used when the User Credential field is blank.

- (Optional) Comments that might be useful to identify the secondary server in the Comments field.

The Last Action Status column in the list of Server Nodes includes the success or failure status of the last performed action. Clicking the **+** icon for the Last Action Status expands the display to show the entire log of actions performed on the server.

Step 7 In the list of Server Nodes, choose the secondary servers to perform the license install.

Step 8 In the toolbar, click the **Verify** icon to verify the connectivity to the selected secondary servers.

Correct any connectivity issues before continuing the license install.

Step 9 (Optional) In the DCNM Install Location field, enter the path on the secondary server for the license install of the DCNM-LAN server.

If the DCNM Install Location field is blank, the Install Manager uses the default path, /usr/local/Cisco/dcm, for the license install of the DCNM-LAN server.

Step 10 In the toolbar, click the **License Install** icon to begin the installation on the selected secondary servers.

Step 11 Monitor the Last Action Status column to determine the status of the license install.

In addition, you may also review the DCNM_Installer_Manager.log file. This file, located at /root/.dcnm, contains the log for all the operations of the Install Manager.

If the license installation operation fails on a secondary server, the installation log of the secondary server is automatically copied to /usr/local/Cisco/dcm/FailureLog_<SECONDARY_SERVER_IP_ADDRESS>.log on the primary server, where <SECONDARY_SERVER_IP_ADDRESS> is the IP address of the secondary server.

Note The Install Manager is a standalone application. The settings specified are not saved and are not persistent. The settings are lost when the Install Manager GUI is closed.

Feature History for Licensing a Cisco DCNM-LAN Deployment

Table 1-4 lists the release history for this feature.

Table 1-4 Feature History for Licensing a Cisco DCNM-LAN Deployment

Feature Name	Releases	Feature Information
Support for a clustered-server environment	5.0(2)	This feature was introduced.
Install Manager	5.1	This feature was introduced.

CHAPTER 1

Upgrading Cisco DCNM-LAN Servers

This chapter describes how to upgrade Cisco Data Center Network Manager for LAN (DCNM-LAN) on a server system where a previous installation of an earlier Cisco DCNM-LAN release is present.

This chapter includes the following sections:

Information About Cisco DCNM-LAN Server Upgrades

This section includes the following topics:

Primary Server Upgrades

You perform a primary server upgrade when you upgrade to a newer release of the Cisco DCNM-LAN server software for either of the following two purposes:

- You are upgrading a single-server Cisco DCNM-LAN environment.
- You are upgrading the primary Cisco DCNM-LAN server in a clustered-server environment.

Note All servers in a Cisco DCNM-LAN server cluster must run an identical release of Cisco DCNM-LAN, such as Cisco DCNM-LAN Release 5.0(2). If you upgrade the primary server, you must upgrade all secondary servers in the cluster.

A primary server upgrades use the Cisco DCNM installer wizard to collect information about how the upgraded Cisco DCNM-LAN server should be configured. After you have provided the installer the information that it needs, it upgrades the server software.

A primary server upgrades also create the upgrade-installation.properties file in the *INSTALL_DIR*/dcm/dcnm/config directory. This file is for use during the upgrade of each secondary server in the server cluster that the primary server belongs to. On a Microsoft Windows server system, the default *INSTALL_DIR* value is C:\Program Files\Cisco Systems. On a RHEL server system, the default *INSTALL_DIR* value is /usr/local/cisco.

Secondary Server Upgrades

you perform a secondary server upgrade when you upgrade secondary Cisco DCNM-LAN servers in a clustered-server environment. This upgrade can be performed only after you upgrade the primary server in the cluster.

A secondary server upgrade is a silent installation. After you run the installer from a command prompt, the installer does not prompt you for information. Instead, a secondary server upgrade uses the information from the upgrade-installer.properties file that was created when you upgraded the primary server in the cluster that the secondary server belongs to.

Using the upgrade-installer.properties file from the primary server ensures that each secondary server is configured identically, as required by Cisco DCNM-LAN clustered-server deployments. For more information, see the "Clustered-Server Configuration Requirements" section on page 1-6.

Upgrading Cisco DCNM-LAN Servers

This section includes the following topics:

Single-Server Cisco DCNM-LAN Upgrade Process

You can upgrade a clustered-server Cisco DCNM-LAN environment.

DETAILED STEPS

Step 1 Ensure that the Cisco DCNM-LAN server system meets all the server system requirements. In particular, ensure that the server system meets the requirements in the *Cisco DCNM Release Notes, Release 5.x*.

For more information, see the "Prerequisites for Installing a Cisco DCNM-LAN Server" section on page 1-5.

Step 2 Download the Cisco DCNM-LAN server software.

For more information, see the "Downloading the Cisco DCNM-LAN Server Software" section on page 1-11.

Step 3 On the Cisco DCNM-LAN server system, upgrade the Cisco DCNM-LAN server software.

For more information, see the "Upgrading a Primary Cisco DCNM-LAN Server" section on page 1-4.

Note If the database used by Cisco DCNM-LAN is remote to the primary server and if the upgrade that you are performing requires database migration, the Cisco DCNM installer warns you that you must perform database migration manually and then run the Cisco DCNM installer again. The warning will indicate where you can find the database migration tool. Instructions for using the database migration tool manually are included in a readme.txt file with the tool.

Step 4 (Optional) If you have not started the Cisco DCNM-LAN server, start it now. For more information about starting a Cisco DCNM-LAN server, see the *Cisco DCNM Fundamentals Guide, Release 5.x*.

Step 5 Install the Cisco DCNM-LAN client. For more information, see the *Cisco DCNM Fundamentals Guide, Release 5.x*.

Clustered-Server Cisco DCNM-LAN Upgrade Process

You can upgrade a clustered-server Cisco DCNM-LAN environment.

DETAILED STEPS

Step 1 Ensure that each server system in the Cisco DCNM-LAN server cluster meets all the server system requirements. In particular, ensure that each server system meets the requirements in the *Cisco DCNM Release Notes, Release 5.x*.

For more information, see the "Prerequisites for Installing a Cisco DCNM-LAN Server" section on page 1-5.

Step 2 Ensure that each server system meets the additional server requirements for a clustered-server deployment.

For more information, see the "Prerequisites for Deploying a Clustered-Server Cisco DCNM-LAN Environment" section on page 1-6.

Step 3 Download the Cisco DCNM-LAN server software.

For more information, see the "Downloading the Cisco DCNM-LAN Server Software" section on page 1-11.

Step 4 On the primary server system, upgrade the Cisco DCNM-LAN server software.

For more information, see the "Upgrading a Primary Cisco DCNM-LAN Server" section on page 1-4.

Note If the database used by Cisco DCNM-LAN is remote to the primary server and if the upgrade that you are performing requires database migration, the Cisco DCNM installer warns you that you must perform database migration manually and then run the Cisco DCNM installer again. The warning will indicate where you can find the database migration tool. Instructions for using the database migration tool manually are included in a readme.txt file with the tool.

Step 5 On each secondary server system, upgrade the Cisco DCNM-LAN server software.

For more information, see the "Upgrading a Secondary Cisco DCNM-LAN Server" section on page 1-6.

Step 6 (Optional) If you have not started all the Cisco DCNM-LAN servers in the cluster, start each server system in the server cluster now. For more information about starting a Cisco DCNM-LAN server cluster, see the *Cisco DCNM Fundamentals Guide, Release 5.x*.

Step 7 Install the Cisco DCNM-LAN client. For more information, see the *Cisco DCNM Fundamentals Guide, Release 5.x*.

Upgrading a Primary Cisco DCNM-LAN Server

You can upgrade a primary Cisco DNCM server to a more recent release of Cisco DCNM-LAN.

BEFORE YOU BEGIN

Note

- For a single-server Cisco DCNM-LAN environment, you must have performed Step 1 through Step 2 in the "Single-Server Cisco DCNM-LAN Upgrade Process" section on page 1-2.
- For a clustered-server Cisco DCNM-LAN environment, you must have performed Step 1 through Step 3 in the "Clustered-Server Cisco DCNM-LAN Upgrade Process" section on page 1-3.

Disable antivirus and instruction detection software on the server system. In general, disable any security software or feature that might interfere with the installation of the Cisco DCNM-LAN server software. After you complete the installation, reenable the software or features.

Note When upgrading a DCNM-LAN server that is also running Fabric Manager, you must first stop Cisco Fabric Manager and uninstall Fabric Manager before proceeding with the upgrade of the DCNM-LAN server. After upgrading the DCNM_LAN server, you can install DCNM-SAN to replace the pre-existing Fabric Manager. For more information about upgrading DCNM-SAN, see Upgrading Cisco DCNM-SAN, page 1-1.

DETAILED STEPS

Step 1 Log into the server with a user account that has the required privileges, as follows:

- For Microsoft Windows, the user account must be a member of the local administrators group.
- For RHEL, the user account must be root.

If you are installing Cisco DCNM-LAN on Microsoft Windows and using Remote Desktop Connection (RDC) to access the Cisco DCNM-LAN server system, start RDC from a command prompt and use the /console option, as follows:

```
C:\>mstsc /console /v:server
```

where *server* is the DNS name or IP address of the Cisco DCNM-LAN server system.

Step 2 If you have not already done so, stop the Cisco DCNM-LAN server.

Step 3 Go to the directory where you downloaded the updated Cisco DCNM-LAN server software and run one of the following files:

- For Microsoft Windows, run the dcnm-k9.*release*.exe file.

- For RHEL, use the following **sh** command:

  `sh dcnm-k9.release.bin`

The Introduction step appears in the Cisco DCNM installer window.

Step 4 Click **Next**.

The Please Read Before Continuing information appears in the Cisco DCNM installer window.

Step 5 Click **Next**.

Step 6 The Choose Install Folder step appears in the Cisco DCNM installer window, do the following:

a. Check the **DCNM-LAN** checkbox.

b. Click **Next**.

A warning dialog box indicates that an existing installation of the Cisco DCNM-LAN server was found.

Step 7 Click **OK**.

Note The database user credential fields are disabled (Step 8 to Step 10) and user intervention is not required.

The Database Options step appears in the Cisco DCNM installer window.

Step 8 In the DB Admin User field, enter the username of a database user account that has administrator permissions in the database.

Step 9 In the DB Admin Password field, type the password for the database administrator username that you specified.

Step 10 Click **Next**.

The Pre-Installation Summary step appears in the Cisco DCNM installer window.

Step 11 Carefully review the summary of your choices. If you need to change anything, click **Previous** until the the Cisco DCNM installer window displays the step that you need to change, and then return to the applicable preceding step.

Step 12 When you are ready to install the Cisco DCNM-LAN server software, click **Next**.

The installer installs the Cisco DCNM-LAN server software.

The Install Complete step appears in the Cisco DCNM installer window.

Caution Clicking **Cancel** after you click **Next** is not recommended. Canceling the operation at this step puts the DCNM server in an inconsistent state and would require you to uninstall DCNM and start the installation process again.

Step 13 Choose whether you want to start the Cisco DCNM-LAN server now. If you start the Cisco DCNM-LAN server now, a splash screen appears while the server starts.

The Install Complete step appears in the Cisco DCNM installer window. The Cisco DCNM instance ID number is displayed.

Step 14 Click **Done**.

Step 15 (Optional) If you need to start the Cisco DCNM-LAN server, see the *Cisco DCNM Fundamentals Guide, Release 5.x*.

Step 16 (Optional) If the server system is the primary server of a clustered-server environment, you must upgrade Cisco DCNM-LAN on each secondary server in the server cluster. For more information, see the "Upgrading a Secondary Cisco DCNM-LAN Server" section on page 1-6.

Upgrading a Secondary Cisco DCNM-LAN Server

Depending on the operating system of the secondary server, you can upgrade the Cisco DCNM-LAN server using the CLI or the DCNM Install Manager tool. You can use the CLI or the DCNM Install Manager tool for a secondary serverthat runs RHEL. For a secondary server that runs Microsoft Windows, you upgrade the Cisco DCNM-LAN server with the CLI.

Upgrading with the CLI

This section describes how to upgrade the Cisco DCNM-LAN server software on a secondary server system of a clustered-server environment.

Note Support for Cisco DCNM-LAN clustered-server environments was introduced in Cisco DCNM-LAN Release 5.0(2); therefore, you cannot perform a secondary server upgrade from a Cisco DCNM-LAN release prior to Release 5.0(2).

The Cisco DCNM installer creates the DCNM_InstallLog.log file in the home directory of the user account that you use to upgrade the secondary server. You can determine the success of the secondary server upgrade installation by monitoring the DCNM_InstallLog.log file.

BEFORE YOU BEGIN

Note You must have performed Step 1 through Step 4 in the "Clustered-Server Cisco DCNM-LAN Upgrade Process" section on page 1-3.

You must have upgraded the Cisco DCNM-LAN server software on the primary server system. The upgrade-installer.properties file, required for secondary server upgrade, is created during the primary server upgrade.

Determine the IP address of the secondary server.

Disable antivirus and instruction detection software on the server system. In general, disable any security software or feature that may interfere with the installation of the Cisco DCNM-LAN server software. After you complete the installation, reenable the software or features.

DETAILED STEPS

Step 1 From the primary server system, get a copy of the upgrade-installer.properties file from the following location:

INSTALL_DIR/dcm/dcnm/config

On a Microsoft Windows server system, the default *INSTALL_DIR* value is C:\Program Files\Cisco Systems. On a RHEL server system, the default *INSTALL_DIR* value is /usr/local/cisco.

Step 2 Log into the secondary server with a user account that has the required privileges, as follows:

- For Microsoft Windows, the user account must be a member of the local administrators group.
- For RHEL, the user account must be root.

If you are installing Cisco DCNM-LAN on Microsoft Windows and using Remote Desktop Connection (RDC) to access the Cisco DCNM-LAN server system, start RDC from a command prompt and use the /console option, as follows:

```
C:\>mstsc /console /v:server
```

where *server* is the DNS name or IP address of the Cisco DCNM-LAN server system.

Step 3 Choose a directory and copy the following files to that directory:

- The upgrade-installer.properties file that you copied from the primary Cisco DCNM-LAN server system.
- The Cisco DCNM-LAN server software that you downloaded.

Step 4 At a command prompt, change directories as needed to ensure that the working directory is the directory that contains the installer.properties file and the Cisco DCNM-LAN server software. On Microsoft Windows, use the **chdir** command without arguments to display the working directory. On RHEL, use the **pwd** command.

Step 5 Run the applicable command as follows:

- For Microsoft Windows:
  dcnm-k9.*release*.exe -i silent -f upgrade-installer.properties -DDCNM_IP_ADDRESS=*server_ip_address*
- For RHEL:
  sh dcnm-k9.*release*.bin -i silent -f upgrade-installer.properties -DDCNM_IP_ADDRESS=*server_ip_address*

For example, to upgrade a secondary Cisco DCNM-LAN Release 5.0(2) server on a Microsoft Windows server system that is assigned the IPv4 address 10.72.139.14, the installation command is as follows:

```
dcnm-k9.5.0.2.exe -i silent -f upgrade-installer.properties -DDCNM_IP_ADDRESS=10.72.189.14
```

Table 1-1 describes the command syntax.

Table 1-1 Secondary Server Upgrade Command Syntax

Option	Description
-i silent	Specifies that the installation is silent.
-f installer.properties	Specifies the upgrade-installer.properties file.
-DDCNM_IP_ADDRESS=*server_ip_address*	Specifies the IPv4 address of the secondary server on which you are installing the Cisco DCNM-LAN server software.

Step 6 Monitor the DCNM_InstallLog.log file to determine the status of the upgrade installation. The Cisco DCNM installer writes the log file to the home directory of the current user account.

Step 7 (Optional) If you want to install a Cisco DCNM-LAN license, see Chapter 1, "Licensing a Cisco DCNM-LAN Deployment."

Upgrading with Install Manager

DCNM Install Manager is a GUI tool for servers that run Linux. It is designed to assist in performing silent mode operations on secondary servers (remote nodes).

Note DCNM Install Manager does not support Windows servers.

Note Disable antivirus and instruction detection software on the server system. In general, disable any security software or feature that might interfere with the upgrade of the Cisco DCNM-LAN server software. After you have completed the upgrade, reenable the software or features.

DETAILED STEPS

Step 1 To access Install Manager, navigate to the **dcnm-install-manager.sh** file that is located in the bin folder where the DCNM-LAN Server was installed.

The default bin folder location for servers running Linux is /usr/local/Cisco/dcm/dcnm/bin.

Step 2 Double click the **dcnm-install-manager.sh** file to launch Install Manager.

Step 3 In the DCNM Installer Folder drop-down list, choose the path that contains the binary executable file for DCNM-LAN server installation.

Step 4 Click the **New** icon in the toolbar near the top of the Install Manager GUI for every secondary server.

A new row in the list of Server Nodes is created every time the New icon is clicked.

Note In the toolbar, click the **Delete** icon to delete a selected row in the list of Server Nodes. This action does not delete a secondary server from the clustered-server environment.

Step 5 For each secondary server represented by a row in the list of Server Nodes, enter the following:

- Server name or IP address in the Server Name/IP Address field.
- Protocol used for connectivity in the Protocol field.

  The protocol is either Telnet or SSH.
- User credentials (user ID and password) used for connecting to the secondary server in the User Credentials field.

  The user credentials are used for SSH connectivity to the server. Telnet connectivity to the server does not require user credentials.

  Alternatively, default user credentials may be set by entering the credentials in the Default Credentials section of the GUI. The default credentials are used when the User Credential field is blank.
- (Optional) Comments that may be useful to identify the secondary server in the Comments field.

The Last Action Status column in the list of Server Nodes includes the success or failure status of the last performed action. Clicking the + icon for the Last Action Status expands the display to show the entire log of actions performed on the server.

Step 6 In the list of Server Nodes, select the secondary servers to perform the upgrade.

Step 7 In the toolbar, click the **Verify** icon to verify the connectivity to the selected secondary servers.

Correct any connectivity issues before continuing the installation.

Step 8 (Optional) In the DCNM Install Location field, enter the path on the secondary server for the installation of the DCNM-LAN server.

If the DCNM Install Location field is blank, the Install Manager uses the default path, /usr/local/Cisco/dcm, for the installation of the DCNM-LAN server.

Step 9 Click the **Install** icon in the toolbar to begin the installation on the selected secondary servers.

Before starting the upgrade, the Install Manager does the following:

- Checks the connectivity to the server.
- Performs upgrade and reinstallation depending on the version already installed.

Step 10 Monitor the Last Action Status column to determine the status of the upgrade.

In addition, you may also review the DCNM_Installer_Manager.log file. This file, located at /root/.dcnm, contains the log for all the operations of the Install Manager.

If the upgrade operation fails on a secondary server, the installation log of the secondary server is automatically copied to /usr/local/Cisco/dcm/FailureLog_<SECONDARY_SERVER_IP_ADDRESS>.log on the primary server, where <SECONDARY_SERVER_IP_ADDRESS> is the IP address of the secondary server.

Step 11 (Optional) Install a Cisco DCNM-LAN license. For more information, see Chapter 1, "Licensing a Cisco DCNM-LAN Deployment."

Note The Install Manager is a standalone application. The settings specified are not saved and are not persistent. The settings are lost when the Install Manager GUI is closed.

Feature History for Upgrading Cisco DCNM-LAN Servers

Table 1-2 lists the release history for this feature.

Table 1-2 Feature History for Upgrading Cisco DCNM-LAN Servers

Feature Name	Releases	Feature Information
Support for a clustered-server environment	5.0(2)	This feature was introduced.
Install Manager	5.1	This feature was introduced.

CHAPTER 1

Configuring Cisco DCNM-LAN Servers

This chapter describes how to configure Cisco Data Center Network Manager for LAN (DCNM-LAN) servers.

This chapter includes the following sections:

Configuring Secure Client Communications

This section describes how to configure Cisco Data Center Network Manager for LAN (DCNM-LAN) for secure client-server communications.

This section includes the following topics:

Information About Secure Client Communications

This section includes the following topics:

Encrypted Client-Server Communications

By default, communication between the Cisco DCNM-LAN client and server is unencrypted; however, you can enable secure client-server communications, which uses Transport Layer Security (TLS), a protocol based on the Secure Sockets Layer (SSL) 3.0 protocol. In particular, communications between the Cisco DCNM-LAN client and the EJB port on the Cisco DCNM-LAN server are encrypted when you enable secure client communications.

Enabling secure client communications does not affect how users download, install, and log into the Cisco DCNM-LAN client.

Firewall Support for Client-Server Communications

Cisco DCNM-LAN supports client-server connections across gateway devices such as a firewall; however, you must configure any gateway devices to allow the connections that the client must open to the Cisco DCNM-LAN server. The ports on the Cisco DCNM-LAN server that gateway devices must permit traffic to reach are listed in Table 1-1.

By default, the secondary server bind port is assigned a random port number when the Cisco DCNM-LAN server starts. To support client-server communications across a gateway device, you must configure the Cisco DCNM-LAN server to use a specific port for the secondary server bind service.

Configuring Secure Client Communications

This section includes the following topics:

Enabling Encrypted Client-Server Communications

You can enable TLS to encrypt client-server communications.

If your Cisco DCNM-LAN deployment is a clustered-server deployment, you must perform this procedure on each server in the cluster.

DETAILED STEPS

Step 1 Stop the Cisco DCNM-LAN server. If you are enabling secure client communications on a server cluster, use the stop-dcnm-cluster script. For single-server deployments, do one of the following:

- Microsoft Windows—Choose **Start > All Programs > Cisco DCNM Server > Stop DCNM Server**.
- RHEL—Use the Stop_DCNM_Server script.

For more information about stopping Cisco DCNM-LAN, see the *Cisco DCNM Fundamentals Guide, Release 5.x*.

Step 2 In a text editor, open the jboss-service.xml file that is at the following location:

INSTALL_DIR\dcm\jboss-4.2.2.GA\server\dcnm\deploy\ejb3.deployer\META-INF\jboss-service.xml

where *INSTALL_DIR* is the Cisco DCNM installation directory. On Microsoft Windows, the default installation directory is C:\Program Files\Cisco Systems. On RHEL systems, the default installation directory is /usr/local/cisco.

Step 3 Find the following section in the file. Verify that the section you find matches the following lines exactly.

```
<!--mbean code="org.jboss.remoting.transport.Connector"
name="jboss.remoting:type=Connector,transport=SslEjb3Connector,handler=ejb3">
  <depends>jboss.aop:service=AspectDeployer</depends>
  <attribute
name="InvokerLocator">sslsocket://${jboss.bind.address}:${cisco.dcnm.remoting.sslejbport:3
843}</attribute>
  <attribute name="Configuration">
    <handlers>
```

```
      <handler
subsystem="AOP">org.jboss.aspects.remoting.AOPRemotingInvocationHandler</handler>
    </handlers>
  </attribute>
</mbean-->
```

The section is commented out using the standard XML comment markers, <!-- and -->.

Step 4 Uncomment the section as follows:

a. From the first line of the section, remove the following three characters from before mbean:

```
!--
```

The changed line should read as follows:

```
<mbean code="org.jboss.remoting.transport.Connector"
name="jboss.remoting:type=Connector,transport=SslEjb3Connector,handler=ejb3">
```

b. From the last line of the section, remove the following two characters after mbean:

```
--
```

The changed line should read as follows:

```
</mbean>
```

Step 5 Save and close the jboss-service.xml file.

Step 6 In a text editor, open the jboss-service.xml file that is at the following location:

INSTALL_DIR\dcm\jboss-4.2.2.GA\server\dcnm\conf\jboss-service.xml

Note This is a different jboss-service.xml file than you opened in Step 2.

Step 7 Find the following section in the file.

```
cisco.dcnm.remoting.transport=socket
cisco.dcnm.remoting.port=3873
cisco.dcnm.remoting.ejbport=3873
cisco.dcnm.remoting.sslejbport=3843
cisco.dcnm.remoting.client.invokerDestructionDelay=0
```

The port numbers at the end of the last three lines may vary from this example, depending upon whether the default port numbers were changed during Cisco DCNM-LAN server installation.

Step 8 Change the cisco.dcnm.remoting.transport value to sslsocket. The changed line should read as follows:

```
cisco.dcnm.remoting.transport=sslsocket
```

Step 9 Change the cisco.dcnm.remoting.port value to match the value specified for cisco.dcnm.remoting.sslejbport. For example, if the Cisco DCNM-LAN server is configured to use the default SSL port, the cisco.dcnm.remoting.sslejbport value is 3843 and the changed line would read as follows:

```
cisco.dcnm.remoting.port=3843
```

Step 10 Change the cisco.dcnm.remoting.client.invokerDestructionDelay value to 30000. The changed line should read as follows:

```
cisco.dcnm.remoting.client.invokerDestructionDelay=30000
```

Step 11 Save and close the jboss-service.xml file.

Step 12 Do one of the following:

- If your Cisco DCNM-LAN deployment is a clustered-server deployment, repeat this procedure on each server in the cluster and then start the servers, beginning with the master server first. Allow at least one minute between starting each server.
- If your deployment is a single-server deployment, start the Cisco DCNM-LAN server.

For more information about starting a single Cisco DCNM-LAN or a cluster of Cisco DCNM-LAN servers, see the *Cisco DCNM Fundamentals Guide, Release 5.x*.

Disabling Encrypted Client-Server Communications

You can disable secure client communications.

If your Cisco DCNM-LAN deployment is a clustered-server deployment, you must perform the following steps on each server in the cluster.

DETAILED STEPS

Step 1 Stop the Cisco DCNM-LAN server. If you are disabling secure client communications on a server cluster, use the stop-dcnm-cluster script. For single-server deployments, do one of the following:

- Microsoft Windows—Choose **Start > All Programs > Cisco DCNM Server > Stop DCNM Server**.
- RHEL—Use the Stop_DCNM_Server script.

For more information about stopping Cisco DCNM-LAN, see the *Cisco DCNM Fundamentals Guide, Release 5.x*.

Step 2 In a text editor, open the jboss-service.xml file that is at the following location:

INSTALL_DIR\dcm\jboss-4.2.2.GA\server\dcnm\deploy\ejb3.deployer\META-INF\jboss-service.xml

where *INSTALL_DIR* is the Cisco DCNM installation directory. On Microsoft Windows, the default installation directory is C:\Program Files\Cisco Systems. On RHEL systems, the default installation directory is /usr/local/cisco.

Step 3 Find the following section in the file. Verify that the section you find matches the following lines exactly.

```
<mbean code="org.jboss.remoting.transport.Connector"
name="jboss.remoting:type=Connector,transport=SslEjb3Connector,handler=ejb3">
  <depends>jboss.aop:service=AspectDeployer</depends>
  <attribute
name="InvokerLocator">sslsocket://${jboss.bind.address}:${cisco.dcnm.remoting.sslejbport:3
843}</attribute>
  <attribute name="Configuration">
    <handlers>
      <handler
subsystem="AOP">org.jboss.aspects.remoting.AOPRemotingInvocationHandler</handler>
    </handlers>
  </attribute>
</mbean>
```

The section is commented out using the standard XML comment markers.

Step 4 Use the standard XML comment markers to comment out the section, as follows:

a. To the first line of the section, add the following three characters before mbean:

```
!--
```

The changed line should read as follows:

```
<!--mbean code="org.jboss.remoting.transport.Connector"
name="jboss.remoting:type=Connector,transport=SslEjb3Connector,handler=ejb3">
```

b. To the last line of the section, add the following two characters after mbean:

```
--
```

The changed line should read as follows:

```
</mbean-->
```

Step 5 Save and close the jboss-service.xml file.

Step 6 In a text editor, open the jboss-service.xml file that is at the following location:

INSTALL_DIR\dcm\jboss-4.2.2.GA\server\dcnm\conf\jboss-service.xml

Note This is a different jboss-service.xml file than you opened in Step 2.

Step 7 Find the following section in the file.

```
cisco.dcnm.remoting.transport=sslsocket
cisco.dcnm.remoting.port=3843
cisco.dcnm.remoting.ejbport=3873
cisco.dcnm.remoting.sslejbport=3843
cisco.dcnm.remoting.client.invokerDestructionDelay=30000
```

The port numbers at the end of the last three lines may vary from this example, depending upon whether the default port numbers were changed during Cisco DCNM-LAN server installation.

Step 8 Change the cisco.dcnm.remoting.transport value to socket. The changed line should read as follows:

```
cisco.dcnm.remoting.transport=socket
```

Step 9 Change the cisco.dcnm.remoting.port value to match the value specified for cisco.dcnm.remoting.ejbport. For example, if the Cisco DCNM-LAN server is configured to use the default EJB port, the cisco.dcnm.remoting.ejbport value is 3873 and the changed line would read as follows:

```
cisco.dcnm.remoting.port=3873
```

Step 10 Change the cisco.dcnm.remoting.client.invokerDestructionDelay value to 0. The changed line should read as follows:

```
cisco.dcnm.remoting.client.invokerDestructionDelay=0
```

Step 11 Save and close the jboss-service.xml file.

Step 12 Do one of the following:

- If your Cisco DCNM-LAN deployment is a clustered-server deployment, repeat this procedure on each server in the cluster and then start the servers, beginning with the master server first. Allow at least one minute between starting each server.
- If your deployment is a single-server deployment, start the Cisco DCNM-LAN server.

For more information about starting a single Cisco DCNM-LAN or a cluster of Cisco DCNM-LAN servers, see the *Cisco DCNM Fundamentals Guide, Release 5.x*.

Specifying a Secondary Server Bind Port

You can configure a Cisco DCNM-LAN server to use a specific secondary server bind port.

If your Cisco DCNM-LAN deployment is a clustered-server deployment, you must perform this procedure on each server in the cluster.

DETAILED STEPS

Step 1 Stop the Cisco DCNM-LAN server. If you are enabling secure client communications on a server cluster, use the stop-dcnm-cluster script. For single-server deployments, do one of the following:

- Microsoft Windows—Choose **Start > All Programs > Cisco DCNM Server > Stop DCNM Server**.
- RHEL—Use the Stop_DCNM_Server script.

For more information about stopping Cisco DCNM-LAN, see the *Cisco DCNM Fundamentals Guide, Release 5.x*.

Step 2 In a text editor, open the remoting-bisocket-service.xml file that is at the following location:

INSTALL_DIR\dcm\jboss-4.2.2.GA\server\dcnm\deploy\jboss-messaging.sar\remoting-bisocket-service.xml

where *INSTALL_DIR* is the Cisco DCNM installation directory. On Microsoft Windows, the default installation directory is C:\Program Files\Cisco Systems. On RHEL systems, the default installation directory is /usr/local/cisco.

Step 3 Find the following section in the file. Verify that the section you find includes the secondaryBindPort line.

```
<!-- Use these parameters to specify values for binding and connecting control connections
to work with your firewall/NAT configuration
<attribute name="secondaryBindPort">xyz</attribute>
<attribute name="secondaryConnectPort">abc</attribute>
-->
```

By default, the section is commented out using the standard XML comment markers, <!-- and -->.

If you have previously specified a secondary server bind port, the section is not commented out.

Step 4 If the section is commented out, uncomment the secondaryBindPort line, as follows:

a. At the end of the second line of the section, add the following three characters from after configuration:

```
-->
```

The changed line should read as follows:

```
to work with your firewall/NAT configuration-->
```

b. At the beginning of the fourth line of the section, add the following four characters:

```
<!--
```

The changed line should read as follows:

```
<!-- <attribute name="secondaryConnectPort">abc</attribute>
```

After you uncomment the section, it should read as follows:

```
<!-- Use these parameters to specify values for binding and connecting control connections
to work with your firewall/NAT configuration-->
```

```
<attribute name="secondaryBindPort">xyz</attribute>
<!--<attribute name="secondaryConnectPort">abc</attribute>
-->
```

Step 5 In the secondaryConnectPort line, specify a port number between the opening and closing attribute elements. For example, if you want to specify port 47900, the secondaryBindPort line should read as follows:

```
<attribute name="secondaryBindPort">47900</attribute>
```

Step 6 Save and close the remoting-bisocket-service.xml file.

Step 7 Do one of the following:

- If your Cisco DCNM-LAN deployment is a clustered-server deployment, repeat this procedure on each server in the cluster and then start the servers, beginning with the master server first. Allow at least one minute between starting each server.
- If your deployment is a single-server deployment, start the Cisco DCNM-LAN server.

For more information about starting a single Cisco DCNM-LAN or a cluster of Cisco DCNM-LAN servers, see the *Cisco DCNM Fundamentals Guide, Release 5.x*.

Configuring SMTP Servers

This section describes how to configure Cisco Data Center Network Manager for LAN (DCNM-LAN) servers to use SMTP servers.

This section includes the following topics:

Information About SMTP Servers

The Cisco DCNM-LAN client supports a feature where you can specify rising or falling threshold rules for sample variables in collected statistical data. When one of these thresholds has been crossed, you can specify that an e-mail alert be sent. The Cisco DCNM-LAN server can be configured to send e-mail to an SMTP server.

Configuring for SMTP Servers

Cisco DCNM-LAN servers are configured to use SMTP servers by setting a property value.

DETAILED STEPS

Step 1 Stop the Cisco DCNM-LAN server. If you are enabling SMTP communications on a server cluster, use the stop-dcnm-cluster script. For single-server deployments, do one of the following:

- Microsoft Windows—Choose **Start > All Programs > Cisco DCNM Server > Stop DCNM Server**.

- RHEL—Use the Stop_DCNM_Server script.

For more information about stopping Cisco DCNM-LAN, see the *Cisco DCNM Fundamentals Guide, Release 5.x*.

Step 2 In a text editor, open the mail-service.xml file at the following location:

INSTALL_DIR\dcm\jboss-4.2.2.GA\server\dcnm\deploy\mail-service.xml

where *INSTALL_DIR* is the Cisco DCNM installation directory. On Microsoft Windows, the default installation directory is C:\Program Files\Cisco Systems. On RHEL systems, the default installation directory is /usr/local/cisco.

Step 3 Find the mail.smtp.host property value and modify it to specify the SMTP gateway server.

For example:

```
<!-- Specify the SMTP gateway server -->
<property name="mail.smtp.host" value="smtp.nosuchhost.nosuchdomain.com"/
```

Step 4 Save and close the mail-service.xml file.

Step 5 Do one of the following:

- If your Cisco DCNM-LAN deployment is a clustered-server deployment, repeat this procedure on each server in the cluster and then start the servers, beginning with the master server first. Allow at least one minute between starting each server.
- If your deployment is a single-server deployment, start the Cisco DCNM-LAN server.

For more information about starting a single Cisco DCNM-LAN or a cluster of Cisco DCNM-LAN servers, see the *Cisco DCNM Fundamentals Guide, Release 5.x*.

Additional References

For additional information related to secure client communications, see the following sections:

- Related Documents, page 1-8
- Standards, page 1-9

Related Documents

Related Topic	Document Title
The process of deploying Cisco DCNM-LAN in your organization	Chapter 1, “Deploying Cisco DCNM-LAN”

Standards

Standards	Title
SSL 3.0	The SSL Protocol, Version 3.0 (http://tools.ietf.org/html/draft-ietf-tls-ssl-version3-00)
TLS 1.2	The Transport Layer Security (TLS) Protocol, Version 1.2 (http://tools.ietf.org/html/rfc5246)

Feature History for Configuring Cisco DCNM-LAN Servers

Table 1-1 lists the release history for this feature.

Table 1-1 Feature History for Secure Client Communications

Feature Name	Releases	Feature Information
Secure client communications	5.0(2)	This feature was introduced.
Configuration for SMTP	5.1	This feature was introduced.

CHAPTER 1

Installing and Administering Cisco DCNM VSB

This chapter describes how to install and administer the Cisco Data Center Network Manager Virtual Service Blade (DCNM VSB) on a Cisco Nexus 1010 Virtual Services switch.

This chapter includes the following sections:

Information About Cisco DCNM VSB

The Cisco Nexus 1010 switch is a shell that hosts multiple Virtual Switch Modules (VSMs) and other service modules such as the Cisco DCNM and Network Analysis Module (NAM) but supresses all of the details about the multiple virtual machines running on a hypervisor. From a network management perspective, the hosted VSMs appear as a cluster. Each Virtual Supervisor Module (VSM) and its associated Virtual Ethernet Modules (VEMs) comprise one virtual switch.

In addition to VSMs, the Cisco Nexus1010 switch can host other service modules. Each of these components is known as a Virtual Service Blade (VSB). The Cisco DCNM VSB enables network administrators to manage the data center LAN infrastructure. The Cisco DCNM VSB is integrated with the Cisco Nexus 1010 switches. The Cisco DCNM VSB extends visibility and interconnects the virtual machines in the Cisco Nexus 1000V switch deployments.

Installing Cisco DCNM VSB

This section describes how to install Cisco DCNM VSB.

This section includes the following topics:

System Requirements

The following table lists the system requirements for the Cisco DCNM VSB.

Table 1-1 Cisco DCNM VSB System Requirements

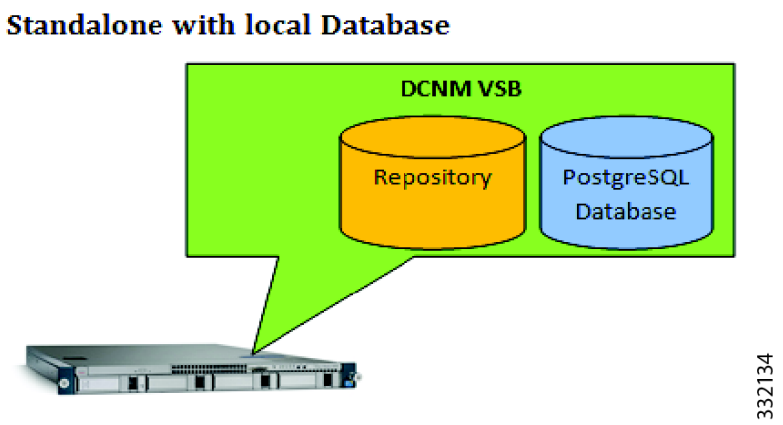
Component	Recommended Requirements
RAM (free)	4 GB
CPU speed	Dual-processor or dual-core CPU
Disk space (free)	80 GB for standalone installation 40 GB for cluster installation
Operating system	Wind River Linux 3.0

Installing Cisco DCNM VSB

Using the local database for stand alone installation. Figure 1-1 shows local database for stand alone installation.

Note When you install Cisco DCNM as a VSB, only DCNM-LAN server components are installed.

Figure 1-1 DCNM VSB with local database



BEFORE YOU BEGIN

You must log in to the Cisco Nexus 1010 switch using the CLI or a web browser.

DETAILED STEPS

Step 1 Copy the Cisco DCNM ISO file to the bootflash:repository location of the Cisco Nexus 1010 switch.

Step 2 Enter the configuration mode and create a VSB.

```
virtual-service-blade VSB-NAME
```

Step 3 Associate the ISO file with the VSB.

```
virtual-service-blade-type new FILE-NAME.iso
```

Step 4 Initiate the Cisco VSB installation as follows:

```
virtual-service-blade VSB-NAME
```

a. Set up a cluster with a redundant Cisco Nexus 1010 switch pair.

```
n1010(config-vsb-config)# enable
```

b. Set up a standalone DCNM VSB on the primary Cisco Nexus 1010 switch.

```
n1010(config-vsb-config)# enable primary
```

c. Set up a standalone DCNM VSB on the secondary Cisco Nexus 1010 switch.

```
n1010(config-vsb-config)# enable secondary
```

Step 5 Enter the name of the VSB image.

```
Enter vsb image:
```

Step 6 Enter **Y** to set up a DCNM standalone VSB.

```
Setup a DCNM Standalone [Y/N]: [N]
```

Step 7 Enter the location of the VSB.

```
Choose the location of VSB[primary/secondary]:[primary]
```

Step 8 Enter the hostname.

```
Enter the hostname: [dcnm-vsb]
```

Step 9 Enter the management IP address.

```
Enter Mgmt IP address:
```

Step 10 Enter the management subnet mask IP address.

```
Enter Mgmt subnet mask Ip address: [255.255.255.0]
```

Step 11 Enter the IP address of the default gateway.

```
Enter IP address of the default gateway:
```

Step 12 Enter the location of the database.

```
Specify the location of the database [local/remote]: [local]
```

Step 13 Enter the DCNM database username.

```
Enter database username for DCNM[dcnmuser]:
```

Step 14 Enter the DCNM database password:

```
Enter database password for DCNM:
```

Step 15 Enter the database administrator username.

```
Enter database administrator username[admin]:
```

Step 16 Enter the database administrator password

```
Enter database administrator password:
```

Step 17 Specify whether or not you want to mount the network file system as a data archive.

```
Mount a network file system as data archive[Y/N]:
```

Installing a Cisco DCNM License on a Cisco Nexus 1010 Switch

You can install a Cisco DCNM license on a Virtual Service Blade (VSB) by using one of the two methods:

- Using a Silent Installer, page 1-4
- Using the GUI to Install the License, page 1-4

Using a Silent Installer

You can use a silent installer on a Cisco Nexus 1010 switch.

BEFORE YOU BEGIN

You must log in to the Cisco Nexus 1010 switch using the CLI or a web browser.

DETAILED STEPS

Step 1 From the Cisco Nexus 1010 switch, log into the VSB.

```
login virtual-service-blade <name_of_VSB>
```

Step 2 Copy the license file to the root directory of the VSB.

In the root directory, you see a link to a script License_Install_DCNM.

Step 3 Execute the script as follows:

```
sh License_Install_DCNM
```

Using the GUI to Install the License

BEFORE YOU BEGIN

You must log in to the Cisco Nexus 1010 switch using the CLI or a web browser.

DETAILED STEPS

Step 1 Download the Reflection tool on a Windows machine.

Step 2 Double-click **Reflection X Manager**.

Step 3 Start a putty session to the VSB.

Note PuTTY is a free and open source terminal emulator application which can act as a client for the SSH, Telnet, rlogin, and raw TCP computing protocols and as a serial console client.

Step 4 From the VSB, enter the following command:

```
export DISPLAY=<ip_address_of_machine_with_reflection>:0.0
```

Step 5 Open the DCNM installer file.

```
sh <name_of_DCNM_EXE>
```

The DCNM installation dialog box appears.

Step 6 Choose **DCNM-LAN** and click **Next**.

Step 7 Browse to the folder where the license file is available and click **Next**.

The Cisco DCNM license is now installed.

Using a Remote Database Server for Standalone and Cluster installations

You can use a remote database for both standalone and cluster mode installations. In a standalone installation, you can configure the installation setup to use a remote Oracle database server. In a cluster mode installation, the remote database (PostgreSQL and Oracle) is shared by all of the nodes in the cluster.

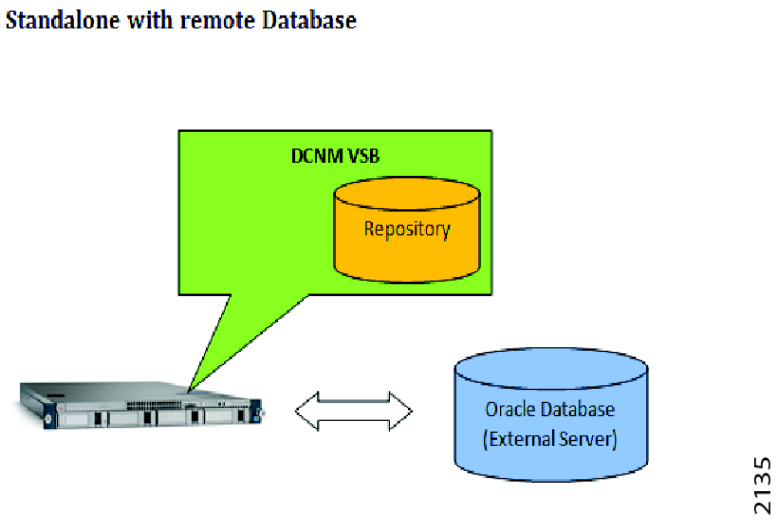
Cisco DCNM installs PostgreSQL database on the Cisco Nexus 1010 switch by default. If you want to use an external database server, you can specify the URL instead of choosing the local database. The IP address entries of the slave nodes should exist in the pg_hba.conf file of the database that resides in the data folder where the PostgreSQL database is installed.

This section includes the following topics:

Using the Remote Database for a Standalone Installation

You can perform a standalone DCNM VSB installation using the remote database. Figure 1-2 shows standalone DCNM VSB installation using the remote database.,

Figure 1-2 DCNM VSB with remote database



BEFORE YOU BEGIN

You must log in to the Cisco Nexus 1010 switch using the CLI or a web browser.

DETAILED STEPS

Step 1 Copy the DCNM ISO file to the bootflash:repository location of the Cisco N1010 switch.

Step 2 Enter the configuration mode and create a VSB.

```
virtual-service-blade VSB-NAME
```

Step 3 Associate the ISO with the VSB.

```
virtual-service-blade-type new FILE-NAME.iso
```

Step 4 Initiate Cisco VSB installation as follows:

```
virtual-service-blade VSB-NAME
```

a. Set up a cluster with a redundant Cisco Nexus 1010 pair of switches.

```
n1010(config-vsb-config)# enable
```

b. Set up a standalone DCNM VSB on the primary Cisco Nexus 1010 switch.

```
n1010(config-vsb-config)# enable primary
```

c. Set up a standalone DCNM VSB on the secondary Cisco Nexus 1010 switch.

```
n1010(config-vsb-config)# enable secondary
```

Step 5 Enter the name of the VSB image.

```
Enter vsb image:
```

Step 6 Enter **Y** to set up a DCNM standalone VSB.

```
Setup a DCNM Standalone [Y/N]:
```

Step 7 Enter the location of the VSB

```
Choose the location of VSB[primary/secondary]:
```

Step 8 Enter the hostname.

```
Enter the hostname: [dcnm-vsb]
```

Step 9 Enter the management IP address.

```
Enter Mgmt IP address:
```

Step 10 Enter the management subnet mask IP address.

```
Enter Mgmt subnet mask Ip address:
```

Step 11 Enter the IP address of the default gateway.

```
Enter IP address of the default gateway:
```

Step 12 Enter the location of the database.

```
Specify the location of the database[local/remote]:
```

Note To use a remote database, you must specify the location of the database as remote.

Step 13 Enter the URL of the remote database.

```
Enter URL for remote database:
```

Note You must enter the URL of the database in the following format: jdbc:postgresql://192.177.121.11:5432/dcmdb.
The pg_hba.conf file should contain the IP addresses of all the VSB nodes. You can locate the pg_hba.conf file in the PostgreSQL install folder /usr/local/cisco/dcm/db/data.
You must stop and start the database after making any changes to the pg_hba.conf file.

Step 14 Enter the DCNM database username.

```
Enter database username for DCNM[dcnmuser]:
```

Step 15 Enter the DCNM database password.

```
Enter database password for DCNM:
```

Step 16 Enter the database administrator username.

```
Enter database administrator username[admin]:
```

Step 17 Enter the database administrator password.

```
Enter database administrator password:
```

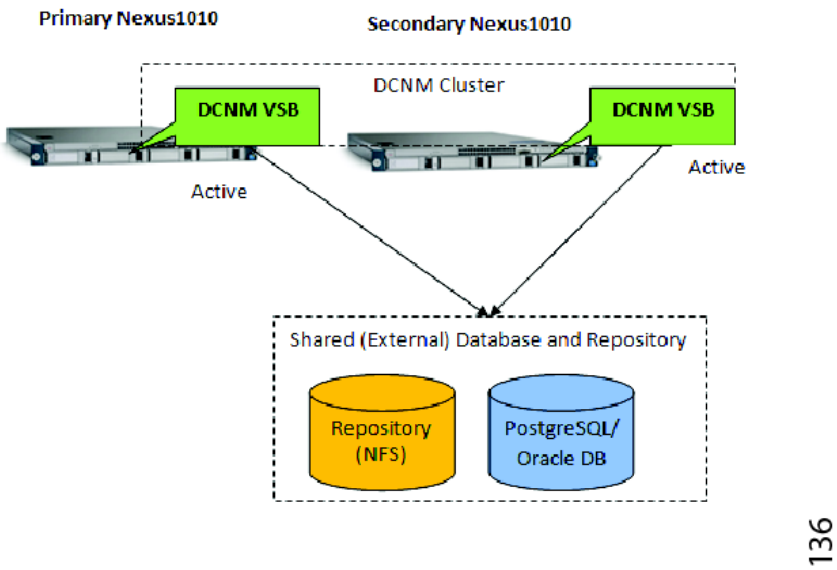
Step 18 Specify whether or not you want to mount the network file system as data archive.

```
Mount a network file system as data archive[Y/N]:
```

Using the Remote Database for an HA-Enabled Cluster Mode Installation

You can perform an HA-enabled cluster mode DCNM VSB installation by using the remote database. Figure 1-3 shows the two node DCNM cluster.

Figure 1-3 Two node DCNM Cluster



BEFORE YOU BEGIN

You must log in to the Cisco Nexus 1010 switch using the CLI or a web browser.

DETAILED STEPS

Step 1 Copy the DCNM ISO file to the bootflash:repository location of the Cisco Nexus 1010 switch.

Step 2 Enter the configuration mode and create a VSB.

```
virtual-service-blade VSB-NAME
```

Step 3 Associate the ISO with the VSB.

```
virtual-service-blade-type new FILE-NAME.iso
```

Step 4 Initiate Cisco VSB installation as follows:

```
virtual-service-blade VSB-NAME
```

a. Set up a standalone DCNM VSB on the primary Cisco Nexus 1010 switch.

```
n1010(config-vsb-config)# enable primary
```

Step 5 Enter the name of the VSB image.

```
Enter vsb image[dcnm-installer.iso]:
```

Step 6 Enter **Y** to set up a DCNM cluster.

```
Setup a DCNM Cluster [Y/N]:
```

Note For the above scenario select Y for step 6. You must use the remote database and data archive directory on the network file system.

Step 7 Enter the hostname.

```
Enter the hostname: [dcnm-vsb]
```

Step 8 Enter the management IP address.

```
Enter Mgmt IP address[172.22.29.123]:
```

Note The VSB and the master node must be under the same subnet.

Step 9 Enter the management IP address for DCNM standby.

```
Enter Management IP address for DCNM on standby N1010[172.22.29.124]:
```

Step 10 Enter the management subnet mask IP address.

```
Enter Mgmt subnet mask Ip address[255.255.255.0]:
```

Step 11 Enter the IP address of the default gateway.

```
Enter IP address of the default gateway[172.22.29.1]:
```

Step 12 Use default multicast addresses for a cluster.

```
Use default multicast addresses for cluster (239.255.153.1-239.255.153.4)?[Y|N]:
```

Note For the first Cisco Nexus 1010 switch you can use the default multicast IP address, but for the second Cisco Nexus 1010 switch it should be same as the first one.

Note If you want to use the default multicast address, enter **Y**. However, you can override the current set of musticast addresses. If you choose the default settings, you can continue with Step 17.

Step 13 Enter the multicast IP address for cluster 1.

```
Enter multicast IP address for cluster (1 of 4)[239.255.153.1]:
```

Step 14 Enter the multicast IP address for cluster 2.

```
Enter multicast IP address for cluster (2 of 4)[239.255.153.2]:
```

Step 15 Enter the multicast IP address for cluster 3.

```
Enter multicast IP address for cluster (3 of 4)[239.255.153.3]:
```

Step 16 Enter the multicast IP address for cluster 4.

```
Enter multicast IP address for cluster (4 of 4)[239.255.153.4]:
```

Step 17 Enter the location of the database.

```
Specify the location of the database[local/remote]:
```

Note To use a remote database, you must specify the location of the database as remote.

Step 18 Enter the URL of the remote database.

```
Enter URL for remote database[jdbc:postgresql://,ip address of database
machine>:5432/dcmdb]:
```

Step 19 Enter the DCNM database username.

```
Enter database username for DCNM[dcnmuser]:
```

Step 20 Enter the DCNM database password.

```
Enter database password for DCNM[dcnmuser]:
```

Step 21 Enter the database administrator username.

```
Enter database administrator username[admin]:
```

Step 22 Enter the database administrator password.

```
Enter database administrator password[admin]:
```

Step 23 Specify whether or not you want to mount the network file system as a data archive.

```
Mount a network file system as data archive[Y/N]:
```

Step 24 Enter the network file system path to mount.

```
Enter NFS share path to mount[Ip-Address of data archive machine:<path>]:
```

Note If you want to use an Network File System (NFS) server as the repository for archiving configuration files and templates, you must specify the shared location. For example, you can specify 10.77.212.81:/opt/share/dcnm-repository where 10.77.212.81 is the NFS server and /opt/share/dcnm-repository is the shared directory.

Using the Local Database for a Secondary Switch Cluster Installation

BEFORE YOU BEGIN

You must log in to the Cisco Nexus 1010 switch using the CLI or a web browser.

DETAILED STEPS

Step 1 Deploy the secondary VSB using the following command:

```
virtual-service-blade <VSB_NAME>
enable secondary
```

Step 2 Deploy the secondary VSB in the standalone mode. Enter the following information:

- Choose the location of VSB[primary/secondary—**[primary] secondary**
- Enter the IP address of the default gateway—Specify the IP address that you wish to configure for the secondary VSB.

Step 3 Once VSB is deployed, uninstall Cisco DCNM in the secondary module using the following command:

```
login virtual-service-blade <VSB_NAME> secondary
root@dcnm-vsb:/root> ./Stop_DCNM_LAN_Server
Shutdown message has been posted to the server.
Server shutdown may take a while - check logfiles for completion
root@dcnm-vsb:/root> ./Uninstall_DCNM
¢   cd /root
¢   ./Stop_DCNM_LAN_Server
¢   ./Uninstall_DCNM
```

Step 4 Login into the primary VSB and perform the following steps:

a. Change the directory to the postgres database installation using the following command:

```
Cd /usr/local/Cisco/dcm/db/data
```

b. Enter the secondary VSB IP address into the pg_hba.conf file available under /usr/local/Cisco/dcm/db/data.

c. Stop and restart the DCNM server of the primary node to enable the changes.

Step 5 Using SFTP file transfer, copy the installer.properties file available in the primary node under */usr/local/Cisco/dcm/dcnm/config* to */root/CSCOdcnm/install* in the secondary node VSB.

Step 6 Install Cisco DCNM in the secondary VSB using the following commands:

```
Cd /root/CSCOdcnm/install
Sh dcnm.bin  -i silent -f installer.properties -DDCNM_IP_ADDRESS=<ip_Address>
-DDATA_PATH=<Path_Loc>
```

Step 7 Once the installation is complete, restart the DCNM server using the following command:

```
root@dcnm-vsb:/root> ./Start_DCNM_LAN_Server
```

Administering the Cisco DCNM VSB

The Cisco DCNM installer binary file in the installer package is available at the following location: /root/CSCOdcnm/install. The default data archive location configured during installation is /root/CSCOdcnm/data_archive. You can override this value by specifying a different location during the Cisco DCNM VSB deployment.

The following table shows the soft links that are available in the **/root** directory of the Cisco DCNM VSB.

Table 1-2 Cisco DCNM Shortcuts

File Name	Purpose
Start_DCNM_LAN_Server	Starts the Cisco DCNM-LAN Server
Stop_DCNM_LAN_Server	Stops the Cisco DCNM-LAN Server
License_Install_DCNM	Installs the license. (You may need to specify the license file)
Uninstall_DCNM	Uninstalls the Cisco DCNM-LAN Server
DCNM_Location	Points to the Cisco DCNM-LAN installation directory

This section includes the following topics:

- Verifying the Status of a Cisco DCNM VSB, page 1-12

- Accessing Cisco DCNM VSB Using the CLI, page 1-12
- Deleting a Cisco DCNM VSB, page 1-12

Verifying the Status of a Cisco DCNM VSB

You can verify the configuration and status of a deployed Cisco DCNM VSB.

DETAILED STEPS

	Command	Purpose
Step 1	`show virtual-service-blade`	Displays all the deployed Cisco DCNM VSBs and the configurations applied to each VSB.
Step 2	`show virtual-service-blade summary`	Displays all the deployed Cisco DCNM VSBs and the summary of each VSB.
Step 3	`show virtual-service-blade-type summary`	Displays all the Cisco DCNM VSBs that are aligned to a VSB type.

Accessing Cisco DCNM VSB Using the CLI

You can access a deployed Cisco DCNM VSB using the CLI.

DETAILED STEPS

	Command	Purpose
Step 1	`login virtual-service-blade` *VSB_NAME* `[primary/secondary]`	Logs in to the respective Cisco DCNM VSB.

Deleting a Cisco DCNM VSB

You can delete a Cisco DCNM VSB.

DETAILED STEPS

	Command	Purpose
Step 1	`shutdown [primary/secondary]`	Powers down the Cisco DCNM VSBs.
Step 2	`no enable [primary/secondary]`	Disables the deployed Cisco DCNM VSBs.
Step 3	`no enable force`	Force disables the deployed Cisco DCNM VSBs
Step 4	`no virtual-service-blade <VSB_NAME>`	Deletes both the primary and secondary Cisco DCNM VSBs.

Managing Cisco DCNM VSBs Using the Attachmate Reflection Tool

Cisco DCNM supports the Attachmate Reflection tool on computers that run windows and connect to VSBs installed on Linux hosts. You can use the Attachmate Reflection tool to upgrade Cisco DCNM VSBs, install licenses, and manage user credentials. You must install the Attachmate Reflection tool on the computer from where you connect to the VSB node.

To access the Cisco DCNM VSB user interface on a computer that runs Windows, enter the following command on the VSB node:

```
export DISPLAY=<ip address>:0.0
```

where the IP address is the IP address of the computer on which the Attachmate Reflection tool is installed.

Using the Attachmate Reflection Tool to Upgrade Cisco DCNM VSBs

You can use the Attachmate Reflection tool to upgrade Cisco DCNM VSBs using the install manager script stored in the /usr/local/cisco/dcm/dcnm/bin.

DETAILED STEPS

Step 1 Run *dcnm-install-manager.sh*.

You see the DCNM Install Manager window.

Step 2 From the DCNM Installer Folder drop-down list, choose the installation folder.

Step 3 From the DCNM License Folder drop-down list, choose the license folder.

Step 4 Specify the Data Path Location, and then click **Install**.

Using the Attachmate Reflection Tool to Install Licenses

You can use the Attachmate Reflection tool to install licenses using the install manager script stored in the /usr/local/cisco/dcm/dcnm/bin.

DETAILED STEPS

Step 1 Run *dcnm-install-manager.sh*.

You see the DCNM Install Manager window.

Step 2 From the DCNM License Folder drop-down list, choose the license folder.

Step 3 Click **Install**.

Using the Attachmate Reflection Tool to Reset User Credentials

You can use the Attachmate Reflection tool to reset Cisco DCNM user credentials using the password reset script stored in the /usr/local/cisco/dcm/dcnm/bin.

To modify user credentials, run *pwreset.sh*.

CHAPTER 1

Uninstalling Cisco DCNM-LAN Servers

This chapter describes how to uninstall a Cisco Data Center Network Manager for LAN (DCNM-LAN) server.

This chapter includes the following sections:

Uninstalling a Primary Cisco DCNM-LAN Server

Uninstalling a primary Cisco DCNM-LAN server uses a graphical uninstallation interface.

BEFORE YOU BEGIN

Stop the Cisco DCNM-LAN server that you want to uninstall. The uninstallation cannot proceed until you stop the Cisco DCNM-LAN server. For more information, see the *Cisco DCNM Fundamentals Guide, Release 5.x*.

DETAILED STEPS

Step 1 Log into the server with a user account that has the required privileges, as follows:

- For Microsoft Windows, the user account must be a member of the local administrators group.
- For RHEL, the user account must be root.

If you are uninstalling Cisco DCNM-LAN on Microsoft Windows and using Remote Desktop Connection (RDC) to access the Cisco DCNM-LAN server system, start RDC from a command prompt and use the /console option, as follows:

```
C:\>mstsc /console /v:server
```

where *server* is the DNS name or IP address of the Cisco DCNM-LAN server system.

Step 2 Start the uninstallation process, as applicable:

- For Microsoft Windows, from the desktop, choose **Start > All Programs > Cisco DCNM Server > Uninstall DCNM**. The location of shortcuts depends upon the choices you made when you installed the Cisco DCNM-LAN server.

  Alternatively, you can run the following executable file:

```
INSTALL_DIR\dcm\dcnm\Uninstall_DCNM\Uninstall DCNM.exe
```

where the default *INSTALL_DIR* value is C:\Program Files\Cisco Systems.

- For RHEL, use the Uninstall_DCNM script, as follows:

```
sh Uninstall_DCNM
```

You can find this script in your home folder or the folder that you specified when setting up the link folder during your installation of Cisco DCNM-LAN.

The Uninstall DCNM-LAN window opens.

Step 3 Click **Uninstall**.

The Deleting DCNM-LAN DB dialog box appears.

Step 4 Do one of the following:

- If you want to retain the data in the Cisco DCNM-LAN database, click **No**.

Note If you intend to reinstall Cisco DCNM-LAN, you must create a new database instance. Database instances from previous Cisco DCNM-LAN installations cannot be specified during installation.

- If you want to delete all data from the Cisco DCNM-LAN database, click **Yes**.

Note All data that Cisco DCNM-LAN has collected is permanently deleted if you delete it.

If you chose to delete the data, the uninstallation process deletes the database.

The uninstallation process removes the Cisco DCNM-LAN server software from the server system.

Step 5 Click **Done**.

Uninstalling a Secondary Cisco DCNM-LAN Server

Depending on the operating system of the secondary server, you can uninstall the Cisco DCNM-LAN server using the CLI or the DCNM-LAN Install Manager tool. You can use the CLI or the DCNM-LAN Install Manager tool for a secondary server that runs RHEL. For a secondary server that runs Microsoft Windows, you uninstall the Cisco DCNM-LAN server with the Windows GUI or the CLI.

Uninstalling with the CLI or Windows GUI

You can uninstall a secondary Cisco DCNM-LAN server on RHEL by using the CLI or for Windows servers, the CLI or a Windows graphical interface.

BEFORE YOU BEGIN

Stop the Cisco DCNM-LAN server that you want to uninstall. The uninstallation cannot proceed until you stop the Cisco DCNM-LAN server. For more information, see the *Cisco DCNM Fundamentals Guide, Release 5.x*.

DETAILED STEPS

Step 1 Log into the server with a user account that has the required privileges, as follows:

- For Microsoft Windows, the user account must be a member of the local administrators group.
- For RHEL, the user account must be root.

If you are uninstalling Cisco DCNM-LAN on Microsoft Windows and using Remote Desktop Connection (RDC) to access the Cisco DCNM-LAN server system, start RDC from a command prompt and use the /console option, as follows:

```
C:\>mstsc /console /v:server
```

where *server* is the DNS name or IP address of the Cisco DCNM-LAN server system.

Step 2 Start the uninstallation process, as applicable:

- For Microsoft Windows, from the desktop, choose **Start > All Programs > Cisco DCNM Server > Uninstall DCNM**. The location of shortcuts depends upon the choices you made when you installed the Cisco DCNM-LAN server.

  Alternatively, you can run the following executable file:
  INSTALL_DIR\dcm\dcnm\Uninstall_DCNM\Uninstall DCNM.exe
  where the default *INSTALL_DIR* value is C:\Program Files\Cisco Systems.
- For RHEL, use the Uninstall_DCNM script, as follows:

  ```
  sh Uninstall_DCNM
  ```

  You can find this script in your home folder or the folder that you specified when setting up the link folder during your installation of Cisco DCNM-LAN.

The uninstallation process removes the Cisco DCNM-LAN server software from the secondary server system.

Step 3 Monitor the DCNM_UninstallLog.log file to determine the status of the uninstall. The Cisco DCNM-LAN uninstaller writes the log file to the home directory of the current user account.

Uninstalling with Install Manager

DCNM-LAN Install Manager is a GUI tool for servers that run Linux. It is designed to assist in performing silent mode operations on secondary servers (remote nodes).

Note DCNM-LAN Install Manager does not support Windows servers.

Note Disable antivirus and instruction detection software on the server system. In general, disable any security software or feature that might interfere with the uninstallation of the Cisco DCNM-LAN server software. After you have completed the uninstallation, reenable the software or features.

DETAILED STEPS

Step 1 To access Install Manager, navigate to the **dcnm-install-manager.sh** file that is located in the bin folder where the DCNM-LAN server was installed.

The default bin folder location for servers that run Linux is /usr/local/Cisco/dcm/dcnm/bin.

Step 2 Double click the **dcnm-install-manager.sh** file to launch Install Manager.

Step 3 In the DCNM Installer Folder drop-down list, choose the path that contains the binary executable file for DCNM-LAN server installation.

Step 4 Click the **New** icon in the toolbar near the top of the Install Manager GUI for every secondary server.

A new row in the list of Server Nodes is created every time the New icon is clicked.

Note In the toolbar, click the **Delete** icon to delete a selected row in the list of Server Nodes. This action does not delete a secondary server from the clustered-server environment.

Step 5 For each secondary server represented by a row in the list of Server Nodes, enter the following:

- Server name or IP address in the Server Name/IP Address field.
- Protocol used for connectivity in the Protocol field.

  The protocol is either Telnet or SSH.
- User credentials (user ID and password) used for connecting to the secondary server in the User Credentials field.

  The user credentials are used for SSH connectivity to the server. Telnet connectivity to the server does not require user credentials.

  Alternatively, default user credentials can be set by entering the credentials in the Default Credentials section of the GUI. The default credentials are used when the User Credential field is blank.
- (Optional) Comments that might be useful to identify the secondary server in the Comments field.

The Last Action Status column in the list of Server Nodes includes the success or failure status of the last performed action. Clicking the **+** icon for the Last Action Status expands the display to show the entire log of actions performed on the server.

Step 6 In the list of Server Nodes, select the secondary servers to perform the uninstallation.

Step 7 In the toolbar, click the **Verify** icon to verify the connectivity to the selected secondary servers.

Correct any connectivity issues before continuing the uninstallation.

Step 8 (Optional) In the DCNM Install Location field, enter the path on the secondary server for the uninstallation of the DCNM-LAN server.

If the DCNM Install Location field is blank, the Install Manager uses the default path, /usr/local/Cisco/dcm, for the uninstallation of the DCNM-LAN server.

Step 9 In the toolbar, click the **Uninstall** icon to begin the uninstall on the selected secondary servers.

Step 10 Monitor the Last Action Status column to determine the status of the uninstallation.

In addition, you can also review the DCNM_Installer_Manager.log file. This file, which is located at /root/.dcnm, contains the log for all the operations of the Install Manager.

If the uninstallation operation fails on a secondary server, review the DCNM_UninstallLog.log file to determine the status of the uninstall. The Cisco DCNM-LAN uninstaller writes the log file to the home directory of the current user account.

Feature History for Uninstalling Cisco DCNM-LAN Servers

Table 1-1 lists the release history for this feature.

Table 1-1 Feature History for Uninstalling Cisco DCNM-LAN Servers

Feature Name	Releases	Feature Information
Secondary server uninstallation	5.0(2)	This feature was introduced.
Install Manager	5.1	This feature was introduced.

CHAPTER 1

Troubleshooting the Cisco DCNM-LAN Server Installation

This chapter describes how to troubleshoot some common issues that you might experience while installing a Cisco Data Center Network Manager for LAN (DCNM-LAN) server with solutions for the issues.

This chapter includes the following sections:

Postgres Database Installation Fails

Check Table 1-1 for symptoms related to an installation failure of the Postgres database. For each symptom that describes your trouble, determine which possible causes apply and follow the corresponding solutions.

Table 1-1 Postgres Database Installation Fails

Symptom	Possible Cause	Solution
Postgres database installation fails.	The username specified to run the Postgres service already exists on the server.	Specify a different username or remove the existing username from the server.
	Antivirus software or intrusion detection software, such as Cisco Security Agent, blocked the installation.	Temporarily disable any antivirus software and intrusion detection software, and then reinstall Cisco DCNM-LAN.

Table 1-1 Postgres Database Installation Fails (continued)

Symptom	Possible Cause	Solution

The PostgreSQL installer shows the following message:
`Failed to run initdb: 128`
	(Microsoft Windows only) Remote Desktop Connection client not running in console mode.	If you are installing Cisco DCNM-LAN on a supported Microsoft Windows operating system and using Remote Desktop Connection (RDC) to access the Cisco DCNM-LAN server system, start RDC from a command prompt and use the /console option, as follows:
		`C:\>mstsc /console /v:server`
		where *server* is the DNS name or IP address of the Cisco DCNM-LAN server system.
		If the /console option not supported in Microsoft Windows version that you are running, use the /admin option, as follows:
		`C:\>mstsc /admin /v:server`

The PostgreSQL installer shows the following message: PostgreSQL installation has failed. `Failed to run initdb: 128`	(Macintosh only) Remote Desktop Connection client not running in console mode.	If you are using Remote Desktop Connection on a Macintosh computer to access the Cisco DCNM-LAN server system follow these steps: 1. Enter the IP Address of the windows server on which the DCNM is installed. 2. Hold down the Command key and click **Connect**. This will force RDC to use console mode. 3. Release the Command key when the authentication window appears.
The PostgreSQL installer shows the following message: `Failed to create process for initdb. The service cannot be started, either because it is disabled or because it has no enabled devices associated with it.`	(Microsoft Windows only) The Secondary Logon service is not running.	Verify that the Secondary Logon service is running. 1. On the Cisco DCNM-LAN server system, open the Control Panel and go to **Administrative Tools > Services**. 2. In the list of services, find the Secondary Logon service. 3. If the status of the Secondary Logon service is not Started, right-click the service and choose **Start**. 4. Close the Services window. 5. Restart the Cisco DCNM-LAN server installation.

Previous Installation Found When No Previous Installation Exists

Table 1-2 lists issues found when no previous installation exists.

Table 1-2 Previous Installation Found when No Previous Installation Exists

Symptom	Possible Cause	Solution
A message wrongly states that a previous installation exists.	The following file has incorrect entries regarding Cisco DCNM-LAN: `C:\Program Files\Zero G Registry\.com.zerog.registry.xml`	1. Perform the steps in the "Editing the Zero G Registry File" section on page 1-3. 2. Install the Cisco DCNM-LAN server.

Editing the Zero G Registry File

You can edit the Zero G Registry file to remove incorrect entries, which might cause the installation of the Cisco DCNM-LAN server to fail.

DETAILED STEPS

Step 1 Make a backup of the .com.zerog.registry.xml file, which is found at the following location:

```
C:\Program Files\Zero G Registry\.com.zerog.registry.xml
```

Step 2 Open the file in a text editor.

Step 3 Within the <products> element, remove the following <product> element and all its descendant elements:

```
<product name="Cisco DCNM" id="9e458447-1ee6-11b2-85ed-d4ed684e9c05" version="4.0.0.0"
copyright="2007". . .
```

Step 4 Within the <components> element, remove every instance of the following <component> element:

```
<component id="9e458484-1ee6-11b2-860c-d4ed684e9c05" version="1.0.0.0"
name="InstallAnywhere VM Component" location="C:\Program Files\Cisco Systems\Cisco
DCNM\jre" vendor="Cisco Systems Inc."/>
```

Step 5 Save and close the file.

Path to the Perl Binary Directory Not Found

Table 1-3 lists the symptoms related to the Perl binary directory. For each symptom that describes your trouble, determine which possible causes apply and follow the corresponding solutions.

Table 1-3 Path to the Perl Binary Directory Not Found

Symptom	Possible Cause	Solution
An error message states that the path to the bin directory for Perl is not in the system PATH environment variable.	Perl is not installed on the server system.	1. Install a supported version of ActivePerl. For more information about ActivePerl, see the "Prerequisites for Installing a Cisco DCNM-LAN Server" section on page 1-5. 2. Ensure that the system PATH environment variable includes the path to the directory that contains the Perl executable. On Microsoft Windows, the default path to the ActivePerl bin directory is C:\Perl\bin. 3. Start the DCNM-LAN server installation again.
	The server system PATH environment variable does not include the path to the directory that contains the Perl executable.	1. Verify that a supported version of ActivePerl is installed on the server system. If not, install a supported version of ActivePerl. For more information about ActivePerl, see the "Prerequisites for Installing a Cisco DCNM-LAN Server" section on page 1-5. 2. Ensure that the system PATH environment variable includes the path to the directory that contains the Perl executable. On Microsoft Windows, the default path to the ActivePerl bin directory is C:\Perl\bin. 3. Start the DCNM-LAN server installation again.

Cisco DCNM-LAN Installer Asks for Another Extraction Location

Table 1-4 lists issues found when a Cisco DCNM-LAN installer asked for another extraction location.

Table 1-4 Cisco DCNM-LAN Installer Asks for Another Extraction Location

Symptom	Possible Cause	Solution
After running the Cisco DCNM-LAN server installer, you see a dialog box with the following message: `Please select another location to extract the installer to`	The Cisco DCNM-LAN installer software is corrupted. This problem can occur if you use FTP or a similar transfer protocol in ASCII mode.	1. Delete the Cisco DCNM-LAN server installer. 2. Download the Cisco DCNM-LAN server software again. For more information, see the "Downloading the Cisco DCNM-LAN Server Software" section on page 1-11. **Note** If you transfer the installer with FTP or a similar protocol, ensure that you use a binary mode to transfer the installer.

INDEX

A

C

D

E

F

H

I

J

L

M

N

O

P

R

S

T

U

W

X

Z