CHAPTER 1

Cisco DCNM をインストールする準備

この章では、Cisco DCNM コンポーネントをインストールする前提条件について説明します。この章の内容は次のとおりです。

- 「Cisco DCNM に関する情報」（P.1-1）

Cisco DCNM に関する情報

ここで説明する内容は、次のとおりです。

- 「Cisco MDS 9000 スイッチ管理および Cisco DCNM-SAN」（P.1-1）
- 「Cisco DCNM の導入に関する情報」（P.1-21）
- 「次の作業」（P.1-29）

Cisco MDS 9000 スイッチ管理および Cisco DCNM-SAN

Cisco DCNM-SAN は、Secure Simple Network Management Protocol version 3（SNMPv3）をサポートする一連のネットワーク管理ツールです。ネットワーク ファブリックをリアルタイムに表示するグラフィカル ユーザ インターフェイス（GUI）を備えており、ユーザは Cisco MDS 9000 ファミリ デバイスおよびサードパーティ製スイッチの設定を管理することができます。Cisco DCNM-SAN を使用すると、コマンドライン インターフェイス（CLI）を使用しなくても、ほとんどのスイッチ コンフィギュレーション コマンドの機能を実行できます。

Cisco DCNM-SAN には、Cisco MDS 9000 ファミリのスイッチの完全な設定機能およびステータス モニタ機能の他に、強力なファイバ チャネル トラブルシューティング ツールもあります。これらの詳細な健全性分析機能および設定分析機能は、Cisco MDS 9000 固有のスイッチ機能であるファイバ チャネル ping および traceroute を使用します。

ここで説明する内容は、次のとおりです。

- 「Cisco MDS 9000 スイッチの管理」（P.1-2）
- 「ストレージ管理ソリューションのアーキテクチャ」（P.1-3）
- 「帯域内管理および帯域外管理」（P.1-3）
- 「Cisco DCNM」（P.1-19）

Cisco MDS 9000 スイッチの管理

Cisco MDS 9000 ファミリ スイッチはさまざまな方法でアクセスおよび設定でき、標準管理プロトコルをサポートしています。表 1-1 に、Cisco MDS 9000 ファミリのスイッチに対するアクセス、モニタ、および設定を行うために Cisco DCNM-SAN がサポートする管理プロトコルを示します。

表 1-1　サポート対象の管理プロトコル

管理プロトコル	目的
Telnet/SSH	Cisco MDS 9000 スイッチの CLI へのリモート アクセスを実現します。
FTP/SFTP/TFTP、SCP	コンフィギュレーション イメージおよびソフトウェア イメージをデバイス間でコピーします。
SNMPv1、v2c、および v3	80 個を超える異なる MIB（管理情報ベース）を含みます。Cisco MDS 9000 ファミリ スイッチは SNMP バージョン 1、2、3、および RMON V1、V2 をサポートします。RMON は、デバイスまたはネットワーク動作の変化に基づいて、しきい値の設定や通知の送信を含む、高度なアラームおよびイベント管理を行います。 デフォルトでは、Cisco DCNM-SAN は Cisco MDS 9000 ファミリ スイッチとの通信に SNMPv3 を使用します。SNMPv3 は暗号化されたユーザ名およびパスワードを使用して、安全な認証を実現します。SNMPv3 にはすべての管理トラフィックを暗号化する機能もあります。
HTTP/HTTPS	Cisco DCNM-SAN Web サービスとの通信や、Cisco DCNM-SAN ソフトウェアの配布およびインストールに使用される Web ブラウザの HTTP および HTTPS が含まれます。HTTP は、Cisco DCNM-SAN Server と Cisco MDS 9000 ファミリ スイッチ間の通信には使用されません。
XML/CIM over HTTP/HTTPS	Cisco SAN-OS および NX-OS で稼働する Storage Area Network（SAN; ストレージ エリア ネットワーク）管理アプリケーションの設計に対する CIM サーバのサポートを含みます。
ANSI T11 FC-GS-3	Fabric Configuration Server（FCS）で管理サーバを定義する際に、Fibre Channel-Generic Services（FC-GS-3）を提供します。Cisco DCNM-SAN はネーム サーバ データベースおよび Fibre Channel Shortest Path First（FSPF）トポロジ データベースに格納された情報以外に、FCS が提供する情報を使用して、詳細なトポロジ ビューを作成し、ファブリックを構成するすべてのデバイスの情報を収集します。

ストレージ管理ソリューションのアーキテクチャ

ストレージ環境に必要な管理サービスは、物理ストレージ ネットワーク デバイスに近い下部レイヤから、アプリケーションとストレージ リソース間のインターフェイスを管理する上部レイヤまで、5 つのレイヤで構成されます。

ストレージ ネットワーク管理のこれらの 5 つのレイヤの内、Cisco DCNM-SAN は、デバイス（要素）管理およびファブリック管理のツールを提供します。一般的に、デバイス管理（単一スイッチ）には Device Manager が最も役に立ち、複数のスイッチに関係するファブリック管理操作を実行するには Cisco DCNM-SAN が効率的です。

上位層管理タスクには、シスコ製またはサードパーティ製のストレージ/ネットワーク管理アプリケーションが提供するツールを使用できます。ストレージ ネットワーク管理の各レイヤの目的および機能の概要を次に示します。

- デバイス管理：システムまたはファブリック内のデバイスを設定および管理するためのツールを提供します。デバイス管理ツールは、初期デバイス設定、しきい値の設定やモニタリング、およびデバイス システムのイメージまたはファームウェアの管理などの作業を、一度に 1 台のデバイスで実行する場合に使用します。
- ファブリック管理：ファブリック全体およびデバイスを表示します。ファブリック管理アプリケーションは、ファブリックの検出、モニタリング、レポート、設定を行います。
- リソース管理：ファブリック帯域幅、接続パス、ディスク、I/O Operations Per Second（IOPS）、CPU、メモリなどのリソース管理ツールを提供します。これらの一部のタスクを実行するには、Cisco DCNM-SAN を使用できます。
- データ管理：データの完全性、アベイラビリティ、およびパフォーマンスを確保するためのツールを提供します。データ管理サービスには、Redundant Array of Independent Disks（RAID）方式、データ レプリケーション方式、バックアップまたはリカバリ要件、およびデータ マイグレーションなどがあります。データ管理機能には、サードパーティ製ツールを使用してください。
- アプリケーション管理：デバイス、ファブリック、リソース、およびアプリケーション データを含むシステム全体の管理ツールを提供します。アプリケーション管理は上記のすべてのコンポーネントを、ストレージ ネットワークを使用するアプリケーションと統合します。アプリケーション管理機能には、サードパーティ製ツールを使用してください。

帯域内管理および帯域外管理

Cisco DCNM-SAN を使用するには、少なくとも 1 つの Cisco MDS 9000 ファミリ スイッチに帯域外（イーサネット）接続を行う必要があります。ファブリックを管理するには、mgmt0 または IP over Fibre Channel（IPFC）のいずれかが必要です。

mgmt0

帯域外管理接続は、スーパーバイザ モジュールの 10/100 Mbps イーサネット インターフェイス（mgmt0 のラベル）です。mgmt0 インターフェイスを管理ネットワークに接続すると、イーサネット上で IP を介してスイッチにアクセスできます。そのためには、ファブリック内の少なくとも 1 台の Cisco MDS 9000 ファミリ スイッチに、イーサネット管理ポートを通して接続する必要があります。その後は、この接続を使用して、帯域内（ファイバ チャネル）接続によるその他のスイッチの管理を実行できます。この接続を使用しない場合は、各スイッチの mgmt0 ポートをイーサネット ネットワークに接続する必要があります。

各スーパーバイザ モジュールは独自にイーサネット接続されますが、冗長スーパーバイザ システム内の 2 つのイーサネット接続は、アクティブまたはスタンバイ モードで動作します。アクティブ スーパーバイザ モジュールは、アクティブな mgmt0 接続のホストとしても機能します。スタンバイ スー

パーバイザ モジュールへのフェールオーバー イベントが発生すると、アクティブ イーサネット接続の IP アドレスおよび MAC（メディア アクセス コントロール）アドレスがスタンバイ イーサネット接続に移動します。

IPFC

帯域内 IP 接続を使用して、ファイバ チャネル ネットワーク上のスイッチを管理することもできます。Cisco MDS 9000 ファミリは、IPFC ネットワークをトランスポートするためのカプセル化方式を定義する RFC 2625 IPFC をサポートします。

IPFC は IP パケットをファイバ チャネル フレームにカプセル化します。これにより、スイッチごとに専用のイーサネット接続を確立しなくても、ファイバ チャネル ネットワーク上で管理情報を伝達できるようになります。この機能を使用すると、帯域内管理ソリューションを完全に構築できます。

前提条件

ここで説明する内容は、次のとおりです。

- 「初回のセットアップ ルーチン」（P.1-6）
- 「スイッチを設定するための準備」（P.1-6）
- 「デフォルトのログイン」（P.1-7）
- 「セットアップ オプション」（P.1-7）
- 「セットアップ情報の指定」（P.1-8）
- 「Enter the switch name: switch_name」（P.1-10）
- 「Cisco MDS 9000 ファミリのスイッチの始動」（P.1-16）
- 「スイッチへのアクセス」（P.1-17）

Cisco DCNM をインストールする前に、Cisco DCNM システムで次の前提条件が満たされていることを確認します。

- Cisco DCNM をインストールする前に、次の場所にあるホスト ファイルで、ホスト名が IP アドレスとマッピングされていることを確認します。
  - Microsoft Windows：C:\WINDOWS\system32\drivers\etc\hosts
  - Linux：/etc/hosts

（注）　Oracle RAC が Cisco DCNM 向けデータベースとして選択された場合は、データベースのホスト IP アドレスと仮想 IP アドレスがそれぞれのホスト名とともにホスト ファイルに追加されていることを確認します。

- RHEL の場合、共有メモリの最大サイズは 256 MB 以上である必要があります。共有メモリの最大サイズを 256 MB に設定するには、次のコマンドを使用します。

  sysctl -w kernel.shmmax=268435456

  この設定（kernel.shmmax=268435456）を /etc/sysctl.conf ファイルに保存する必要があります。この設定が存在しなかったり、268435456 未満に設定されていたりすると、サーバ システムの再起動後に Cisco DCNM サーバが失敗します。詳細については、次の URL を参照してください。

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

サーバ システムは、DNS サーバに登録されている必要があります。サーバには他のプログラムが実行されていません。

- リモート PostgreSQL データベース サーバを使用する場合は、Cisco DCNM ホスト IP が、PostgreSQL のインストール ディレクトリにある pg_hba.conf ファイルに追加されていることを確認します。エントリが追加された後で、DB を再起動します。

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

- Cisco DCNM をインストールするユーザには、ユーザ アカウントを作成し、サービスを起動するためのすべての管理者権限が必要です。また、すべてのポートへのアクセス権も必要です。Cisco DCNM サーバと PostgreSQL データベースは、1098、1099、4444、4445、8009、8083、8090、8092、8093、514、5432 のポートを使用します。
- サーバの初回接続時に、Cisco DCNM は、正しい Sun Java Virtual Machine バージョンがワークステーションにインストールされているかどうかを確認します。Cisco DCNM は、インストール中にバージョン 1.6(x) を検索します。必要な場合は、Sun Java Virtual Machine ソフトウェアをインストールします。
- Windows の場合、リモート Cisco DCNM のインストールまたはアップグレードは、VNC を使用したコンソールまたは Remote Desktop Client（RDC）のコンソール モードで行う必要があります（RDC が /Console オプションで使用されていることを確認します）。データベースのインストールおよびアップグレードすべてでローカル コンソールが必要であるため、このプロセスはデフォルト PostgreSQL データベースを Cisco DCNM と一緒に使用する場合に非常に重要です。
- Windows Vista システムに Cisco DCNM をインストールする前に、User Account Control（UAC）をオフにします。UAC をオフにするには、[Start] > [Control Panel] > [User Accounts] > [Turn User Account Control on or off] を選択し、[Use User Account Control (UAC) to help protect your computer] チェックボックスをオフにして、[OK] をクリックします。[Restart Now] をクリックして変更内容を適用します。
- Telnet Client アプリケーションはデフォルトでは Microsoft Windows Vista にインストールされていません。Telnet Client をインストールするには、[Start] > [Programs] > [Control Panel] > [Turn Windows features on or off] を選択します（UAC をオンにしている場合、続行するための権限を付与する必要があります）。[Telnet Client] チェックボックスをオンにして、[OK] をクリックします。
- Java 要件が異なっている場合でも、Cisco DCNM と同じ PC 上で CiscoWorks を実行できます。Cisco DCNM 用に新しい Java バージョンをインストールする場合は、CiscoWorks に必要な古い Java バージョンを上書きしないようにしてください。両方の Java バージョンは PC 上 で共存できます。

（注）　Cisco DCNM インストーラを起動する場合に、**console** コマンド オプションはサポートされません。

（注）　Cisco DCNM インストーラを GUI モードで使用するには、VNC または XWindows を使用してリモート サーバにログインする必要があります。Telnet または SSH を使用して Cisco DCNM を GUI モードでインストールすることはできません。

Cisco DCNM にアクセスする前に、次のタスクを実行する必要があります。

- 管理するスイッチごとに、スーパーバイザ モジュールを搭載します。
- スーパーバイザ モジュールには、セットアップ ルーチンまたは CLI を使用して次の値を設定します。
  - mgmt0 インターフェイスに割り当てられる IP アドレス

  - SNMP 資格情報（v3 ユーザ名およびパスワードまたは v1/v2 コミュニティ）：ファブリック内のすべてのスイッチに対して同じユーザ名およびパスワードを維持します。

初回のセットアップ ルーチン

Cisco MDS 9000 ファミリのスイッチに初めてアクセスすると、セットアップ プログラムが実行され、IP アドレスや、スイッチがスーパーバイザ モジュールのイーサネット インターフェイスを介して通信するために必要なその他の設定情報を入力するよう求められます。この情報は、スイッチを設定および管理するために必要です。IP アドレスは、CLI からだけ設定できます。すべての Cisco MDS 9000 ファミリ スイッチにおいて、デフォルト ユーザはネットワーク管理者（admin）です。デフォルトのユーザはどの時点でも変更できません。Cisco MDS 9000 ファミリのすべてのスイッチに、強固なパスワードを明示的に設定する必要があります。セットアップ方法は、新しいスイッチを追加するサブネットによって異なります。

- 帯域外管理：スーパーバイザ モジュールの前面パネルのイーサネット ポートを介したネットワーク接続を提供します。
- 帯域内管理：スイッチ管理用の IP over Fibre Channel（IPFC）を提供します。帯域内管理機能は NMS（Network Management System; ネットワーク管理システム）に透過的です。

（注）　IP アドレスは、CLI からだけ設定できます。初回のスイッチ始動時に、IP アドレスを割り当ててください。この手順を実行すると、Cisco DCNM-SAN は管理ポートを介してスイッチに到達できるようになります。

スイッチを設定するための準備

Cisco MDS 9000 ファミリのスイッチを初めて設定する際には、事前に次の情報を用意しておく必要があります。

- 次に示す管理者パスワード
  - 管理者パスワードの作成（必須）
  - その他のログイン アカウントおよびパスワードの作成（任意）
- スイッチ管理インターフェイスの IP アドレス：管理インターフェイスには、帯域外イーサネット インターフェイスまたは帯域内のファイバ チャネル インターフェイス（推奨）を使用できます。
- スイッチ管理インターフェイスのサブネット マスク（任意）
- 次の IP アドレス
  - 送信先プレフィックス、送信先プレフィックスのサブネット マスク、およびネクストホップの IP アドレス（IP ルーティングをイネーブルにする場合）。さらに、デフォルト ネットワークの IP アドレスも用意します（任意）。
  - あるいは、デフォルト ネットワークの IP アドレスも用意します（任意）。
- スイッチの SSH サービス：この任意のサービスをイネーブルにする場合は、SSH キーのタイプ（dsa/rsa/rsa1）とキー ビット数（768 ～ 2048）を選択します。
- DNS IP アドレス（任意）
- デフォルト ドメイン名（任意）
- NTP サーバの IP アドレス（任意）
- SNMP コミュニティ ストリング（任意）

- スイッチ名：これは、スイッチ プロンプトに使用されます（任意）。

（注）　SNMP アクセスをイネーブルにする場合は、必ず IP ルート、IP デフォルト ネットワーク アドレス、および IP デフォルト ゲートウェイ アドレスを設定してください。IP ルーティングがイネーブルの場合、スイッチは IP ルートとデフォルト ネットワーク IP アドレスを使用します。IP ルーティングがディセーブルの場合、スイッチはデフォルト ゲートウェイ IP アドレスを使用します。

（注）　インストール時に Cisco DCNM-SAN Server が特定のインターフェイスにバインドするように設定されている場合を除き、Cisco DCNM-SAN Server のホスト名エントリが DNS サーバに存在していることを確認する必要があります。

デフォルトのログイン

すべての Cisco MDS 9000 ファミリ スイッチにおいて、デフォルト ユーザはネットワーク管理者（admin）です。デフォルトのユーザはどの時点でも変更できません。（『*Security Configuration Guide, Cisco DCNM for SAN*』を参照）。

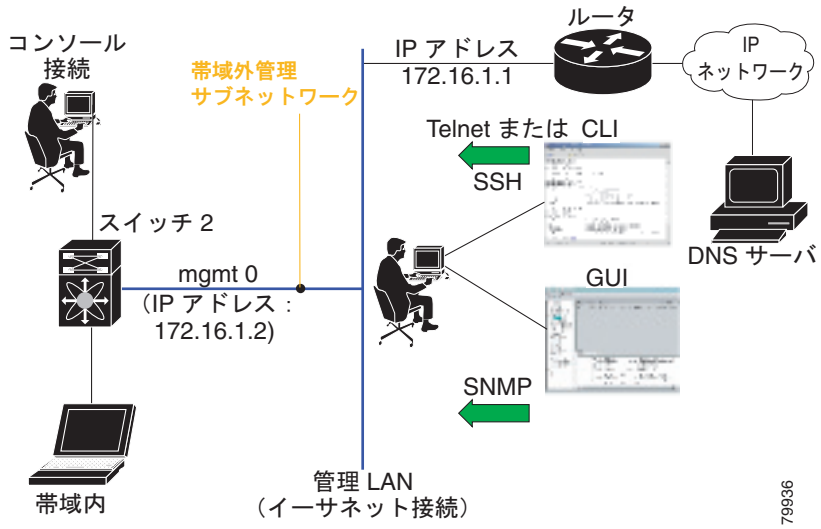
Cisco MDS 9000 ファミリのいずれのスイッチにも、安全なパスワードを強制するオプションがあります。パスワードが簡潔である場合（短く、解読しやすい場合）、パスワード設定は拒否されます。安全なパスワードを設定します（『*Security Configuration Guide, Cisco DCNM for SAN*』を参照）。パスワードの設定後に、その新しいパスワードを忘れてしまった場合は、パスワードを回復することもできます（『*Security Configuration Guide, Cisco DCNM for SAN*』を参照）。

セットアップ オプション

セットアップ方法は、新しいスイッチを追加するサブネットによって異なります。スイッチ外部からの管理接続をイネーブルにするには、Cisco MDS 9000 ファミリ スイッチに IP アドレスを設定する必要があります（図 1-1 を参照）。

（注）　ここでは、帯域外管理や帯域内管理など、いくつかの概念について簡単に説明します。これらの概念については、以降の章でも詳しく説明します。

図 1-1　スイッチへの管理者アクセス



セットアップ情報の指定

ここでは、帯域外と帯域内の両方の管理について、初回のスイッチ設定方法を説明します。

（注）　任意のプロンプトで Ctrl+C キーを押すと、残りの設定オプションを飛ばして、設定手順を先に進めることができます。管理者用の新しいパスワードの入力は必須の手順であり、飛ばすことはできません。

ヒント　以前に設定した項目の値を再度入力しない場合や、入力を省略する場合は、Enter キーを押します。デフォルトの回答が見つからない場合（たとえば、スイッチ名）、スイッチは以前の設定を使用して、次の質問にスキップします。

帯域外管理の設定

ステップ 11c および ステップ 11d 以降に説明する手順の および の両方に **Yes** を入力すると、帯域内管理と帯域外管理の両方を設定できます。

手順の詳細

ステップ 1　スイッチの電源を入れます。Cisco MDS 9000 ファミリのスイッチは自動的にブートします。

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

ステップ 2　**Yes** と入力して、安全なパスワードを強制します。

a. 管理者パスワードを入力します。

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

b. 管理者パスワードを確認します。

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

ヒント　パスワードが簡潔である場合（短く、解読しやすい場合）、パスワード設定は拒否されます。サンプル設定のように、強力なパスワードを設定してください。パスワードでは、大文字と小文字が区別されます。『*Security Configuration Guide, Cisco DCNM for SAN*』に示されている要件を満たすパスワードを明示的に設定する必要があります。

ステップ 3　**yes** と入力すると、セットアップ モードが開始されます。

（注）　このセットアップ ユーティリティでは、手順に従って、システムの基本的な設定を行えます。セットアップで設定されるのは、システムの管理に必要な接続のみです。

```
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
```

セットアップ ユーティリティでは、手順に従って、基本的な設定プロセスを完了できます。どのプロンプトでも、Ctrl を押した状態で C を押すと、設定プロセスが終了します。

ステップ 4　管理者用の新しいパスワードを入力します（デフォルトは admin）。

```
Enter the password for admin: admin
```

ステップ 5　**yes** を入力して、追加のアカウントを作成します（デフォルトは no）。

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

初回のセットアップ時に、管理者のアカウント以外にもう 1 つユーザ アカウント（network-admin ロール）を作成できます。デフォルトのロールと権限については、『*Security Configuration Guide, Cisco DCNM for SAN*』を参照してください。

（注）　ユーザ ログイン ID には、数字以外の文字を含める必要があります。

a. ユーザ ログイン ID [administrator] を入力します。

```
Enter the user login ID: user_name
```

b. ユーザ パスワードを入力します。

```
Enter the password for user_name: user-password
```

c. ユーザ パスワードを確認します。

```
Confirm the password for user_name: user-password
```

ステップ 6　**yes** を入力して SNMPv3 アカウントを追加します（デフォルトは no）。

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

a. ユーザ名を入力します（デフォルトは admin）。

```
SNMPv3 user name [admin]: admin
```

b. SNMPv3 パスワードを入力します（8 文字以上）。デフォルトは **admin123** です。

```
SNMPv3 user authentication password: admin_pass
```

ステップ 7　**yes** を入力して、読み取り専用または読み取り書き込みの SNMP コミュニティ ストリングを設定します（デフォルトは no）。

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

a. SNMP コミュニティ ストリングを入力します。

```
SNMP community string: snmp_community
```

ステップ 8　スイッチの名前を入力します。

```
Enter the switch name: switch_name
```

ステップ 9　**yes** と入力し（デフォルトは yes）、帯域外管理を設定します。

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

a. mgmt0 IP アドレスを入力します。

```
Mgmt0 IPv4 address: ip_address
```

b. mgmt0 サブネット マスクを入力します。

```
Mgmt0 IPv4 netmask: subnet_mask
```

ステップ 10　**yes** を入力して、デフォルト ゲートウェイを設定します（推奨）（yes がデフォルト）。

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

a. デフォルト ゲートウェイ IP アドレスを入力します。

```
IPv4 address of the default gateway: default_gateway
```

ステップ 11　**yes** を入力して、帯域内管理、スタティック ルート、デフォルト ネットワーク、DNS、ドメイン名などの拡張 IP オプションを設定します（デフォルトは **no**）。

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

a. 帯域内管理の設定プロンプトに **no** を入力します（no がデフォルト）。

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

b. **yes** を入力して、IP ルーティング機能をイネーブルにします（デフォルトは no）。

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

c. **yes** を入力して、スタティック ルートを設定します（推奨）（デフォルトは no）。

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

送信先プレフィックスを入力します。

```
Destination prefix: dest_prefix
```

送信先プレフィックス マスクを入力します。

```
Destination prefix mask: dest_mask
```

ネクストホップ IP アドレスを入力します。

```
Next hop ip address: next_hop_address
```

（注）　SNMP アクセスをイネーブルにする場合は、必ず IP ルート、デフォルト ネットワーク IP アドレス、およびデフォルト ゲートウェイ IP アドレスを設定してください。IP ルーティングがイネーブルの場合、スイッチは IP ルートとデフォルト ネットワーク IP アドレスを使用します。IP ルーティングがディセーブルの場合、スイッチはデフォルト ゲートウェイ IP アドレスを使用します。

d. **yes** を入力して、デフォルト ネットワークを設定します（推奨）（デフォルトは no）。

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

デフォルト ネットワーク IP アドレスを入力します。

（注）　デフォルト ネットワーク IP アドレスは、ステップ 11c で入力した送信先プレフィックスです。

```
Default network IP address [dest_prefix]: dest_prefix
```

e. **yes** を入力して、DNS IP アドレスを設定します（デフォルトは no）。

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

DNS IP アドレスを入力します。

```
DNS IPv4 address: name_server
```

f. **yes** を入力して、デフォルト ドメイン名を設定します（デフォルトは no）。

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

デフォルト ドメイン名を入力します。

```
Default domain name: domain_name
```

ステップ 12　**yes** を入力して、Telnet サービスをイネーブルにします（デフォルトは no）。

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

ステップ 13　**yes** を入力して、SSH サービスをイネーブルにします（no がデフォルト）。

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

ステップ 14　SSH キーのタイプを入力します。

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

ステップ 15　指定範囲内でキーのビット数を入力します。

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

ステップ 16　**yes** を入力して、NTP サーバを設定します（デフォルトは no）。

```
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. NTP サーバの IP アドレスを入力します。

```
NTP server IP address: ntp_server_IP_address
```

ステップ 17　**noshut** を入力して、デフォルト スイッチ ポート インターフェイスを noshut 状態にします（デフォルトは shut）。

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

ステップ 18　**on** と入力して（デフォルトは on）、スイッチ ポート トランク モードを設定します。

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

ステップ 19　**no** と入力して、スイッチ ポートのモード F を設定します（on がデフォルト）。

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

ステップ 20　**permit** と入力して（デフォルトは deny）、デフォルトのゾーン ポリシー設定を拒否します。

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

デフォルト ゾーンのすべてのメンバーへのトラフィック フローを許可します。

ステップ 21　**yes** と入力して（デフォルトは no）、フル ゾーン セットの配布をディセーブルにします（『*Fabric Configuration Guide, Cisco DCNM for SAN*』を参照）。フル ゾーン セット配布機能について、スイッチ全体のデフォルトをディセーブルにします。

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

新しい設定を参照します。ここまでに入力した設定を確認して修正します。

ステップ 22　設定に問題がなければ、**no** と入力します（デフォルトは no）。

```
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
```

ステップ 23　**yes** と入力すると、この設定を保存して使用できます（デフォルトは yes）。

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

注意　ここで、設定を保存しておかないと、次回のスイッチ再起動時に設定が更新されません。**yes** と入力すると、新しい設定が保存され、キックスタート イメージとシステム イメージも自動的に設定されます。

帯域内管理の設定

帯域内管理の論理インターフェイスは VSAN 1 です。この管理インターフェイスはファイバ チャネル インフラストラクチャを使用して IP トラフィックを伝送します。VSAN 1 のインターフェイスはファブリック内のすべてのスイッチで作成されます。スイッチにはそれぞれ同じサブネットワークの IP アドレスが設定された VSAN 1 インターフェイスを割り当てる必要があります。IP ネットワークへのアクセスを提供するスイッチを指すデフォルト ルートをファイバ チャネル ファブリックのスイッチすべてに対して設定します（『*Fabric Configuration Guide, Cisco DCNM for SAN*』を参照）。

（注）　次に説明する手順のステップ 9c およびステップ 9d の両方に **Yes** を入力すると、帯域内管理と帯域外管理の両方を設定できます。

手順の詳細

ステップ 1　スイッチの電源を入れます。Cisco MDS 9000 ファミリのスイッチは自動的にブートします。

ステップ 2　管理者用の新しいパスワードを入力します。

```
Enter the password for admin: 2004asdf*lkjh18
```

ヒント　パスワードが簡潔である場合（短く、解読しやすい場合）、パスワード設定は拒否されます。設定例で示されたような強固なパスワードを設定してください。パスワードでは、大文字と小文字が区別されます。『*Security Configuration Guide, Cisco DCNM for SAN*』の項「*User Accounts*」に示されている要件を満たすパスワードを明示的に設定する必要があります。

ステップ 3　**yes** と入力すると、セットアップ モードが開始されます。

```
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
```

セットアップ ユーティリティでは、手順に従って、基本的な設定プロセスを完了できます。どのプロンプトでも、Ctrl を押した状態で C を押すと、設定プロセスが終了します。

ステップ 4　追加のアカウントを作成しない場合は、**no** を入力します（no がデフォルト）。

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

ステップ 5　読み取り専用または読み取り書き込みの SNMP コミュニティ ストリングを設定します。

a. **no** を入力して読み取り専用の SNMP コミュニティ ストリングの設定を回避します（デフォルトは no）。

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

ステップ 6　スイッチの名前を入力します。

（注）　スイッチの名前は、英数字 32 文字以内で指定してください。デフォルトは **switch** です。

```
Enter the switch name: switch_name
```

ステップ 7　帯域外管理を設定する設定プロンプトに **no** を入力します（デフォルトは yes）。

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

ステップ 8　デフォルト ゲートウェイの設定に **yes** を入力します（yes がデフォルト）。

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

a. デフォルト ゲートウェイ IP アドレスを入力します。

```
IP address of the default gateway: default_gateway
```

ステップ 9　**yes** を入力して、帯域内管理、スタティック ルート、デフォルト ネットワーク、DNS、ドメイン名などの拡張 IP オプションを設定します（デフォルトは no）。

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

a. 帯域内管理の設定プロンプトに **yes** を入力します（デフォルトは no）。

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

VSAN 1 IP アドレスを入力します。

```
VSAN1 IP address: ip_address
```

サブネット マスクを入力します。

```
VSAN1 IP net mask: subnet_mask
```

b. **no** を入力して IP ルーティング機能をイネーブルにします（yes がデフォルト）。

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

c. スタティック ルートの設定に **no** を入力します（デフォルトは yes）。

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

d. デフォルト ネットワークの設定に **no** を入力します（デフォルトは yes）。

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

e. DNS IP アドレスの設定に **no** を入力します（デフォルトは yes）。

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

f. **no** を入力して、デフォルト ドメイン名の設定を省略します（no がデフォルト）。

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

ステップ 10　**no** を入力して、Telnet サービスをディセーブルにします（デフォルトは yes）。

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

ステップ 11　**yes** を入力して、SSH サービスをイネーブルにします（no がデフォルト）。

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

ステップ 12　生成する SSH キーの種類を入力します（『*Security Configuration Guide, Cisco DCNM for SAN*』を参照）。

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

ステップ 13　指定範囲内でキーのビット数を入力します。

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

ステップ 14　NTP サーバの設定に **no** を入力します（no がデフォルト）。

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

ステップ 15　**shut** を入力して、デフォルト スイッチ ポート インターフェイスを shut 状態にします（shut がデフォルト）。

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

（注）　管理イーサネット インターフェイスはこの時点ではシャットダウンされません。シャットダウンされるのはファイバ チャネル、iSCSI、FCIP、およびギガビット イーサネット インターフェイスだけです。

ステップ 16　スイッチ ポート トランク モードの設定に **auto** を入力します（デフォルトは off）。

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

ステップ 17　**deny** を入力して、デフォルト ゾーン ポリシーの設定を拒否します（deny がデフォルト）。

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

デフォルト ゾーンのすべてのメンバーへのトラフィック フローを拒否します。

ステップ 18　**no** を入力して、フル ゾーン セットの配布をディセーブルにします（no がデフォルト）。

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

フル ゾーン セット配布機能について、スイッチ全体のデフォルト値をディセーブルにします。

新しい設定を参照します。ここまでに入力した設定を確認して修正します。

ステップ 19　設定に問題がなければ、**no** と入力します（デフォルトは no）。

```
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
```

ステップ 20　**yes** と入力すると、この設定を保存して使用できます（yes がデフォルト）。

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

注意　ここで、設定を保存しておかないと、次回のスイッチ再起動時に設定が更新されません。**yes** と入力して、新しい設定を保存します。これによって、キックスタート イメージとシステム イメージも自動的に設定されます。

setup コマンドの使用方法

後で初期設定を変更する場合は、EXEC モードで **setup** コマンドを入力します。

```
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
```

セットアップ ユーティリティでは、手順に従って、基本的な設定プロセスを完了できます。

Cisco MDS 9000 ファミリのスイッチの始動

ここでは、スイッチの始動など、ハードウェア インストレーション時に完了しておく必要のある作業手順をまとめます。これらの作業を完了しないと、スイッチを設定できません。

（注）　初回のスイッチ始動時には CLI を使用する必要があります。

手順の詳細

ステップ 1　新しい Cisco MDS 9000 ファミリ スイッチの物理的な接続を確認します。次の接続を確認してください。

- コンピュータ端末（または端末サーバ）にコンソール ポートが物理的に接続されている。
- 管理 10/100 イーサネット ポート（mgmt0）が外部ハブ、スイッチ、またはルータに接続されている。

詳細については、（該当製品の）『*Cisco MDS 9000 Family Hardware Installation Guide*』を参照してください。

ヒント 後で使用するためにホスト ID 情報を控えておいてください（たとえば、ライセンス機能をイネーブルにする場合など）。ホスト ID 情報は、スイッチに同梱されている Proof of Purchase 文書に記載されています。

ステップ 2　デフォルトのコンソール パラメータが、スイッチのコンソール ポートに接続されているコンピュータ ターミナル（またはターミナル サーバ）と値が同じであることを確認します。

- 9600 ボー
- 8 データ ビット
- 1 ストップ ビット
- パリティなし

ステップ 3　スイッチの電源を入れます。スイッチは自動的にブートし、ターミナル ウィンドウに switch# プロンプトが表示されます。

スイッチへのアクセス

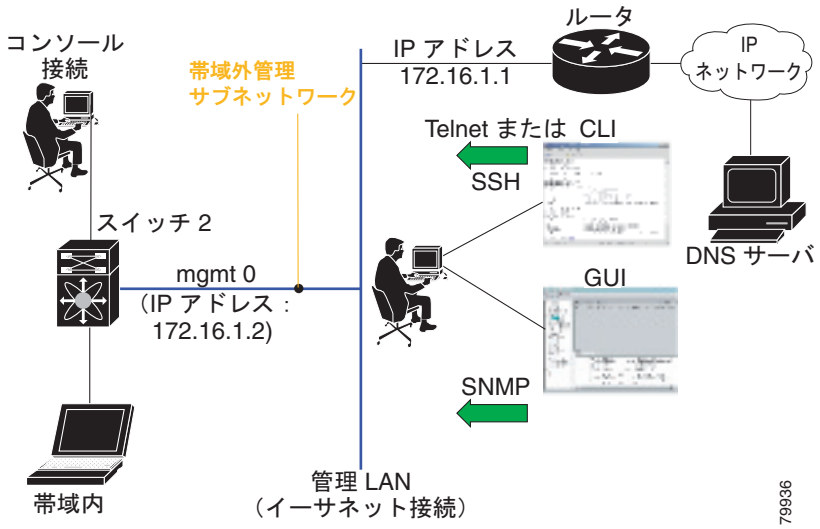
初期設定後は、次の 3 つのいずれかの方法でスイッチにアクセスできます。

- シリアル コンソール アクセス：シリアル ポート接続を使用して CLI にアクセスできます。
- 帯域内 IP（IPFC）アクセス：Telnet または SSH を使用して Cisco DCNM-SAN 9000 ファミリのスイッチにアクセスできます。または SNMP を使用して Cisco DCNM-SAN アプリケーションに接続できます。
- 帯域外（10/100BASE-T イーサネット）アクセス：Telnet または SSH を使用して Cisco MDS 9000 ファミリのスイッチにアクセスできます。または SNMP を使用して Cisco DCNM-SAN アプリケーションに接続できます。

初回の設定後は、次の 3 つのいずれかの方法でスイッチにアクセスできます（図 1-2 を参照）。

- シリアル コンソール アクセス：シリアル ポート接続を使用して CLI にアクセスできます。
- 帯域内 IP（IPFC）アクセス：Telnet または SSH を使用して Cisco MDS 9000 ファミリのスイッチにアクセスできます。または Cisco DCNM-SAN を使用してスイッチにアクセスできます。
- 帯域外（10/100BASE-T イーサネット）アクセス：Telnet または SSH を使用して Cisco MDS 9000 ファミリのスイッチにアクセスできます。または Cisco DCNM-SAN を使用してスイッチにアクセスできます。

図 1-2　スイッチ アクセスのオプション



サポート対象のソフトウェア

（注）　サポートされたソフトウェアの最新情報については、『*Cisco DCNM Release Notes, Release 6.x*』を参照してください。

Cisco DCNM および Cisco Device Manager では、次のソフトウェアがテスト済みです。

- オペレーティング システム
  - サーバ：Windows 2003、Windows 2008 Standard SP2 エディション（32 ビットまたは 64 ビット）、Windows 2008 R2 Sp1（64 ビット）、RHEL 5.4/5.5/5.6/5.7（32 ビットおよび 64 ビット）
  - クライアント：Windows XP および Windows 7（32 ビットおよび 64 ビット）
  - Red Hat Enterprise Linux AS Release 5.4

  （注）　Cisco DCNM-SAN と Cisco DCNM-LAN サーバを Windows 7（32 ビットおよび 64 ビット）プラットフォームにインストールすることはできません。

- Java
  - Sun JRE と JDK 1.6(x) はサポートされています。
  - Java Web Start 1.6 u31
- ブラウザ

Adobe Flash 10 をサポートする次の一般的な Web ブラウザは Cisco DCNM-LAN および Cisco DCNM-SAN と使用できます。

  - Internet Explorer
  - Firefox
- データベース
  - Oracle Database 10g Express、Oracle Enterprise Edition 10g、Oracle Enterprise Edition 11g、および 11gR2 Enterprise Edition（ファブリックが大規模な場合は、Oracle 11gR2 Enterprise Edition を推奨します）。
  - Oracle RAC
  - PostgreSQL 8.2、8.3（Windows および Red Hat Enterprise Linux AS Release 5）
  - PostgreSQL 8.1（Solaris 9 および 10）
- セキュリティ
  - Cisco ACS 3.1 および 4.0
  - PIX ファイアウォール
  - IP テーブル
  - SSH v2
  - Global Enforce SNMP Privacy Encryption
  - HTTPS
- VMware サポート対象バージョン
  - EsX 4.5
  - ESXi 4.5 および 5.0

Cisco DCNM

Cisco DCNM を使用すると、コマンドライン インターフェイス（CLI）を使用しなくても、ほとんどのスイッチ コンフィギュレーション コマンドの機能を実行できます。

Cisco DCNM-SAN には、Cisco MDS 9000 スイッチの完全な設定機能およびステータス モニタ機能の他に、強力なファイバ チャネル トラブルシューティング ツールもあります。これらの詳細な状況分析機能および設定分析機能には、MDS 9000 固有のスイッチ機能であるファイバ チャネル ping および traceroute が利用されます。

Cisco DCNM-SAN には、次の管理アプリケーションが含まれます。

- 「Cisco DCNM Server」（P.1-20）
- 「Cisco DCNM-SAN Client」（P.1-20）
- 「Device Manager」（P.1-20）
- 「Performance Manager」（P.1-20）
- 「Cisco DCNM Web Client」（P.1-20）
- 「Cisco DCNM-LAN Client」（P.1-20）

Cisco DCNM Server

Cisco DCNM-SAN Server コンポーネントは、Cisco DCNM-SAN を実行する前に起動する必要があります。Windows PC では、Cisco DCNM-SAN Server はサービスとしてインストールされます。このサービスを管理するには、[Control Panel] の [Windows Services] を使用します。Cisco DCNM-SAN Server は物理および論理ファブリックを検出し、SNMP トラップ、Syslog メッセージ、および Performance Manager しきい値イベントをリッスンします。

（注）　Cisco DCNM-SAN スタンドアロンは、Cisco DCNM 6.1.x リリースでサポートされません。

Cisco DCNM-SAN Client

DCNM-SAN Client では、Cisco MDS 9000 ファミリ スイッチ、サードパーティ製スイッチ、ホスト、ストレージ デバイスなどのネットワーク ファブリックのマップが表示されます。Cisco DCNM-SAN Client では、Cisco DCNM-SAN Server の機能にアクセスする複数のメニューが提供されます。

Device Manager

Cisco MDS NX-OS Release 5.2(1) 以降、Cisco DCNM-SAN により Device Manager が自動的にインストールされます。Device Manager は、1 台のスイッチに対し 2 つのビューを表示します。

- Device View：スイッチ コンフィギュレーションがグラフィック表示され、統計情報および設定情報にアクセスできます。
- Summary View：スイッチの xE ポート（ISL [スイッチ間リンク]）、Fx ポート（ファブリック ポート）、Nx ポート（接続先ホストおよびストレージ）や、ファイバ チャネルおよび IP ネイバー デバイスのサマリーが表示されます。サマリーまたは詳細統計情報は図示したり、印刷したり、タブ区切りフォーマットでファイルに保存したりできます。

Performance Manager

Performance Manager は SNMP を使用してデータを取り込み、詳細なトラフィック分析を行います。このデータはさまざまなグラフおよびチャートに変換され、あらゆる Web ブラウザで表示できます。

Cisco DCNM Web Client

Cisco DCNM Web Client を使用すると、オペレータは Web ブラウザを使用してリモートで Cisco MDS および Nexus のイベント、パフォーマンス、およびインベントリをモニタし、これらのレポートを取得できます。ライセンス処理と検出も Cisco DCNM Web Client で行えます。

Cisco DCNM-LAN Client

Cisco DCNM-LAN Client には、Cisco Nexus 7000 シリーズ、Cisco Nexus 5000 シリーズ、Cisco Nexus 4000 シリーズ、Cisco Nexus 3000 シリーズ、および Cisco Nexus 1000 シリーズのスイッチと Catalyst 6500 シリーズのスイッチを含む検出されたイーサネット ネットワークのマップが表示されます。Cisco DCNM-LAN Client は、イーサネット スイッチのイーサネット インターフェイスをプロビジョニングおよびモニタリングします。また、vPC、VDC、FabricPath などの複雑な機能の設定を可能にし、vPC のトポロジ表現、ポート チャネル、VLAN マッピング、および FabricPath を提供します。

Cisco DCNM の導入に関する情報

ここで説明する内容は、次のとおりです。

- 「データベースのサポート」（P.1-21）
- 「オペレーティング システム」（P.1-21）
- 「VMware のサポート」（P.1-22）
- 「Cisco DCNM SAN クラスタおよびフェデレーションの要件」（P.1-22）
- 「サーバ ポート」（P.1-23）
- 「クラスタ化されたサーバの Cisco DCNM-LAN の要件」（P.1-24）
- 「単一サーバの Cisco DCNM 環境の導入」（P.1-25）
- 「フェデレーション Cisco DCNM 環境またはクラスタ化サーバ Cisco DCNM 環境の導入」（P.1-27）
- 「単一サーバの Cisco DCNM 環境の導入」（P.1-29）

（注）　Cisco DCNM は、Cisco DCNM-SAN フェデレーションまたは Cisco DCNM-LAN クラスタ モデルとして導入できます。Cisco DCNM-SAN フェデレーションの場合、データベース URL（プロパティ）は、フェデレーション内のすべての Cisco DCNM-SAN ノードで同じである必要があります。Cisco DCNM-LAN クラスタの場合、データベース URL（プロパティ）、パーティション名、およびマルチキャスト アドレスは、クラスタ内のすべての Cisco DCNM-LAN ノードで同じである必要があります。Cisco DCNM が SAN フェデレーションで導入された場合は、Cisoc DCNM-SAN と Cisco DCNM-LAN の両方で同じデータベース スキーマを単一製品として使用するため、Cisco DCNM-LAN もクラスタ モードで導入する必要があります。Cisco DCNM-LAN がクラスタとして導入された場合は、Cisco DCNM-SAN をフェデレーションとして導入する必要があります。

データベースのサポート

Cisco DCNM では、次のデータベースをサポートします。

- PostgreSQL 8.2
- PostgreSQL 8.3
- Oracle Database 10g
- Oracle Database 11g
- Oracle RAC 10g および 11g

Cisco DCNM インストーラでは、サポートされているデータベースがインストールされていない場合に、PostgreSQL 8.3 をインストールできます。

オペレーティング システム

サポートされているサーバ オペレーティング システムのエディションについては、次の URL にある『*Cisco DCNM Release Notes, Release 6.x*』を参照してください。

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

Cisco DCNM は、次のオペレーティング システムのサポートされているバージョンにインストールできます。

- Microsoft Windows Server

サーバ システムで実行されているオペレーティング システムが Microsoft Windows の場合、Cisco DCNM サーバ ソフトウェアはサービスとして実行されます。デフォルトでは、サーバ システムを起動すると Cisco DCNM サーバが自動的に開始されます。

- Red Hat Enterprise Linux

VMware のサポート

Cisco DCNM は、Cisco DCNM-LAN がサポートする互換性がある Windows オペレーティング システムまたは Linux オペレーティング システムを使用する VMware 仮想マシンへの Cisco DCNM サーバのインストールをサポートします。以下の要件が適用されます。

- VMware サーバ ソフトウェアのバージョンが、サポートされているバージョンでなければなりません。
- Cisco DCNM サーバをインストールする仮想マシンで、すべてのサーバ要件が満たされている必要があります。

サポートされている VMware サーバ ソフトウェアおよびその他のサーバ要件の最新情報については、次の URL にある『*Cisco DCNM Release Notes, Release 6.x*』を参照してください。

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

Cisco DCNM SAN クラスタおよびフェデレーションの要件

初めて Cisco DCNM をインストールするときに、Cisco DCNM がフェデレーションまたはクラスタ モードで導入されていて、異なるサブネットにある場合は、Cisco DCNM-LAN サービスを起動しないでください。インストール手順の最後で、[Start LAN and SAN services] チェックボックスをオフにし、Cisco DCNM-SAN サービスを手動で起動します。

サイレント インストールを行う場合は、installer.properties ファイルの Start_DCNM でプロパティ値を FALSE に変更します。

アップグレード時に既存の Cisco DCNM-SAN 5.x フェデレーション ノードが異なるサブネットに属する場合は、Cisco DCNM-LAN サービスを起動しないでください。Cisco DCNM-LAN（クラスタ）は、Cisco DCNM-LAN ノードが異なるサブネットに属する展開をサポートしません。これは、データベースが破損することがあるためです。Cisco DCNM サービスを起動および停止するには Cisco DCNM ショートカットを使用せずに、次の方法で Cisco DCNM-SAN サービスを手動で起動します。

- Microsoft Windows の場合：[Control panel] > [Services] > [Start DCNM-SAN Service] を選択するか、*Cisco DCNM Install folder*\fm\bin に移動して、**Fmserver** と入力し、Cisco DCNM サービスを起動します。
- Linux の場合：*Cisco DCNM Install folde*>/fm/bin に移動し、**./Fmserver start** と入力します。

Cisco DCNM-LAN サーバ クラスタでは、1 つのサーバがマスター サーバの役割を担い、残りのサーバがメンバー サーバになります。マスター サーバになるのは、開始時間が最も古いサーバです。したがって、マスター サーバにするサーバは、そのサーバを最初に開始することによって制御できます。クラスタ化されたサーバ環境での Cisco DCNM-LAN の動作については、『*Cisco DCNM Fundamentals ガイド、リリース 6.x*』のクラスタ管理機能の説明を参照してください。

サーバ クラスタの管理を簡素化するために、プライマリ Cisco DCNM サーバをマスター サーバとして使用することを推奨します。そのためには、クラスタ内の他のサーバを開始する前にプライマリ サーバを開始します。

Cisco DCNM Release 6.x 以降、推奨シナリオは、ノード全体での Cisco DCNM-LAN クラスタリングおよび DCNM-SAN フェデレーションであり、初めて Cisco DCNM をインストールする場合、次のシナリオは推奨されません。

- DCNM-LAN クラスタリング セットアップなしの DCNM-SAN フェデレーション モード

- DCNM-SAN フェデレーション セットアップなしの DCNM-LAN クラスタリング モード

詳細については、「フェデレーション Cisco DCNM 環境またはクラスタ化サーバ Cisco DCNM 環境の導入」（P.1-27）を参照してください。

サーバ ポート

Cisco DCNM-LAN サーバは、いくつかのポートで Cisco DCNM-LAN クライアントからのネットワーク トラフィックを受信できる必要があります。Cisco DCNM-LAN クライアントから Cisco DCNM-LAN サーバに送信されるトラフィックを制御するすべてのネットワーク ゲートウェイ デバイスで、Cisco DCNM-LAN サーバが使用するように設定されているポートに送信されたトラフィックを許可する必要があります。

表 1-2 に、Cisco DCNM-LAN サーバのサービスがリッスンするクライアント通信用のデフォルト ポートを示します。設定できないポートが 1 つありますが、その他のポートは設定できます。ポートの不一致はサーバ インストーラによって自動的に解決されます。

表 1-2　クライアント通信用のデフォルト TCP ポート

サービス名	SAN 用デフォルト ポート	LAN 用デフォルト ポート	設定可能かどうか
RMI	1198	1098	インストール時に設定可能
Naming Service	9099	1099	インストール時に設定可能
SSL	3943	3843	インストール時に設定可能
EJB	3973	3873	インストール時に設定可能
Server Bind 1	5644	4445	インストール時に設定可能
Server Bind 2	5446	4446	インストール時に設定可能
JMS	5457	4457	インストール時に設定可能
Syslog（システム メッセージ）Receiver	5545	5445	インストール時に設定可能
AJP Connector	9009	8009	インストール時に設定可能
Web サーバ	80	8080	インストール時に設定可能
Web サービス	9093	8083	インストール時に設定可能
RMI Object	244444	14444	インストール時に設定可能
UIL2	—	8093	インストール時に設定可能

クラスタ化サーバ展開では、クラスタ内の Cisco DCNM-LAN サーバが、クラスタ パーティション名に対するマルチキャスト UDP メッセージをリッスンします。表 1-3 に、Cisco DCNM-LAN サーバがリッスンするサーバ クラスタ通信用のデフォルト ポートを示します。クラスタ化サーバ展開でサポートされているトポロジではクラスタ内のサーバ間にゲートウェイ デバイスを配置できないため、これは参照用です。一部のポートは設定できませんが、その他のポートはサーバのインストール時に設定できます。3 つのポートのデフォルト値はインストーラ ソフトウェアによって作成されます。

表 1-3　クラスタ化されたサーバ通信用のデフォルト ポート

サービス名	プロトコル	デフォルト ポート	設定可能かどうか
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	インストール時に決定	インストール時に設定可能
Multicast port	UDP	インストール時に決定	インストール時に設定可能
Multicast port	UDP	インストール時に決定	インストール時に設定可能

クラスタ化されたサーバの Cisco DCNM-LAN の要件

ここで説明する内容は、次のとおりです。

- 「クラスタ化されたサーバの Cisco DCNM-LAN 環境の導入の前提条件」（P.1-24）
- 「クラスタ化されたサーバの設定の要件」（P.1-25）

クラスタ化されたサーバの Cisco DCNM-LAN 環境の導入の前提条件

クラスタ化されたサーバの Cisco DCNM-LAN 環境の導入を開始する前に、クラスタ内のサーバ システムで次の要件が満たされていることを確認する必要があります。

- クラスタ内のすべてのサーバ システムで次のものが同一でなければなりません。
  - オペレーティング システム
  - CPU の数
  - CPU 速度
  - メモリ
- Cisco DCNM-LAN サーバを VMware 仮想マシンにインストールする場合は、次の追加の要件も満たされている必要があります。
  - クラスタ内のすべてのサーバが仮想マシンにインストールされている必要があります。仮想サーバ システムと物理サーバ システムが混在するサーバ クラスタを導入できません。
- クラスタ内のすべてのサーバが同じイーサネット ネットワーク セグメントのサーバを使用する必要があります。スイッチやハブを使用してサーバを相互接続することはできますが、Cisco DCNM-LAN 展開のサーバ間にルーティング デバイスを配置できません。
- Cisco DCNM-LAN ユーザの RADIUS または TACACS+ 認証を使用する場合は、認証サーバがクラスタ内のすべての Cisco DCNM-LAN サーバからの認証要求を受け入れるように設定されていることを確認する必要があります。
- クラスタ内のすべてのサーバでネットワーク タイム プロトコル（NTP）をイネーブルにする必要があります。

クラスタ化されたサーバの設定の要件

クラスタ化されたサーバの Cisco DCNM-LAN 環境の導入時に、次の要件が満たされている必要があります。

- クラスタ内のすべてのサーバで同一リリースの Cisco DCNM-LAN（Cisco DCNM Release 5.0(2) など）が実行されている必要があります。
- 次の情報をすべてのサーバで同じように指定する必要があります。
  - クラスタ パーティション名
  - マルチキャスト アドレスおよびポート
  - Cisco DCNM-LAN データベースのパスおよび資格情報
  - 認証設定

  この要件は、セカンダリ サーバのインストール プロセスで満たされます。詳細については、「セカンダリ サーバのインストール」を参照してください。
- 各サーバのインストール時に指定されたアーカイブ ディレクトリが同じディレクトリを参照している必要があります。このディレクトリへのパスは、各サーバで異なる場合があります。この共有ディレクトリは外部共有ディレクトリであり、すべての Cisco DCNM-LAN サーバが読み取りまたは書き込み権限でアクセスできる必要があります。たとえば、Microsoft Windows にインストールされた 2 つの Cisco DCNM-LAN サーバで別のパス（X:\DCNM\data や F:\data など）を使用できますが、その 2 つのパスは同じディレクトリを参照する必要があります。
- クラスタ内のすべてのサーバで安全なクライアント通信をイネーブルまたはディセーブルにする必要があります。

単一サーバの Cisco DCNM 環境の導入

単一サーバ環境で Cisco DCNM を導入できます。単一サーバ環境では、Cisco DCNM サーバ ソフトウェアを実行する単一のサーバ システムがプライマリ Cisco DCNM サーバになります。以下の手順は、単一サーバの Cisco DCNM 環境を導入するために実行する必要がある一般的な手順です。

はじめる前に

Cisco DCNM サーバを実行するサーバ システムで、Cisco DCNM サーバのシステム要件が満たされている必要があります。システム要件の詳細については、『*Cisco DCNM Release Notes, Release 6.x*』を参照してください。

手順の詳細

ステップ 1　Cisco DCNM サーバをインストールするサーバ システムで、サーバ システムのすべての要件が満たされていることを確認します。

詳細については、「クラスタ化されたサーバの Cisco DCNM-LAN の要件」（P.1-24）を参照してください。

ステップ 2　Cisco DCNM サーバ ソフトウェアをダウンロードします。Cisco DCNM-SAN、Cisco DCNM-LAN、および SMI-S が、Cisco DCNM インストールの一部としてインストールされます。

詳細については、「次の作業」（P.1-29）を参照してください。

ステップ 3　インストール済みのデータベースを使用する場合は、そのデータベースで次の準備が完了していることを確認します。

- PostgreSQL：単一の Cisco DCNM サーバが PostgreSQL サーバ システムに対してリモートである場合は、Cisco DCNM サーバからの接続を許可するように PostgreSQL サーバを設定する必要があります。詳細については、「PostgreSQL データベースの準備」（P.2-8）を参照してください。

  Cisco DCNM サーバを PostgreSQL ソフトウェアと同じサーバ システムにインストールする場合は、追加のデータベースの準備は必要ありません。
- Oracle：Cisco DCNM では、Oracle データベースのいくつかの設定をデフォルト設定より高い値に変更する必要があります。詳細については、「Oracle データベースの準備」（P.2-3）を参照してください。
- Oracle RAC

ステップ 4　サーバ システムに Cisco DCNM-LAN サーバ ソフトウェアをインストールします。

詳細については、「プライマリ Cisco DCNM-LAN サーバのインストール」を参照してください。

ステップ 5　（任意）クライアントとサーバ間の通信を暗号化する場合は、クライアントとサーバ間の通信に TLS を使用するよう Cisco DCNM-LAN サーバを設定します。

詳細については、「クライアント / サーバ間の暗号化通信のイネーブル化」（P.8-2）を参照してください。

ステップ 6　（任意）ファイアウォールやその他のゲートウェイ デバイスの外側にある Cisco DCNM-LAN クライアントがその内側にある Cisco DCNM-LAN サーバと通信できるようにする場合は、次の手順を実行します。

a. Cisco DCNM-LAN サーバで特定のセカンダリ サーバのバインド ポートを設定します。

詳細については、「セカンダリ サーバのバインド ポートの指定」（P.8-6）を参照してください。

b. Cisco DCNM-LAN サーバが使用するポート（指定したセカンダリ サーバのバインド ポートを含む）への Cisco DCNM-LAN クライアントからの接続を許可するようにファイアウォールやゲートウェイ デバイスを設定します。

Cisco DCNM-LAN サーバが使用するポートの詳細については、「サーバ ポート」（P.1-23）を参照してください。

c. Cisco DCNM-SAN サーバが使用するポートへの Cisco DCNM-SAN クライアントからの接続を許可するファイアウォールまたはゲートウェイ デバイスの設定については、「ファイアウォール背後での Cisco DCNM の実行」（P.3-18）を参照してください。

ステップ 7　（任意）インストール時に Cisco DCNM サーバを起動しなかった場合は、ここで Cisco DCNM-LAN サーバを起動します。詳細については、『*Cisco DCNM Fundamentals ガイド、リリース 6.x*』を参照してください。

ステップ 8　Cisco DCNM ライセンスは、Cisco DCNM Web クライアントを使用してインストールできます。ライセンスの詳細については、第 6 章「Cisco Data Center Network Manager 向けライセンスのインストールおよび管理」を参照してください。

ステップ 9　Cisco DCNM-LAN および Cisco DCNM-SAN クライアントをインストールします。詳細については、『*Cisco DCNM Fundamentals ガイド、リリース 6.x*』を参照してください。

ステップ 10　Cisco DCNM Web クライアントを使用して、1 つまたは複数のデバイスに対してデバイス検出を実行します。Cisco DCNM Web クライアントで、[Add Data Source] をクリックしてデバイスの検出を開始します。詳細については、『*Cisco DCNM Fundamentals ガイド、リリース 6.x*』を参照してください。

ステップ 11　Cisco DCNM による管理対象デバイスの設定とモニタを開始します。Cisco DCNM の使用の詳細については、次の URL にある Cisco DCNM-LAN および Cisco DCNM-SAN コンフィギュレーション ガイドを参照してください。

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

フェデレーション Cisco DCNM 環境またはクラスタ化サーバ Cisco DCNM 環境の導入

Cisco DCNM サーバ クラスタには、1 つのプライマリ サーバと 1 ～ 4 つのセカンダリ サーバが含まれます。以下の手順は、クラスタ化サーバの Cisco DCNM 環境を導入するために実行する必要がある一般的な手順です。

（注）　Cisco DCNM クラスタを仮想環境にインストールする場合は、仮想マシンが同じホストに存在するようにしてください。

はじめる前に

Cisco DCNM サーバ ソフトウェアを実行するすべてのサーバ システムで、Cisco DCNM サーバのシステム要件が満たされている必要があります。システム要件の詳細については、『*Cisco DCNM Release Notes, Release 6.x*』を参照してください。

手順の詳細

ステップ 1　Cisco DCNM-LAN サーバ クラスタと DCNM-SAN フェデレーション クラスタに含まれる各サーバ システムで、サーバ システムのすべての要件が満たされていることを確認します。

詳細については、「クラスタ化されたサーバの Cisco DCNM-LAN の要件」（P.1-24）を参照してください。

ステップ 2　各サーバ システムで、フェデレーション クラスタ化サーバの導入に対する追加のサーバ要件が満たされていることを確認します。

詳細については、「クラスタ化されたサーバの Cisco DCNM-LAN 環境の導入の前提条件」（P.1-24）を参照してください。

ステップ 3　Cisco DCNM サーバ ソフトウェアをダウンロードします。Cisco DCNM-SAN、Cisco DCNM-LAN、および SMI-S エージェントが、Cisco DCNM インストールの一部としてインストールされます。

詳細については、「次の作業」（P.1-29）を参照してください。

ステップ 4　インストール済みのデータベースを使用する場合は、そのデータベースが次のように準備されていることを確認します。

- PostgreSQL：クラスタ内の各リモート サーバからの接続を許可するように PostgreSQL サーバを設定する必要があります。詳細については、「PostgreSQL データベースの準備」（P.2-8）を参照してください。

  いずれかの Cisco DCNM サーバを PostgreSQL ソフトウェアと同じサーバ システムにインストールする場合は、そのローカルにインストールされた Cisco DCNM サーバについては PostgreSQL サーバで接続を受け入れるように設定する必要はありません。

  （注）　リモート PostgreSQL サーバを使用する Cisco DCNM サーバは、PostgreSQL サーバが Cisco DCNM サーバ システムからのリモート接続を受け入れるように設定されていないと失敗します。

- Oracle：Cisco DCNM では、Oracle データベースのいくつかの設定をデフォルト設定より高い値に変更する必要があります。詳細については、「Oracle データベースの準備」（P.2-3）を参照してください。
- OracleRAC

ステップ 5　クラスタ内のすべての Cisco DCNM サーバが共通のデータおよびファイルをアーカイブするために使用できる共有ディレクトリを設定します。このディレクトリへのパスは、各サーバで異なる場合があります。Cisco DCNM 共有ディレクトリは外部共有ディレクトリであり、すべての Cisco DCNM サーバが読み取りまたは書き込み権限でアクセスできる必要があります。たとえば、Microsoft Windows にインストールされた 2 つの Cisco DCNM サーバで別のパス（X:\DCNM\data と F:\data など）を使用できますが、その 2 つのパスは同じディレクトリを参照している必要があります。

ステップ 6　プライマリ サーバ システムに Cisco DCNM サーバ ソフトウェアをインストールします。

詳細については、「プライマリ Cisco DCNM-LAN サーバのインストール」を参照してください。

ステップ 7　プライマリ Cisco DCNM サーバの間に PostgreSQL サーバをインストールした場合は、クラスタ内の各セカンダリ Cisco DCNM サーバからの接続を許可するように PostgreSQL サーバを設定する必要があります。（セカンダリ サーバは PostgreSQL サーバに対してリモートであるため）。詳細については、「PostgreSQL データベースの準備」（P.2-8）を参照してください。

（注）　リモート PostgreSQL サーバを使用する Cisco DCNM-LAN サーバ インストールは、PostgreSQL サーバが Cisco DCNM-LAN サーバ システムからのリモート接続を受け入れるように設定されていない場合に失敗します。

ステップ 8　各セカンダリ サーバ システムに Cisco DCNM サーバ ソフトウェアをインストールします。

（注）　クラスタ内のすべてのノードは、同じ Cisco DCNM パーティション名を持ち、マルチキャスト IP アドレスを持つ必要があります。

詳細については、「セカンダリ Cisco DCNM-LAN サーバのインストール」を参照してください。

ステップ 9　（任意）セキュアなクライアント通信を使用する場合は、TLS を使用してクライアント / サーバ通信を暗号化できるようにクラスタ内のすべての Cisco DCNM サーバを設定します。

詳細については、「クライアント / サーバ間の暗号化通信のイネーブル化」（P.8-2）を参照してください。

ステップ 10　（任意）ファイアウォールやその他のゲートウェイ デバイスの外側にある Cisco DCNM-LAN クライアントがその内側にある Cisco DCNM-LAN サーバ クラスタと通信できるようにする場合は、次の手順を実行します。

a. クラスタ内の各 Cisco DCNM-LAN サーバで、同じ特定のセカンダリ サーバのバインド ポートを設定します。

詳細については、「セカンダリ サーバのバインド ポートの指定」（P.8-6）を参照してください。

b. クラスタ内の各 Cisco DCNM-LAN サーバが使用するポート（指定したセカンダリ サーバのバインド ポートを含む）への Cisco DCNM-LAN クライアントからの接続を許可するようにファイアウォールやゲートウェイ デバイスを設定します。

Cisco DCNM サーバが使用するポートの詳細については、「サーバ ポート」（P.1-23）を参照してください。

c. DCNM-SAN サーバが使用するポートへの Cisco DCNM-SAN クライアントからの接続を許可するファイアウォールまたはゲートウェイ デバイスの設定については、「ファイアウォール背後での Cisco DCNM の実行」（P.3-18）を参照してください。

ステップ 11　（任意）フェデレーションまたはクラスタ内のすべての Cisco DCNM サーバを起動していない場合は、ここでサーバ クラスタ内の各サーバ システムを起動します。Cisco DCNM-LAN サーバ クラスタの起動の詳細については、『*Cisco DCNM Fundamentals ガイド、リリース 6.x*』を参照してください。

ステップ 12　Cisco DCNM（SAN および LAN）クライアントをインストールします。詳細については、『*Cisco DCNM Fundamentals ガイド、リリース 6.x*』を参照してください。

ステップ 13　Cisco DCNM Web クライアントを使用して、1 つまたは複数のデバイスに対してデバイス検出を実行します。Cisco DCNM Web クライアントで、[Add Data Source] をクリックしてデバイスの検出を開始します。詳細については、『*Cisco DCNM Fundamentals ガイド、リリース 6.x*』を参照してください。

ステップ 14　Cisco DCNM による管理対象デバイスの設定とモニタを開始します。Cisco DCNM の使用の詳細については、次の URL にある Cisco DCNM-LAN コンフィギュレーション ガイドを参照してください。

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

単一サーバの Cisco DCNM 環境の導入

Cisco DCNM Release 6.x 以降では、クラスタ化されたサーバ環境で Cisco DCNM を導入できます。

Microsoft Windows プラットフォームへの Cisco DCNM サーバのインストールについては、「Windows への Cisco DCNM のインストール」（P.3-2）を参照してください。

スクリプトを使用した Cisco DCNM サーバのインストールについては、「サイレント インストーラを使用した Cisco DCNM のインストール」（P.3-8）を参照してください。

VSB を使用した Cisco DCNM のインストールについては、「Cisco Nexus 1010 スイッチでの Cisco DCNM VSB のインストールおよび管理」（P.4-1）を参照してください。

次の作業

デフォルト設定の検討後、その設定の変更や、他の設定または管理作業を実行できます。初回の設定に使用できるのは、CLI だけです。ただし、続けて他のソフトウェア機能を設定したり、初期設定後にスイッチにアクセスする際には、CLI または Device Manager および Cisco DCNM アプリケーションを使用できます。