



CHAPTER 5

IP サービスの設定

Cisco MDS 9000 ファミリ スイッチは、イーサネットとファイバチャネルインターフェイス間で IP トラフィックをルーティングできます。VSAN 間でトラフィックをルーティングするには、IP スタティック ルーティング機能を使用します。この機能を使用するには、VSAN をそれぞれ異なる IP サブネットワークに配置する必要があります。各 Cisco MDS 9000 ファミリ スイッチは、Network Management System (NMS; ネットワーク管理システム) に関する次のサービスを提供します。

- スーパーバイザ モジュールの前面パネルにある帯域外イーサネット インターフェイス (mgmt0) での IP 転送
- IP over Fibre Channel (IPFC) 機能を使用した帯域内ファイバチャネルインターフェイスでの IP 転送：IPFC はカプセル化技術を使用してファイバチャネル上で IP フレームを送信する手順を規定します。IP フレームはファイバチャネルフレームにカプセル化されるため、オーバーレイイーサネットネットワークを使用しなくても、ファイバチャネルネットワーク上で NMS 情報を伝達できます。
- IP ルーティング (デフォルト ルーティングおよびスタティック ルーティング)：外部ルータを必要としない設定の場合は、スタティック ルーティングを使用してデフォルト ルートを設定できます。

スイッチは Virtual Router Redundancy Protocol (VRRP; 仮想ルータ冗長プロトコル) 機能の RFC 2338 標準に準拠します。VRRP は、冗長な代替パスをゲートウェイ スイッチに提供する、再起動可能なアプリケーションです。



(注) IPv6 の設定については、第 8 章「ギガビットイーサネットインターフェイスの IP バージョン 6 (IPv6) の設定」を参照してください。

この章の内容は、次のとおりです。

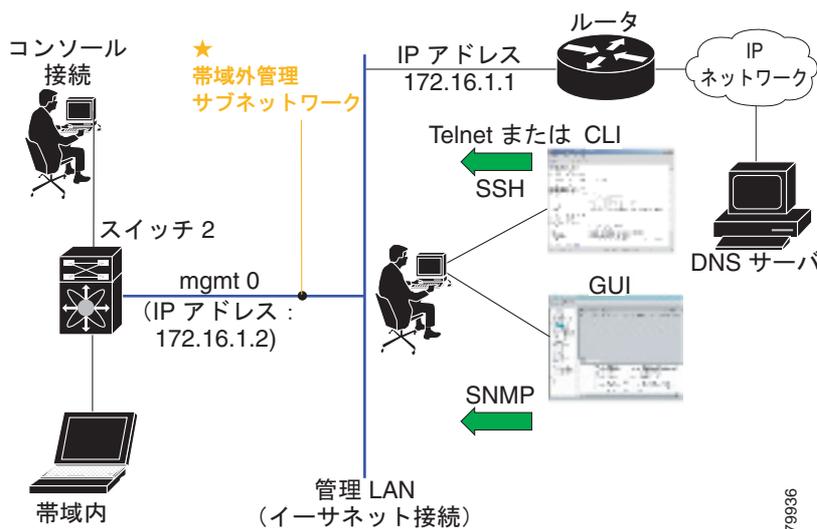
- 「トラフィック管理サービス」(P.5-2)
- 「管理インターフェイスの設定」(P.5-2)
- 「デフォルト ゲートウェイ」(P.5-3)
- 「IPv4 デフォルト ネットワークの設定」(P.5-6)
- 「IPFC」(P.5-7)
- 「IPv4 スタティック ルート」(P.5-8)
- 「オーバーレイ VSAN」(P.5-8)
- 「複数の VSAN の設定」(P.5-10)
- 「仮想ルータ冗長プロトコル」(P.5-11)

- 「DNS サーバの設定」(P.5-15)
- 「デフォルト設定」(P.5-15)

トラフィック管理サービス

帯域内オプションは RFC 2625 標準に準拠し、これに従います。ファイバチャネルインターフェイス上で IP プロトコルが稼動する NMS ホストは、IPFC 機能を使用してスイッチにアクセスできます。NMS にファイバチャネル HBA がない場合でも、いずれかのスイッチをファブリックへのアクセスポイントとして使用して、帯域内管理を実行できます (図 5-1 を参照してください)。

図 5-1 スイッチへのアクセスの管理



管理インターフェイスの設定

スイッチ上の管理インターフェイスでは、同時に複数の Telnet または SNMP セッションが利用できます。スイッチは、管理インターフェイスを介してリモートで設定できますが、スイッチにアクセスできるようにするには、まず IP バージョン 4 (IPv4) パラメータ (IP アドレス、サブネットマスク) または IP バージョン 6 (IPv6) アドレスおよびプレフィクス長を設定する必要があります。IPv6 アドレスの設定については、第 8 章「ギガビットイーサネットインターフェイスの IP バージョン 6 (IPv6) の設定」を参照してください。

ディレクタクラスのスイッチでは、1 つの IP アドレスを使用してスイッチを管理します。アクティブなスーパーバイザモジュールの管理 (mgmt0) インターフェイスはこの IP アドレスを使用します。スタンバイスーパーバイザモジュール上の mgmt0 インターフェイスは、非アクティブなままで、スイッチオーバーが発生するまでアクセスできません。スイッチオーバーが行われると、スタンバイスーパーバイザモジュール上の mgmt0 インターフェイスがアクティブになり、アクティブであったスーパーバイザモジュールと同じ IP アドレスを引き継ぎます。



(注)

MDS 管理イーサネット インターフェイスが接続されるイーサネット スイッチのポートは、スイッチポートではなく、ホストポート（アクセスポートとも呼ばれます）として設定します。（イーサネットスイッチ上の）そのポートのスパニングツリー設定はディセーブルにしてください。このようにすることで、イネーブルの場合にイーサネットスイッチが実行するイーサネットスパニングツリー処理の遅延による MDS 管理ポートの遅延を避けることができます。シスコイーサネットスイッチで、Cisco IOS の **switchport host** コマンドまたは Catalyst OS の **set port host** コマンドのいずれかを使用します。イーサネットスイッチの設定ガイドを参照してください。



(注)

手動による管理インターフェイスの設定を始める前に、スイッチの IP アドレスと IP サブネットマスクを取得します。また、コンソールケーブルがコンソールポートに接続されていることを確認します。

Device Manager を使用して IPv6 用に mgmt0 イーサネット インターフェイスを設定する手順は、次のとおりです。

- ステップ 1 [Interface] > [Mgmt] > [Mgmt0] を選択します。
- ステップ 2 説明を入力します。
- ステップ 3 インターフェイスの管理状態を選択します。
- ステップ 4 [CDP] チェックボックスをオンにして、CDP をイネーブルにします。
- ステップ 5 IP アドレス マスクを入力します。
- ステップ 6 [Apply] をクリックして、変更を適用します。

デフォルト ゲートウェイ

Cisco MDS 9000 ファミリー スイッチで、デフォルト ゲートウェイ IPv4 アドレスを設定できます。

ここで説明する内容は、次のとおりです。

- 「デフォルト ゲートウェイの概要」 (P.5-3)
- 「デフォルト ゲートウェイの設定」 (P.5-4)

デフォルト ゲートウェイの概要

デフォルト ゲートウェイ IPv4 アドレスを設定する場合は、IPv4 スタティック ルーティング属性 (IP デフォルト ネットワーク、送信先プレフィクス、送信先マスク、およびネクスト ホップ アドレス) も使用する必要があります。



ヒント

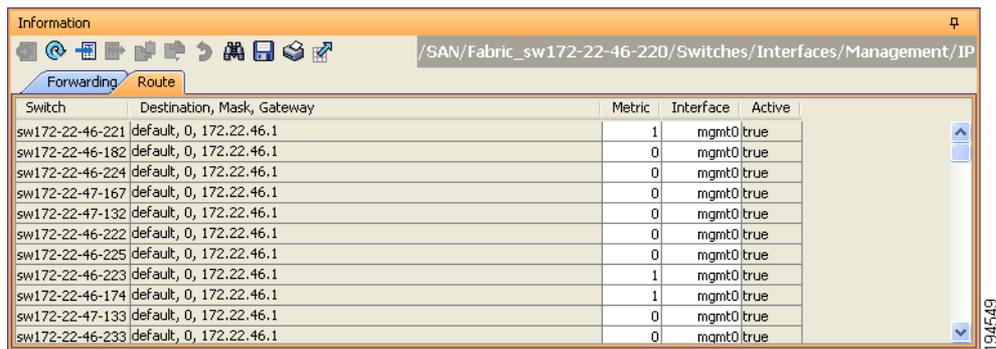
スタティック ルートの IP 転送およびデフォルト ネットワークの詳細を設定する場合は、デフォルト ゲートウェイがイネーブルであるか、またはディセーブルであるかに関係なく、これらの IPv4 アドレスが使用されます。これらの IP アドレスが設定されているにもかかわらず、使用できない場合、スイッチは代わりにデフォルト ゲートウェイ IP アドレスを使用します (デフォルト ゲートウェイ IP アドレスが設定されている場合)。スイッチのすべてのエントリに IP アドレスが設定されていることを確認してください。

デフォルト ゲートウェイの設定

Device Manager を使用して IP ルートを設定する手順は、次のとおりです。

- ステップ 1** [Switches] > [Interfaces] > [Management] を選択して、[Physical Attributes] ペインで [IP] を選択します。
- ステップ 2** [Information] ペインで [Route] タブをクリックします。
- 図 5-2 に示すように、各 IP ルートのスイッチ名、宛先、マスク、ゲートウェイ、メトリック、インターフェイス、およびアクティブ ステータスを示す [IP Route] ウィンドウが表示されます。

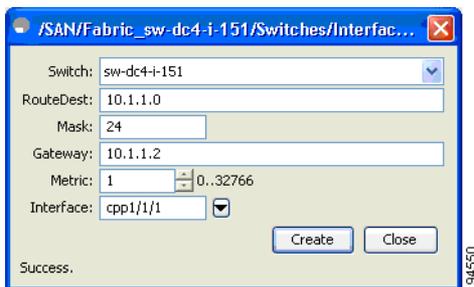
図 5-2 複数のスイッチの IP ルート



Switch	Destination, Mask, Gateway	Metric	Interface	Active
sw172-22-46-221	default, 0, 172.22.46.1	1	mgmt0	true
sw172-22-46-182	default, 0, 172.22.46.1	0	mgmt0	true
sw172-22-46-224	default, 0, 172.22.46.1	0	mgmt0	true
sw172-22-47-167	default, 0, 172.22.46.1	0	mgmt0	true
sw172-22-47-132	default, 0, 172.22.46.1	0	mgmt0	true
sw172-22-46-222	default, 0, 172.22.46.1	0	mgmt0	true
sw172-22-46-225	default, 0, 172.22.46.1	0	mgmt0	true
sw172-22-46-223	default, 0, 172.22.46.1	1	mgmt0	true
sw172-22-46-174	default, 0, 172.22.46.1	1	mgmt0	true
sw172-22-47-133	default, 0, 172.22.46.1	0	mgmt0	true
sw172-22-46-233	default, 0, 172.22.46.1	0	mgmt0	true

- ステップ 3** [Create Row] アイコンをクリックして、新しい IP ルートを追加します。
- 図 5-3 のようなダイアログボックスが表示されます。

図 5-3 [User-Defined Command] ダイアログボックス



Switch: sw-dc4-i-151

RouteDest: 10.1.1.0

Mask: 24

Gateway: 10.1.1.2

Metric: 1 (0..32766)

Interface: cpp1/1/1

Buttons: Create, Close

Success.

- ステップ 4** このウィンドウのフィールドに入力します。
- [Switch] フィールドにスイッチ名を入力します。
 - [Routedest] および [Mask] フィールドに宛先ネットワーク ID およびサブネット マスクを入力し、スタティック ルートを設定します。
 - [Gateway] フィールドにシードスイッチの IP アドレスを入力し、デフォルト ゲートウェイを設定します。
 - [Metric] および [Interface] フィールドを設定します。



(注) Cisco NX-OS リリース 4.2(1) 以降の場合、新しい IP ルートを作成するときに CPP インターフェイスを選択することもできます。

ステップ 5 [Create] アイコンをクリックします。

Device Manager を使用して IP ルートの設定またはデフォルト ゲートウェイの識別を行う手順は、次のとおりです。

ステップ 1 [IP] > [Routes] を選択します。

[IP Routes] ウィンドウが表示されます。

ステップ 2 [Create] をクリックして、スイッチの新しい IP ルートを作成、またはデフォルト ゲートウェイを識別します。

図 5-4 のようなダイアログボックスが表示されます。

図 5-4 [User-Defined Command] ダイアログボックス



ステップ 3 このウィンドウのフィールドに入力します。

- [Switch] フィールドにスイッチ名を入力します。
- [Routedest] および [Mask] フィールドに宛先ネットワーク ID およびサブネット マスクを入力し、スタティック ルートを設定します。
- [Gateway] フィールドにシード スイッチの IP アドレスを入力し、デフォルト ゲートウェイを設定します。
- [Metric] および [Interface] フィールドを設定します。



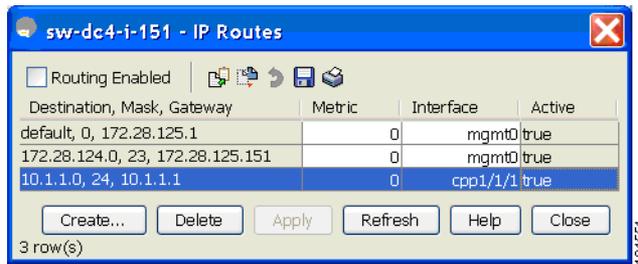
(注) Cisco NX-OS リリース 4.2(1) 以降の場合、新しい IP ルートを作成するときに CPP インターフェイスを選択することもできます。

CPP インターフェイスを選択した場合、スイッチは、入力 CPP により割り当てられる IP アドレスおよびマスクを使用して IP ルート プレフィクスを生成します。

ステップ 4 [Create] をクリックして IP ルートを追加します。

新しい IP ルートが作成されます (図 5-5 を参照してください)。

図 5-5 [IP Routes] ウィンドウ



(注) スイッチにより生成される CPP インターフェイスの IP ルートを削除することはできません。CPP インターフェイスの IP ルートを削除しようとする、SNMP により次に示すエラー メッセージが表示されます。

```
ip: route type not supported.
```

IPv4 デフォルト ネットワークの設定

IPv4 デフォルト ネットワーク アドレスが割り当てられている場合、スイッチはこのネットワークへのルートを最終的なルートと見なします。IPv4 デフォルト ネットワーク アドレスを使用できない場合は、IPv4 デフォルト ゲートウェイ アドレスが使用されます。IPv4 デフォルト ネットワーク アドレスが設定された各ネットワークのルートは、デフォルト ルート候補としてフラグが設定されます (ルートが使用可能な場合)。



ヒント

スタティック ルートの IP 転送およびデフォルト ネットワークの詳細を設定する場合は、デフォルト ゲートウェイがイネーブルであるか、またはディセーブルであるかに関係なく、これらの IPv4 アドレスが使用されます。これらの IPv4 アドレスが設定されているにもかかわらず、使用できない場合、スイッチは代わりにデフォルト ゲートウェイ IPv4 アドレスを使用します (デフォルト ゲートウェイ IP アドレスが設定されている場合)。IPv4 を使用している場合は、必ず、すべてのエントリに IPv4 アドレスを設定してください。

イーサネット インターフェイスが設定されている場合、スイッチは IP ネットワークのゲートウェイ ルータを指していなければなりません。ホストはゲートウェイ スイッチを使用して、ゲートウェイにアクセスします。このゲートウェイ スイッチは、デフォルト ゲートウェイとして設定されます。ゲートウェイ スイッチと同じ VSAN に接続されたファブリック内のこのほかのスイッチも、ゲートウェイ スイッチを通して接続できます。この VSAN に接続されたすべてのインターフェイスに、ゲートウェイ スイッチの VSAN IPv4 アドレスを設定する必要があります (図 5-6 を参照してください)。

図 5-6 オーバーレイ VSAN 機能

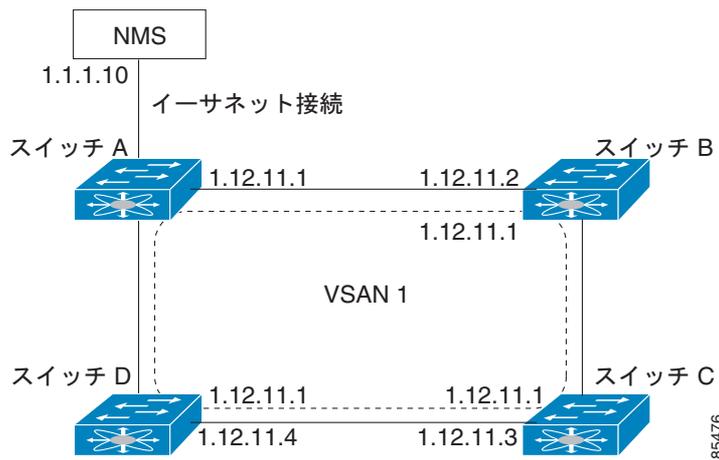


図 5-1 で、スイッチ A の IPv4 アドレスは 1.12.11.1、スイッチ B の IPv4 アドレスは 1.12.11.2、スイッチ C の IPv4 アドレスは 1.12.11.3、スイッチ D の IPv4 アドレスは 1.12.11.4 です。スイッチ A はイーサネット接続されたゲートウェイスイッチです。NMS は IPv4 アドレス 1.1.1.10 を使用して、ゲートウェイスイッチに接続しています。オーバーレイされた VSAN 1 内の任意のスイッチに転送されるフレームは、ゲートウェイスイッチを通してルーティングされます。他のスイッチにゲートウェイスイッチの IPv4 アドレス (1.12.11.1) を設定すると、ゲートウェイスイッチはフレームを目的の送信先に転送できるようになります。同様に、VSAN 内の非ゲートウェイスイッチからイーサネット環境にフレームを転送する場合も、ゲートウェイスイッチを通してフレームがルーティングされます。

転送がディセーブル (デフォルト) である場合、IP フレームはインターフェイス間で送信されません。このような場合、ソフトウェアは帯域内オプション (ファイバチャネルトラフィックの場合) および mgmt0 オプション (イーサネットトラフィックの場合) を使用して、2 つのスイッチ間でローカルに IP ルーティングを実行します。

VSAN 作成時に、VSAN インターフェイスは自動作成されません。インターフェイスは手動で作成する必要があります。

IPFC

IPFC は、ファイバチャネルインターフェイス経由の IP 転送または (ギガビットイーサネット mgmt0 インターフェイスを使用した帯域外でなく) 帯域内スイッチ管理を提供します。IPFC を使用すると、カプセル化を使用してファイバチャネル経由で IP フレームを伝送するように指定できます。IP フレームはファイバチャネルフレームにカプセル化されるため、オーバーレイイーサネットネットワークを使用しなくても、ファイバチャネルネットワーク上で NMS 情報を伝達できます。

VSAN インターフェイスを作成すると、その VSAN の IP アドレスを指定できます。IPv4 アドレスまたは IPv6 アドレスを指定できます。



(注)

Cisco MDS 9000 ファミリースイッチで IPv6 を設定する方法については、第 8 章「ギガビットイーサネットインターフェイスの IP バージョン 6 (IPv6) の設定」を参照してください。

IPFC 設定時の注意事項

IPFC を設定する場合は、次の注意事項に従ってください。

1. 必要な場合、帯域内管理に使用する VSAN を作成します。
2. VSAN インターフェイスの IPv4 アドレスとサブネット マスクを設定します。
3. IPv4 ルーティングをイネーブルにします。
4. 接続を確認します。

IPv4 スタティック ルート

ネットワーク構成で外部ルータが必要でない場合は、MDS スイッチに IPv4 スタティック ルーティングを設定できます。



(注)

IPv6 スタティック ルーティングを設定する手順については、[第 8 章「ギガビット イーサネット インターフェイスの IP バージョン 6 \(IPv6\) の設定」](#)を参照してください。

スタティック ルーティングは、スイッチに IPv4 ルートを設定するメカニズムです。複数のスタティック ルートを設定できます。

VSAN に複数の出力点が存在する場合は、適切なゲートウェイ スイッチにトラフィックが転送されるように、スタティック ルートを設定します。帯域外管理インターフェイスとデフォルト VSAN 間、または直接接続された VSAN 間のゲートウェイ スイッチでは、IPv4 ルーティングはデフォルトでディセーブルです。

オーバーレイ VSAN

ここでは、オーバーレイ VSAN およびオーバーレイ VSAN の設定方法について説明します。

ここで説明する内容は、次のとおりです。

- [「オーバーレイ VSAN の概要」 \(P.5-8\)](#)
- [「オーバーレイ VSAN の設定」 \(P.5-9\)](#)

オーバーレイ VSAN の概要

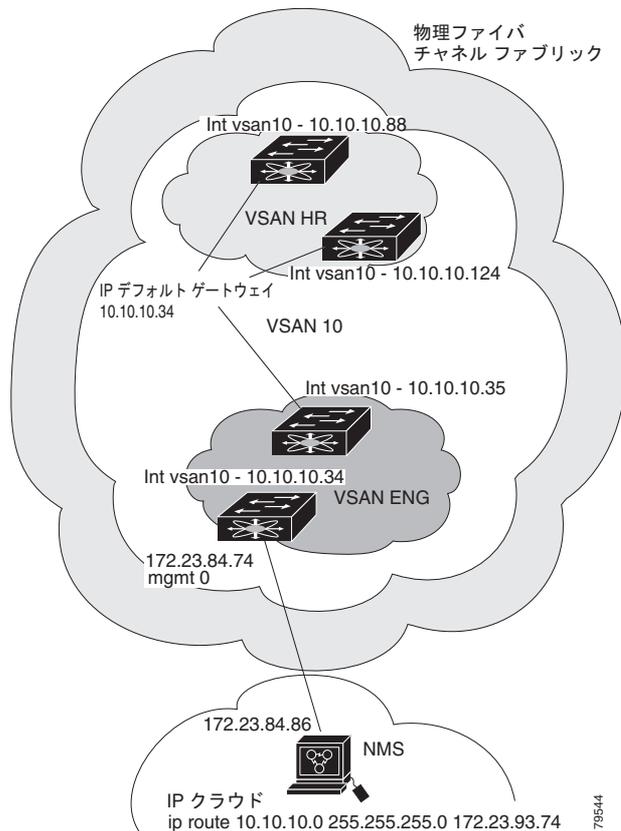
VSAN では、個別のファブリック サービス インスタンスを実行する複数の論理 SAN を 1 つの大規模な物理ネットワーク上でオーバーレイすることにより、より大規模な SAN を構成できます。このようなファブリック サービスの分離によって、ファブリックの再構成やエラー状態が個々の VSAN 内に限定されるため、ネットワークの安定性が向上します。また、物理的に分離された SAN と同じように、各 VSAN を隔離することができます。トラフィックが VSAN 境界を通過したり、デバイスが複数の VSAN に属したりすることはできません。VSAN ごとにファブリック サービスのインスタンスが個別に実行されるため、各 VSAN には独自のゾーン サーバが設定され、VSAN 機能を使用しなくても SAN とまったく同じ方法でゾーンを設定できます。

オーバーレイ VSAN の設定

オーバーレイ VSAN を設定する手順は、次のとおりです。

- ステップ 1** ファブリック内のすべてのスイッチの VSAN データベースに、VSAN を追加します。
- ステップ 2** ファブリック内のすべてのスイッチに VSAN 用の VSAN インターフェイスを作成します。VSAN に属するすべての VSAN インターフェイスに、同じサブネットに属する IP アドレスが設定されます。IP 側に IPFC クラウドへのルートを作成します。
- ステップ 3** ファイバチャネル ファブリック内のスイッチごとに、NMS アクセスを提供するスイッチを指すデフォルト ルートを設定します。
- ステップ 4** NMS を指すスイッチに、デフォルト ゲートウェイ (ルート) と IPv4 アドレスを設定します (図 5-7 を参照してください)。

図 5-7 オーバーレイ VSAN の設定例



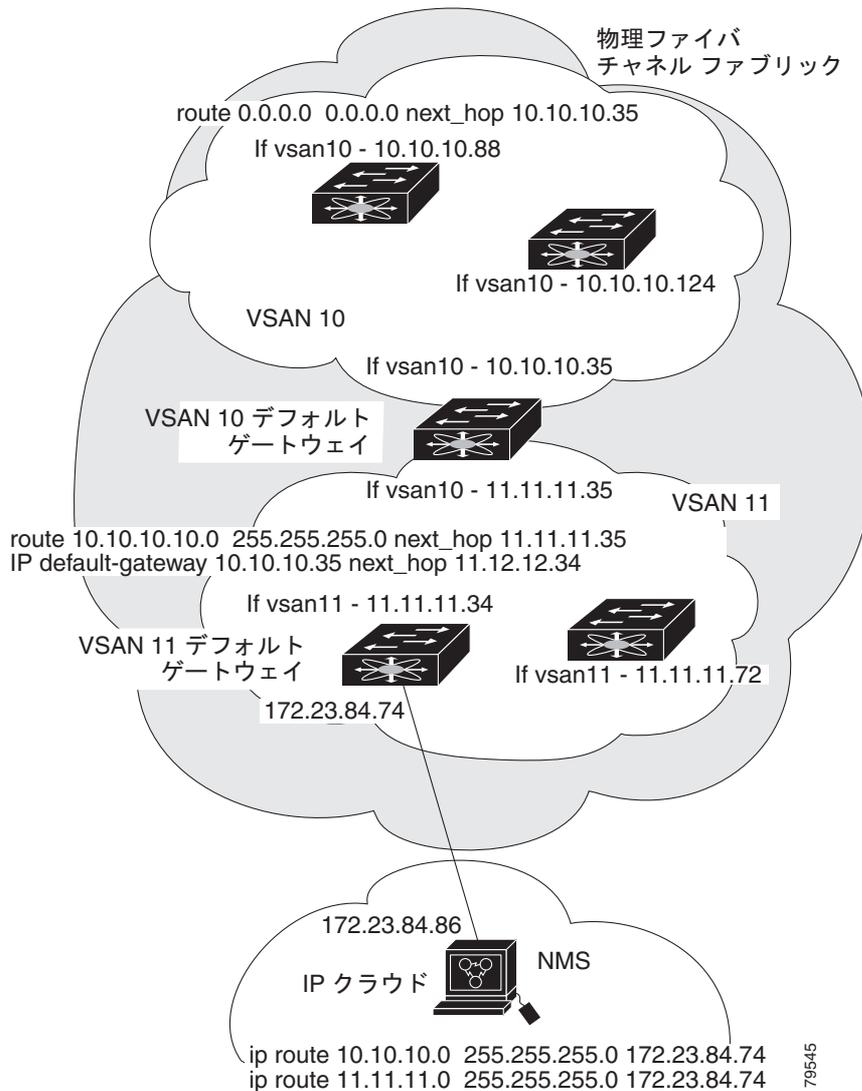
複数の VSAN の設定

複数の VSAN を使用して、管理ネットワークを複数のサブネットに分割することができます。アクティブ インターフェイスは、イネーブにする VSAN インターフェイスのスイッチ上に存在する必要があります。

複数の VSAN を設定する手順は、次のとおりです。

- ステップ 1** ファブリック内の任意のスイッチの VSAN データベースに、VSAN を追加します。
- ステップ 2** ファブリック内の任意のスイッチに、該当する VSAN 用の VSAN インターフェイスを作成します。
- ステップ 3** 対応する VSAN と同じサブネットの各 VSAN インターフェイスに、IP アドレスを割り当てます。
- ステップ 4** ファイバチャネル スイッチおよび IP クラウド上で複数のスタティック ルートを定義します(図 5-8 を参照してください)。

図 5-8 複数の VSAN の設定例



仮想ルータ冗長プロトコル

Cisco MDS 9000 ファミリ スイッチは、仮想ルータ冗長プロトコル (VRRP) 機能の RFC 2338 標準に準拠しています。ここでは、VRRP 機能について詳細に説明します。

ここで説明する内容は、次のとおりです。

- 「VRRP の概要」(P.5-11)
- 「VRRP の設定」(P.5-13)

VRRP の概要

VRRP を使用すると、NMS に接続されているゲートウェイ スイッチへの冗長な代替パスが確立されません。VRRP には次の特性および利点があります。

- VRRP は再起動可能なアプリケーションです。
- VRRP マスターに障害が発生すると、アドバタイズが 3 回行われるまでの間に、VRRP バックアップが処理を引き継ぎます。
- VRRP over Ethernet、VRRP over VSAN、およびファイバ チャネルの機能は、RFC 2338 および draft-ietf-vrrp-ipv6 の定義に従って実装されます。
- Virtual Router (VR; 仮想ルータ) は一意の仮想ルータ IP、仮想ルータ MAC、および VR ID によって、各 VSAN、およびイーサネット インターフェイスにマッピングされます。
- 別の仮想ルータ IP マッピングを使用することにより、VR ID を複数の VSAN で再利用することができます。
- IPv4 および IPv6 の両方がサポートされています。
- 管理インターフェイス (mgmt 0) は仮想ルータ グループを 1 つだけサポートしています。他のすべてのインターフェイスは、IPv4 と IPv6 を合わせて、最大 7 つの仮想ルータ グループをサポートしています。各 VSAN には最大で 255 個の仮想ルータ グループを割り当てることができます。
- VRRP セキュリティには、認証なし、単純なテキスト認証、および MD5 認証の 3 つのオプションがあります。



(注) IPv6 を使用している場合は、インターフェイスに IPv6 アドレスを設定するか、またはインターフェイスで IPv6 をイネーブルにする必要があります。IPv6 の詳細については、[第 8 章「ギガビット イーサネット インターフェイスの IP バージョン 6 \(IPv6\) の設定」](#)を参照してください。

図 5-9 で、スイッチ A は VRRP マスター スイッチ、スイッチ B は VRRP バックアップ スイッチです。両方のスイッチに、IP アドレスと VRRP のマッピングが設定されています。その他のスイッチでは、スイッチ A がデフォルト ゲートウェイとして設定されます。スイッチ A に障害が発生すると、スイッチ B が自動的にマスターになり、ゲートウェイ機能を引き継ぐため、他のスイッチのルーティング設定を変更する必要はありません。

図 5-9 VRRP の機能

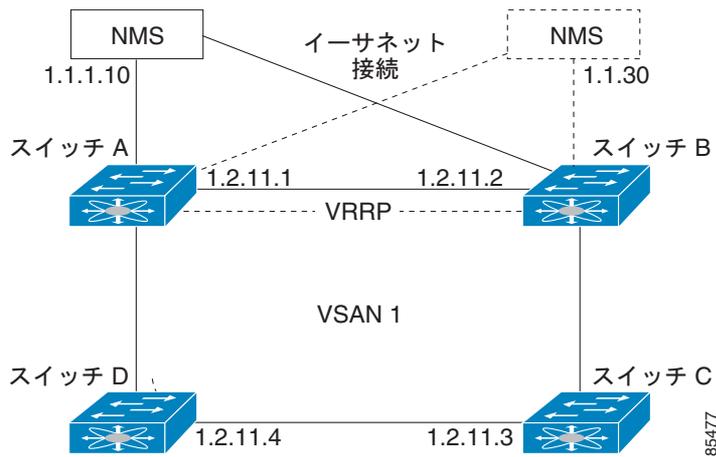
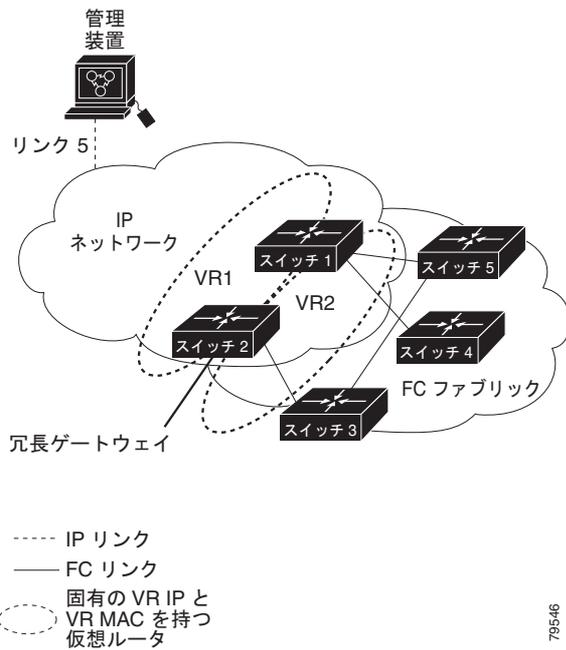


図 5-10 のファブリック例では、複数のインターフェイスタイプにまたがる仮想ルータを設定できないため、2 つの仮想ルータ グループ (VR 1 および VR 2) が存在します。スイッチ 1 とスイッチ 2 の両方で、イーサネット インターフェイスは VR 1 内に、FC インターフェイスは VR 2 内にあります。各仮想ルータは、VSAN インターフェイスおよび VR ID によって一意に識別されます。

図 5-10 冗長ゲートウェイ



VRRP の設定

ここでは VRRP を設定する方法について説明します。ここで説明する内容は、次のとおりです。

- 「仮想ルータの追加および削除」 (P.5-13)
- 「仮想ルータの起動」 (P.5-13)
- 「仮想ルータ IP アドレスの追加」 (P.5-13)
- 「仮想ルータのプライオリティの設定」 (P.5-14)
- 「アドバタイズ パケットのタイム インターバルの設定」 (P.5-14)
- 「プライオリティのプリエンプトの設定またはイネーブル化」 (P.5-14)
- 「仮想ルータの認証の設定」 (P.5-14)
- 「インターフェイスのステート追跡に基づいたプライオリティ」 (P.5-15)

仮想ルータの追加および削除

すべての VRRP の設定は、VRRP が稼動するファブリック内のスイッチ間で複製する必要があります。



(注)

ギガビットイーサネットポートに設定できる VRRP グループの総数は、メイン インターフェイスとサブインターフェイスを合わせて、7 グループまでです。この制限は、IPv4 グループおよび IPv6 グループの両方に適用されます。

仮想ルータの起動

デフォルトで、仮想ルータは常にディセーブルです。VRRP を設定できるのは、この状態がイネーブルの場合だけです。VR をイネーブルにする前に、少なくとも 1 つの IP アドレス (IPv4 または IPv6) を設定してください。

仮想ルータ IP アドレスの追加

仮想ルータには、1 つの仮想ルータ IP アドレスを設定できます。設定された IP アドレスがインターフェイス IP アドレスと同じである場合、このスイッチは自動的に IP アドレスを所有します。IPv4 アドレスまたは IPv6 アドレスのいずれかを設定できます。

VRRP 仕様に従うと、仮想ルータはパケットを転送するネクスト ホップ ルータであるため、マスター VRRP ルータは仮想ルータの IP アドレスへ送信されたパケットを削除します。ただし、MDS スイッチでは、アプリケーションが、仮想ルータの IP アドレスへ送信されたパケットを受け付け、アプリケーションへ配信することを要求する場合があります。仮想ルータ IPv4 アドレスの **secondary** オプションを使用すると、VRRP ルータは、マスターである場合、これらのパケットを受け入れます。

Device Manager で仮想ルータの IP アドレスを管理する場合は、次の手順を実行します。

- ステップ 1** [IP] > [VRRP] を選択します。[VRRP] ダイアログボックスに [Operations] タブが表示されます。
- ステップ 2** [VRRP] ダイアログボックスの [IP Addresses] タブをクリックします。

- ステップ 3** 新しい VRRP エントリを作成するには、[Create] をクリックします。[Create VRRP IP Addresses] ウィンドウが表示されます。
- ステップ 4** このウィンドウのフィールドに入力し、新しい VRRP IP アドレスを作成して、[OK] または [Apply] をクリックします。

仮想ルータのプライオリティの設定

仮想ルータのプライオリティには、1 ~ 254 を割り当てることができます。1 が最低プライオリティ、254 が最高プライオリティです。セカンダリ IP アドレスを持つスイッチのデフォルト値は 100、プライマリ IP アドレスを持つスイッチのデフォルト値は 255 です。

アドバタイズ パケットのタイム インターバルの設定

IPv4 を使用するインターフェイスでは、アドバタイズ パケットのタイム インターバルの有効範囲は、1 ~ 255 秒です。デフォルト値は 1 秒です。スイッチにプライマリ IP アドレスが設定されている場合は、この期間を指定する必要があります。

プライオリティのプリエンプトの設定またはイネーブル化

プライオリティが高いバックアップ仮想ルータが、プライオリティの低いマスター仮想ルータをプリエンプトできるようにします。



(注) 仮想 IP アドレスがインターフェイスの IP アドレスでもある場合、プリエンプトは暗黙的に適用されません。



(注) VRRP のプリエンプトは、IP ストレージのギガビットイーサネット インターフェイスではサポートされません。

仮想ルータの認証の設定

VRRP セキュリティには、単純なテキスト認証、MD5 認証、および認証なしの 3 つのオプションがあります。

- 単純なテキスト認証の場合は、同じ仮想ルータに参加するすべてのスイッチで、1 ~ 8 文字の一意のパスワードを使用します。このパスワードは、他のセキュリティ パスワードと異なるものに設定する必要があります。
- MD5 認証の場合は、同じ仮想ルータに参加するすべてのスイッチで、16 文字の一意の鍵を使用します。この秘密鍵は、同じ仮想ルータ内のすべてのスイッチで共有されます。
- デフォルトのオプションは、認証なしです。

VRRP サブモードで認証オプションを使用して鍵を設定したり、コンフィギュレーション ファイルを使用して鍵を配布したりすることができます。このオプションで割り当てられた Security Parameter Index (SPI; セキュリティ パラメータ インデックス) 設定は、VSAN ごとに一意でなければなりません。



(注) すべての VRRP 設定を複製する必要があります。



(注) VRRP ルータ認証は、IPv6 には適用されません。

インターフェイスのステート追跡に基づいたプライオリティ

インターフェイスのステート追跡機能では、スイッチ内の他のインターフェイスのステートに基づいて、仮想ルータのプライオリティが変更されます。追跡対象のインターフェイスがダウンすると、プライオリティは仮想ルータのプライオリティ値に戻ります（「[仮想ルータのプライオリティの設定](#)」(P.5-14) を参照してください)。追跡対象のインターフェイスが起動すると、仮想ルータのプライオリティはインターフェイスのステート追跡機能の値に戻ります。指定された VSAN インターフェイスまたは管理インターフェイス (mgmt 0) のいずれかのステートを追跡できます。インターフェイスのステート追跡機能は、デフォルトではディセーブルです。



(注) インターフェイス追跡機能を使用するには、インターフェイスでプリエンプトをイネーブルにする必要があります。「[プライオリティのプリエンプトの設定またはイネーブル化](#)」(P.5-14) を参照してください。

DNS サーバの設定

スイッチ上の DNS クライアントは DNS サーバと通信して、IP アドレスとネーム サーバを対応付けます。

DNS サーバは、次のいずれかの場合、2 回試行された後に削除されることがあります。

- IP アドレスまたはスイッチ名が正しく設定されていない
- 外的要因により（制御不可能な理由により）DNS サーバに到達できない



(注) Telnet ホストにアクセスするときに、(何らかの理由により) DNS サーバに到達できない場合、スイッチ ログインプロンプトが表示されるまでの期間が長くなる場合があります。この場合は、DNS サーバが正しく設定されていて、到達可能であるかを確認してください。

デフォルト設定

表 5-1 に、DNS 機能のデフォルト設定を示します。

表 5-1 DNS のデフォルト設定

パラメータ	デフォルト
ドメイン ルックアップ	ディセーブル
ドメイン名	ディセーブル
ドメイン	なし

表 5-1 DNS のデフォルト設定 (続き)

パラメータ	デフォルト
ドメイン サーバ	なし
最大ドメイン サーバ	6

表 5-2 に、VRRP 機能のデフォルト設定を示します。

表 5-2 VRRP のデフォルト設定

パラメータ	デフォルト
仮想ルータ状態	ディセーブル
VSAN 当たりの最大グループ数	255
ギガビットイーサネットポート当たりの最大グループ数	7
プライオリティのプリエンプト	ディセーブル
仮想ルータのプライオリティ	セカンダリ IP アドレスを持つスイッチは 100 プライマリ IP アドレスを持つスイッチは 255
プライオリティ インターフェイス追跡機能	ディセーブル
アドバタイズ インターバル	IPv4 は 1 秒 IPv6 は 100 センチ秒