



CHAPTER 5

IP サービスの設定

この章では、次の事項について説明します。

- 「IP サービスの概要」(P.5-1)
- 「注意事項と制限」(P.5-7)
- 「デフォルト設定」(P.5-8)
- 「IP サービスの設定」(P.5-8)
- 「複数の VSAN の設定」(P.5-11)
- 「VRRP の設定」(P.5-12)
- 「IP サービスのフィールドの説明」(P.5-14)
- 「その他の関連資料」(P.5-25)

IP サービスの概要

Cisco MDS 9000 ファミリー 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 ファミリー スイッチは、Network Management System (NMS; ネットワーク管理システム) に対して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 フレームを伝送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 情報を伝送できます。
- 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 インターフェイスでの IPv6 の設定」を参照してください。

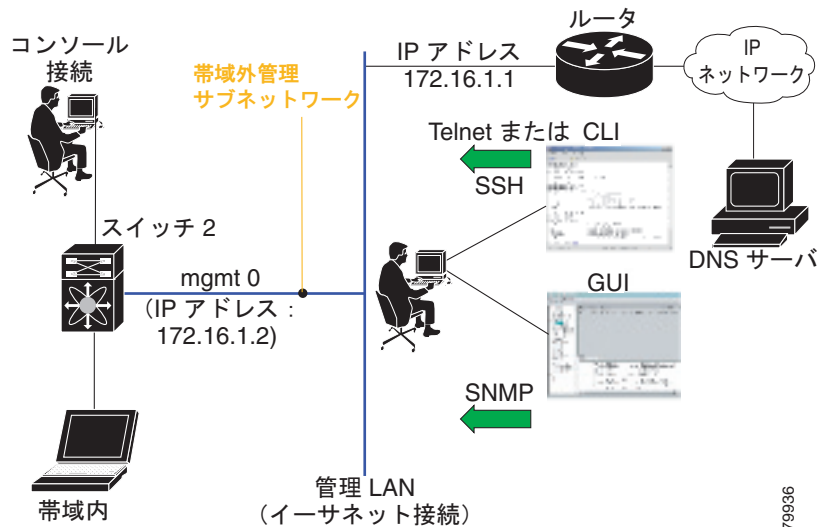
ここでは、次の内容について説明します。

- 「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 ゲートウェイの概要」(P.5-3)
- 「IPv4 デフォルト ネットワークの設定」(P.5-3)
- 「IPFC」(P.5-5)
- 「IPv4 スタティック ルートの概要」(P.5-5)
- 「オーバーレイ VSAN の概要」(P.5-5)
- 「VRRP の概要」(P.5-5)
- 「DNS サーバの設定」(P.5-7)

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)。

図 5-1 スイッチへの管理者アクセス



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は、同時に複数の Telnet または SNMP セッションを許可します。管理インターフェイスを介してスイッチを遠隔から設定できますが、スイッチにアクセスできるようにまず 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 インターフェイスでの 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 管理インターフェイスが接続されているイーサネット スイッチ上のポートは、スイッチ ポートの代わりにホスト ポート (アクセス ポートともいう) として設定する必要があります。(イーサネット スイッチ上の) そのポートのスパニング ツリー設定をディセーブルにする必要があります。これにより、(スパニング ツリー設定がイネーブルであればイーサネット スイッチが実行する) イーサネット スパニング ツリー処理の待ち時間による MDS 管理ポートの起動待ち時間を回避できます。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。

デフォルト ゲートウェイの概要

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。

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。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。

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。

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実際の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 IPv4 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、スイッチのすべてのエントリに IPv4 アドレスを設定するようにしてください。

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別のスイッチも、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 5-2 を参照してください)。

図 5-2 オーバーレイ VSAN 機能

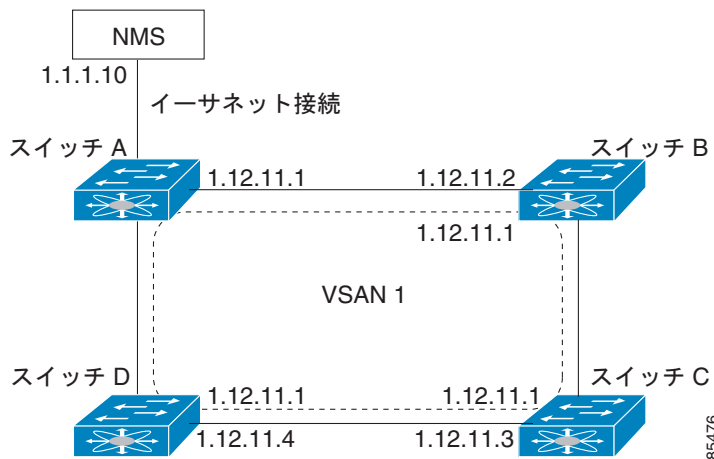


図 5-1 で、スイッチ A の IPv4 アドレスは 1.12.11.1、スイッチ B の IPv4 アドレスは 1.12.11.2、スイッチ C の IPv4 アドレスは 1.12.11.3、スイッチ D の IPv4 アドレスは 1.12.11.4 です。スイッチ A はイーサネット接続されたゲートウェイ スイッチです。NMS は IPv4 アドレス 1.1.1.10 を使用して、ゲートウェイ スイッチに接続しています。オーバーレイされた VSAN 1 内の任意のスイッチに転送されるフレームは、ゲートウェイ スイッチを通してルーティングされます。他のスイッチにゲートウェイ スイッチの IPv4 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、(ギガビット イーサネット `mgmt 0` インターフェイスを使用した帯域外でなく) ファイバ チャネル インターフェイス経由の帯域内スイッチ管理での IP 転送を提供します。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 フレームを送信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 インターフェイスでの IPv6 の設定」を参照してください。

IPv4 スタティック ルートの概要

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。

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 インターフェイスでの IPv6 の設定」を参照してください。

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、ファブリックの再設定やエラー状態が個々の VSAN 内に限定されるので、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 を隔離できます。トラフィックは VSAN 境界を通過できず、デバイスは複数の VSAN に属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 機能を持たない SAN とまったく同じ方法でゾーンを設定できます。

VRRP の概要

Cisco MDS 9000 ファミリー 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 標準に準拠しています。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す。VRRP には次の機能があります。

- 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 の仕様に従って実装されます。
- 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 をあわせて、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 インターフェイスでの IPv6 の設定」](#)を参照してください。

図 5-3 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 5-3 VRRP の機能

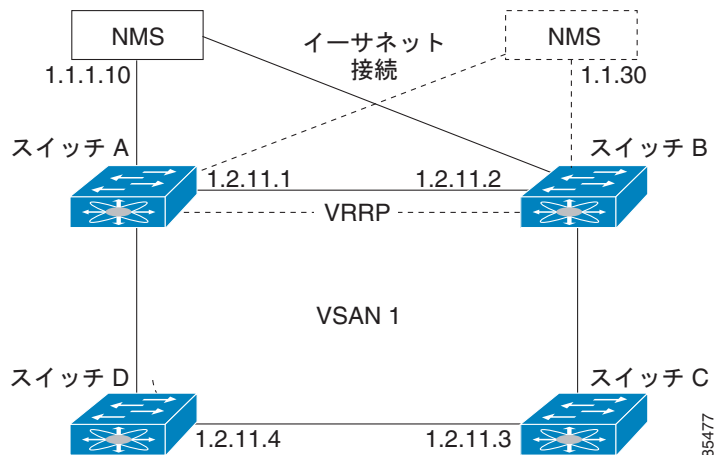
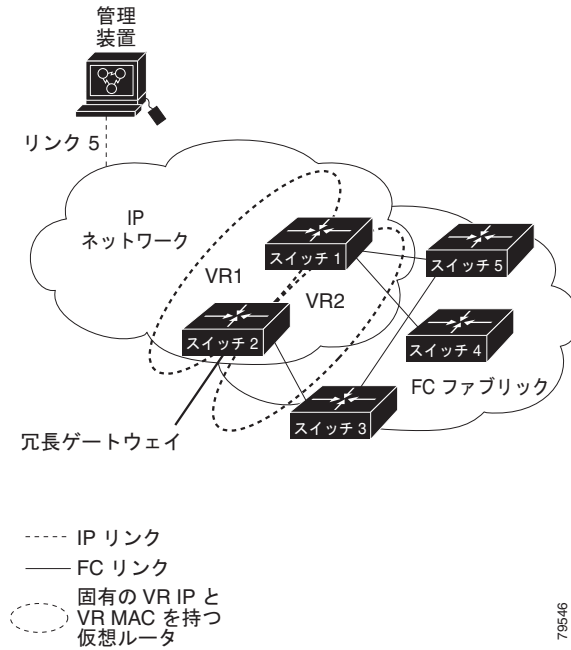


図 5-4 のファブリック例では、複数のインターフェイス タイプにまたがる仮想ルータを設定できないため、2 つの仮想ルータ グループ (VR 1 および VR 2) が存在します。スイッチ 1 とスイッチ 2 の両方で、イーサネット インターフェイスは VR 1 内に、FC インターフェイスは VR 2 内にあります。各仮想ルータは、VSAN インターフェイスおよび VR ID によって一意に識別されます。

図 5-4 冗長ゲートウェイ



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、次のいずれかの理由で、2 回試行されたあと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場合
- 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場合



(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ことがあります。この場合は、DNS サーバが正しく設定されていて、到達可能であることを確認してください。

注意事項と制限

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。

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 のデフォルト設定値

パラメータ	デフォルト
ドメイン参照	ディセーブル
ドメイン名	ディセーブル
ドメイン	なし
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 のデフォルト設定値

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
アダプタイズ インターバル	IPv4 は 1 秒 IPv6 は 100 センチ秒

IP サービスの設定

ここでは、次の内容について説明します。

- 「[管理インターフェイスの設定](#)」(P.5-8)
- 「[デフォルト ゲートウェイの設定](#)」(P.5-9)
- 「[オーバーレイ VSAN の設定](#)」(P.5-10)

管理インターフェイスの設定

手順の詳細

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] の順に選択します。
 - 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 ゲートウェイの設定

手順の詳細

IP ルートを設定するには、次の手順に従ってください。

-
- 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。
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。
 - 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。
 - 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、スイッチ上で新しい IP ルートの作成またはデフォルト ゲートウェイの識別を行います。
 - 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 プレフィックスを生成します。

ステップ 4 [Create] をクリックして、IP ルートを追加します。



(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.
```

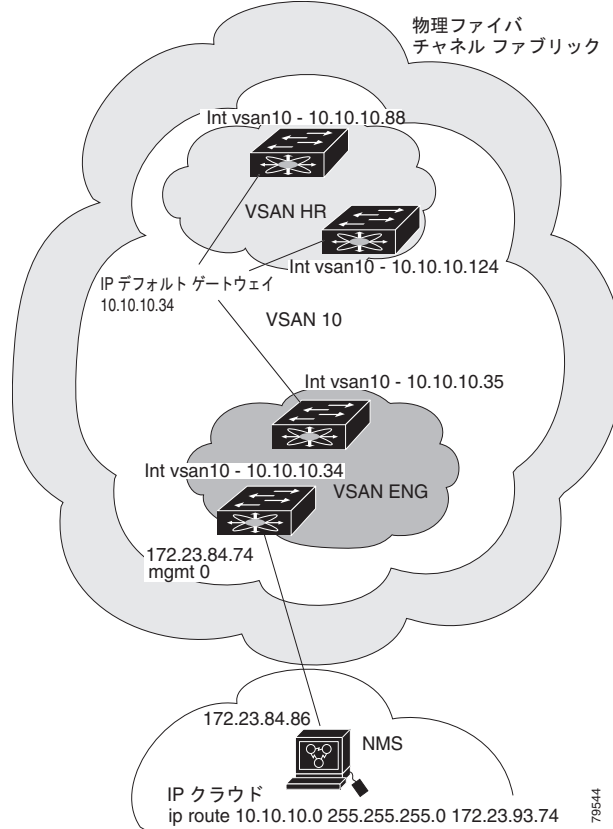
オーバーレイ VSAN の設定

手順の詳細

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 5-5 を参照)。

図 5-5 オーバーレイ VSAN の設定例



(注) 図 5-5 に示す管理インターフェイスを設定するには、イーサネット ネットワークの IPv4 アドレスへのデフォルトゲートウェイを設定します。

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できます。アクティブ インターフェイスは、イネーブルにする 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。

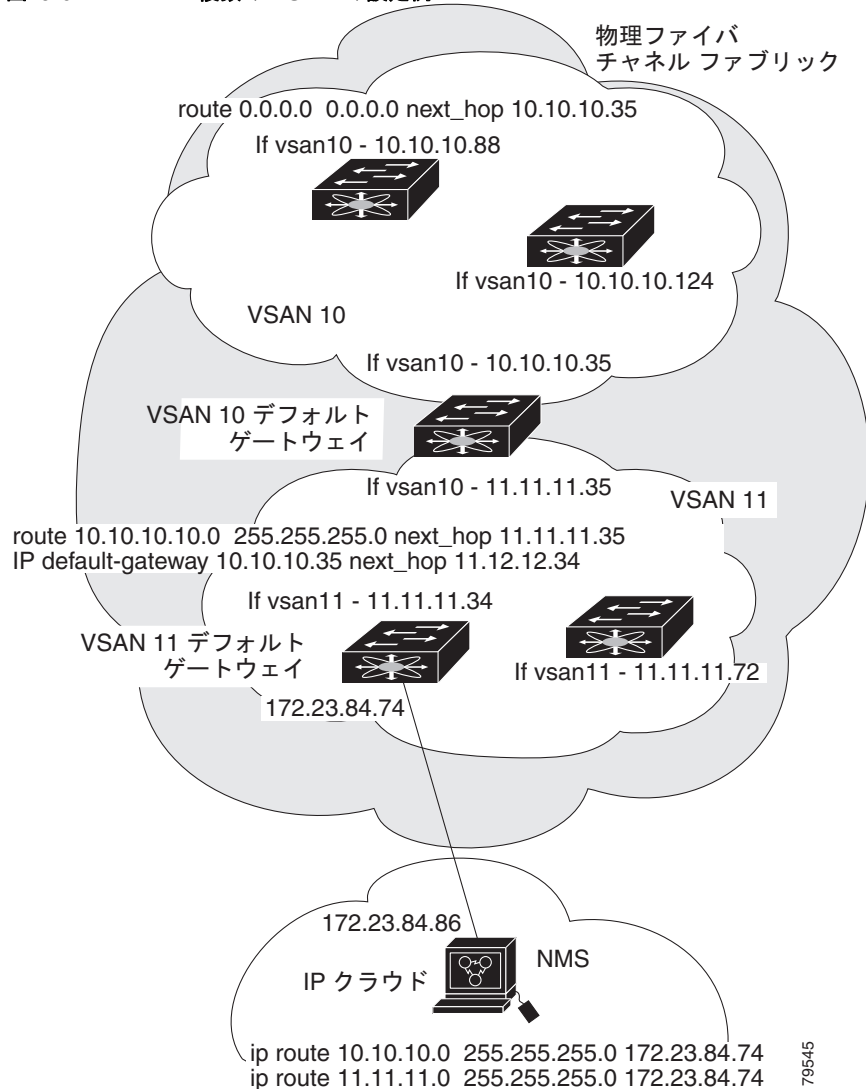
手順の詳細

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 チャンネル 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 5-6 を参照)。

図 5-6 複数の VSAN の設定例



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。内容は次のとおりです。

- ・「仮想ルータ IP アドレスの追加」(P.5-13)
- ・「仮想ルータ認証の設定」(P.5-13)
- ・「インターフェイス プライオリティの追跡」(P.5-14)

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その 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 アドレスにアドレス指定されたパケットを廃棄します。ただし MDS スイッチでは、一部のアプリケーションにおいて、仮想ルータの IP アドレスにアドレス指定されたパケットを受け付け、アプリケーションに配信することが必要となります。仮想ルータ IPv4 アドレスに対して **secondary** オプションを使用することによって、VRRP ルータは、マスターの場合、これらのパケットを受け入れます。

手順の詳細

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 エントリを作成し、[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て新しい VRRP IP Address を作成し、[OK] または [Apply] をクリックします。
-

仮想ルータ認証の設定

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 文字の一意のキーを使用します。この秘密キーは、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キーを設定し、コンフィギュレーション ファイルを使用してキーを配信できます。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 プライオリティの追跡

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（「[仮想ルータ認証の設定](#)」(P.5-13) を参照してください)。追跡対象インターフェイスがアップすると、仮想ルータのプライオリティはインターフェイス ステートを追跡する値に戻ります。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 ステート トラッキングを動作させるには、インターフェイス上でプリエンプトをイネーブルにする必要があります。

IP サービスのフィールドの説明

ここでは、各フィールドについて説明します。

IP Routes

フィールド	説明
Routing Enabled	このチェックボックスをオンにすると、スイッチが IP ルータとして機能します。
Destination, Mask, Gateway	このルートのネクスト ホップに到達するために経由するローカル インターフェイスを識別する値。
Metric	このルートのプライマリ ルーティング メトリック。
Interface	このルートのネクスト ホップに到達するために経由するローカル インターフェイス。
Active	ルートがアクティブかどうかを示します。

IP Statistics ICMP

フィールド	説明
InParmProbs	受信した ICMP パラメータ問題メッセージの数。
OutParmProbs	送信した ICMP パラメータ問題メッセージの数。
InSrcQuenches	受信した ICMP ソース クエンチ メッセージの数。
InRedirects	受信した ICMP リダイレクト メッセージの数。
InEchos	受信した ICMP エコー (要求) メッセージの数。
InEchoReps	受信した ICMP エコー応答メッセージの数。
InTimestamps	受信した ICMP タイムスタンプ (要求) メッセージの数。
InTimestampReps	受信した ICMP タイムスタンプ応答メッセージの数。

フィールド	説明
InAddrMasks	受信した ICMP アドレス マスク要求メッセージの数。
InAddrMaskReps	受信した ICMP アドレス マスク応答メッセージの数。
InDestUnreachs	受信した ICMP 宛先到達不能メッセージの数。
InTimeExcds	受信した ICMP 時間超過メッセージの数。
OutSrcQuenchs	送信した ICMP ソース クエンチ メッセージの数。
OutRedirects	送信した ICMP リダイレクト メッセージの数。ホストはリダイレクトを送信しないため、ホストではこの値が常に N/A となります。
OutEchos	送信した ICMP エコー (要求) メッセージの数。
OutEchoReps	送信した ICMP エコー応答メッセージの数。
OutTimestamps	送信した ICMP タイムスタンプ (要求) メッセージの数。
OutTimestampReps	送信した ICMP タイムスタンプ応答メッセージの数。
OutAddrMasks	送信した ICMP アドレス マスク要求メッセージの数。
OutAddrMaskReps	送信した ICMP アドレス マスク応答メッセージの数。
OutDestUnreachs	送信した ICMP 宛先到達不能メッセージの数。
OutTimeExcds	送信した ICMP 時間超過メッセージの数。

IP Statistics IP

フィールド	説明
InHdrErrors	チェックサムの誤り、バージョン番号の不一致、その他のフォーマットエラー、存続可能時間の超過、IP オプションの処理中に発見されたエラーなど、IP ヘッダーにエラーがあるため廃棄された入力データグラムの数。
InAddrErrors	IP ヘッダーの宛先フィールドにある IP アドレスが、このエンティティで受信する有効なアドレスではないために廃棄された入力データグラムの数。エンティティが IP ゲートウェイではなく、データグラムを転送しない場合、このカウンタには宛先アドレスがローカルアドレスではないために廃棄されたデータグラムが含まれます。
InUnknownProtos	正常に受信されたが、不明または未サポートのプロトコルであるために廃棄されたローカル アドレス宛データグラムの数。
InDiscards	継続した処理を阻止するような問題は発生していないが、(バッファ領域の不足などが原因で) 廃棄された入力 IP データグラムの数。このカウンタには、再構成の待機中に廃棄されたデータグラムは含まれません。
OutDiscards	宛先への転送を阻止するような問題は発生していないが、(バッファ領域の不足などが原因で) 廃棄された出力 IP データグラムの数。このカウンタには、ipForwDatagrams でカウントされたデータグラムの中で、この (任意の) 廃棄基準と一致するすべてのフレームが含まれます。

フィールド	説明
OutNoRoutes	宛先に転送するためのルートが見つからないために廃棄された IP データグラムの数。このカウンタには、ipForwDatagrams でカウントされたフレームの中で、このルートなし基準と一致するものすべてが含まれます。これには、すべてのデフォルトルートがダウンしているためにホストがルーティングできなかったすべてのデータグラムが含まれます。
FragFails	このエンティティでフラグメント化する必要があるが、Don't Fragment フラグが設定されているなどの理由でフラグメント化できず、廃棄された IP データグラムの数。
ReasmFails	IP 再構成アルゴリズムで検出された障害（タイムアウト、エラーなど）の数。一部のアルゴリズム（特に RFC 815 のアルゴリズム）では、受信ごとにフラグメントを結合し、フラグメントの数を追跡しきれないため、これは廃棄された IP フラグメントの数とは限りません。
InReceives	受信エラーがあったものも含めて、インターフェイスから受信した入力データグラムの合計数。
InDelivers	IP ユーザ プロトコルに正常に配信された入力データグラムの合計数（ICMP を含む）。
OutRequests	転送要求の中でローカル IP ユーザ プロトコル（ICMP を含む）が IP に指定された、IP データグラムの合計数。このカウンタには、ipForwDatagrams でカウントされたデータグラムは含まれません。
ForwDatagrams	このエンティティが最終 IP 宛先ではなく、最終宛先に転送するためのルートの検出が試行された、入力データグラムの数。IP ルータとして機能しないエンティティでは、このエンティティによってソースルーティングされ、ソースルート オプションが正常に処理されたフレームだけがこのカウンタに含まれます。
FragOKs	このエンティティで正常にフラグメント化された IP データグラムの数。
FragCreates	このエンティティでのフラグメント化によって生成された IP データグラム フラグメントの数。
ReasmReqds	このエンティティで再構成する必要のある、受信した IP フラグメントの数。
ReasmOKs	正常に再構成された IP データグラムの数。

IP Statistics SNMP

フィールド	説明
BadVersions	SNMP エンティティに配信されたが、サポートされていない SNMP バージョンだった SNMP メッセージの合計数。
BadCommunityNames	認識されない SNMP コミュニティ名を使用している SNMP エンティティに配信された SNMP メッセージの合計数。
BadCommunityUses	SNMP エンティティに配信され、メッセージで指定された SNMP コミュニティで許可されていない SNMP 処理を表す SNMP メッセージの合計数。

フィールド	説明
ASNParseErrs	受信した SNMP メッセージをデコードするときに、SNMP エンティティで発生した ASN.1 エラーまたは BER エラーの合計数。
TooBigs	SNMP プロトコル エンティティに配信され、エラー状態フィールドの値が tooBig だった SNMP PDU の合計数。
SilentDrops	SNMP エンティティに配信され、空の変数バインド フィールドを持つ代替 Response-PDU を含んだ応答のサイズが、ローカル制限または要求の発信元に関連する最大メッセージ サイズよりも大きかったため自動的にドロップされた、GetRequest-PDU、GetNextRequest-PDU、GetBulkRequest-PDU、SetRequest-PDU、および InformRequest-PDU の合計数。
ProxyDrops	SNMP エンティティに配信され、プロキシ ターゲットへの（変換された）メッセージ送信が、Response-PDU を返さないなどの方法（タイムアウト以外）で失敗したため自動的にドロップされた、GetRequest-PDU、GetNextRequest-PDU、GetBulkRequest-PDU、SetRequest-PDU、および InformRequest-PDU の合計数。
NoSuchNames	SNMP プロトコル エンティティに配信され、エラー状態フィールドの値が noSuchName だった SNMP PDU の合計数。
BadValues	SNMP プロトコル エンティティに配信され、エラー状態フィールドの値が badValue だった SNMP PDU の合計数。
ReadOnlyls	SNMP プロトコル エンティティに配信され、エラー状態フィールドの値が readOnly だった有効な SNMP PDU の合計数。エラー状態フィールドに値 readOnly を含んだ SNMP PDU の生成は、誤った実装の SNMP を検出する手段として用意されたものであるため、これが生成されるのはプロトコル エラーです。
GenErrs	SNMP プロトコル エンティティに配信され、エラー状態フィールドの値が genErr だった SNMP PDU の合計数。
Pkts	転送サービスから SNMP エンティティに配信されたメッセージの合計数。
GetRequests	SNMP プロトコル エンティティによって受け入れられ、処理された SNMP Get-Request PDU の合計数。
GetNexts	SNMP プロトコル エンティティによって受け入れられ、処理された SNMP Get-Next PDU の合計数。
SetRequests	SNMP プロトコル エンティティによって受け入れられ、処理された SNMP Set-Request PDU の合計数。
OutTraps	SNMP プロトコル エンティティで生成された SNMP Trap PDU の合計数。
OutGetResponses	SNMP プロトコル エンティティで生成された SNMP Get-Response PDU の合計数。
OutPkts	SNMP プロトコル エンティティから転送サービスに渡された SNMP メッセージの合計数。
TotalReqVars	有効な SNMP Get-Request と Get-Next PDU を受信した結果として、SNMP プロトコル エンティティによって正常に取得された MIB オブジェクトの合計数。
TotalSetVars	有効な SNMP Set-Request PDU を受信した結果として、SNMP プロトコル エンティティによって正常に変更された MIB オブジェクトの合計数。

IP Statistics UDP

フィールド	説明
InErrors	宛先ポートでアプリケーションが待ち受けていないこと以外の理由で配信できなかった、受信した UDP データグラムの数。
InDatagrams	UDP ユーザに配信された UDP データグラムの合計数。
OutDatagrams	このエンティティから送信された UDP データグラムの合計数。
NoPorts	宛先ポートでアプリケーションが待ち受けていなかった、受信した UDP データグラムの合計数。

mgmt0 Statistics

フィールド	説明
InErrors	インターフェイスで受信したエラーの合計数。
OutErrors	インターフェイスで送信したエラーの合計数。
InDiscards	インターフェイスで受信した廃棄の合計数。
OutDiscards	インターフェイスで送信した廃棄の合計数。
RxBytes	受信した合計バイト数。
TxBytes	送信した合計バイト数。
RxFrames	受信したフレームの合計数。
TxFrames	送信したフレームの合計数。

TCP UDP TCP

フィールド	説明
State	この TCP 接続の状態。

TCP UDP UDP

フィールド	説明
Port	この UDP リスナーのローカル ポート番号。

VRRP General

フィールド	説明
IP Address Type, Vrid, Interface	IP アドレスのタイプ (IPv4、IPv6、または DNS)、仮想ルータ ID、およびインターフェイス。
Admin	仮想ルータの管理状態 (active または notInService)。
Oper	仮想ルータの現在の状態。定義済みの値は次の 3 つです。 <ul style="list-style-type: none"> initialize : すべての仮想ルータがスタートアップ イベントを待っていることを示しています。 backup : 仮想ルータがマスター ルータのアベイラビリティを監視していることを示しています。 master : 仮想ルータが、このルータに関連付けられた IP アドレスにフレームを転送していることを示しています。
Priority	仮想ルータのマスター選択プロセスに使用されるプライオリティを指定します。値が大きいほどプライオリティが高くなります。マスタールータからプライオリティ 0 が送信された場合は、このルータが VRRP への参加を終了し、バックアップ仮想ルータが新しいマスターに移行する必要があることを示しています。プライオリティ 255 は、関連する IP アドレスを所有するルータに使用されます。
AdvInterval	アドバタイズメント メッセージの送信間隔 (秒数)。VRRP アドバタイズメントを送信するのはマスター ルータだけです。
PreemptMode	プライオリティの高い仮想ルータが、プライオリティの低いマスターと入れ替わるかどうかを制御します。
UpTime	この仮想ルータが、いつ初期化済み状態から変化するか。
Version	この VRRP インスタンスが実行している VRRP のバージョン。
AcceptMode	マスター状態の仮想ルータが IPv6 アドレスを所有していない場合に、アドレス所有者のその IPv6 アドレス宛ての packets をそのまま受け付けるかどうかを制御します。True の場合、マスター状態の仮想ルータは受け付けます。False の場合、マスター状態の仮想ルータは受け付けません。

VRRP IP Addresses

フィールド	説明
Interface, VRRP ID, IP Address	インターフェイス、仮想ルータの冗長プロトコル ID、および関連する IP アドレス。

VRRP Statistics

フィールド	説明
IP Address Type, VrId, Interface	IP アドレスのタイプ (IPv4、IPv6、または DNS)、仮想ルータ ID、およびインターフェイス。
LastAdvRx	この仮想ルータが受信した VRRP アドバタイズメントの合計数。
Protocol Traffic MasterIpAddr	マスター ルータの実際の (プライマリ) IP アドレス。この仮想ルータが前回受信した VRRP アドバタイズメントに送信元としてリストされた IP アドレスです。
Protocol Traffic BecomeMaster	仮想ルータの状態が MASTER に遷移した合計回数。
Priority 0 Rx	仮想ルータが受信した、プライオリティ 0 の VRRP フレームの合計数。
Priority 0Tx	仮想ルータが送信した、プライオリティ 0 の VRRP フレームの合計数。
AuthErrors InvalidType	不明な認証タイプで受信したフレームの合計数。
Other Errors dvIntervalErrors	ローカル仮想ルータに設定されたアドバタイズメント間隔とは異なる間隔で受信した VRRP アドバタイズメント フレームの合計数。
Other Errors IpTtlErrors	仮想ルータが受信した、IP TTL (存続可能時間) が 255 以外の VRRP フレームの合計数。
Other Errors InvalidTypePktsRcvd	仮想ルータが受信した、タイプ フィールドが無効な値の VRRP フレームの合計数。
Other Errors AddressListErrors	アドレス リストが仮想ルータにローカルで設定したリストと一致しない、受信したフレームの合計数。
OtherErrors PacketLengthErrs	フレーム長が VRRP ヘッダーよりも短い、受信したフレームの合計数。
RefreshRate	リフレッシュの時間間隔。

CDP General

フィールド	説明
Enable	Cisco Discovery Protocol が実行されているかどうか。CDP がディセーブルになると CacheTable のエントリが削除されます。
MessageInterval	CDP メッセージが生成される間隔。デフォルト値は 60 秒です。
HoldTime	受信デバイスが CDP メッセージを保持している時間。デフォルト値は 180 秒です。
LastChange	キャッシュ テーブルが最後に変更されたのはいつか。

CDP Neighbors

フィールド	説明
Switch	このエンティティのインターネットアドレス。
Local Interface	このリンクが関連する FCIP デバイスのインターフェイスを識別する一意の値。
DeviceName	リモート デバイスの名前。規定では、デバイスの完全修飾ドメイン名です。
DeviceID	最新の CDP メッセージでレポートされたデバイス ID 文字列。
DevicePlatform	最新の CDP メッセージでレポートされたバージョン文字列。
Interface	最新の CDP メッセージでレポートされたポート ID 文字列。
IPAddress	最近受信した CDP メッセージのアドレス TLV でレポートされた、デバイスの SNMP エージェントの（最初の）ネットワーク層アドレス。
NativeVLAN	最新の CDP メッセージでレポートされた、リモート デバイスのインターフェイスのネイティブ VLAN。値 0 は、最新の CDP メッセージでネイティブ VLAN フィールド (TLV) がレポートされなかったことを示します。
PrimaryMgmtAddr	最近受信した CDP メッセージでレポートされた、デバイスが SNMP メッセージを受け付ける（最初の）ネットワーク層アドレスを示します。
SecondaryMgmtAddr	最近受信した CDP メッセージでレポートされた、デバイスが SNMP メッセージを受け付ける代替ネットワーク層アドレスを示します。

iSNS Profiles

フィールド	説明
Addr	iSNS サーバのアドレス。
Port	iSNS サーバの TCP ポート。

iSNS Servers

フィールド	説明
Name	iSNS サーバの名前。
TcpPort	iSNS メッセージで使用される TCP ポート。このサーバで TCP がサポートされていない場合、値は 0 になります。
Uptime	サーバがアクティブ状態を続けている時間。
ESI Non Response Threshold	エンティティが iSNS データベースから登録解除される前に送信され、応答を受信しない ESI メッセージの数。
# Entities	サーバの iSNS に登録されたエンティティの数。
# Portals	サーバの iSNS に登録されたポータルの数。

フィールド	説明
# Portal Groups	サーバの iSNS に登録されたポータル グループの数。
# iSCSI Devices	サーバの iSNS に登録された iSCSI ノードの数。

iSNS Entities

フィールド	説明
Entity ID	エンティティの iSNS エンティティ識別子。
Last Accessed	エンティティが最後にアクセスされた時刻。

iSNS クラウド検出

フィールド	説明
AutoDiscovery	自動クラウド検出をオンするかどうか。
DiscoveryDelay	連続した IP クラウド検出を実行する継続時間。
Discovery	実行する IP ネットワーク検出コマンド。 <ul style="list-style-type: none"> all : ファブリック内のすべてのギガビット イーサネット インターフェイスに対して IP ネットワーク検出を実行します。 noOp (デフォルト) : 何も実行しません。
CommandStatus	ライセンスのインストール/アンインストール/更新動作の状態。 <ul style="list-style-type: none"> success : 検出動作が正常に完了した。 nProgress : 検出動作が進行中。 none : 検出動作が実行されていない。 NoIpNetworkNameSpecified : IP クラウド名が指定されていない。 invalidNetworkName : IP クラウドが設定されていない。 NoIPSPortNameSpecified : インデックスが指定されていない場合はギガビット イーサネット ポート。 invalidIPSPortName : 無効なギガビット イーサネット ポート インターフェイス。 generalISNSFailure : 一般的な iSNS サーバ障害。

iSNS Clouds

フィールド	説明
Id	IP クラウドの ID。
Switch WWN	このテーブル内のスイッチの WWN。

iSNS Cloud Interfaces

フィールド	説明
Name, Switch WWN, Interface, Address	クラウドの名前、スイッチの WWN、インターフェイス、およびアドレス。

Monitor Dialog Controls

フィールド	説明
Line Chart	データを折れ線グラフで表した新しいウィンドウを開きます。
Area Chart	データを面グラフで表した新しいウィンドウを開きます。
Bar Chart	データを棒グラフで表した新しいウィンドウを開きます。
Pie Chart	データを円グラフで表した新しいウィンドウを開きます。
Reset Cumulative Counters	[Column Data] の表示モードが [Cumulative] に設定されている場合に、カウンタを 0 にリセットします。
Export to File	標準の [Save] ダイアログボックスを表示します。データは .TXT ファイルで保存されます。
Print	標準の [Print] ダイアログボックスを表示します。
Update Frequency	監視ダイアログ内でデータを更新する間隔。
Column Data	監視ダイアログに表示されるデータのタイプを指定します。 <ul style="list-style-type: none"> • Absolute Value : スイッチを起動してからの合計量を表示します。これがエラー モニタリングのデフォルトです。 • Cumulative : ダイアログを表示してからの合計量を表示します。[Reset Cumulative Counters] ボタンをクリックしてカウンタをリセットすると、累積データの新しいセットを収集できます。 • Minimum/sec : リフレッシュ間隔ごとの 1 秒間の最小値を表示します。 • Maximum/sec : リフレッシュ間隔ごとの 1 秒間の最大値を表示します。 • Last Value/sec : リフレッシュ間隔ごとの 1 秒間の最新の値を表示します。これがトラフィック モニタリングのデフォルト設定です。
Elapsed	ダイアログが表示されてからの経過時間。[Reset Cumulative Counters] ボタンをクリックしてこのカウンタをリセットすると、累積データの新しいセットを収集できます。

iSNS Details iSCSI Nodes

フィールド	説明
Name	ストレージ ノードに関連付けられた発信側またはターゲットの iSCSI 名。
Type	この iSCSI ノードの機能を定義する Node Type ビットマップ。31 はターゲット、30 は発信側、29 は制御で、その他はすべて予約されています。
Alias	iSCSI ノードのエイリアス名。
ScnBitmap	ノードの State Change Notification (SCN) ビットマップ。
WWN Token	オプションのグローバルに固有な 64 ビット整数値。ファイバ チャネル ファブリック内での iSCSI デバイスのノードの WWN を表すために使用できます。
AuthMethod	この iSCSI ノードで有効な iSCSI 認証方法。

iSNS Details Portals

フィールド	説明
Addr	このポータルインターネット アドレス。
TcpPort	このポータルのポート番号。
SymName	このポータルのオプションのシンボリック名。
EsiInterval	このポータルの Entity Status Inquiry (ESI) 間隔。
TCP ESI	ESI モニタリングに使用される TCP ポート番号。
TCP Scn	iSNS サーバからの SCN メッセージの受信に使用される TCP ポート番号。
SecurityInfo	ポータル セキュリティ ビットマップ属性に登録されたポータルのセキュリティ属性設定。

その他の関連資料

IPS の実装に関する追加情報については、次を参照してください。

- 「関連資料」 (P.5-25)
- 「標準」 (P.5-25)
- 「RFC」 (P.5-25)
- 「MIB」 (P.5-25)

関連資料

関連項目	参照先
『Cisco MDS 9000 Family Command Reference』	『Cisco MDS 9000 Family Command Reference, Release 5.0(1a)』

標準

標準	タイトル
この機能によってサポートされる新しい標準または変更された標準はありません。またこの機能による既存標準のサポートに変更はありません。	—

RFC

RFC	タイトル
この機能によってサポートされる新しい RFC または変更された RFC はありません。また既存 RFC のサポートに変更はありません。	—

MIB

MIB	MIB リンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。また既存 MIB のサポートに変更はありません。	MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 http://www.cisco.com/dc-os/mibs

