CHAPTER 44

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、ネットワーク管理システム（NMS）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。

スイッチは仮想ルータ冗長プロトコル（VRRP）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。

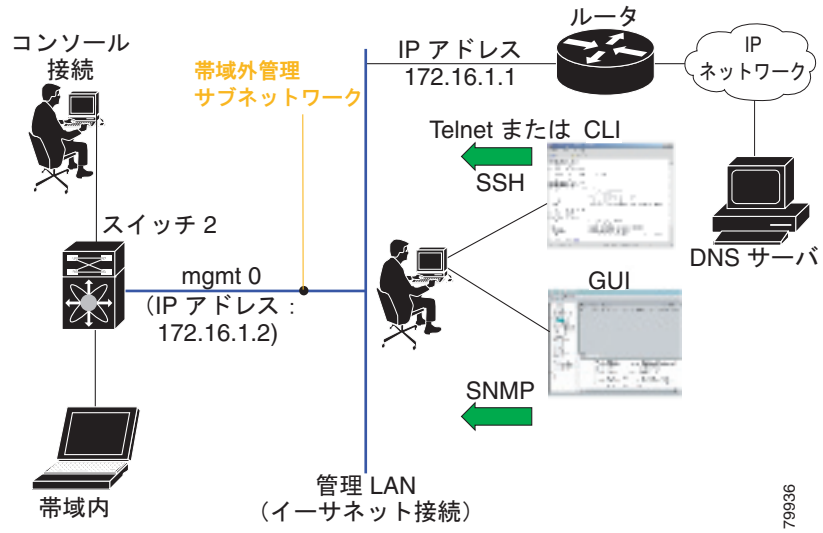
（注） IPv6 の設定については、第 47 章「ギガビット イーサネット インターフェイスでの IPv6 の設定」を参照してください。

この章は、次の項で構成されています。

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。FC インターフェイス上で IP プロトコルが稼働する 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 44-1 を参照）。

図 44-1　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ッ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 47 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。シスコ製イーサネット スイッチの場合は、IOS の **switchport host** コマンドまたは Catalyst OS の **set port host** を使用します。イーサネット スイッチのコンフィギュレーション 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。

IPv4 の mgmt0 イーサネット インターフェイスを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config terminal` `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# interface mgmt0` `switch(config-if)#`	管理イーサネット インターフェイス（mgmt0）のインターフェイス コンフィギュレーション モードを開始します。
ステップ 3	`switch(config-if)# ip address 10.1.1.1 255.255.255.0`	管理インターフェイスの IPv4 アドレス（10.1.1.1）および IPv4 サブネット マスク（255.255.255.0）を入力します。
ステップ 4	`switch(config-if)# no shutdown`	インターフェイスをイネーブルにします。

IPv6 の mgmt0 イーサネット インターフェイスを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config terminal` `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# interface mgmt0` `switch(config-if)#`	管理イーサネット インターフェイス（mgmt0）のインターフェイス コンフィギュレーション モードを開始します。
ステップ 3	`switch(config-if)# ipv6 address 2001:0db8:800:200c::417a/64`	管理インターフェイスの IPv6 アドレス（2001:0DB8:800:200C::417A）および IPv6 プレフィックス長（/64）を入力し、インターフェイスの IPv6 処理をイネーブルにします。
	`switch(config-if)# ipv6 enable`	インターフェイスのリンク ローカル IPv6 アドレスを自動的に設定し、インターフェイスの IPv6 処理をイネーブルにします。
ステップ 4	`switch(config-if)# no shutdown`	インターフェイスをイネーブルにします。

デフォルト ゲートウェイ

Cisco MDS 9000 ファミリ 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。

この項では、次のトピックについて取り上げます。

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 コマンド（IP デフォルト ネットワーク、送信先プレフィックス、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。

スイッチのすべてのエントリでの IP アドレスの設定については、「初回のセットアップ ルーチン」（P.5-2）を参照してください。

スイッチのデフォルト ゲートウェイの IP アドレスを設定するには **ip default-gateway** コマンドを使用し、デフォルト ゲートウェイの IPv4 アドレスが設定されていることを確認するには **show ip route** コマンドを使用します。

デフォルト ゲートウェイの設定

デフォルト ゲートウェイを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t` `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# ip default-gateway 1.12.11.1`	デフォルト ゲートウェイの IPv4 アドレスを設定します。

デフォルト ゲートウェイの設定の確認

デフォルト ゲートウェイの設定を確認するには、**show ip route** コマンドを使用します。

```
switch# show ip route

Codes: C - connected, S - static

Gateway of last resort is 1.12.11.1

S 5.5.5.0/24 via 1.1.1.1, GigabitEthernet1/1
C 1.12.11.0/24 is directly connected, mgmt0
C 1.1.1.0/24 is directly connected, GigabitEthernet1/1
C 3.3.3.0/24 is directly connected, GigabitEthernet1/6
C 3.3.3.0/24 is directly connected, GigabitEthernet1/5
S 3.3.3.0/24 via 1.1.1.1, GigabitEthernet1/1
```

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 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。

スイッチのすべてのエントリでの IP アドレスの設定については、「初回のセットアップ ルーチン」（P.5-2）を参照してください。

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 44-2 を参照）。

図 44-2　オーバーレイ VSAN 機能

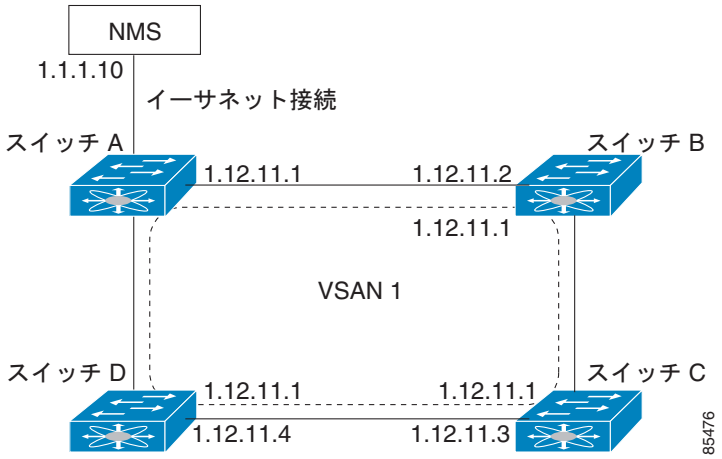


図 44-2 で、スイッチ A の IPv4 アドレスは 1.12.11.1、スイッチ B の IPv4 アドレスは 1.12.11.2、スイッチ C の IPv4 アドレスは 1.12.11.3、スイッチ D の IPv4 アドレスは 1.12.11.4 です。スイッチ A はイーサネット接続されたゲートウェイ スイッチです。NMS は IPv4 アドレス 1.1.1.10 を使用して、ゲートウェイ スイッチに接続しています。オーバーレイされた VSAN 1 内の任意のスイッチに転送されるフレームは、ゲートウェイ スイッチを通してルーティングされます。他のスイッチにゲートウェイ スイッチの IPv4 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（「VSAN インターフェイス」（P.13-40）を参照）。

IPv4 アドレスを使用してデフォルト ネットワークを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# ip default-network 190.10.1.0`	デフォルト ネットワークの IPv4 アドレス（190.10.1.0）を設定します。
	`switch(config)# ip route 10.0.0.0 255.0.0.0 131.108.3.4` `switch(config)# ip default-network 10.0.0.0`	ネットワーク 10.0.0.0 へのスタティック ルートをスタティック デフォルト ルートとして定義します。

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 IP 転送または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 スイッチで IPv6 を設定する方法については、第 47 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。

このトピックには、次の事項が含まれます。

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。

VSAN の IPv4 アドレスの設定

VSAN インターフェイスを作成し、そのインターフェイスの IPv4 アドレスを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# interface vsan 10` `switch(config-if)#`	指定された VSAN（10）のインターフェイスを設定します。
ステップ 3	`switch(config-if)# ip address 10.0.0.12 255.255.255.0`	選択したインターフェイスの IPv4 アドレスおよびネットマスクを設定します。
ステップ 4	`switch(config-if)# no shutdown`	インターフェイスをイネーブルにします。

VSAN インターフェイスの設定の確認

VSAN インターフェイスの設定を確認するには、**show interface vsan** コマンドを使用します。

（注）　前に VSAN インターフェイスを設定した場合のみ、このコマンドの出力を表示できます。

```
switch# show interface vsan 1
vsan1 is down (Administratively down)
    WWPN is 10:00:00:0c:85:90:3e:85, FCID not assigned
    Internet address is 10.0.0.12/24
    MTU 1500 bytes, BW 1000000 Kbit
    0 packets input, 0 bytes, 0 errors, 0 multicast
    0 packets output, 0 bytes, 0 errors, 0 dropped
```

IPv4 ルーティングのイネーブル化

デフォルトでは、IPv4 ルーティング機能はすべてのスイッチでディセーブルです。

IPv4 ルーティング機能をイネーブルにするには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# ip routing`	IPv4 ルーティングをイネーブルにします（デフォルトではディセーブル）。
ステップ 3	`switch(config)# no ip routing`	IPv4 ルーティングをディセーブルにし、工場出荷時の設定に戻します。

IPv4 ルーティング設定の確認

IPv4 ルーティング設定を確認するには、**show ip routing** コマンドを使用します。

```
switch(config)# show ip routing
ip routing is enabled
```

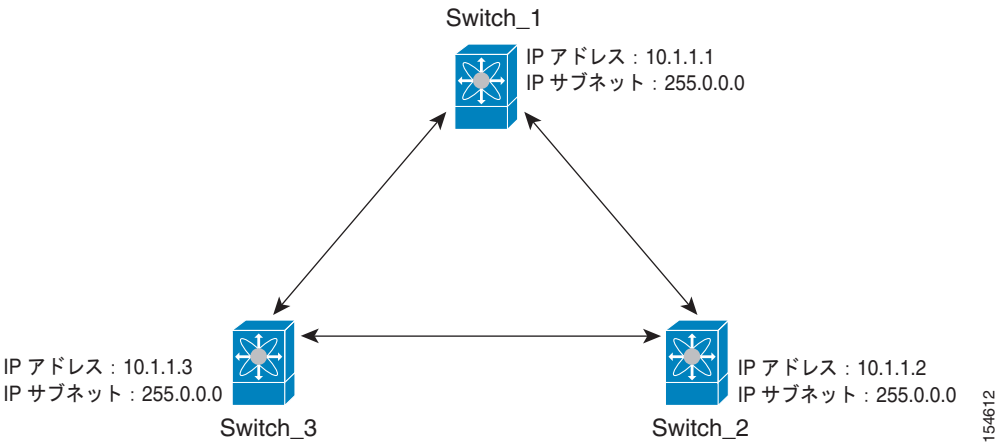
IPFC の設定例

ここでは、IPFC の設定例について説明します。図 44-3 にネットワーク例を示します。

ネットワーク例に次のリンクがあります。

- Switch_1 は、mgmt 0 インターフェイスによってメイン ネットワークに接続され、ISL によってファブリックに接続されています。
- Switch_2 および Switch_3 は、ISL によってファブリックに接続されていますが、メイン ネットワークに接続されていません。

図 44-3　IPFC のネットワーク例



次に、図 44-3 のネットワーク例の Switch_1 を設定する方法を示します。

ステップ 1　VSAN インターフェイスを作成し、インターフェイス コンフィギュレーション サブモードを開始します。

```
switch_1# config t
switch_1(config)# interface vsan 1
switch_1(config-if)#
```

ステップ 2　IP アドレスおよびサブネット マスクを設定します。

```
switch_1(config-if)# ip address 10.1.1.1 255.0.0.0
```

ステップ 3　VSAN インターフェイスをイネーブルにし、インターフェイス コンフィギュレーション サブモードを終了します。

```
switch_1(config-if)# no shutdown
switch_1(config-if)# exit
switch_1(config)#
```

ステップ 4　IPv4 ルーティングをイネーブルにします。

```
switch_1(config)# ip routing
switch_1(config)# exit
switch_1#
```

ステップ 5　ルートを表示します。

```
switch_1# show ip route

Codes: C - connected, S - static

C 172.16.1.0/23 is directly connect, mgmt0
C 10.0.0.0./8 is directly connected, vsan1
```

次に、図 44-3 のネットワーク例の Switch_2 を設定する方法を示します。

ステップ 1　mgmt 0 インターフェイスをイネーブルにします。

（注）　コンソール接続を使用してこのスイッチを設定します。

```
switch_2# config t
switch_2(config)# interface mgmt 0
switch_2(config-if)# no shutdown
switch_2(config-if)# exit
switch_2(config)#
```

ステップ 2　VSAN インターフェイスを作成し、インターフェイス コンフィギュレーション サブモードを開始します。

```
switch_2# config t
switch_2(config)# interface vsan 1
switch_2(config-if)#
```

ステップ 3　IP アドレスおよびサブネット マスクを設定します。

```
switch_2(config-if)# ip address 10.1.1.2 255.0.0.0
```

ステップ 4　VSAN インターフェイスをイネーブルにし、インターフェイス コンフィギュレーション サブモードを終了します。

```
switch_2(config-if)# no shutdown
switch_2(config-if)# exit
switch_2(config)#
```

ステップ 5　IPv4 ルーティングをイネーブルにします。

```
switch_2(config)# ip routing
switch_2(config)# exit
switch_2#
```

ステップ 6　ルートを表示します。

```
switch_2# show ip route

Codes: C - connected, S - static

C 10.0.0.0./8 is directly connected, vsan1
```

ステップ 7　Switch_1 への接続を確認します。

```
switch_2# ping 10.1.1.1
PING 10.1.1.1 (10.1.1.1) 56(84) bytes of data.
64 bytes from 10.1.1.1: icmp_seq=1 ttl=64 time=0.618 ms
64 bytes from 10.1.1.1: icmp_seq=2 ttl=64 time=0.528 ms
64 bytes from 10.1.1.1: icmp_seq=3 ttl=64 time=0.567 ms

--- 10.1.1.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 4998 ms
rtt min/avg/max/mdev = 0.528/0.570/0.618/0.057 ms
```

次に、図 44-3 のネットワーク例の Switch_3 を設定する方法を示します。

ステップ 1　mgmt 0 インターフェイスをイネーブルにします。

（注）　コンソール接続を使用してこのスイッチを設定します。

```
switch_3# config t
switch_3(config)# interface mgmt 0
switch_3(config-if)# no shutdown
switch_3(config-if)# exit
switch_3(config)#

switch_3# config t
switch_3(config)# interface vsan 1
switch_3(config-if)#
```

ステップ 2　IP アドレスおよびサブネット マスクを設定します。

```
switch_3(config-if)# ip address 10.1.1.3 255.0.0.0
```

ステップ 3　VSAN インターフェイスをイネーブルにし、インターフェイス コンフィギュレーション サブモードを終了します。

```
switch_3(config-if)# no shutdown
switch_3(config-if)# exit
switch_3(config)#
```

ステップ 4　IPv4 ルーティングをイネーブルにします。

```
switch_3(config)# ip routing
switch_3(config)# exit
switch_3#
```

ステップ 5　ルートを表示します。

```
switch_3# show ip route

Codes: C - connected, S - static

C 10.0.0.0./8 is directly connected, vsan1
```

ステップ 6　Switch_1 への接続を確認します。

```
switch_3# ping 10.1.1.1
PING 10.1.1.1 (10.1.1.1) 56(84) bytes of data.
64 bytes from 10.1.1.1: icmp_seq=1 ttl=64 time=1.19 ms
64 bytes from 10.1.1.1: icmp_seq=2 ttl=64 time=0.510 ms
64 bytes from 10.1.1.1: icmp_seq=3 ttl=64 time=0.653 ms
```

```
--- 10.1.1.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2008 ms
rtt min/avg/max/mdev = 0.510/0.787/1.199/0.297 ms
```

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、「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」（P.47-1）を参照してください。

この項では、次のトピックについて取り上げます。

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。

IPv4 スタティック ルートの設定

IPv4 スタティック ルートを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t`	コンフィギュレーション モードに入ります。

ステップ 2	`switch(config)# ip route <network IP address> <netmask> <next hop IPv4 address> distance <number> interface <vsan number>`
	
	For example:
	`switch(config)# ip route 10.0.0.0 255.0.0.0 20.20.20.10 distance 10 interface vsan 1`
	`switch(config)#`
		指定した IPv4 アドレス、サブネット マスク、ネクスト ホップ、ディスタンス、およびインターフェイスについてスタティック ルートを設定します。

IPv4 スタティック ルート情報の確認

IPv4 スタティック ルートの設定を確認するには、**show ip route** コマンドを使用します。

```
switch# show ip route configured
Destination          Gateway             Mask Metric        Interface

         default      172.22.95.1          0.0.0.0      0            mgmt0
        10.1.1.0          0.0.0.0    255.255.255.0      0            vsan1
     172.22.95.0          0.0.0.0    255.255.255.0      0            mgmt0
```

アクティブで接続されている IPv4 スタティック ルートを確認するには、**show ip route** コマンドを使用します。

```
switch# show ip route

Codes: C - connected, S - static

Default gateway is 172.22.95.1

C 172.22.95.0/24 is directly connected, mgmt0
C 10.1.1.0/24 is directly connected, vsan1
```

例 44-1　　IP ルーティング状態の表示

```
switch# show ip routing
ip routing is disabled
```

ARP の表示とクリア

Cisco MDS 9000 ファミリ スイッチのアドレス解決プロトコル（ARP）エントリを表示、削除、またはクリアできます。ARP 機能はすべてのスイッチでイネーブルです。

- ARP テーブルを表示するには、**show arp** コマンドを使用します。

  ```
  switch# show arp
  Protocol Address           Age (min)  Hardware Addr  Type  Interface
  Internet  171.1.1.1               0  0006.5bec.699c  ARPA  mgmt0
  Internet  172.2.0.1               4  0000.0c07.ac01  ARPA  mgmt0
  ```

- ARP テーブルから ARP エントリを削除するには、コンフィギュレーション モードで **no arp** コマンドを使用します。

  ```
  switch(config)# no arp 172.2.0.1
  ```

- ARP テーブルからすべてのエントリを削除するには、**clear arp** コマンドを使用します。ARP テーブルは、デフォルトでは空です。

  ```
  switch# clear arp-cache
  ```

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。

この項では、次のトピックについて取り上げます。

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。

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。

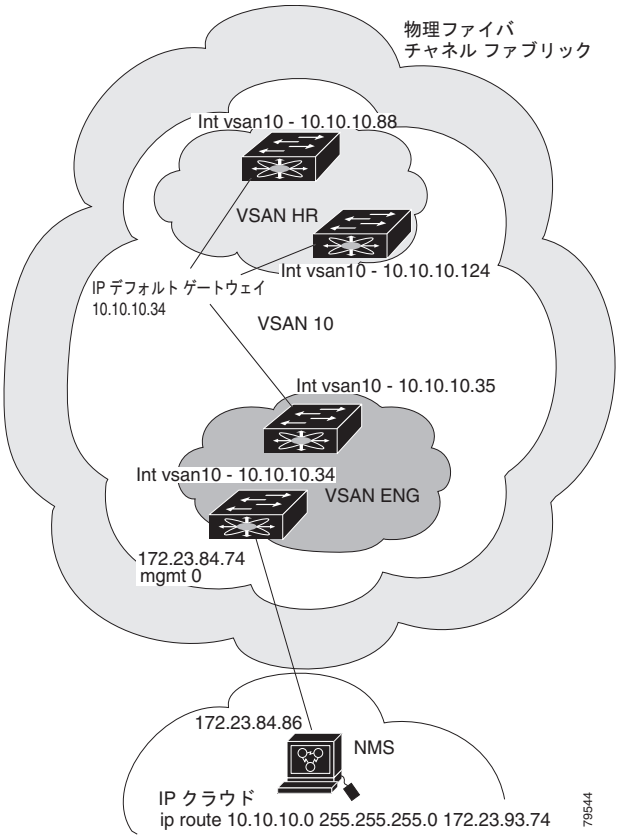
ステップ 1　ファブリック内のすべてのスイッチの VSAN データベースに、VSAN を追加します。

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 44-4 を参照）。

図 44-4　オーバーレイ VSAN の設定例



（注）　図 44-4 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。

次の手順では、1 台のスイッチにオーバーレイ VSAN を設定します。この手順をファブリックのスイッチごとに繰り返す必要があります。

1 台のスイッチにオーバーレイ VSAN を設定するには（図 44-4 の例を使用）、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# vsan database` `switch-config-vsan-db#`	VSAN データベースを設定します。
ステップ 3	`switch--config-vsan-db# vsan 10 name MGMT_VSAN`	ファイバ チャネル ファブリックのすべてのスイッチの VSAN データベースに VSAN を定義します。
ステップ 4	`switch--config-vsan-db# exit` `switch(config)#`	VSAN データベース モードを終了します。
ステップ 5	`switch(config)# interface vsan 10` `switch(config-if)#`	VSAN インターフェイス（VSAN 10）を作成します。

	コマンド	目的
ステップ 6	`switch(config-if)# ip address 10.10.10.0 netmask 255.255.255.0`	このスイッチに IPv4 アドレスとサブネット マスクを割り当てます。
ステップ 7	`switch(config-if)# no shutdown`	設定されたインターフェイスをイネーブルにします。
ステップ 8	`switch(config-if)# end` `switch#`	EXEC モードに戻ります。
ステップ 9	`switch# exit`	スイッチを終了し、NMS に戻ります。この例では、NMS は、ファイバ チャネル ファブリックにアクセスできるエッジのイーサネット管理インターフェイスと同じサブネット上にあると見なされます。

図 44-4 に示す NMS ステーションを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	`nms# route ADD 10.10.10.0 MASK 255.255.255.0 172.22.93.74`	ファイバ チャネル ファブリックにアクセスできるエッジ スイッチの管理インターフェイスを指す NMS のスタティック ルートを定義します。

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している必要があります。

複数の VSAN を設定する手順は、次のとおりです。

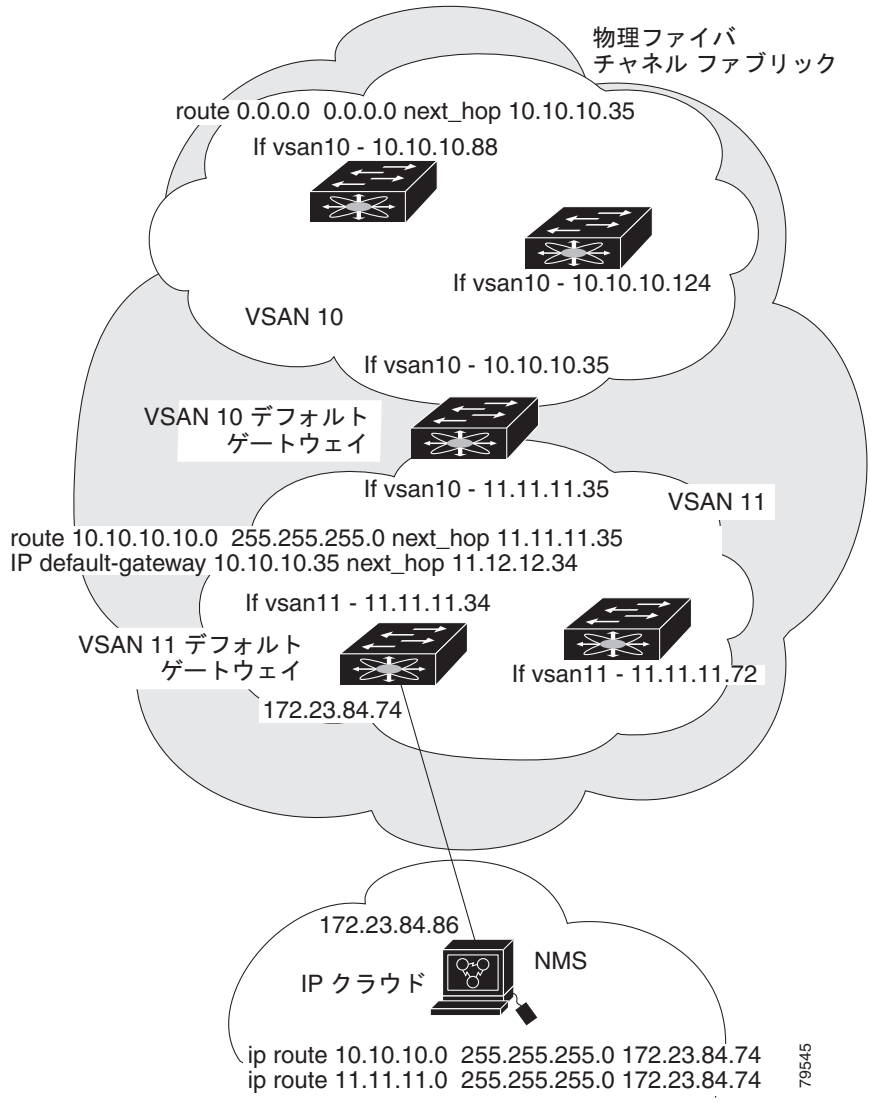
ステップ 1　ファブリック内の任意のスイッチの VSAN データベースに、VSAN を追加します。

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 44-5 を参照）。

図 44-5　複数の VSAN の設定例



オーバーレイ VSAN を設定するには（図 44-5 の例を使用）、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# vsan database` `switch-config-vsan-db#`	VSAN データベースを設定します。
ステップ 3	`switch-config-vsan-db# vsan 10 name MGMT_VSAN_10` `switch-config-vsan-db#`	VSAN 10 のすべてのスイッチの VSAN データベースに VSAN を定義します。
ステップ 4	`switch-config-vsan-db# exit` `switch(config)#`	VSAN データベース コンフィギュレーション サブモードを終了します。
ステップ 5	`switch-config-vsan-db# vsan 11 name MGMT_VSAN_11` `switch-config-vsan-db#`	VSAN 11 のすべてのスイッチの VSAN データベースに VSAN を定義します。

	コマンド	目的
ステップ 6	`switch-config-vsan-db# exit` `switch(config)#`	VSAN データベース コンフィギュレーション サブモードを終了します。
ステップ 7	`switch(config)# interface vsan 10` `switch(config-if)#`	VSAN 10 のインターフェイス コンフィギュレーション サブモードを開始します。
ステップ 8	`switch(config-if)# ip address 10.10.10.0 netmask 255.255.255.0` `switch(config-if)#`	このインターフェイスの IPv4 アドレスおよびサブネット マスクを割り当てます。
ステップ 9	`switch(config-if)# no shutdown`	VSAN 10 の設定済みインターフェイスをイネーブルにします。
ステップ 10	`switch(config-if)# exit` `switch(config)#`	VSAN 10 インターフェイス モードを終了します。
ステップ 11	`switch(config)# interface vsan 11` `switch(config-if)#`	VSAN 11 のインターフェイス コンフィギュレーション サブモードを開始します。
ステップ 12	`switch(config-if)# ip address 11.11.11.0 netmask 255.255.255.0` `switch(config-if)#`	このインターフェイスの IPv4 アドレスおよびサブネット マスクを割り当てます。
ステップ 13	`switch(config-if)# no shutdown`	VSAN 11 の設定済みインターフェイスをイネーブルにします。
ステップ 14	`switch(config-if)# end` `switch#`	EXEC モードに戻ります。
ステップ 15	`switch# exit`	スイッチを終了し、NMS に戻ります。この例では、NMS は、ファイバ チャネル ファブリックにアクセスできるエッジのイーサネット管理インターフェイスと同じサブネット上にあると見なされます。
ステップ 16	`NMS# route ADD 10.10.10.0 MASK 255.255.255.0 172.22.93.74`	IPv4 クラウドにアクセスできるエッジ スイッチの管理インターフェイスを指す NMS のスタティック ルートを定義します。
ステップ 17	`NMS# route ADD 11.11.11.0 MASK 255.255.255.0 172.22.93.74`	ファイバ チャネル ファブリックにアクセスできるエッジ スイッチの管理インターフェイスを指す NMS の VSAN 11 のスタティック ルートを定義します。
ステップ 18	`switch# route 10.10.10.0 255.255.255.0 next_hop 11.11.11.35`	サブネット 11 からサブネット 10 に到達するルートを定義します。

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。

この項では、次のトピックについて取り上げます。

- 「VRRP の概要」（P.44-18）
- 「VRRP の設定」（P.44-19）

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す。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（VRRP）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 47 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 44-6 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 44-6　VRRP の機能

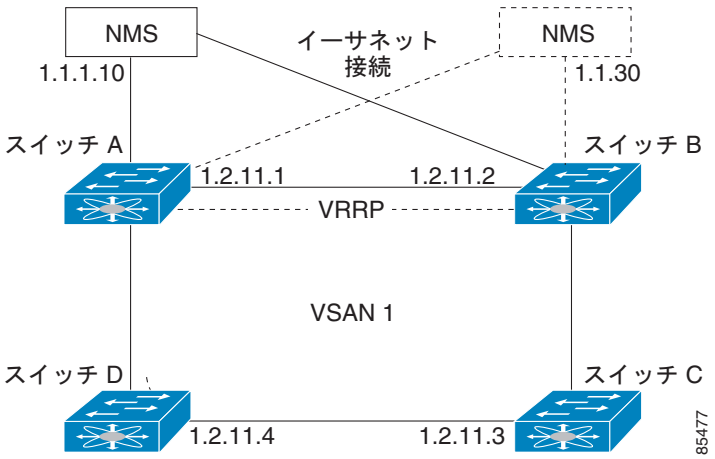
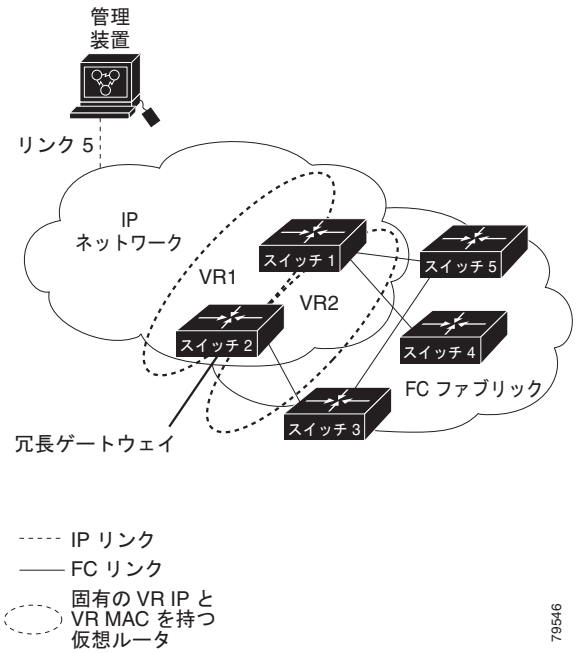


図 44-7 のファブリック例では、複数のインターフェイス タイプにまたがる仮想ルータを設定できないため、2 つの仮想ルータ グループ（VR 1 および VR 2）が存在します。スイッチ 1 とスイッチ 2 の両方で、イーサネット インターフェイスは VR 1 内に、FC インターフェイスは VR 2 内にあります。各仮想ルータは、VSAN インターフェイスおよび VR ID によって一意に識別されます。

図 44-7　　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。内容は次のとおりです。

仮想ルータの追加および削除

すべての VRRP の設定は、VRRP が稼働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あわせて 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。

IPv4 の VR を作成または削除するには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t` `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# interface vsan 10` `switch(config-if)#`	VSAN インターフェイス（VSAN 10）を設定します。
ステップ 3	`switch(config-if)# vrrp 250` `switch(config-if-vrrp)#`	VR ID 250 を作成します。
	`switch(config-if)# no vrrp 250`	VR ID 250 を削除します。

IPv6 の VR を作成または削除するには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t` `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# interface vsan 10` `switch(config-if)#`	VSAN インターフェイス（VSAN 10）を設定します。
ステップ 3	`switch(config-if)# vrrp ipv6 250` `switch(config-if-vrrp-ipv6)#`	VR ID 250 を作成します。
	`switch(config-if)# no vrrp ipv6 250`	VR ID 250 を削除します。

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。

IPv4 に対して仮想ルータ設定をイネーブルまたはディセーブルにするには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch(config-if-vrrp)# no shutdown`	VRRP コンフィギュレーションをイネーブルにします。
	`switch(config-if-vrrp)# shutdown`	VRRP コンフィギュレーションをディセーブルにします。

IPv6 に対して設定された仮想ルータをイネーブルまたはディセーブルにするには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch(config-if-vrrp-ipv6)# no shutdown`	VRRP コンフィギュレーションをイネーブルにします。
	`switch(config-if-vrrp-ipv6)# shutdown`	VRRP コンフィギュレーションをディセーブルにします。

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。

仮想ルータの IPv4 アドレスを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# interface vsan 10` `switch(config-if)#`	VSAN インターフェイス（VSAN 10）を設定します。
ステップ 3	`switch(config-if)# ip address 10.0.0.12 255.255.255.0`	IPv4 アドレスとサブネット マスクを設定します。IPv4 アドレスは、VRRP が追加される前に設定する必要があります。
ステップ 4	`switch(config-if)# vrrp 250` `switch(config-if-vrrp)#`	VR ID 250 を作成します。
ステップ 5	`switch(config-if-vrrp)# address 10.0.0.10`	選択した VR の IPv4 アドレスを設定します。 **（注）** この IPv4 アドレスは、インターフェイスの IPv4 アドレスと同じサブネットになければなりません。
	`switch(config-if-vrrp)# no address 10.0.0.10`	選択した VR の IP アドレスを削除します。
ステップ 6	`switch(config-if-vrrp)# address 10.0.0.10 secondary`	選択した VR のセカンダリとして IP アドレス（10.0.0.10）を設定します。 **（注）** **secondary** オプションは、VRRP ルータが仮想ルータの IP アドレスに送信されたパケットを受け付け、渡す必要があるアプリケーションにのみ使用してください。たとえば、iSNS はこのオプションが必要です（「iSNS サーバのイネーブル化」（P.43-87）を参照）。
	`switch(config-if-vrrp)# no address 10.0.0.10 secondary`	選択した VR のセカンダリとしての IP アドレス（10.0.0.10）を削除します。

仮想ルータの IPv6 アドレスを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# interface vsan 12` `switch(config-if)#`	VSAN インターフェイス（VSAN 12）を設定します。
ステップ 3	`switch(config-if)# interface ipv6 address 2001:0db8:800:200c::417a/64`	IP アドレスとプレフィックスを設定します。IPv6 アドレスは、VRRP が追加される前に設定する必要があります。
ステップ 4	`switch(config-if)# vrrp ipv6 200` `switch(config-if-vrrp-ipv6)#`	VR ID 200 を作成します。
ステップ 5	`switch(config-if-vrrp-ipv6)# address 2001:0db8:800:200c::417a`	単一のプライマリ リンクローカル IPv6 アドレスまたは複数のセカンダリ IPv6 アドレスのいずれかを割り当てます。 **（注）** この IPv6 アドレスが物理 IPv6 アドレスと同じである場合、このスイッチは自動的にこの IPv6 アドレスの所有者になります。
	`switch(config-if-vrrp-ipv6)# no address 2001:0db8:800:200c::417a`	選択した VR の IPv6 アドレスを削除します。

仮想ルータのプライオリティ

割り当てることができる仮想ルータのプライオリティの有効範囲は、1 ～ 254 です。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。

IPv4 を使用して仮想ルータのプライオリティを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# interface vsan 10` `switch(config-if)#`	VSAN インターフェイス（VSAN 10）を設定します。
ステップ 3	`switch(config-if)# vrrp 250` `switch(config-if-vrrp)#`	仮想ルータを作成します。
ステップ 4	`switch(config-if-vrrp)# priority 2`	選択した VRRP のプライオリティを設定します。 **（注）** プライオリティ 255 はプリエンプション処理できません。
	`switch(config-if-vrrp)# no priority`	デフォルト値（セカンダリ IPv4 アドレスを持つスイッチの場合は 100、プライマリ IPv4 アドレスを持つスイッチの場合は 255）に戻します。

IPv6 を使用して仮想ルータのプライオリティを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# interface vsan 12` `switch(config-if)#`	VSAN インターフェイス（VSAN 12）を設定します。

	コマンド	目的
ステップ 3	`switch(config-if)# vrrp ipv6 200` `switch(config-if-vrrp-ipv6)#`	仮想ルータを作成します。
ステップ 4	`switch(config-if-vrrp-ipv6)# priority 2`	選択した VRRP のプライオリティを設定します。 （注）　プライオリティ 255 はプリエンプション処理できません。
	`switch(config-if-vrrp-ipv6)# no priority`	デフォルト値（セカンダリ IPv6 アドレスを持つスイッチの場合は 100、プライマリ IPv6 アドレスを持つスイッチの場合は 255）に戻します。

アドバタイズメント パケットのタイム インターバル

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。

IPv4 を使用して仮想ルータのアドバタイズメント パケットのタイム インターバルを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# interface vsan 10` `switch(config-if)#`	VSAN インターフェイス（VSAN 10）を設定します。
ステップ 3	`switch(config-if)# vrrp 50` `switch(config-if-vrrp)#`	仮想ルータを作成します。
ステップ 4	`switch(config-if-vrrp)# advertisement-interval 15`	アドバタイズメント フレームの送信間隔を秒数で設定します。範囲は 1 ～ 255 です。
	`switch(config-if-vrrp)# no advertisement-interval`	デフォルト値（1 秒）に戻します。

IPv6 を使用して仮想ルータのアドバタイズメント パケットのタイム インターバルを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# interface vsan 12` `switch(config-if)#`	VSAN インターフェイス（VSAN 12）を設定します。
ステップ 3	`switch(config-if)# vrrp ipv6 200` `switch(config-if-vrrp-ipv6)#`	仮想ルータを作成します。
ステップ 4	`switch(config-if-vrrp-ipv6)#` `advertisement-interval 150`	アドバタイズメント フレームの送信間隔をセンチ秒数で設定します。指定できる範囲は 100 ～ 4095 です。デフォルトは 100 センチ秒です。
	`switch(config-if-vrrp-ipv6)# no` `advertisement-interval`	デフォルト値（100 センチ秒）に戻します。

プライオリティのプリエンプション

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することをイネーブルにできます。

（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、プリエンプションは暗黙的に適用されます。

（注） VRRP のプリエンプションは、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。

IPv4 を使用する場合にプリエンプションをイネーブルまたはディセーブルにするには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# interface vsan 10` `switch(config-if)#`	VSAN インターフェイス（VSAN 10）を設定します。
ステップ 3	`switch(config-if)# vrrp 250` `switch(config-if-vrrp)#`	仮想ルータを作成します。
ステップ 4	`switch(config-if-vrrp)# preempt`	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ション処理できるようにします。 **（注）** このプリエンプションは、プライマリ IP アドレスには適用されません。
	`switch(config-if-vrrp)# no preempt`	preempt オプションをディセーブルにし（デフォルト）、マスターがプライオリティ レベルを維持できるようにします。

IPv6 を使用する場合にプリエンプションをイネーブルまたはディセーブルにするには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# interface vsan 12` `switch(config-if)#`	VSAN インターフェイス（VSAN 12）を設定します。
ステップ 3	`switch(config-if)# vrrp ipv6 200` `switch(config-if-vrrp-ipv6)#`	仮想ルータを作成します。
ステップ 4	`switch(config-if-vrrp-ipv6)# preempt`	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ション処理できるようにします。 **（注）** このプリエンプションは、プライマリ IP アドレスには適用されません。
	`switch(config-if-vrrp-ipv6)# no preempt`	preempt オプションをディセーブルにし（デフォルト）、マスターがプライオリティ レベルを維持できるようにします。

仮想ルータ認証

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セキュリティ パラメータ インデックス（SPI）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。

仮想ルータの認証オプションを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# interface vsan 1` `switch(config-if)#`	VSAN インターフェイス（VSAN 1）を設定します。
ステップ 3	`switch(config-if)# vrrp 250` `switch(config-if-vrrp)#`	仮想ルータを作成します。
ステップ 4	`switch(config-if-vrrp)# authentication text password`	単純なテキスト認証オプションを指定し、このオプションのパスワードを指定します。
	`switch(config-if-vrrp)# authentication md5 password2003 spi 0x2003`	MD5 認証オプションを割り当て、このオプションにキーと一意の SPI 値を指定します。SPI および有効範囲は 0x100 ～ 0xFFFFFFFF です。
	`switch(config-if-vrrp)# no authentication`	デフォルトの認証なしオプションを割り当てます。

インターフェイス ステート トラッキングに基づくプライオリティ

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。トラッキング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」（P.44-22）を参照）。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ション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ション」（P.44-24）を参照してください。

IPv4 を使用して仮想ルータのインターフェイス プライオリティを追跡するには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# interface vsan 10` `switch(config-if)#`	VSAN インターフェイス（VSAN 10）を設定します。
ステップ 3	`switch(config-if)# vrrp 250` `switch(config-if-vrrp)#`	仮想ルータを作成します。
ステップ 4	`switch(config-if-vrrp)# preempt`	プライオリティのプリエンプション処理をイネーブルにします。
ステップ 5	`switch(config-if-vrrp)# track interface mgmt 0 priority 2`	管理インターフェイスのステートに基づいて、変更する仮想ルータのプライオリティを指定します。
	`switch(config-if-vrrp)# no track`	トラッキング機能をディセーブルにします。

IPv6 を使用して仮想ルータのインターフェイス プライオリティを追跡するには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# interface vsan 12` `switch(config-if)#`	VSAN インターフェイス（VSAN 12）を設定します。
ステップ 3	`switch(config-if)# vrrp ipv6 200` `switch(config-if-vrrp-ipv6)#`	仮想ルータを作成します。
ステップ 4	`switch(config-if-vrrp-ipv6)# preempt`	プライオリティのプリエンプション処理をイネーブルにします。
ステップ 5	`switch(config-if-vrrp-ipv6)# track interface mgmt 0 priority 2`	管理インターフェイスのステートに基づいて、変更する仮想ルータのプライオリティを指定します。 **（注）** プライオリティ トラッキングを有効にするには、トラッキング対象のインターフェイスで IPv6 をイネーブルにします（「IPv6 用の基本的な接続の設定」（P.47-11）を参照）。IPv6 がイネーブルでない場合、インターフェイス ステートは、インターフェイスの実際のステートに関係なく、IPv6 上の VRRP によって down として扱われます。
	`switch(config-if-vrrp-ipv6)# no track`	トラッキング機能をディセーブルにします。

IPv4 VRRP 情報の表示

設定された IPv4 VRRP 情報を表示するには、**show vrrp vr** コマンドを使用します（例 44-2 ～ 44-4 を参照）。

例 44-2　IPv4 VRRP 設定情報の表示

```
switch# show vrrp vr 7 interface vsan 2 configuration
vr id 7 configuration
admin state down
priority 100
no authentication
advertisement-Interval 1
```

```
preempt yes
tracking interface vsan1 priority 2
protocol IP
```

例 44-3　IPv4 VRRP 状態情報の表示

```
switch# show vrrp vr 7 interface vsan 2 status
vr id 7 status
MAC address 00:00:5e:00:01:07
Operational state: init
```

例 44-4　IPv4 VRRP 統計情報の表示

```
switch# show vrrp vr 7 interface vsan 2 statistics
vr id 7 statistics
Become master 0
Advertisement 0
Advertisement Interval Error 0
Authentication Failure 0
TTL Error 0
Priority 0 Received 0
Priority 0 Sent 0
Invalid Type 0
Mismatch Address List 0
Invalid Authentication Type 0
Mismatch Authentication 0
Invalid Packet Length 0
```

IPv6 VRRP 情報の表示

設定された IPv6 VRRP 情報を表示するには、**show vrrp ipv6 vr** コマンドを使用します（例 44-5 ～ 例 44-9 を参照）。

例 44-5　IPv6 VRRP 情報の表示

```
switch# show vrrp ipv6 vr 1
      Interface  VR IpVersion Pri   Time Pre State   VR IP addr
---------------------------------------------------------------------------
        GigE1/5   1   IPv6    100  100cs     master  2004::1
        GigE1/6   1   IPv6    100  100cs     backup  2004::1
```

例 44-6　IPv6 VRRP インターフェイス設定情報の表示

```
switch# show vrrp ipv6 vr 1 interface gigabitethernet 1/5 configuration
IPv6 vr id 1 configuration
admin state up
priority 100
associated ip: 2004::1
advertisement-interval 100
preempt no
protocol IPv6
```

例 44-7　　IPv6 VRRP インターフェイス状態情報の表示

```
switch# show vrrp ipv6 vr 1 interface gigabitethernet 1/5 status
IPv6 vr id 1 status
MAC address 00:00:5e:00:02:01
Operational state: master
Up time 37 min,  10 sec
Master IP address: fe80::20c:30ff:feda:96dc
```

例 44-8　　IPv6 VRRP 統計情報の表示

```
switch# show vrrp ipv6 vr 1 interface gigabitethernet 1/5 statistics
IPv6 vr id 1 statistics
Become master 1
Advertisement 0
Advertisement Interval Error 0
TTL Error 0
Priority 0 Received 0
Priority 0 Sent 0
Invalid Type 0
Mismatch Address List 0
Invalid Packet Lenght 0
```

VRRP 統計情報の表示

設定された IPv6 VRRP 情報を表示するには、**show vrrp statistics** コマンドを使用します（例 44-9 を参照）。

例 44-9　　VRRP 累積統計情報の表示

```
switch# show vrrp statistics
Invalid checksum 0
Invalid version 0
Invalid VR ID 0
```

VRRP 統計情報のクリア

スイッチ上のすべてのインターフェイスのすべての VRRP 統計情報をクリアするには、**clear vrrp statistics** コマンドを使用します（例 44-10 を参照）。

例 44-10　　VRRP 統計情報のクリア

```
switch# clear vrrp Statistics
```

指定されたインターフェイスの IPv4 および IPv6 VRRP 統計情報の両方をクリアするには、**clear vrrp vr** コマンドを使用します（例 44-10 を参照）。

例 44-11　　指定したインターフェイスの VRRP 統計情報をクリアします。

```
switch# clear vrrp vr 1 interface vsan 1
```

特定の IPv4 仮想ルータについて、すべての統計情報をクリアするには、**clear vrrp ipv4** コマンドを使用します（例 44-12 を参照）。

例 44-12　　指定したインターフェイスの VRRP IPv4 統計情報のクリア

```
switch# clear vrrp ipv4 vr 7 interface vsan 2
```

特定の IPv6 仮想ルータについて、すべての統計情報をクリアするには、**clear vrrp ipv6** コマンドを使用します（例 44-13 を参照）。

例 44-13　　指定したインターフェイスの VRRP IPv6 統計情報のクリア

```
switch# clear vrrp ipv6 vr 7 interface vsan 2
```

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。

DNS サーバを設定するには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t` `switch(config)#`	コンフィギュレーション モードに入ります。
ステップ 2	`switch(config)# ip domain-lookup`	IP ドメイン ネーム システム（DNS）ベースのホスト名からアドレスへの変換をイネーブルにします。
	`switch(config)# no ip domain-lookup`	（デフォルト）IP DNS ベースのホスト名からアドレスへの変換をディセーブルにし、出荷時のデフォルトに戻します。
ステップ 3	`switch(config)# ip domain-name cisco.com`	非修飾ホスト名を完成するためのデフォルトのドメイン名機能をイネーブルにします。ドメイン名を含まない IP ホスト名（つまりドットのない名前）にはドットと cisco.com が追加され、その後でホスト テーブルに追加されます。
	`switch(config)# no ip domain-name cisco.com`	（デフォルト）ドメイン名をディセーブルにします。

	コマンド	目的

ステップ 4	`switch(config)# ip domain-list harvard.edu`
	`switch(config)# ip domain-list stanford.edu`
	`switch(config)# ip domain-list yale.edu`
		デフォルト ドメイン名のフィルタを、**ip domain-list** グローバル コンフィギュレーション コマンドを使用して、非修飾ホスト名を完成させるために定義します。このフィルタで最大 10 ドメイン名を定義できます。フィルタから名前を削除するには、このコマンドの **no** 形式を使用します。

	`switch(config)# no ip domain-list`	定義したフィルタを削除し、出荷時のデフォルトに戻します。ドメインはデフォルトで設定されていません。
	（注） ドメイン リストを設定していない場合は、**ip domain-name** グローバル コンフィギュレーション コマンドで指定したドメイン名が使用されます。ドメイン リストを設定した場合、デフォルトのドメイン名は使用されません。**ip domain-list** コマンドは **ip domain-name** コマンドと似ていますが、**ip domain-list** コマンドを使用すると、ドメインのリストを定義して、リストの順番でドメインが検索されるところが異なっています。	
ステップ 5	`switch(config)# ip name-server 15.1.0.1 2001:0db8:800:200c::417a`	プライマリ サーバとして最初のアドレス（15.1.0.1）およびセカンダリ サーバとして 2 番目のアドレス（2001:0db8:800:200c::417a）を指定します。最大 6 台のサーバを設定できます。
	`switch(config)# no ip name-server`	設定したサーバを削除し、出荷時のデフォルトに戻します。サーバはデフォルトでは設定されていません。
ステップ 6	**（注）** または、（IP アドレスの代わりに）スイッチ名を使用して DNS エントリを設定できます。設定したスイッチ名が自動的に対応する IP アドレスを検索します。	

DNS ホスト情報の表示

DNS 設定を表示するには、**show hosts** コマンドを使用します（例 44-14 を参照）。

例 44-14　設定されたホストの詳細の表示

```
switch# show hosts
Default domain is cisco.com

Domain list: ucsc.edu harvard.edu yale.edu stanford.edu

Name/address lookup uses domain service

Name servers are 15.1.0.1 15.2.0.0
```

デフォルト設定

表 44-1 に、DNS 機能のデフォルト設定を示します。

表 44-1　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

表 44-1　DNS のデフォルト設定値 （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 44-2 に、VRRP 機能のデフォルト設定を示します。

表 44-2　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ション	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