CHAPTER 40

VRF-Lite の設定

Virtual Private Network（VPN; バーチャル プライベート ネットワーク）は、ISP バックボーン ネットワーク上でお客様にセキュアな帯域幅共有を提供します。VPN は、共通ルーティング テーブルを共有するサイトの集合です。カスタマーのサイトは、1 つまたは複数のインターフェイスでサービス プロバイダーのネットワークに接続され、サービス プロバイダーが各インターフェイスを VPN ルーティング テーブルに対応付けます。VPN ルーティング テーブルは、VPN Routing/Forwarding（VRF; VPN ルーティング / 転送）テーブルと呼ばれます。

Catalyst 4500 シリーズ スイッチは、VRF-Lite 機能を使用して Customer Edge（CE; カスタマー エッジ）デバイスで複数の VRF インスタンスをサポートします。（VRF-Lite は、Multi-VRF CE、または Multi-VRF CE デバイスともいいます）。VRF-Lite によって、サービス プロバイダーは 1 つのインターフェイスを使用して、重複する IP アドレスを持つ複数の VPN をサポートできます。

（注） Cisco IOS Release 12.2(52)SG から、Catalyst 4500 シリーズ スイッチでは、ルーティング プロトコル OSPF/EIGRP/BGP での VRF-Lite NSF サポートがサポートされています。

（注） スイッチでは、VPN のサポートのためにマルチプロトコル ラベル スイッチング（MPLS）が使用されません。MPLS VRF の詳細については、次の URL で『*Cisco IOS Switching Services Configuration Guide*』を参照してください。

http://www.cisco.com/en/US/docs/ios/mpls/configuration/guide/mp_vpn_ipv4_ipv6_ps6922_TSD_Products_Configuration_Guide_Chapter.html

この章の内容は、次のとおりです。

- 「VRF-Lite ステータスの表示」（P.40-17）

（注）　この章で使用するスイッチ コマンドの構文および使用方法の詳細については、次の URL で『*Cisco Catalyst 4500 Series Switch Command Reference*』と関連資料を参照してください。

http://www.cisco.com/en/US/products//hw/switches/ps4324/index.html

『Catalyst 4500 Series Switch Command Reference』に掲載されていないコマンドについては、より詳細な Cisco IOS ライブラリを参照してください。次の URL で『*Cisco IOS Command Reference*』と関連資料を参照してください。

http://www.cisco.com/en/US/products/ps6350/index.html

VRF-Lite について

VRF-Lite の機能によって、サービス プロバイダーは、VPN 間で重複した IP アドレスを使用できる複数の VPN をサポートできます。VRF-Lite は入力インターフェイスを使用して異なる VPN のルートを区別し、各 VRF に 1 つまたは複数のレイヤ 3 インターフェイスを対応付けて仮想パケット転送テーブルを形成します。VRF のインターフェイスは、イーサネット ポートなどの物理インターフェイス、または VLAN SVI などの論理インターフェイスにすることができますが、レイヤ 3 インターフェイスは、一度に複数の VRF に属することはできません。

（注）　VRF-Lite インターフェイスは、レイヤ 3 インターフェイスである必要があります。

VRF-Lite には次のデバイスが含まれます。

- CE デバイスにおいて、カスタマーは、1 つまたは複数のプロバイダー エッジ（PE）ルータへのデータ リンクを介してサービス プロバイダー ネットワークにアクセスできます。CE デバイスは、サイトのローカル ルートをプロバイダー エッジ ルータにアドバタイズし、そこからリモート VPN ルートを学習します。Catalyst 4500 シリーズ スイッチは CE にすることができます。
- プロバイダー エッジ（PE）ルータは、スタティック ルーティングまたはルーティング プロトコル（BGP、RIPv1、RIPv2 など）を使用して、CE デバイスとルーティング情報を交換します。

  PE では、直接接続された VPN の VPN ルートを維持することだけが必要とされます。サービス プロバイダーのすべての VPN ルートを PE が維持する必要はありません。各 PE ルータは、直接接続しているサイトごとに VRF を維持します。すべてのサイトが同じ VPN に存在する場合は、PE ルータの複数のインターフェイスを 1 つの VRF に関連付けることができます。各 VPN は、指定された VRF にマッピングされます。PE ルータは、ローカル VPN ルートを CE から学習したあとで、IBGP を使用して別の PE ルータと VPN ルーティング情報を交換します。
- プロバイダー ルータ（またはコア ルータ）とは、サービス プロバイダー ネットワーク内にあり、CE デバイスに接続していないすべてのルータです。

VRF-Lite を使用すると、複数のお客様が 1 つの CE を共有できます。また、1 つの物理リンクのみが CE と PE 間に使用されます。共有 CE は、お客様ごとに別々の VRF テーブルを維持し、独自のルーティング テーブルに基づいて、お客様ごとにパケットをスイッチングまたはルーティングします。VRF-Lite は限定された PE の機能を CE デバイスに拡張して、個別の VRF テーブルを保守する機能を付与し、VPN のプライバシーおよびセキュリティをブランチ オフィスまで拡張します。

図 40-1 は、各 Catalyst 4500 シリーズ スイッチが複数の仮想 CE として動作する構成を示します。VRF-Lite はレイヤ 3 機能であるため、VRF の各インターフェイスはレイヤ 3 インターフェイスである必要があります。

図 40-1　複数の仮想 CE として動作する Catalyst 4500 シリーズ スイッチ

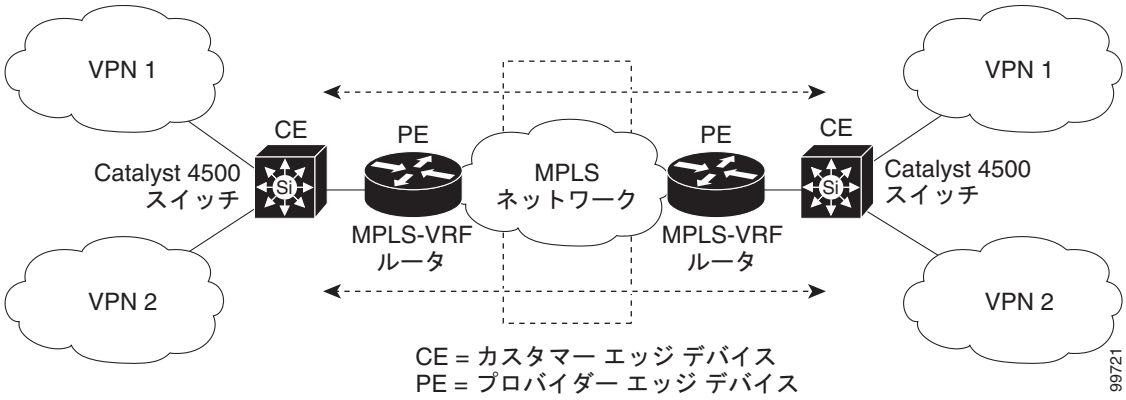


図 40-1 で、VRF-Lite の CE 対応ネットワークでのパケット転送プロセスについて説明します。

- CE が VPN からパケットを受信すると、CE は入力インターフェイスに基づいたルーティング テーブルを検索します。ルートが見つかると、CE はパケットを PE に転送します。
- 入力 PE は、CE からパケットを受信すると、VRF 検索を実行します。ルートが見つかると、ルータは対応する MPLS ラベルをパケットに追加し、MPLS ネットワークに送信します。
- 出力 PE は、ネットワークからパケットを受信すると、ラベルを除去してそのラベルを使用し、正しい VPN ルーティング テーブルを識別します。次に、出力 PE が通常のルート検索を行います。ルートが見つかると、パケットを正しい隣接デバイスに転送します。
- CE が出力 PE からパケットを受信すると、CE は入力インターフェイスを使用して正しい VPN ルーティング テーブルを検索します。ルートが見つかると、CE はパケットを VPN 内に転送します。

VRF を設定するには、VRF テーブルを作成し、VRF に対応付けられたレイヤ 3 インターフェイスを指定します。次に、VPN および CE と PE 間でルーティング プロトコルを設定します。BGP は、プロバイダーのバックボーンで VPN のルーティング情報を配布するために使用される優先ルーティング プロトコルです。VRF-Lite ネットワークには、次の 3 つの主要なコンポーネントがあります。

- VPN ルート ターゲット コミュニティ : VPN コミュニティの他のすべてのメンバをリストします。VPN コミュニティ メンバごとに VPN ルート ターゲットを設定する必要があります。
- VPN コミュニティ PE ルータのマルチプロトコル BGP ピアリング : VPN コミュニティのすべてのメンバに VRF の到着可能性情報を伝播します。VPN コミュニティのすべての PE ルータで BGP ピアリングを設定する必要があります。
- VPN 転送 : VPN サービスプロバイダー ネットワークのすべての VPN コミュニティ メンバ間のすべてのトラフィックを転送します。

VRF-Lite のデフォルト設定

表 40-1 に、VRF のデフォルト設定を示します。

表 40-1　VRF のデフォルト設定

機能	デフォルト設定
VRF	ディセーブル。VRF は定義されていません。
マップ	インポート マップ、エクスポート マップ、ルート マップは定義されていません。
VRF 最大ルート数	なし。
転送テーブル	インターフェイスのデフォルトは、グローバル ルーティング テーブルです。

VRF-Lite 設定時の注意事項

ネットワークに VRF を設定する場合に、次の点に留意してください。

- VRF-Lite が設定されたスイッチは複数のカスタマーで共有され、すべてのカスタマーが独自のルーティング テーブルを持ちます。
- カスタマーは別々の VRF テーブルを使用するので、同じ IP アドレスを再利用できます。別々の VPN では IP アドレスの重複が許可されます。
- VRF-Lite では、複数のカスタマーが PE と CE の間で同一の物理リンクを共有できます。複数の VLAN を持つトランク ポートでは、パケットがお客様間で分離されます。すべてのカスタマーが独自の VLAN を持ちます。
- VRF-Lite は、すべての MPLS-VRF 機能（ラベル交換、Label Distribution Protocol（LDP）の隣接関係、またはラベル付きパケット）をサポートしていません。
- PE ルータでは、VRF-Lite の使用と複数の CE の使用には違いがありません。図 40-1 では、複数の仮想レイヤ 3 インターフェイスが VRF-Lite デバイスに接続されています。
- Catalyst 4500 シリーズ スイッチは、物理ポート、VLAN SVI、またはその 2 つの組み合わせを使用した VRF の設定をサポートしています。アクセス ポートまたはトランク ポート経由で SVI を接続できます。
- お客様は、別のお客様と重複しないかぎり、複数の VLAN を使用できます。お客様の VLAN は、スイッチに保存されている適切なルーティング テーブルの識別に使用される特定のルーティング テーブル ID にマッピングされます。
- レイヤ 3 TCAM リソースは、すべての VRF 間で共有されます。各 VRF が十分な CAM 領域を持つようにするには、**maximum routes** コマンドを使用します。
- VRF を使用した Catalyst 4500 シリーズ スイッチは、1 つのグローバル ネットワークと最大 64 の VRF をサポートできます。サポートされるルートの総数は、TCAM のサイズに制限されます。
- CE と PE 間のほとんどのルーティング プロトコル（BGP、OSPF、EIGRP、RIP、およびスタティック ルーティング）を使用できます。ただし、次の理由から External BGP（EBGP）を使用することを推奨します。
  - BGP では、複数の CE とのやり取りに複数のアルゴリズムを必要としません。
  - BGP は、さまざまな管理者によって稼働するシステム間でルーティング情報を渡すように設計されています。
  - BGP では、ルートの属性を CE に簡単に渡すことができます。
- VRF-Lite は、Interior Gateway Routing Protocol（IGRP）および ISIS をサポートしません。
- VRF-Lite は、パケット スイッチング レートに影響しません。

- Cisco IOS Release 12.2(50)SG から、マルチキャストと VRF は、レイヤ 3 インターフェイスに一緒に設定できます。
- Catalyst 4500 シリーズ スイッチでは、すべての PIM プロトコル（PIM-SM、PIM-DM、PIM-SSM、PIM BiDIR）がサポートされます。
- **router ospf** の **capability vrf-lite** サブコマンドは、PE と CE 間のルーティング プロトコルとして OSPF が設定されている場合に使用する必要があります。

VRF の設定

1 つまたは複数の VRF を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Switch(config)# ip routing`	IP ルーティングをイネーブルにします。
ステップ 3	`Switch(config)# ip vrf` *vrf-name*	VRF 名を指定し、VRF コンフィギュレーション モードを開始します。
ステップ 4	`Switch(config-vrf)# rd` *route-distinguisher*	ルート識別子を指定して VRF テーブルを作成します。Autonomous System（AS; 自律システム）番号および任意の数（xxx:y）または IP アドレスおよび任意の数（A.B.C.D:y）のどちらかを入力します。
ステップ 5	`Switch(config-vrf)# route-target {export | import | both}` *route-target-ext-community*	指定された VRF のインポート、エクスポート、またはインポートおよびエクスポート ルート ターゲット コミュニティのリストを作成します。AS システム番号と任意の番号（xxx:y）または IP アドレスと任意の番号（A.B.C.D:y）を入力します。 **（注）** このコマンドは、BGP が動作している場合にのみ有効です。
ステップ 6	`Switch(config-vrf)# import map` *route-map*	（任意）VRF にルート マップを対応付けます。
ステップ 7	`Switch(config-vrf)# interface` *interface-id*	インターフェイス コンフィギュレーション モードを開始して、VRF に対応付けるレイヤ 3 インターフェイスを指定します。インターフェイスはルーテッド ポートまたは SVI に設定できます。
ステップ 8	`Switch(config-if)# ip vrf forwarding` *vrf-name*	VRF をレイヤ 3 インターフェイスに対応付けます。
ステップ 9	`Switch(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 10	`Switch# show ip vrf [brief | detail | interfaces] [vrf-name]`	設定を確認します。設定した VRF に関する情報を表示します。
ステップ 11	`Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

（注） 次のコマンドの構文および使用方法の詳細については、このリリースのスイッチ コマンド リファレンスと、http://www.cisco.com/en/US/docs/ios/ipswitch/command/reference/isw_book.html にある『*Cisco IOS Switching Services Command Reference*』を参照してください。

VRF を削除してすべてのインターフェイスを削除するには、**no ip vrf** *vrf-name* グローバル コンフィギュレーション コマンドを使用します。VRF からあるインターフェイスを削除するには、**no ip vrf forwarding** インターフェイス コンフィギュレーション コマンドを使用します。

VRF 認識サービスの設定

IP サービスは、グローバルなインターフェイス上と、グローバルなルーティング インスタンス内で設定できます。IP サービスは複数のルーティング インスタンス上で稼働するように拡張されます。これが、VRF 認識です。システム内の任意の設定済み VRF であればいずれも、VRF 認識サービス用に指定できます。

VRF 認識サービスは、プラットフォームから独立したモジュールに実装されています。VRF は、Cisco IOS 内の複数のルーティング インスタンスを提供します。各プラットフォームには、サポートする VRF 数に関して独自の制限があります。

VRF 認識サービスには、次の特性があります。

- ユーザは、ユーザ指定の VRF 内のホストに ping を実行できます。
- ARP エントリは、個別の VRF で学習されます。ユーザは、特定の VRF の ARP エントリを表示できます。

これらのサービスは VRF 認識です。

- ARP
- ping
- 簡易ネットワーク管理プロトコル（SNMP）
- Unicast Reverse Path Forwarding（uRPF; ユニキャスト RPF）
- Syslog
- traceroute
- FTP および TFTP
- Telnet および SSH
- NTP

ARP のユーザ インターフェイスの設定

VRF 認識サービスを ARP 用に設定するには、次の作業を実行します。

コマンド	目的
`Switch# show ip arp vrf vrf-name`	指定された VRF で、ARP テーブル（スタティック エントリおよびダイナミック エントリ）を表示します。
`Switch(config)# arp vrf vrf-name ip-address mac-address ARPA`	指定された VRF でスタティック ARP エントリを作成します。

PING のユーザ インターフェイスの設定

VRF 認識 PING を実行するには、次の作業を行います。

コマンド	目的
Switch# **ping vrf** *vrf-name* **ip-host**	指定された VRF で、IP ホストまたはアドレスに対して PING を実行します。

SNMP のユーザ インターフェイスの設定

VRF 認識サービスを SNMP 用に設定するには、次の作業を実行します。

	コマンド	目的
ステップ 1	Switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# **snmp-server trap authentication vrf**	VRF で、パケットに対して SNMP トラップをイネーブルにします。
ステップ 3	Switch(config)# **snmp-server** *engineID* **remote** *host* **vrf** *vpn-instance engine-id string*	スイッチ上で、リモート SNMP エンジンの名前を設定します。
ステップ 4	Switch(config)# **snmp-server host** *host* **vrf** *vpn-instance* **traps** *community*	SNMP トラップ動作の受信側、および SNMP トラップの送信に使用される VRF テーブルを指定します。
ステップ 5	Switch(config)# **snmp-server host** *host* **vrf** *vpn-instance* **informs** *community*	SNMP 通知動作の受信先を指定し、SNMP 通知の送信に使用される VRF テーブルを指定します。
ステップ 6	Switch(config)# **snmp-server user** *user group* **remote** *host* **vrf** *vpn-instance security model*	SNMP アクセス用に、VRF 上にあるリモート ホストの SNMP グループにユーザを追加します。
ステップ 7	Switch(config)# **end**	特権 EXEC モードに戻ります。

uRPF のユーザ インターフェイスの設定

VRF に割り当てられているインターフェイス上で、uRPF を設定できます。送信元の検索が VRF テーブルで実行されます。

VRF 認識サービスを uRPF 用に設定するには、次の作業を実行します。

	コマンド	目的
ステップ 1	Switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# **interface** *interface-id*	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、設定するレイヤ 3 インターフェイスを指定します。
ステップ 3	Switch(config-if)# **no switchport**	レイヤ 2 コンフィギュレーション モードからインターフェイスを削除します（物理インターフェイスの場合）。
ステップ 4	Switch(config-if)# **ip vrf forwarding** *vrf-name*	インターフェイス上で VRF を設定します。
ステップ 5	Switch(config-if-vrf)# **ip address** *ip-address subnet-mask*	インターフェイスの IP アドレスを入力します。

	コマンド	目的
ステップ 6	`Switch(config-if-vrf)# ip verify unicast source reachable-via rx allow-default`	インターフェイス上で uRPF をイネーブルにします。
ステップ 7	`Switch(config-if-vrf)# end`	特権 EXEC モードに戻ります。

Syslog のユーザ インターフェイスの設定

VRF 認識サービスを Syslog 用に設定するには、次の作業を実行します。

	コマンド	目的
ステップ 1	`Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Switch(config)# logging on`	ストレージ ルータ イベント メッセージのロギングを、イネーブルまたは一時的にディセーブルにします。
ステップ 3	`Switch(config)# logging host` *ip-address* **vrf** *vrf-name*	ロギング メッセージが送信される Syslog サーバのホスト アドレスを指定します。
ステップ 4	`Switch(config)# logging buffered` *logging buffered size* **debugging**	メッセージを内部バッファにロギングします。
ステップ 5	`Switch(config)# logging trap debugging`	Syslog サーバに送信されるロギング メッセージを制限します。
ステップ 6	`Switch(config)# logging facility` *facility*	ロギング ファシリティにシステム ロギング メッセージを送信します。
ステップ 7	`Switch(config)# end`	特権 EXEC モードに戻ります。

Traceroute のユーザ インターフェイスの設定

Traceroute に対して VRF 認識サービスを設定するには、次の作業を実行します。

コマンド	目的
traceroute vrf *vrf-name ipaddress*	宛先アドレスを取得する VPN VRF の名前を指定します。

FTP および TFTP のユーザ インターフェイスの設定

FTP と TFTP が VRF 認識となるには、FTP と TFTP CLI をいくつか設定する必要があります。たとえば、インターフェイスに接続する VRF テーブル（たとえば、E1/0）テーブルを使用する場合、特定のルーティング テーブルを使用するように [t]ftp に通知されるように **ip [t]ftp source-interface E1/0** コマンドを設定する必要があります。この例では、VRF テーブルが宛先 IP アドレスを検索するのに使用されます。これらの変更には下位互換性があり、既存の動作には影響を及ぼしません。VRF がそのインターフェイスに設定されていない場合でも、送信元インターフェイス CLI を使用して、特定のインターフェイスにパケットを送信できます。

FTP 接続の送信元 IP アドレスを指定するには、**ip ftp source-interface** show モード コマンドを使用します。接続が確立されているインターフェイスのアドレスを使用するには、**no** 形式のコマンドを使用します。

FTP および TFTP のユーザ インターフェイスを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Switch(config)# ip ftp source-interface interface-type interface-number`	FTP 接続の発信元 IP アドレスを指定します。
ステップ 3	`Switch(config)# end`	特権 EXEC モードに戻ります。

TFTP 接続の送信元 IP アドレスとしてインターフェイスの IP アドレスを指定するには、**ip tftp source-interface** show モード コマンドを使用します。デフォルトに戻るには、**no** 形式のコマンドを使用します。

	コマンド	目的
ステップ 1	`Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Switch(config)# ip tftp source-interface interface-type interface-number`	TFTP 接続用の送信元 IP アドレスを指定します。
ステップ 3	`Switch(config)# end`	特権 EXEC モードに戻ります。

Telnet および SSH のユーザ インターフェイスの設定

Telnet および SSH の使用に関する VRF 認識を設定するには、次の作業を行います。

コマンド	目的
`Switch# telnet ip-address/vrf vrf-name`	指定された VRF で、IP ホストまたはアドレスに Telnet 経由で接続します。
`Switch# ssh -l username -vrf vrf-name ip-host`	指定された VRF で、IP ホストまたはアドレスに SSH 経由で接続します。

NTP のユーザ インターフェイスの設定

VRF 認識を NTP 用に設定するには、次の作業を実行します。

コマンド	目的
`Switch# ntp server vrf vrf-name ip-host`	指定された VRF で NTP サーバを設定します。
`Switch# ntp peer vrf vrf-name ip-host`	指定された VRF で NTP ピアを設定します。

TACACS+ サーバ用の Per-VRF の設定

TACACS+ サーバ機能の per-VRF は TACACS+ サーバの per- 仮想単位ルート転送（per-VRF）の認証、認可、アカウンティング（AAA）を設定することができます。

TACACS+ サーバの per-VRF を設定する前に、AAA およびサーバ グループを設定しておく必要があります。VRF ルーティング テーブル（ステップ 3 および 4 で示すように）を作成し、インターフェイスを設定する（ステップ 6、7、および 8）ことができます。TACACS+ サーバの per-VRF 単位の実際の設定は、ステップ 10 ～ 13 で行われます。

	コマンドまたはアクション	目的
ステップ 1	`Switch> enable`	特権 EXEC モードをイネーブルにします。 プロンプトが表示されたら、パスワードを入力します。
ステップ 2	`Switch# configure terminal`	グローバル 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)# ip vrf` *vrf-name*	VRF テーブルを設定し、VRF コンフィギュレーション モードを開始します。
ステップ 4	`Switch (config-vrf)# rd` *route-distinguisher*	VRF インスタンスに対するルーティングおよびフォワーディング テーブルを作成します。
ステップ 5	`Switch (config-vrf)# exit`	VRF コンフィギュレーション モードを終了します。
ステップ 6	`Switch (config)# interface` *interface-name*	インターフェイスを設定し、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 7	`Switch (config-if)# ip vrf forwarding` *vrf-name*	インターフェイスに VRF を設定します。
ステップ 8	`Switch (config-if)# ip address` *ip-address mask* [**secondary**]	インターフェイスのプライマリまたはセカンダリ IP アドレスを設定します。
ステップ 9	`Switch (config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。
ステップ 10	**aaa group server tacacs+** *group-name* **例：** `Switch (config)# aaa group server tacacs+ tacacs1`	異なる TACACS+ サーバ ホストを別々のリストと方式にグループ化し、server-group コンフィギュレーション モードを開始します。
ステップ 11	**server-private** {*ip-address* | *name*} [**nat**] [**single-connection**] [**port** *port-number*] [**timeout** *seconds*] [**key** [**0** | **7**] *string*] **例：** `Switch (config-sg-tacacs+)# server-private 10.1.1.1 port 19 key cisco`	グループ サーバに対するプライベート TACACS+ サーバの IP アドレスを設定します。
ステップ 12	`Switch (config-sg-tacacs+)# ip vrf forwarding` *vrf-name*	AAA TACACS+ サーバ グループの VRF リファレンスを設定します。
ステップ 13	`Switch (config-sg-tacacs+)# ip tacacs source-interface` *subinterface-name*	すべての発信 TACACS+ パケットに対して、指定されたインターフェイスの IP アドレスを使用します。
ステップ 14	`Switch (config-sg-tacacs)# exit`	server-group コンフィギュレーション モードを終了します。

次の例で、per-VRF TACACS+ の設定に必要なすべての手順をリストします。

```
Switch> enable
Switch# configure terminal
Switch (config)# ip vrf cisco
Switch (config-vrf)# rd 100:1
Switch (config-vrf)# exit
Switch (config)# interface Loopback0
Switch (config-if)# ip vrf forwarding cisco
Switch (config-if)# ip address 10.0.0.2 255.0.0.0
Switch (config-if)# exit
Switch (config-sg-tacacs+)# ip vrf forwarding cisco
Switch (config-sg-tacacs+)# ip tacacs source-interface Loopback0
Switch (config-sg-tacacs)# exit
```

TACACS+ サーバの per-VRF の設定の詳細については、『*Cisco IOS Per VRF for TACACS + Server, Release 12.3(7)T*』を参照してください。

マルチキャスト VRF の設定

VRF テーブル内でマルチキャストを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Switch(config)# ip routing`	IP ルーティングをイネーブルにします。
ステップ 3	`Switch(config)# ip vrf` *vrf-name*	VRF 名を指定し、VRF コンフィギュレーション モードを開始します。
ステップ 4	`Switch(config-vrf)# ip multicast-routing vrf` *vrf-name*	（任意）VRF テーブルでグローバル マルチキャスト ルーティングをイネーブルにします。
ステップ 5	`Switch(config-vrf)# rd` *route-distinguisher*	ルート識別子を指定して VRF テーブルを作成します。Autonomous System（AS; 自律システム）番号および任意の数（xxx:y）または IP アドレスおよび任意の数（A.B.C.D:y）のどちらかを入力します。
ステップ 6	`Switch(config-vrf)# route-target {export | import | both}` *route-target-ext-community*	指定された VRF のインポート、エクスポート、またはインポートおよびエクスポート ルート ターゲット コミュニティのリストを作成します。AS システム番号と任意の番号（xxx:y）または IP アドレスと任意の番号（A.B.C.D:y）を入力します。 *ルート ターゲット ext コミュニティ*値は、ステップ 4 で入力した *route-distinguisher* 値と同じです。
ステップ 7	`Switch(config-vrf)# import map` *route-map*	（任意）VRF にルート マップを対応付けます。
ステップ 8	`Switch(config-vrf)# interface` *interface-id*	インターフェイス コンフィギュレーション モードを開始して、VRF に対応付けるレイヤ 3 インターフェイスを指定します。有効なインターフェイスは、ルーテッド ポートまたは SVI です。
ステップ 9	`Switch(config-if)# ip vrf forwarding` *vrf-name*	VRF をレイヤ 3 インターフェイスに対応付けます。
ステップ 10	`Switch(config-if)# ip address` *ip-address* **mask**	レイヤ 3 インターフェイスの IP アドレスを設定します。

	コマンド	目的
ステップ 11	Switch(config-if)# **ip pim** [**sparse-dense mode** | **dense-mode** | **sparse-mode**]	VRF に関連付けられているレイヤ 3 インターフェイス上で、PIM をイネーブルにします。
ステップ 12	Switch(config-if)# **end**	特権 EXEC モードに戻ります。
ステップ 13	Switch# **show ip vrf** [**brief** | **detail** | **interfaces**] [*vrf-name*]	設定を確認します。設定した VRF に関する情報を表示します。
ステップ 14	Switch# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

Multi-VRF CE 内でのマルチキャスト設定の詳細については、『*Cisco IOS IP Multicast Configuration Guide, Release 12.4*』を参照してください。

VRF を削除してすべてのインターフェイスを削除するには、**no ip vrf** *vrf-name* グローバル コンフィギュレーション コマンドを使用します。VRF からあるインターフェイスを削除するには、**no ip vrf forwarding** インターフェイス コンフィギュレーション コマンドを使用します。

VPN ルーティング セッションの設定

VPN 内のルーティングは、サポートされるルーティング プロトコル（RIP、OSPF、または BGP）、またはスタティック ルーティングで設定できます。ここで説明する設定は OSPF のものですが、その他のプロトコルでも手順は同じです。

VPN に OSPF を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# **router ospf** *process-id* **vrf** *vrf-name*	OSPF ルーティングをイネーブルにし、VPN 転送テーブルを指定して、ルータ 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-router)# **log-adjacency-changes**	（任意）隣接状態（デフォルト）の変更を記録します。
ステップ 4	Switch(config-router)# **redistribute bgp** *autonomous-system-number* subnets	BGP ネットワークから OSPF ネットワークに情報を再配布するようにスイッチを設定します。
ステップ 5	Switch(config-router)# **network** *network-number* **area** *area-id*	OSPF が動作するネットワーク アドレスとマスク、およびそのネットワーク アドレスのエリア ID を定義します。
ステップ 6	Switch(config-router)# **end**	特権 EXEC モードに戻ります。
ステップ 7	Switch# **show ip ospf** *process-id*	OSPF ネットワークの設定を確認します。
ステップ 8	Switch# **copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

VPN 転送テーブルと OSPF ルーティング プロセスの関連付けを解除するには、**no router ospf** *process-id* **vrf** *vrf-name* グローバル コンフィギュレーション コマンドを使用します。

次の例は、VRF-RED という名前の単一の VRF を設定します。

```
Switch(config)# ip vrf VRF-RED
Switch(config-vrf)# rd 1:1
Switch(config-vrf)# exit
```

```
Switch(config)# router eigrp virtual-name
Switch(config-router)# address-family ipv4 vrf VRF-RED autonomous-system 1
Switch(config-router-af)# network 10.0.0.0 0.0.0.255
Switch(config-router-af)# topology base
Switch(config-router-topology)# default-metric 10000 100 255 1 1500
Switch(config-router-topology)# exit-af-topology
Switch(config-router-af)# exit-address-family
```

BGP PE/CE ルーティング セッションの設定

CE ルーティング セッションに BGP PE を設定するには、次の作業を行います。

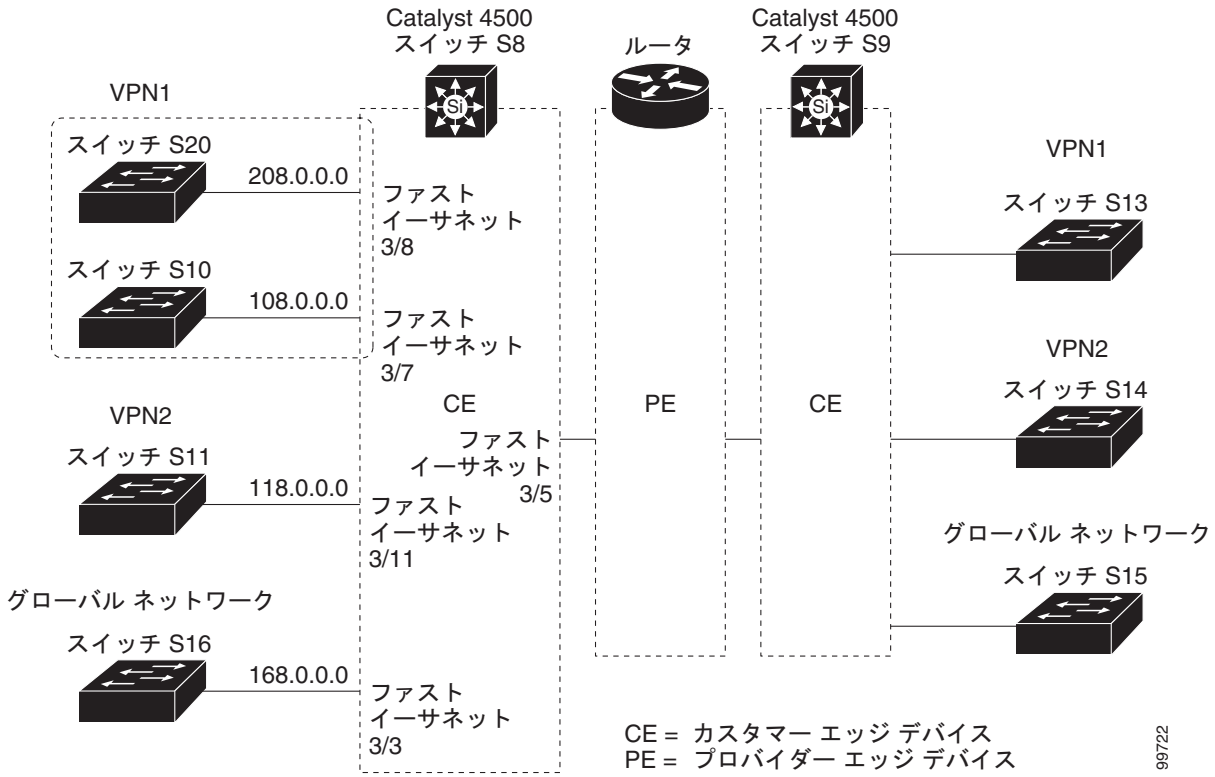
	コマンド	目的
ステップ 1	`Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	`Switch(config)# router bgp` *autonomous-system-number*	その他の BGP ルータに渡された AS 番号で BGP ルーティング プロセスを設定し、ルータ コンフィギュレーション モードを開始します。
ステップ 3	`Switch(config-router)# network` *network-number* **mask** *network-mask*	BGP を使用してアナウンスするネットワークおよびマスクを指定します。
ステップ 4	`Switch(config-router)# redistribute ospf` *process-id* `match internal`	OSPF 内部ルートを再配布するようにスイッチを設定します。
ステップ 5	`Switch(config-router)# network` *network-number* **area** *area-id*	OSPF が動作するネットワーク アドレスとマスク、およびそのネットワーク アドレスのエリア ID を定義します。
ステップ 6	`Switch(config-router-af)#` **address-family ipv4 vrf** *vrf-name*	PE から CE のルーティング セッションの BGP パラメータを定義し、VRF アドレス ファミリ モードを開始します。
ステップ 7	`Switch(config-router-af)# neighbor` *address* **remote-as** *as-number*	PE と CE ルータの間の BGP セッションを定義します。
ステップ 8	`Switch(config-router-af)# neighbor` *address* **activate**	IPv4 アドレス ファミリのアドバタイズメントをアクティブ化します。
ステップ 9	`Switch(config-router-af)# end`	特権 EXEC モードに戻ります。
ステップ 10	`Switch# show ip bgp [ipv4] [neighbors]`	BGP 設定を確認します。
ステップ 11	`Switch# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

BGP ルーティング プロセスを削除するには、**no router bgp** *autonomous-system-number* グローバル コンフィギュレーション コマンドを使用します。ルーティング特性を削除するには、コマンドにキーワードを指定してこのコマンドを使用します。

VRF-Lite の設定例

図 40-2 は、図 40-1 と同じネットワークの物理接続を単純化した例です。VPN1、VPN2、およびグローバル ネットワークで使用されるプロトコルは OSPF です。CE/PE 接続には BGP が使用されます。次の例のコマンドは、CE スイッチ S8 を設定する方法を示し、スイッチ S20 および S11 の VRF 設定、およびスイッチ S8 のトラフィックに関連する PE ルータ コマンドが含まれます。その他のスイッチの設定のコマンドは含まれていませんが、類似したものになります。

図 40-2　VRF-Lite の設定例



スイッチ S8 の設定

スイッチ S8 上のルーティングをイネーブルにし、VRF を設定します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip routing
Switch(config)# ip vrf v11
Switch(config-vrf)# rd 800:1
Switch(config-vrf)# route-target export 800:1
Switch(config-vrf)# route-target import 800:1
Switch(config-vrf)# exit
Switch(config)# ip vrf v12
Switch(config-vrf)# rd 800:2
Switch(config-vrf)# route-target export 800:2
Switch(config-vrf)# route-target import 800:2
Switch(config-vrf)# exit
```

スイッチ S8 上でループバックおよび物理インターフェイスを設定します。ファスト イーサネット インターフェイス 3/5 は、PE へのトランク接続です。インターフェイス 3/7 および 3/11 は、VPN に接続します。

```
Switch(config)# interface loopback1
Switch(config-if)# ip vrf forwarding v11
Switch(config-if)# ip address 8.8.1.8 255.255.255.0
Switch(config-if)# exit

Switch(config)# interface loopback2
Switch(config-if)# ip vrf forwarding v12
```

```
Switch(config-if)# ip address 8.8.2.8 255.255.255.0
Switch(config-if)# exit

Switch(config)# interface FastEthernet3/5
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# no ip address
Switch(config-if)# exit

Switch(config)# interface FastEthernet3/8
Switch(config-if)# switchport access vlan 208
Switch(config-if)# no ip address
Switch(config-if)# exit

Switch(config)# interface FastEthernet3/11
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# no ip address
Switch(config-if)# exit
```

スイッチ S8 上で使用される VLAN を設定します。VLAN 10 は、CE と PE 間の VRF 11 によって使用されます。VLAN 20 は、CE と PE 間の VRF 12 によって使用されます。VLAN 118 および 208 は、それぞれスイッチ S11 およびスイッチ S20 を含む VPN の VRF に使用されます。

```
Switch(config)# interface Vlan10
Switch(config-if)# ip vrf forwarding v11
Switch(config-if)# ip address 38.0.0.8 255.255.255.0
Switch(config-if)# exit

Switch(config)# interface Vlan20
Switch(config-if)# ip vrf forwarding v12
Switch(config-if)# ip address 83.0.0.8 255.255.255.0
Switch(config-if)# exit

Switch(config)# interface Vlan118
Switch(config-if)# ip vrf forwarding v12
Switch(config-if)# ip address 118.0.0.8 255.255.255.0
Switch(config-if)# exit

Switch(config)# interface Vlan208
Switch(config-if)# ip vrf forwarding v11
Switch(config-if)# ip address 208.0.0.8 255.255.255.0
Switch(config-if)# exit
```

VPN1 および VPN2 に OSPF ルーティングを設定します。

```
Switch(config)# router ospf 1 vrf vl1
Switch(config-router)# redistribute bgp 800 subnets
Switch(config-router)# network 208.0.0.0 0.0.0.255 area 0
Switch(config-router)# exit
Switch(config)# router ospf 2 vrf vl2
Switch(config-router)# redistribute bgp 800 subnets
Switch(config-router)# network 118.0.0.0 0.0.0.255 area 0
Switch(config-router)# exit
```

CE から PE のルーティングに BGP を設定します。

```
Switch(config)# router bgp 800
Switch(config-router)# address-family ipv4 vrf vl2
Switch(config-router-af)# redistribute ospf 2 match internal
Switch(config-router-af)# neighbor 83.0.0.3 remote-as 100
Switch(config-router-af)# neighbor 83.0.0.3 activate
Switch(config-router-af)# network 8.8.2.0 mask 255.255.255.0
Switch(config-router-af)# exit
```

```
Switch(config-router)# address-family ipv4 vrf v11
Switch(config-router-af)# redistribute ospf 1 match internal
Switch(config-router-af)# neighbor 38.0.0.3 remote-as 100
Switch(config-router-af)# neighbor 38.0.0.3 activate
Switch(config-router-af)# network 8.8.1.0 mask 255.255.255.0
Switch(config-router-af)# end
```

スイッチ S20 の設定

CE に接続するように S20 を設定します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip routing
Switch(config)# interface Fast Ethernet 0/7
Switch(config-if)# no switchport
Switch(config-if)# ip address 208.0.0.20 255.255.255.0
Switch(config-if)# exit

Switch(config)# router ospf 101
Switch(config-router)# network 208.0.0.0 0.0.0.255 area 0
Switch(config-router)# end
```

スイッチ S11 の設定

CE に接続するように S11 を設定します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip routing
Switch(config)# interface Gigabit Ethernet 0/3
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# no ip address
Switch(config-if)# exit

Switch(config)# interface Vlan118
Switch(config-if)# ip address 118.0.0.11 255.255.255.0
Switch(config-if)# exit

Switch(config)# router ospf 101
Switch(config-router)# network 118.0.0.0 0.0.0.255 area 0
Switch(config-router)# end
```

PE スイッチ S3 の設定

スイッチ S3（ルータ）上では、次のコマンドはスイッチ S8 への接続だけを設定します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip vrf v1
Router(config-vrf)# rd 100:1
Router(config-vrf)# route-target export 100:1
Router(config-vrf)# route-target import 100:1
Router(config-vrf)# exit

Router(config)# ip vrf v2
```

```
Router(config-vrf)# rd 100:2
Router(config-vrf)# route-target export 100:2
Router(config-vrf)# route-target import 100:2
Router(config-vrf)# exit

Router(config)# ip cef
Router(config)# interface Loopback1
Router(config-if)# ip vrf forwarding v1
Router(config-if)# ip address 3.3.1.3 255.255.255.0
Router(config-if)# exit

Router(config)# interface Loopback2
Router(config-if)# ip vrf forwarding v2
Router(config-if)# ip address 3.3.2.3 255.255.255.0
Router(config-if)# exit

Router(config)# interface Fast Ethernet3/0.10
Router(config-if)# encapsulation dot1q 10
Router(config-if)# ip vrf forwarding v1
Router(config-if)# ip address 38.0.0.3 255.255.255.0
Router(config-if)# exit

Router(config)# interface Fast Ethernet3/0.20
Router(config-if)# encapsulation dot1q 20
Router(config-if)# ip vrf forwarding v2
Router(config-if)# ip address 83.0.0.3 255.255.255.0
Router(config-if)# exit

Router(config)# router bgp 100
Router(config-router)# address-family ipv4 vrf v2
Router(config-router-af)# neighbor 83.0.0.8 remote-as 800
Router(config-router-af)# neighbor 83.0.0.8 activate
Router(config-router-af)# network 3.3.2.0 mask 255.255.255.0
Router(config-router-af)# exit
Router(config-router)# address-family ipv4 vrf vl
Router(config-router-af)# neighbor 83.0.0.8 remote-as 800
Router(config-router-af)# neighbor 83.0.0.8 activate
Router(config-router-af)# network 3.3.1.0 mask 255.255.255.0
Router(config-router-af)# end
```

VRF-Lite ステータスの表示

VRF-Lite の設定およびステータスに関する情報を表示するには、次の作業のいずれかを行います。

コマンド	目的
Switch# **show ip protocols vrf** *vrf-name*	VRF に対応付けられたルーティング プロトコル情報を表示します。
Switch# **show ip route vrf** *vrf-name* [**connected**] [*protocol* [*as-number*]] [**list**] [**mobile**] [**odr**] [**profile**] [**static**] [**summary**][**supernets-only**]	VRF に対応付けられた IP ルーティング テーブル情報を表示します。
Switch# **show ip vrf** [**brief** | **detail** | **interfaces**] [*vrf-name*]	定義された VRF インスタンスに関する情報を表示します。
Switch# **show ip mroute vrf** *instance-name a.b.c.d* | **active** | **bidriectional**| **count** | **dense**| **interface** | **proxy** | **pruned** | **sparse** | **ssm** | **static** | **summary**	定義された VRF インスタンスに関する情報を表示します。

次に、VRF インスタンス内のマルチキャスト ルート テーブル情報を表示する例を示します。

```
Switch# show ip mroute vrf mcast2 234.34.10.18
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group
       V - RD & Vector, v - Vector
Outgoing interface flags: H - Hardware switched, A - Assert winner
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode

(*, 234.34.10.18), 13:39:21/00:02:58, RP 1.1.1.1, flags: BC
  Bidir-Upstream: Vlan134, RPF nbr 172.16.34.1
  Outgoing interface list:
    Vlan45, Forward/Sparse-Dense, 00:00:02/00:02:57, H
    Vlan134, Bidir-Upstream/Sparse-Dense, 13:35:54/00:00:00, H
```

（注） 表示される情報の詳細については、次の URL にある『*Cisco IOS Switching Services Command Reference*』を参照してください。

http://www.cisco.com/en/US/docs/ios/ipswitch/command/reference/isw_book.html