CHAPTER 4

MPLS の設定

Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）では、レイヤ 2（データリンク レイヤ）スイッチングのパフォーマンスおよび機能と、実績のあるレイヤ 3（ネットワーク レイヤ）ルーティングのスケーラビリティを組み合わせることができます。サービス プロバイダーは MPLS を使用することにより、ネットワーク利用率を大幅に高めるという課題を解決すると同時に、既存のネットワーク インフラストラクチャを損なわずにサービスを差別化することができます。MPLS アーキテクチャは柔軟性があり、レイヤ 2 テクノロジーをどのように組み合わせた場合でも利用することができます。MPLS はすべてのレイヤ 3 プロトコルに対してサポートされており、現在のネットワークで一般に提供されるスケーリングよりも優れたスケーリングが可能です。

この章では、次の MPLS 関連機能について説明します。

- MPLS VPN での eBGP および iBGP に関する BGP マルチパス ロード シェアリング（p.4-2）
- 6VPE（p.4-8）
- VRF 単位のセッション制限（p.4-16）
- HDVRF（p.4-22）

MPLS の詳細については、第 3 章「MPLS VPN に対するリモート アクセスの設定」および『*Multiprotocol Label Switching on Cisco Routers*』Release 12.1(3)T フィーチャ モジュールを参照してください。

MPLS VPN での eBGP および iBGP に関する BGP マルチパス ロード シェアリング

ロード シェアリングの概念を使用すると、Cisco 10000 シリーズ ルータで、特定の宛先への最適パスを複数利用できます。最適パスは静的に取得されるか、または RIP、BGP、OSPF、IGRP などの動的プロトコルによって取得されます。IP ルーティング テーブルに格納する最適パス、およびトラフィック転送に使用する最適パスは、最適パス アルゴリズムによって決定されます。

MPLS Virtual Private Network（VPN; バーチャル プライベート ネットワーク）の external Border Gateway Protocol（eBGP）および internal BGP（iBGP）に関する BGP マルチパスロード シェアリング機能を使用すると、MPLS VPN を使用するように設定された BGP ネットワーク内の eBGP および iBGP パスに、マルチパス ロード シェアリングを設定できます。BGP マルチパス ロード シェアリングは、ロード シェアリングの開発機能およびサービス提供機能を向上させます。また、マルチホーム Autonomous System（AS; 自律システム）、およびマルチホーム ネットワークとスタブ ネットワークから eBGP と iBGP パスを両方ともインポートする Provider Edge（PE ; プロバイダー エッジ）ルータに対して有効です。

BGP は許可されている最大数までのパスを導入します（最大許可数は **maximum-paths** コマンドを使用して設定します）。BGP は最適パス アルゴリズムを使用して、1 つのマルチパスを最適パスとして選択し、これを Routing Information Base（RIB）に挿入して、BGP ピアにアドバタイズします。その他のマルチパスも RIB に挿入できますが、最適パスに選択されるパスは 1 つのみです。

（注）　PRE2 に設定可能な最大パス数は 6 です。

Cisco Express Forwarding（CEF; シスコ エクスプレス フォワーディング）はマルチパスを使用してロード シェアリングを実行します。ロード シェアリングはパケット単位、または送信元 / 宛先ペア単位で実行できます。MPLS VPN の eBGP および iBGP に関する BGP マルチパス ロード シェアリング機能は、デフォルトで、Interior Gateway Protovol（IGP）に関してコストが同等でない複数の BGP パスを選択して、不等価コストのロード シェアリングを実行します。この機能をイネーブルにするには、eBGP および iBGP パスをインポートする Virtual Routing And Forwarding（VRF; VPN ルーティングおよび転送）インスタンスが含まれた MPLS VPN をルータに設定します。VRF ごとにマルチパス数を個別に設定できます。

（注）　MPLS VPN の eBGP および iBGP に関する BGP マルチパス ロード シェアリング機能は、既存の発信ルーティング ポリシーの設定パラメータ内で動作します。

MPLS VPN での eBGP および iBGP に関する BGP マルチパス ロード シェアリング機能は、次の項目で説明します。

MPLS VPN での eBGP および iBGP に関する BGP マルチパス ロード シェアリング機能の履歴

Cisco IOS リリース	説明	必要な PRE
12.3(7)XI1	この機能が Cisco 10000 シリーズ ルータに導入されました。	PRE2
12.2(28)SB	この機能が Cisco IOS Release 12.2(28)SB に統合されました。	PRE2
12.2(33)SB	Cisco 10000 シリーズ ルータに IGP 収束アクセラレーション機能が追加されました。	PRE3 および PRE4

MPLS VPN での eBGP および iBGP に関する BGP マルチパス ロード シェアリングの制約事項

MPLS VPN での eBGP および iBGP に関する BGP マルチパス ロード シェアリング機能には、次の制約事項があります。

- Cisco 10000 シリーズ ルータは再帰的ロード シェアリングをサポートしますが、次の制約事項があります。

  再帰的ロード シェアリングでは、パケット転送に必要な情報は少なくとも 2 回検索する必要があります。最初の検索で、最終宛先に到達するために使用される PE ルータが判別されます。2 回めの検索で、（最初に検索された）PE ルータへの到達方法が判別されます。

  MPLS VPN が設定されている場合、CEF は再帰的ロード シェアリングを使用します。最初の検索は VPN ラベルを、2 回めの検索は IGP ラベルを提供します。PXF の場合は、パケットを転送するときに、VPN および IGP ラベルを両方とも提供する検索を 1 回のみ実行します。これは CEF の場合の 2 回の検索が 1 つに結合されたものです。PXF がパケットを転送する場合の再帰的ロード シェアリングの制約事項は、次のとおりです。

  Cisco 10000 シリーズ PE ルータと P ルータ間に複数の IGP パスが存在する場合、タグ単位のロード シェアリングのみがサポートされます。つまり、PXF には 1 つのパスのみがプログラムされ、このパスはラウンドロビン方式で選択されます。このパスはプレフィクス設定時に選択されるため、どのプレフィクスに対してどのパスが選択されるかは、予測できません。選択されたパスは、ルーティング テーブル内でのプレフィクスの設定順序によって決まります。IGP パスの帯域幅は、パス選択時に考慮されません。

（注）　Cisco IOS Release 12.2(33)SB 以降、Cisco 10000 シリーズ ルータでは PRE3 および PRE4 エンジン上で MPLS VPN シナリオの IGP および VPN のロード バランシングをサポートしています。これにより、ロード バランシング時の IGP ルータのフェールオーバーをより高速に行うことができます。

- ルーティング テーブルに複数の iBGP パスが格納されている場合、ルート リフレクタは 1 つのパス（1 つのネクストホップ）のみをアドバタイズします。ルータがルート リフレクタの背後にある場合、VRF ごとにそれぞれ異なるルート識別子（RD）が設定されていないかぎり、マルチホーム サイトに接続されたルータの一部はアドバタイズされません。

- 複数の iBGP パスを持つ BGP プレフィクスに対応する IP ルーティング テーブル エントリは、それぞれ追加メモリを使用します。使用可能なメモリが少ないルータでは（特に、ルータがインターネット ルーティング テーブル全体を伝送している場合）、この機能を使用しないことを推奨します。

MPLS VPN での eBGP および iBGP に関する BGP マルチパス ロード シェアリングの要件

MPLS VPN での eBGP および iBGP に関する BGP マルチパス ロード シェアリング機能には、次の要件があります。

- eBGP および iBGP ルートによるロード シェアリングを設定する前に、MPLS VRF を設定する必要があります。

MPLS VPN での eBGP および iBGP に関する BGP マルチパス ロード シェアリングの設定

MPLS VPN での eBGP および iBGP に関する BGP マルチパス ロード シェアリング機能を設定するには、次の設定作業を行います。

- eBGP および iBGP に関するマルチパス ロード シェアリングの設定（p.4-4）
- eBGP および iBGP に関するマルチパス ロード シェアリングの確認（p.4-5）

eBGP および iBGP に関するマルチパス ロード シェアリングの設定

マルチパス ロード シェアリング用の iBGP および eBGP ルートを設定するには、グローバル コンフィギュレーション モードを開始して、次のコマンドを入力します。

	コマンド	目的
ステップ 1	`Router(config)# router bgp as-number`	BGP プロセスを実行するようにルータを設定し、ルータ設定モードを開始します。
ステップ 2	`Router(config-router)# address-family ipv4 vrf vrf-name`	IPv4 セッション用の VRF インスタンスを設定し、アドレス ファミリ設定モードを開始します。
ステップ 3	`Router(config-router-af)# maximum-paths eibgp number-of-paths`	ルーティング テーブルに導入できるパラレルな iBGP および eBGP ルートの数を設定します。PRE2 に設定可能な最大パス数は 6 です。 （注）**maximum-paths eibgp** コマンドは、アドレス ファミリ IPv4 VRF 設定モードで設定する必要があります。その他のアドレス ファミリ設定モードではこのコマンドを設定できません。

例 4-1 では、IPv4 セッション用の VRF（*main*）を設定し、アドレス ファミリ設定モードで 4 つの eBGP または iBGP パスをマルチパスとして選択するようにルータを設定します。

例 4-1　eBGP および iBGP に関するマルチパス ロード シェアリングの設定

```
Router(config)# router bgp 50
Router(config-router)3 address-family ipv4 vrf main
Router(config-router-af)# maximum-paths eibgp 4
```

eBGP および iBGP に関するマルチパス ロード シェアリングの確認

ロードシェアリング用の iBGP および eBGP ルートが設定されたことを確認するには、特権 EXEC モードで次のいずれかのコマンドを入力します。

コマンド	目的
`Router# show ip bgp vpnv4 all`	BGP データベース内の使用可能な VPNv4 情報をすべて表示します。
`Router# show ip route vrf vrf-name`	VRF インスタンスに関連する IP ルーティング テーブルを表示します。

MPLS VPN での eBGP および iBGP に関する BGP マルチパス ロード シェアリングの設定例

ここでは、次の設定例を示します。

- eBGP および iBGP に関するマルチパス ロード シェアリングの設定例（p.4-5）
- eBGP および iBGP に関するマルチパス ロード シェアリングの確認（p.4-6）

eBGP および iBGP に関するマルチパス ロード シェアリングの設定例

例 4-2 では、アドレス ファミリ設定モードで 6 つの eBGP または iBGP パスをマルチパスとして選択するようにルータを設定します。

例 4-2　eBGP および iBGP に関するマルチパス ロード シェアリングの設定

```
Router(config)# router bgp 100
Router(config-router)# address-family ipv4 vrf vrf-1
Router(config-router-af)# maximum-paths eibgp 6
```

eBGP および iBGP に関するマルチパス ロード シェアリングの確認

例 4-3 に、**show ip bgp vpnv4** コマンドを入力した場合の出力例を示します。出力の 3 行め（Multipath:eiBGP）は、マルチパス ロード シェアリングが有効であることを示します。

例 4-3　eBGP および iBGP に関するマルチパス ロード シェアリングの確認

```
Router# show ip bgp vpnv4 all 10.22.22.0

BGP routing table entry for 10:1:22.22.22.0/24, version 19
Paths: (5 available, best #5)
Multipath:eiBGP
    Advertised to non peer-group peers:
    10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5
    22
        10.0.0.0 (metric 20) from 10.0.0.4 (10.0.0.4)
            Origin IGP, metric 0, localpref 100, valid, internal, multipath
            Extended Community:0x0:0:0 RT:100:1 0x0:0:0
            Originator:10.0.0.2, Cluster list:10.0.0.4
    22
        10.0.0.2 (metric 20) from 10.0.0.5 (10.0.0.5)
            Origin IGP, metric 0, localpref 100, valid, internal, multipath
            Extended Community:0x0:0:0 RT:100:1 0x0:0:0
            Originator:10.0.0.2, Cluster list:10.0.0.5
    22
        10.0.0.2 (metric 20) from 10.0.0.2 (10.0.0.2)
            Origin IGP, metric 0, localpref 100, valid, internal, multipath
            Extended Community:RT:100:1 0x0:0:0
    22
        10.0.0.2 (metric 20) from 10.0.0.3 (10.0.0.3)
            Origin IGP, metric 0, localpref 100, valid, internal, multipath
            Extended Community:0x0:0:0 RT:100:1 0x0:0:0
            Originator:10.0.0.2, Cluster list:10.0.0.3
    22
        10.1.1.12 from 10.1.1.12 (10.22.22.12)
            Origin IGP, metric 0, localpref 100, valid, internal, multipath, best
            Extended Community:RT:100:1
```

eBGP および iBGP に関する BGP マルチパス ロード シェアリングのモニタリングおよびメンテナンス

iBGP および eBGP のマルチパス ロード シェアリング情報を表示するには、特権 EXEC モードで次のいずれかのコマンドを入力します。

コマンド	目的
Router# **show ip bgp all neighbors**	ネイバーとの TCP 接続および BGP 接続に関する情報を表示します。
Router# **show ip bgp vpnv4 all** *ip-prefix*/*length*	MPLS VPN 内のネットワークの属性およびマルチパスを表示します。 *ip-prefix* オプションは IP プレフィクス アドレス（ドット付き 10 進表記）です。*length* オプションはマスク長（0 ～ 32）です。*length* オプションを使用する場合は、スラッシュ記号を含める必要があります。
Router# **show ip bgp vpnv4 all labels**	Network Layer Reachability Information（NLRI; ネットワーク レイヤ到着可能性情報）プレフィクスごとに着信および発信 BGP ラベルを表示します。
Router# **show ip bgp vpnv4 rd** *route-distinguisher*	RD が一致する NLRI プレフィクスを表示します。

コマンド	目的
Router# **show ip bgp vpnv4 all summary**	BGP ネイバーのステータスを表示します。
Router# **show ip bgp vpnv4 vrf** *vrf-name*	指定された VRF インスタンスに関連する NLRI プレフィクスを表示します。
Router# **show ip route vrf** *vrf-name ip-prefix*	MPLS VPN 内のネットワークのルーティング情報を表示します。

6VPE

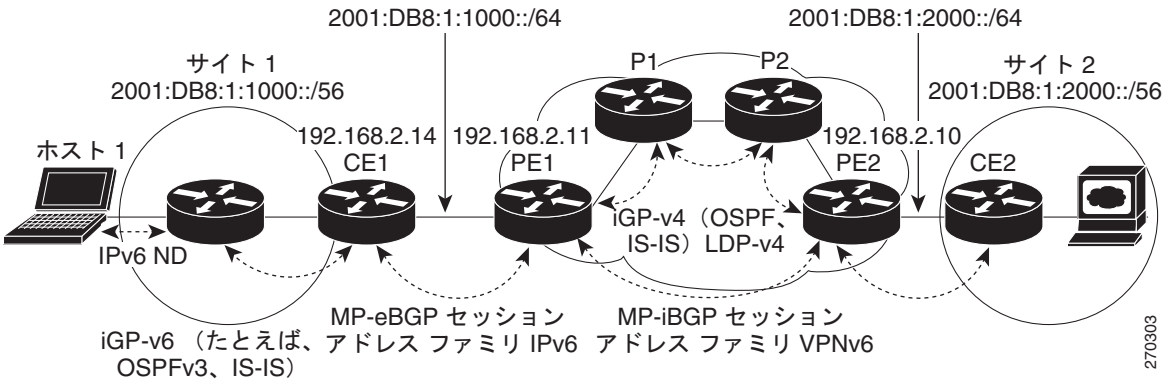
マルチプロトコル BGP は、IPv4 と IPv6 で MPLS IPv6 VPN アーキテクチャの中心となるものです。これは、サービス プロバイダー バックボーンで IPv6 ルートを配布するのに使用され、オーバーラッピング アドレス、再配布ポリシー、およびスケーラビリティ問題と連動する同じ一連のメカニズムを使用します。6VPE 機能は IOS 実装で、RFC 4659 で規定されています。

IPv6 はグローバルな IP Unicast prefix（RFC 3587）または Unicast IPv6 Local Addressing（RFC 4193）を使用することにより、オーバーラッピング アドレス スペースを回避します。マルチプロトコル BGP を使用 してルートを再配布するために、NLRI の 3 タプル 形式（長さ、IPv6 プレフィクス、ラベル）が定義されています。拡張コミュニティ アトリビュート — ルート ターゲット — は、エクスポートされたルートにタグ付けし、インポートされたルートをフィルタリングすることにより、ルーティング情報を再配布するのに使用されます。

スケーラビリティに関しては、ルーティング パスを集約し、PE のフル メッシュを回避するのにルート リフレクタが使用されます。IPv6 の BGP 機能 は、IPv4 の場合と同様で、ルート リフレッシュ、自動ルート フィルタリング、およびアウトバウンド ルート フィルタリングなど、PE ごとに保有されるルート数を削減するのに役立てることができます。

図 4-1 に、IPv6 VPN アーキテクチャの重要な特徴について示します。

図 4-1　単純な IPv6 VPN アーキテクチャ



6VPE 機能については、次の項目で説明します。

- 6VPE の機能履歴（p.4-9）
- 6VPE の実装に関する要件（p.4-9）
- 6VPE の実装に関する制約事項（p.4-9）
- 6VPE の設定作業（p.4-9）
- 6VPE の設定例（p.4-14）
- 6VPE のモニタリングおよびメンテナンス（p.4-16）

6VPE の機能履歴

Cisco IOS リリース	説明	必要な PRE
12.2(33)SB	この機能が Cisco 10000 シリーズ ルータに導入されました。	PRE2、PRE3 および PRE4
12.2(33)SB2	この機能は、Cisco 10000 シリーズ ルータでの AS 間オプションをサポートします。	PRE3 および PRE4

6VPE の実装に関する要件

IPv6 VPN 動作を設定する場合、ネットワーク上で次の Cisco IOS サービスが稼働している必要があります。

- プロバイダー バックボーン ルータ内での MPLS
- プロバイダー ルータおよび VPN PE ルータでの VPN コード付き MPLS
- VPN サービスを提供するすべてのルータでの BGP
- すべての MPLS がイネーブルのルータでの CEF スイッチング
- VPN PE ルータで **ipv6 unicast-routing** コマンドがイネーブルである。

6VPE の実装に関する制約事項

6VPE 機能には次の制約事項があります。

- 6VPE は MPLS IPv4 の信号送信先コアによりサポートされます。MPLS IPv6 の信号送信先コアはサポートされません。
- サポートされる IPv6 VRF の最大数は 2038 です（グローバル ルーティング インスタンスを含む）。ただし、2038 の VRF で、eBGP セッションは 1200 しかサポートされず、残りの VRF はスタティック ルーティングされます。
- すべての IPv6 VRF でサポートされるルートの最小数は、50,000 で（グローバル ルーティング インスタンスを含む）、VRF ごとに約 24 ルートとなります。

6VPE の設定作業

ヒント　12.2(33)SRB リリースでは、6VPE 機能の実装が導入されました。この機能の基本的な情報については、次の URL で、『*Cisco IOS IPv6 Configuration Library*』の「Implementing IPv6 Addressing and Basic Connectivity」を参照してください。
http://www.cisco.com/en/US/docs/ios/12_2t/ipv6/v6addres.html

6VPE では次のリストに示す設定作業があります。これらの作業の詳細については、次の URL で『*Cisco IOS IPv6 Configuration Guide*』Release 12.2SR の「Implementing IPv6 VPN over MPLS (6VPE)」を参照してください。

http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-ov_mpls_6vpe.html

- IPv6 の VRF インスタンスの設定
- インターフェイスへの VRF のバインディング
- PE と CE 間のルーティング用スタティック ルートの設定
- PE と CE 間の eBGP セッションの設定

- iBGP 用 IPv6 VPN アドレス ファミリの設定
- スケーラビリティ向上のためのルート リフレクタの設定
- インターネット アクセスの設定

（注）　**mpls ipv6 vrf** コマンドは、IPv6 の VRF を設定する手順の 1 つとして記載されていましたが、Cisco 10000 シリーズ ルータではサポートしません。

6VPE 機能は、Cisco 10000 シリーズ ルータ上で次の機能の設定もサポートします。

- BGP 機能（p.4-10）
- IPv6 インターネット アクセス（p.4-12）
- VRF 認識ルータ アプリケーション（p.4-12）
- VRF-Lite（p.4-12）
- QoS 機能（p.4-13）

BGP 機能

Cisco 10000 シリーズ ルータでは、6VPE 機能により次の機能がサポートされます。

- Site of Origin（SoO）

  SoO は、デュアルホームの CE の場合にルーティング ループを防止するために使用されます。6VPE 機能では、IPv6 VPN を制御するため、現在 IPv4 VPN でサポートされているのと同じ方法で SoO アトリビュートをサポートします。

  この機能の設定についての詳細は、次の URL で『*EIGRP MPLS VPN PE-CE Site of Origin (SoO)*』の「How to Configure EIGRP MPLS VPN PE-CE Site of Origin (SoO) Support」を参照してください。

  http://www.cisco.com/en/US/docs/ios/12_4/ip_route/configuration/guide/h_mvesoo_ps6350_TSD_Products_Configuration_Guide_Chapter.html#wp1048097

- ASN Override

  グローバルな ASN が指定されている場合、サイトを一意に識別するため、BGP は ASN を自動的に一意の数字に置き換えます。6VPE 機能では、IPv4 VPN で現在サポートされているのと同じ方法で、***[as-override]*** キーワードを使用することにより、ASN Override BGP 機能をサポートします。

- Allow-AS-in

  BGP スピーカーは通常、**AS_PATH** アトリビュート内に自身の ASN を含むアップデートを受信した場合、これを無視します。ハブ & スポーク トポロジの場合、このチェックを省略する必要があります。6VPE 機能では、IPv4 VPN で現在サポートされているのと同じ方法で、**allowas-in** キーワードを使用することにより、Allow-AS-in BGP 機能をサポートします。

- BGP プレフィクス リスト フィルタリング

  6VPE 機能では、設定済みの IPv6 プレフィクスに基づいて、MP-BGP IPv6 アドバタイズメントをフィルタリングする機能をサポートします。

  この機能の設定については、次の URL で『*Cisco IOS IP Configuration Guide*』Release 12.2 の「Configuring BGP」の章で「Configuring BGP Filtering Using Prefix Lists」を参照してください。

  http://www.cisco.com/en/US/docs/ios/12_2/ip/configuration/guide/1cfbgp.html#wp1001470

- BGP AS パス フィルタリング

  6VPE 機能では、設定済みの AS パスに基づいて、MP-BGP IPv6 アドバタイズメントをフィルタリングする機能をサポートします。

  この機能の設定については、次の URL で『*Cisco IOS IP Configuration Guide*』Release 12.2 の「Configuring BGP」の章で「Configuring BGP Path Filtering by Neighbor」を参照してください。

http://www.cisco.com/en/US/docs/ios/12_2/ip/configuration/guide/1cfbgp.html#wp1001644

- BGP 最大プレフィクス

  6VPE 機能では、所定の CE により学習される BGP ルート数の上限をサポートします。6VPE 機能では、IPv4 VPN で現在サポートされているのと同じ方法で、***[maximum-prefix]*** キーワードを使用することにより、Max Prefix BGP 機能をサポートします。

  この機能の設定については、次の URL で『*Cisco IOS IP Configuration Guide*』Release 12.2 の「Configuring BGP」の章で「Configuring BGP」を参照してください。

  http://www.cisco.com/en/US/docs/ios/12_2/ip/configuration/guide/1cfbgp.html

- BGP ルート リフレッシュ

  BGP ルート リフレッシュを使用すると、MP-BGP スピーカー（PE と CE、またはいずれか）は別の BGP スピーカーに MP-BGP のアップデートを再送するよう要求できます。

  この機能の設定については、次の URL で『*Cisco IOS IP Configuration Guide*』Release 12.2 の「Configuring BGP」の章で「Configuring BGP」を参照してください。

  http://www.cisco.com/en/US/docs/ios/12_2/ip/configuration/guide/1cfbgp.html

- AS バウンダリでのルート ターゲットの書き換え

  6VPE 機能では、IPv4 VPN が現在サポートするのと同じ方法で、AS バウンダリでのルート ターゲットの書き換え機能をサポートします。

  この機能の設定についての詳細は、次の URL で『*Cisco IP Solution Center MPLS VPN User Guide*』5.0 の「Inter-AS RT-Rewrite section in the Spanning Multiple Autonomous Systems」を参照してください。

  http://www.cisco.com/en/US/docs/net_mgmt/ip_solution_center/5.0.1/mpls_vpn/user/guide/multauto.html#wp631364

- BGP マルチパス

  6VPE 機能では、eBGP マルチパス、iBGP マルチパス、eiBGP マルチパス、および VPN-IPv6 アドレス ファミリの IPv6 VPN に対する Demilitarized Zone（DMZ; 非武装地帯）リンク帯域幅ベースのロード バランシングをサポートします。ロード バランシングは、VPN-IPv4 アドレス ファミリの IPv4 VPN が現在サポートするのと同じ方法でサポートされます。

（注） 6VPE 機能では、パケット単位のロード シェアリングをサポートしません。

この機能の設定についての詳細は、次の URL で『*BGP Multipath Load Sharing for Both eBGP and iBGP in an MPLS-VPN*』の「How to Configure BGP Multipath Load Sharing for Both eBGP and iBGP in an MPLS-VPN」を参照してください。

http://www.cisco.com/en/US/docs/ios/iproute/configuration/guide/irp_bgp_ebgp_ibgp.html#wp1054087

- VRF 認識 BGP ダンプニング

  6VPE 機能では、IPv4 VPN でサポートされるのと同じ VRF 単位の BGP ダンプニング メカニズムをサポートするため、BGP ダンプニングは VRF ごとに個別に制御されます。

  この機能の設定については、次の URL で『*Cisco IOS IP Routing Protocols Configuration Guide*』Release 12.4 の「Configuring Internal BGP Features」の章で「Configuring Route Dampening」を参照してください。

  http://www.cisco.com/en/US/docs/ios/12_4/ip_route/configuration/guide/1cfbgph.html#wp1002395

IPv6 インターネット アクセス

ほとんどの VPN サイトでは、インターネットへのアクセスが必要となります。IPv6 VPN では、VPN のインターネット アクセスをイネーブルにするため、次のインターネット アクセス モデルをサポートします。

- モデル 1：非 VRF インターネット アクセスの場合

  一部の VPN では、1 つまたは複数のサイトで、非 VRF インターフェイスに付加されたファイアウォールなどのインターネット ゲートウェイを使用して、Internet Service Provider（ISP; インターネット サービス プロバイダー）へのインターネット アクセスを取得できます。ISP は、VPN サービスを提供している Service Provider（SP; サービス プロバイダー）と同じ組織である場合もそうでない場合もあります。インターネット ゲートウェイとの間のトラフィックは、PE ルータのデフォルトのフォワーディング テーブルに応じてルーティングされます。

- モデル 2：一部の VPN は、VRF インターフェイスを介してインターネット アクセスを取得する場合があります。

  PE が VRF インターフェイス上でパケットを受信し、そのパケットの宛先アドレスが VRF 内のいずれのルートにも一致しない場合、パケットは PE のデフォルト フォワーディング テーブルに照合されます。パケットが PE のデフォルトのフォワーディング テーブルに一致した場合は、MPLS によって転送されるのではなく、インターネットへのバックボーンを介して何も使用せずに転送されます。このモデルでは、デフォルトのフォワーディング テーブルにインターネット ルートのフルセットが装備されているか、または同様の装備を持つ別のルータに接続された単一のデフォルト ルートがあるか、いずれかです。

- モデル 3：IPv6 グローバル テーブルにより解決できる VRF 内のスタティック ルートの使用。

  IPv6 グローバル テーブルでは、現在 IPv4 VPN でサポートされているのと同じ方法で VRF のスタティック ルートを解決することができます。すなわち、IPv6 VRF では、ネットワーク管理者は、CE からインターネットへのアウトバウンド トラフィック用の IPv6 インターネット ゲートウェイに接続されたスタティック ルートをデフォルト ルートとして追加できます。

- モデル 4：VRF 内のすべてのインターネット ルート

  インターネット ルートを含む VRF では、VRF インターフェイスを介してインターネット アクセスを取得できます。このモデルには VRF へのインターネット ルートの再配布が含まれます。

VRF 認識ルータ アプリケーション

Cisco 10000 シリーズ ルータでは、6VPE 機能により次の機能がサポートされます。

- VRF 認識 PING

  VRF 認識 PING **ping vrf** [*VRF name*] [*IPv6-address*] コマンドがサポートされます。

- VRF 認識 Traceroute

  VRF 認識 Traceroute **traceroute vrf** [*VRF name*] [*IPv6-address*] コマンドがサポートされます。

- VRF 認識 Telnet

  VRF 認識 Telnet **telnet vrf** [*VRF name*] [*IPv6-address*] コマンドがサポートされます。

VRF-Lite

VRF-Lite（マルチ VRF CE とも呼ばれる）は、CE ルータ上に複数のルーティング インスタンスがある IP ルーティングの拡張機能です。VRF-Lite の機能は、次のとおりです。

- 各 VPN カスタマーの IP ルーティング テーブルと IP フォワーディング テーブルを別々に維持することにより、レイヤ 3 VPN サービスを可能にします。
- 入力インターフェイスを使用して、ルートとその他の VPN を区別します。
- 1 つまたは複数のインターフェイスを各 VRF に対応付けることにより、仮想パケット フォワーディング テーブルを形成します。いかなる場合も、インターフェイスは複数の VRF に属することはできません。

- 異なる VRF 間のオーバーラッピング ユニキャスト IP アドレスをサポートします。

VRF-lite は通常、Customer Edge（CE; カスタマー エッジ）の MPLS VPN とともに導入され、1 つのスイッチ上の複数のカスタマーをサポートします。6VPE 機能では、IPv4 VPN が現在サポートするのと同じ方法で、VRF-lite 機能をサポートします。

QoS 機能

Cisco 10000 シリーズ ルータでは、6VPE 機能により次の機能がサポートされます。

- 入力 PE 上の DiffServ

  6VPE 機能では、入力 PE 上で、現在 IPv4 VPN でサポートされているのと同じ QoS（Quality of Service）メカニズムを IPv6 VPN でサポートします。
- 出力 PE 上の DiffServ

  6VPE 機能では、出力 PE 上で、現在 IPv4 VPN でサポートされているのと同じ QoS メカニズムを IPv6 VPN でサポートします。
- FRF.12

  6VPE では、PE から CE へのフレームリレー接続上で、IPv4 トラフィックのほかに IPv6 トラフィックの FRF.12 フラグメンテーションとインターリービングをサポートします。

  設定作業については、次の URL で『*Cisco 10000 Series Router Quality of Service Configuration Guide*』の「Fragmenting and Interleaving Real-Time and Nonreal-Time Packets」を参照してください。

  http://www.cisco.com/en/US/docs/routers/10000/10008/configuration/guides/qos/10qlfi.html#wp1043021

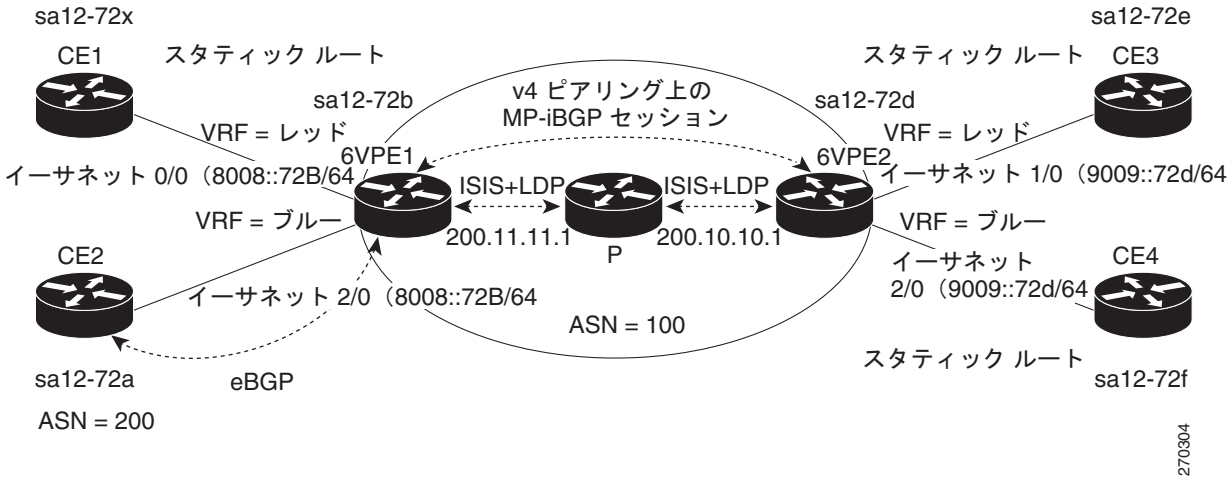
（注） IPv6 パケットが IPv6 用に設定された入力インターフェイスに着信する場合、パケットに Differentiated Services Code Point（DSCP; DiffServ コード ポイント）値のセットがあるか、DSCP 値をマーキングするように IPv6 QoS のセットアップがルータ上で行われます。MPLS 出力インターフェイスを介して送信されるこのパケットは、MPLS Experimental（EXP）ビットにマッピングされる DSCP 値を受け取ります。マッピングにより、IPv6 QoS 値は対応する MPLS に伝播されます。

ヒント IPv4 MPLS コア ネットワークの設定については、次の URL で『*Configuring a Basic MPLS VPN*』を参照してください。
http://www.cisco.com/en/US/tech/tk436/tk428/technologies_configuration_example09186a00800a6c11.shtml

6VPE の設定例

図 4-2 は、次に続く例 4-4 について説明しています。

図 4-2　6VPE



例 4-4　6VPE の設定

```
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname sa14-72b
!
logging snmp-authfail
logging queue-limit 100
!
clock timezone GMT 0
ip subnet-zero
ip cef
!
ipv6 unicast-routing
vrf definition blue
 rd 200:1
 address-family ipv6
 route-target export 200:1
 route-target import 200:1
 exit-address-family
!
vrf definition red
 rd 100:1
 address-family ipv6
 route-target export 100:1
 route-target import 100:1
 exit-address-family
!
ipv6 cef
mpls ldp logging neighbor-changes
mpls ldp router-id Loopback0
!
!
interface Loopback0
```

```
 ip address 200.11.11.1 255.255.255.255
 ipv6 address BEEF:11::1/64
 ipv6 nd prefix default 0 0 off-link no-autoconfig
 no ipv6 mfib fast
!
interface Ethernet0/0
 vrf forwarding red
 ip address 50.1.1.2 255.255.255.0
 no ip route-cache
 no ip mroute-cache
 ipv6 address 4000::72B/64
 ipv6 address 8008::72B/64
 ipv6 nd prefix default infinite infinite
 no ipv6 mfib fast
!
interface Ethernet1/0
 ip address 40.1.1.2 255.255.255.0
 ip router isis
 no ip mroute-cache
 mpls ip
!
interface Ethernet2/0
 vrf forwarding blue
 ip address 90.1.1.2 255.255.255.0
 ipv6 address 8008::72B/64
 no ipv6 mfib fast
!
router isis
 net 49.0000.0000.0002.00
 redistribute connected metric 50
 passive-interface Loopback0
!
router bgp 100
 bgp log-neighbor-changes
 neighbor 200.10.10.1 remote-as 100
 neighbor 200.10.10.1 update-source Loopback0
 neighbor 8008::72a remote-as 200
 !
 address-family ipv4
 neighbor 200.10.10.1 activate
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family ipv4 multicast
 no auto-summary
 exit-address-family
 !
 address-family vpnv6
 neighbor 200.10.10.1 activate
 neighbor 200.10.10.1 send-community extended
 exit-address-family
 !
 address-family ipv6 vrf red
 no synchronization
 redistribute connected
 exit-address-family
 !
 address-family ipv6 vrf blue
 neighbor 8008::72a activate
 no synchronization
 redistribute connected
 exit-address-family
!
ip classless
no ip http server
!
end
```

6VPE のモニタリングおよびメンテナンス

6VPE のモニタリングおよびメンテナンスの情報については、次の URL で『*Cisco IOS IPv6 Configuration Guide, Release 12.4T*』の「Implementing IPv6 VPN over MPLS (6VPE)」の章で「Verifying and Troubleshooting IPv6 VPN」を参照してください。

http://www.cisco.com/en/US/docs/ios/12_2t/ipv6/SA_vpnv6_ps6441_TSD_Products_Configuration_Guide_Chapter.html#wp1078529

VRF 単位のセッション制限

VRF 単位のセッション制限機能を使用すると、特定の Virtual Private Dialup Network（VPDN; バーチャル プライベート ダイヤルアップ ネットワーク）テンプレートに関連付けられた VPDN グループに対して確立できるセッション数を制限することができます。従来は、ルータに設定されたすべての VPDN グループを単一のテンプレートに関連付けていました。VRF 単位のセッション制限機能を使用することにより、複数の VPDN テンプレート（デフォルト VPDN テンプレートを含む）を作成したり、定義したり、名前をつけることができます。その後、特定の VPDN テンプレートに VPDN グループを関連付けることができます。VPDN テンプレートのグループ セッション制限を設定することにより、VPDN テンプレートに関連付けられたすべての VPDN グループに許可されている同時セッションの最大数を制限することができます。

デフォルト VPDN テンプレート（名前のない VPDN テンプレート）にグループ セッション制限を設定した場合は、名前付きの VPDN テンプレートに関連付けられていないすべての VPDN グループで、セッション制限が同じになります。現在アクティブなセッション数よりも小さいグループ セッション制限を設定した場合、セッションは終端されず、新しいセッションを開始できません。たとえば、50 のセッションがアクティブである場合に、グループ セッション制限を 30 に設定すると、ルータはアクティブなセッションを終端せず、新しいセッションの開始を許可しません。

VPDN テンプレートに VPDN グループが関連付けられていて、かつ VPDN グループにセッション制限が設定されている場合に、VPDN グループの値が VPDN テンプレートの値よりも小さければ、VPDN グループ セッション制限の値は VPDN テンプレート セッション制限よりも優先します。

VPDN グループを一度に関連付けることができるのは、1 つの VPDN テンプレートのみです。名前付き VPDN テンプレートに VPDN グループを関連付けてから、別の VPDN テンプレートに同じ VPDN グループを関連付けると、VPDN グループは最初の VPDN テンプレートから解除されて、2 番めの VPDN テンプレートに関連付けられます。

まだ設定されていない名前付き VPDN テンプレートに VPDN グループを関連付けた場合、その VPDN グループではシステム デフォルトが使用されます。

session-limit グローバル コンフィギュレーション コマンドは、**group session-limit** VPDN テンプレート設定コマンドよりも優先します。**session-limit** コマンドは、VPDN セッション数を制限し、**group session-limit** コマンドは特定の VPDN テンプレートに関連付けられたすべての VPDN グループに対して許可されている同時セッションの最大数を指定します。

VRF 単位のセッション制限機能については、次の項目で説明します。

VPDN グループへの VPDN パラメータの適用

デフォルトでは、ルータは次の方法で、VPDN グループに VPDN パラメータを適用します。

- 各 VPDN グループに設定された VPDN パラメータは、常にその VPDN グループに適用されます。
- VPDN テンプレート内で設定された VPDN パラメータは、各 VPDN グループ設定で指定されていない設定に適用されます。
- VPDN パラメータのシステム デフォルト設定は、各 VPDN グループまたは VPDN テンプレートに設定されていない設定に適用されます。

no source vpdn-template コマンドを使用して VPDN テンプレートと VPDN グループの関連付けを解除すると、次の方法で VPDN グループに VPDN パラメータが適用されます。

- 各 VPDN グループに設定された VPDN パラメータは、常にその VPDN グループに適用されます。
- VPDN パラメータのシステム デフォルト設定は、各 VPDN グループまたは VPDN テンプレートに設定されていない設定に適用されます。

VPDN テンプレートの設定

VPDN グループの設定に使用できるコマンドの中には、VPDN テンプレートの設定に使用できないものもあります。VPDN テンプレートの設定に使用できるコマンドのリストについては、『*Session Limit Per VRF*』Release 12.2(4)B フィーチャ モジュールの **vpdn-template** コマンド リファレンス ページを参照してください。

VRF 単位のセッション制限機能の履歴

Cisco IOS リリース	説明	必要な PRE
12.2(15)BX	この機能が Cisco IOS Release 12.2(15)BX に統合されました。	PRE2
12.3(7)XI1	この機能が Cisco IOS Release 12.3(7)XI1 に統合されました。	PRE2
12.2(28)SB	この機能が Cisco IOS Release 12.2(28)SB に統合されました。	PRE2

VRF 単位のセッション制限の制約事項

VRF 単位のセッション制限機能には、次の制約事項があります。

- VPDN テンプレートのネストはサポートされていません。VPDN グループを一度に関連付けることができるのは、1 つの VPDN テンプレートのみです。名前付き VPDN テンプレートに VPDN グループを関連付けてから、別の VPDN テンプレートに同じ VPDN グループを関連付けると、VPDN グループは最初の VPDN テンプレートから解除されて、2 番めの VPDN テンプレートに関連付けられます。
- まだ設定されていない名前付き VPDN テンプレートに VPDN グループを関連付けた場合、その VPDN グループではシステム デフォルトが使用されます。

- **session-limit** グローバル コンフィギュレーション コマンドは、**group session-limit** VPDN テンプレート設定コマンドよりも優先します。
- VPDN グループの値が VPDN テンプレートの値よりも小さい場合、VPDN グループ セッション制限は VPDN テンプレート セッション制限よりも優先します。

VRF 単位のセッション制限の要件

VRF 単位のセッション制限機能には、次の要件があります。

- ルータ上で VPDN がイネーブルであり、少なくとも 1 つの VPDN グループが設定されていること。VPDN 設定を確立する前に、ルータに L2TP 接続を行う必要があります。

VRF 単位のセッション制限の設定

Cisco 10000 シリーズ ルータに VRF 単位のセッション制限機能を設定するには、グローバル コンフィギュレーション モードを開始して次のコマンドを入力します。

	コマンド	目的
ステップ 1	`Router(config)# vpdn enable`	ルータ上で VPDN ネットワーキングをイネーブルにして、ローカル データベース内およびリモート認証サーバ上にトンネル定義が存在する場合、これらを参照するようにルータに通知します。
ステップ 2	`Router(config)# vpdn session-limit` *sessions*	ルータに確立できる同時 VPN セッション数を制限します。 *sessions* オプションは、ルータに対して許可する同時 VPN セッション数の最大値です。有効値は、1 ～ 10000 です。
ステップ 3	`Router(config)# vpdn-template` *template-name*	VPDN テンプレートを設定し、VPDN グループ設定モードを開始します。 *template-name* オプションは、VPDN テンプレートの名前です。
ステップ 4	`Router(config-vpdn)# group session-limit` *number*	ステップ 3 で指定した VPDN テンプレートに関連付けられたすべての VPDN グループに対して許可される同時セッションの最大数を指定します。 *number* オプションは、1 ～ 32767 の値です。
ステップ 5	追加の VPDN テンプレートを設定するには、ステップ 2 およびステップ 3 を再度行います。	
ステップ 6	`Router(config-vpdn)# exit`	VPDN グループ設定モードを終了します。
ステップ 7	`Router(config)# vpdn-group` *tag*	VPDN グループを、カスタマーまたは VPDN プロファイルに関連付けます。 *tag* オプションは、VPDN グループの名前です。

ステップ 8	`Router(config-vpdn)# accept-dialin`
	
	or
	
	`Router(config-vpdn)# request-dialout`
		ルータにダイヤルイン要求の受け入れを許可して、VPDN ダイヤルイン受け入れグループ設定モードを開始します。
		
		ルータに L2TP ダイヤルアウト要求の送信を許可して、VPDN ダイヤルアウト要求グループ設定モードを開始します。

	コマンド	目的

ステップ 9	`Router(config-vpdn-acc-in)# protocol protocol`
	
	or
	
	`Router(config-vpdn-req-out)# protocol protocol`
		使用するトンネリング プロトコルを指定します。

ステップ 10	`Router(config-vpdn-acc-in)# exit`
	
	or
	
	`Router(config-vpdn-req-out)# exit`
		VPDN ダイヤルイン受け入れまたは VPDN ダイヤルアウト要求グループ設定モードを終了します。

ステップ 11	`Router(config-vpdn)# source vpdn-template template-name`	指定されていないすべてのパラメータに VPDN テンプレートの設定を使用するように、VPDN グループを設定します。 *template-name* オプションは、VPDN グループに関連付けられた VPDN テンプレートの名前です。
ステップ 12	`Router(config-vpdn)# session-limit session-number`	VPDN グループ上で許可されるセッション数を制限します。 *session-number* オプションは、指定された VPDN グループで許可されているセッションの最大数です。有効値は 0 ～ 32,767 です。
ステップ 13	追加の VPDN グループでセッション数の制限を設定するには、ステップ 7 ～ステップ 12 を再度行います。	

VRF 単位のセッション制限の設定確認

VRF 単位のセッション制限機能の設定を確認するには、特権 EXEC モードで次のコマンドを入力します。

コマンド	目的
`Router# show running-config`	ルータの現在の設定を表示します。このコマンドの出力を調べて、VPDN テンプレート グループの設定を確認します。
`Router# show vpdn session`	すべてのアクティブ トンネルのステータスを表示します。

VRF 単位のセッション制限の設定例

例 4-5 では、VPDN グループ *group1*、*group2*、および *group3* を作成します。VPDN group1 および group2 は、セッション数が 10 に制限されているデフォルト VPDN テンプレートに関連付けられています。VPDN group1 および group2 で使用できる同時セッション数は、合計で 10 のみです。たとえば、group1 に 3 つのセッションがある場合、group2 ではセッションを 7 つしか使用できません。

例 4-5 では、**session-limit 5** コマンドを使用して、VPDN group1 のセッション数を 5 に制限しています。また、**session-limit 20** コマンドを使用して、VPDN group2 のセッション数を 20 に制限しています。ただし、すでに述べたように、デフォルト VPDN テンプレートのセッション制限は 10 です。したがって、VPDN group1 と group2 のセッション数の合計は、10 を超えることができません。group1 に 5 つのセッションがある場合、group2 ではセッションを 5 つしか使用できません。group1 にアクティブなセッションがない場合は、group2 に **session-limit 20** コマンドが設定されていても、group2 は最大 10 のセッションを使用できます。

例 4-5 では、VPDN group3 にセッション制限が設定されていません。**no source vpdn-template** コマンドを使用すると、デフォルト VPDN テンプレートから group3 が解除されます。

例 4-5　VRF 単位のセッション制限の設定

```
vpdn-template
 group session-limit 10
 exit

vpdn-group group2
 accept-dialin
  protocol any
  exit
 session-limit 20
 exit

vpdn-group group1
 accept-dialin
  protocol any
  exit
 session-limit 5

vpdn-group group3
 accept-dialin
  protocol any
  exit
 no source vpdn-template
```

例 4-6 では、デフォルト VPDN テンプレートおよび 3 つの VPDN グループ（groupA、groupB、および groupC）を作成します。デフォルト VPDN テンプレートの設定で述べたように、デフォルト テンプレートに関連付けられたすべての VPDN グループで許可されている合計セッション数の最大値は 10 です。デフォルト VPDN テンプレートのローカル名は local-name です。例 4-6 では、セッション制限が 50 である VPDN テンプレート templateA も作成します。templateA に関連付けられたすべての VPDN グループの合計セッション数は、各 VPDN グループに設定されたセッション制限に関係なく、50 以下になります。VPDN groupA および groupB は VPDN templateA に関連付けられていて、それぞれのセッション数は 30 に制限されています。groupA および groupB は VPDN templateA に関連付けられているため、ローカル名としてホスト名 host1 を使用しています。

例 4-6 では、特定の VPDN テンプレートに VPDN groupC を関連付けるために、**source vpdn-template** コマンドを使用していません。したがって、デフォルトでは、VPDN groupC はデフォルト VPDN テンプレート（グループのセッション制限が 10）に関連付けられています。VPDN groupC は、デフォルト VPDN テンプレートからローカル名 local-name を引き継ぎます。

例 4-6　VRF 単位のセッション制限の設定

```
hostname host1
vpdn-template
 group session-limit 10
 local name local-name
 exit

vpdn-template templateA
 group session-limit 50
 exit

vpdn-group groupA
 accept-dialin
  protocol any
  exit
 source vpdn-template templateA
 session-limit 30
 exit

vpdn-group groupB
 accept-dialin
  protocol any
  exit
 source vpdn-template templateA
 session-limit 30
 exit

vpdn-group groupC
 accept-dialin
  protocol any
```

VRF 単位のセッション制限のモニタリングおよびメンテナンス

VRF 単位のセッション制限機能の監視およびメンテナンスを行うには、特権 EXEC モードで次のコマンドを入力します。

コマンド	目的
Router# **show vpdn session** [**all** [**interface** | **tunnel** | **username**] | **packets** | **sequence** | **state** | timers | **window**]	インターフェイス、トンネル、ユーザ名、パケット、ステータス、ウィンドウ統計情報など、VPDN セッション情報を表示します。 オプションは、次のとおりです。 • **all** — アクティブ セッションのすべてのセッション情報 • **all interface** — 特定のセッションに関連付けられたインターフェイス • **all tunnel** — トンネル アトリビュート フィルタ • **all username** — ユーザ名フィルタ • **packets** — パケットおよびバイト数 • **sequence** — シーケンス番号 • **state** — 各セッションの状態 • **timers** — タイマー情報 • **window** — ウィンドウ情報
Router# **show vpdn**	すべてのアクティブ VPDN トンネルのサマリーを表示します。
Router# **show vpdn group** *name*	指定した VPDN グループのセッション制限セット、およびアクティブなセッション数とトンネル数を表示します。
Router# **show vpdn history failure**	VPDN ユーザ障害に関する情報を表示します。

HDVRF

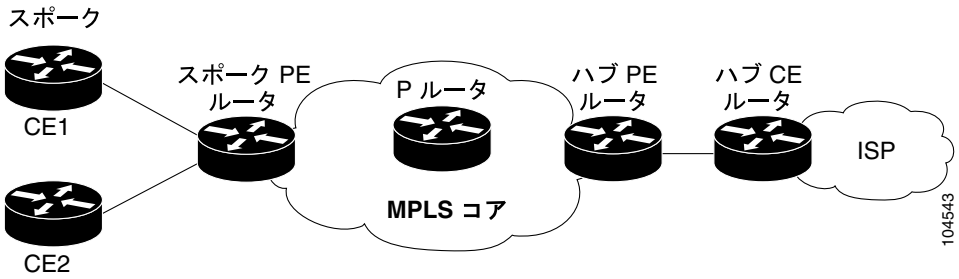
Half-Duplex VRF（HDVRF; 半二重 VRF）機能を使用することにより、MPLS VPN サービスの加入者はスケーラブルなハブ & スポーク接続を実現できます。これらの加入者はホールセール プロバイダーの PE ルータに接続して、同じサービスまたは異なるサービス（同じ VRF または異なる VRF など）を使用します。HDVRF 機能はスポーク PE ルータでの加入者間のローカル接続を禁止して、加入者がハブ サイトで接続されるようにします。同じ PE ルータに接続しているすべてのサイトは、ハブ サイトを使用してサイト間トラフィックを転送する必要があります。これにより、スポーク サイトでのルーティングは、常にアクセス側インターフェイスからネットワーク側インターフェイスに対して、またはネットワーク側インターフェイスからアクセス側インターフェイスに対して実行されます。アクセス側からアクセス側へのルーティングは発生しません。

複数のスポーク CE ルータ（別名スポーク）が同じ PE ルータに接続しているハブ & スポーク トポロジでは、PE ルータはアップストリーム ISP を介してトラフィックを送受信せずに、スポークをローカルにスイッチングします。Cisco IOS Release 12.2(16)BX2 より前のリリースでは、スポークが同じ PE ルータに接続されている場合、スポーク間のトラフィックが常にホールセール サービス プロバイダーと ISP 間の中央リンクを通過するように、各 VRF 内の各スポークを設定する必要がありました。ただし、このソリューションを管理できるのは、スポーク数が比較的少ない場合のみです。多数のスポークが同じ PE ルータに接続されている場合、スポークごとに 1 つの VRF を設定する作業が複雑になったり、メモリ使用率が大幅に増加することがあります。この状況は特に、レイヤ 3 VPN への高密度のリモート アクセスをサポートする大規模なホールセール サービス プロバイダー環境で生じます。

HDVRF 機能は、ハブ & スポーク トポロジの従来の制限を解消します。その方法として、スポークごとに VRF が 1 つという要件を解除し、加入者トラフィックがアップストリーム ISP によってリモート ネットワークにルーティングされているか、またはローカルにあるいはリモートに接続された別の加入者にルーティングされているかに関係なく、加入者トラフィックが常にホールセール サービス プロバイダーと ISP 間の中央リンクを通過するようにしています。

図 4-3 に、HDVRF のハブ & スポーク トポロジ例を示します。

図 4-3　HDVRF のハブ & スポーク トポロジ



HDVRF 機能については、次の項目で説明します。

- アップストリームおよびダウンストリーム VRF（p.4-23）
- RPF チェックのサポート（p.4-23）
- HDVRF 用の RADIUS 機能の履歴（p.4-23）
- HDVRF の制約事項（p.4-24）
- HDVRF の要件（p.4-24）
- HDVRF の設定作業（p.4-24）

アップストリームおよびダウンストリーム VRF

HDVRF は 2 つの単一方向 VRF（別名アップストリーム VRF およびダウンストリーム VRF）を使用して、スポークとハブ PE ルータ間で IP トラフィックを転送します。

アップストリーム VRF は、スポークから MPLS VPN バックボーンに IP トラフィックを転送する場合に使用します。この VRF には、通常、デフォルト ルートのみが含まれます。ただし、設定によっては、サマリー ルートや複数のデフォルト ルートなどの情報が含まれることがあります。デフォルト ルートは、アップストリーム ISP に接続しているハブ PE ルータのインターフェイスを指します。Cisco 10000 シリーズ ルータは、ハブ PE ルータまたは Home Gateway（HG; ホーム ゲートウェイ）が送信するルーティング アップデートからデフォルト ルートの情報を動的に取得します。アップストリーム VRF にはスポークが接続している Virtual Access Interface（VAI; バーチャル アクセス インターフェイス）も含まれますが、その他のローカル インターフェイスは含まれません。

ダウンストリーム VRF は、MPLS コアからスポークにトラフィックを転送する場合に使用します。この VRF には、Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）サーバからインポートされたスポークの PPP ピア ルートおよびユーザ単位のスタティック ルートが含まれます。また、ハブ PE ルータからインポートされたルートも含まれます。これらのルートは、特定のサービスに関連付けられた加入者の、動的に割り当てられた VAI です。

Cisco 10000 シリーズ ルータはダウンストリーム VRF から Multiprotocol Border Gateway Protocol（MP-BGP）にルートを再配布します。通常、スポーク PE ルータは、接続されたスポークの MPLS コアを介してサマリー ルートをアドバタイズします。ハブ PE ルータに設定されたアップストリーム VRF は、アドバタイズされたサマリー ルートをインポートします。

RPF チェックのサポート

Reverse Path Forwarding（RPF）チェックを行うと、IP パケットがルータに入るときに、正しい着信インターフェイスを使用するように設定できます。HDVRF 機能はスポーク側インターフェイスでユニキャスト RPF チェックをサポートします。ダウンストリームおよびアップストリーム転送にはそれぞれ異なる VRF が使用されるため、HDVRF はダウンストリーム VRF で送信元アドレス チェックが行われるように RPF メカニズムを拡張します。

HDVRF 用の RADIUS 機能の履歴

Cisco IOS リリース	説明	必要な PRE
12.2(16)BX2	この機能が Cisco 10000 シリーズ ルータに導入されました。	PRE2
12.3(7)XI1	この機能が Cisco IOS Release 12.3(7)XI1 に統合されました。	PRE2
12.2(28)SB	この機能が Cisco IOS Release 12.2(28)SB に統合されました。	PRE2

HDVRF の制約事項

HDVRF 機能には、次の制約事項があります。

- アップストリームおよびダウンストリーム VRF では、HDVRF が設定されたインターフェイス上でルーティング プロトコルがサポートされません。
- HDVRF が適用されるのは、Virtual Access Interface（VAI ; バーチャル アクセス インターフェイス）およびバーチャル テンプレート インターフェイスのみです。サポートされるのは IP アンナンバード インターフェイスのみです。
- Routing with Bridged Encapsulation（RBE）では、HDVRF はサポートされません。

HDVRF の要件

HDVRF 機能には、次の要件があります。

- スポーク PE ルータ上で、Cisco IOS Release 12.2(16)BX2、Cisco IOS Release 12.3(7)XI1、またはそれ以上のリリースが稼働していること
- Performance Routing Engine（PRE）（部品番号 ESR-PRE2）が、ルータのシャーシに搭載されていること

HDVRF の設定作業

HDVRF 機能を設定するには、次の設定作業を行います。

- LAC および PE ルータでのアップストリームおよびダウンストリーム VRF の設定（p.4-24）
- VRF の関連付け（p.4-25）
- RADIUS の設定（p.4-26）

LAC および PE ルータでのアップストリームおよびダウンストリーム VRF の設定

PE ルータにアップストリームおよびダウンストリーム VRF を設定するには、グローバル コンフィギュレーション モードを開始して次のコマンドを入力します。

	コマンド	目的
ステップ 1	`Router(config)# ip vrf vrf-name`	VRF 設定モードを開始し、VRF 名を割り当てて VRF インスタンスを定義します。
ステップ 2	`Router(config-vrf)# rd route-distinguisher`	ルーティングおよび転送テーブルを作成します。
ステップ 3	`Router(config-vrf)# route-target {import | export | both} route-target-ext-community`	指定された VRF に、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 リストを作成します。 **import** キーワードは、アップストリーム VRF を作成する場合に必要です。アップストリーム VRF は、ハブ PE ルータからデフォルト ルートをインポートする場合に使用します。 **export** キーワードは、ダウンストリーム VRF を作成する場合に必要です。ダウンストリーム VRF は、VRF で処理される所定のサービスのすべての加入者のルートをエクスポートする場合に使用します。

例 4-7 に、D という名前のダウンストリーム VRF を設定する例を示します。

例 4-7　ダウンストリーム VRF の設定

```
Router(config)# ip vrf D
Router(config-vrf)# description Downstream VRF - to subscribers
Router(config-vrf)# rd 1:8
Router(config-vrf)# route-target export 1:100
```

例 4-8 に、U という名前のアップストリーム VRF を設定する例を示します。

例 4-8　アップストリーム VRF の設定

```
Router(config)# ip vrf U
Router(config-vrf)# description Upstream VRF - to hub PE
Router(config-vrf)# rd 1:0
Router(config-vrf)# route-target import 1:0
```

VRF の関連付け

PE ルータで VRF の定義および設定を行ったあと、各 VRF を以下のインターフェイスに関連付けます。

- インターフェイスまたはサブインターフェイス
- バーチャル テンプレート インターフェイス

バーチャル テンプレート インターフェイスは、VAI を作成および設定するのに使用されます。バーチャル テンプレート インターフェイスの設定については、「バーチャル テンプレート インターフェイスの設定」（p.3-18）を参照してください。

VRF を関連付けるには、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、PE ルータで次のコマンドを入力します。

	コマンド	目的
ステップ 1	`Router(config-if)# ip vrf forwarding` *vrf-name*	指定された VRF にインターフェイスを関連付けます。 *vrf-name* はインターフェイスに関連付けられた VRF の名前です。
ステップ 2	`Router(config-if)# ip unnumbered` *type number*	インターフェイスに明示的な IP アドレスを割り当てずに、インターフェイスでの IP 処理をイネーブルにします。 *type* および *number* の引数は、IP アドレスが割り当てられたルータ上の他のインターフェイスのタイプおよび番号を示します。このインターフェイスは、他のアンナンバード インターフェイスではありません。 **（注）** Cisco 10000 シリーズ ルータが HDVRF 機能でサポートするのは、非番号インターフェイスのみです。
ステップ 3	`Router(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。

	コマンド	目的
ステップ 4	`Router(config)# interface virtual-template number`	バーチャル テンプレート 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 モードを開始します。
ステップ 5	`Router(config-if)# ip vrf forwarding vrf-name1 [downstream vrf-name2]`	指定された VRF にバーチャル テンプレート インターフェイスを関連付けます。 *vrf-name1* 引数は、バーチャル テンプレート インターフェイスに関連付けられた VRF の名前です。 *vrf-name2* 引数は、PPP ピア ルートおよび AAA サーバからのすべてのユーザ単位ルートが導入されるダウンストリーム VRF の名前です。AAA サーバが使用される場合、VRF メンバーシップは AAA サーバによって提供されます。バーチャル テンプレートに VRF メンバーを設定する必要はありません。

例 4-9 では、vpn1 という名前の VRF に Virtual-Template1 インターフェイスを関連付けて、D という名前のダウンストリームを指定します。

例 4-9　ダウンストリーム VRF とバーチャル テンプレート インターフェイスの関連付け

```
Router(config)# interface Virtual-Template1
Router(config-if)# ip vrf forwarding vpn1 downstream D
Router(config-if)# ip unnumbered Loopback1
Router(config-if)# no peer default ip address
Router(config-if)# ppp authentication chap vpn1
Router(config-if)# ppp authorization vpn1
Router(config-if)# ppp accounting vpn1
```

RADIUS の設定

AAA サーバ用のダウンストリーム VRF を設定するには、次のシスコ アトリビュート値を入力します。

```
cisco-avpair = "ip:vrf-id=vrf-name1 downstream vrf-name2"
```

値は次のとおりです。

vrf-name1 引数は、サブインターフェイスまたはバーチャル テンプレート インターフェイスに関連付けられた VRF の名前です。

vrf-name2 引数は、AAA サーバからのすべての加入者ルートが導入されるダウンストリーム VRF の名前です。

（注）　**lcp:interface-config** RADIUS アトリビュートを使用しないで、**ip:vrf-id** RADIUS アトリビュート（Cisco IOS ソフトウェアでサポートされている場合）を使用することを推奨します。フル バーチャル インターフェイスが使用される **lcp:interface-config** アトリビュートと異なり、**ip:vrf-id** アトリビュートではバーチャル サブインターフェイスが使用されるため、スケーラビリティが大幅に向上します。

例 4-10 に、AAA サーバに D という名前のダウンストリーム VRF を設定する例を示します。

例 4-10　RADIUS でのダウンストリーム VRF の設定

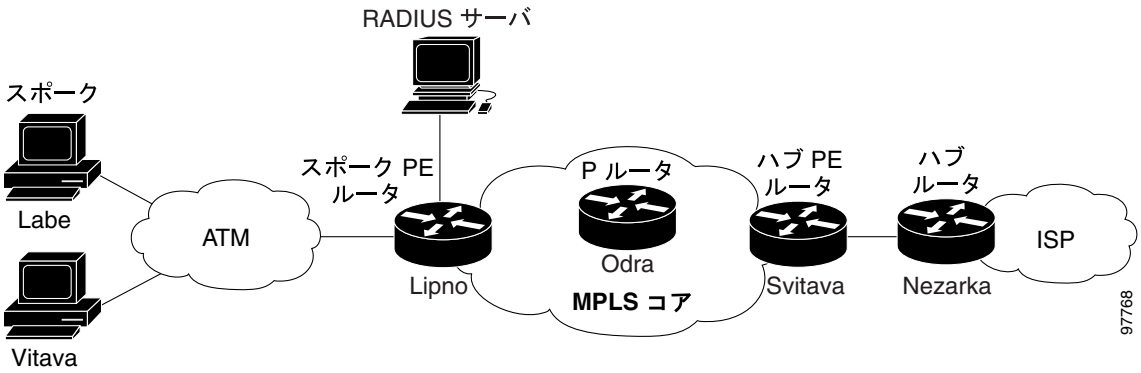
```
cisco-avpair = "ip:vrf-id=U downstream D"
```

HDVRF の設定例

ここでは、次の設定例を示します。これらの例では、図 4-4 のハブ & スポーク トポロジを使用します。

- HDVRF のハブ & スポーク設定例（p.4-27）
- RADIUS の設定例（p.4-28）

図 4-4　半二重トポロジの設定例



HDVRF のハブ & スポーク設定例

例 4-11 に、2 つの PPPoE クライアントをスポーク PE ルータ *Lipno* 上の単一の VRF ペアに接続する例を示します。どちらの PPPoE クライアントも同じ VRF に設定されていますが、すべての通信はハブ PE ルータを使用して行われます。スポーク PE には HDVRF が設定されています。クライアント設定は RADIUS サーバからスポーク PE にダウンロードされます。

例 4-11　スポーク PE ルータの設定

```
aaa new-model
!
aaa group server radius R
 server 22.0.20.26 auth-port 1812 acct-port 1813
!
aaa authentication ppp default group radius
aaa authorization network default group radius
!
ip vrf D
 description Downstream VRF - to spokes
 rd 1:8
 route-target export 1:100
!
ip vrf U
 description Upstream VRF - to hub
 rd 1:0
 route-target import 1:0
```

```
!
vpdn enable
!
vpdn-group U
 accept-dialin
  protocol pppoe
  virtual-template 1
!
interface Loopback0
ip address 100.0.0.8 255.255.255.255
!
interface Loopback2
ip unnumbered Loopback2
 ip vrf forwarding U
 ip address 2.0.0.8 255.255.255.255
!
interface ATM2/0
 pvc 3/100
  protocol pppoe
 !
 pvc 3/101
  protocol pppoe
 !
interface Virtual-Template1
 no ip address
 ppp authentication chap
!
router bgp 1
 no synchronization
 neighbor 100.0.0.34 remote-as 1
 neighbor 100.0.0.34 update-source Loopback0
 no auto-summary
 !
address-family vpnv4
  neighbor 100.0.0.34 activate
  neighbor 100.0.0.34 send-community extended
  no auto-summary
  exit-address-family
 !
 address-family ipv4 vrf U
  no auto-summary
  no synchronization
  exit-address-family
 !
 address-family ipv4 vrf D
  redistribute static
  no auto-summary
  no synchronization
  exit-address-family
!
ip local pool U-pool 2.8.1.1 2.8.1.100
!
radius-server host 22.0.20.26 auth-port 1812 acct-port 1813
radius-server key cisco
```

RADIUS の設定例

例 4-12 に、RADIUS サーバに HDVRF サポートを設定する例を示します。この例では、スポークはデフォルト設定を引き継ぎます。HDVRF がユーザ単位のスタティック ルートをサポートすることを示すために、スポークごとに複数のスタティック ルートが定義されています。HDVRF 機能を使用する場合、スポークごとにスタティック ルートを定義する必要がありません。この設定は、FreeRADIUS 0.8.1 でテストされています。

例 4-12　HDVRF 用の RADIUS の設定

```
DEFAULT Service-Type == Framed-User
        Framed-Protocol = PPP,
        cisco-avpair = "ip:vrf-id=U downstream D",
        cisco-avpair = "ip:ip-unnumbered=Loopback 2",
        cisco-avpair = "ip:addr-pool=U-pool",
        Fall-Through = Yes

labe    Auth-Type := Local, User-Password == "labe"
        cisco-avpair = "ip:route=2.0.0.5 255.255.255.255"

vltava  Auth-Type := Local, User-Password == "vltava"
        cisco-avpair = "ip:route=2.0.0.2 255.255.255.255"
```

（注）　**lcp:interface-config** RADIUS アトリビュートを使用しないで、**ip:vrf-id** RADIUS アトリビュート（Cisco IOS ソフトウェアでサポートされている場合）を使用することを推奨します。フル バーチャル インターフェイスが使用される **lcp:interface-config** アトリビュートと異なり、**ip:vrf-id** アトリビュートではバーチャル サブインターフェイスが使用されるため、スケーラビリティが大幅に向上します。

HDVRF のモニタリングおよびメンテナンス

アップストリームおよびダウンストリーム VRF を監視およびメンテナンスするには、特権 EXEC モードで次のいずれかのコマンドを入力します。

コマンド	目的
Router# **show cef interface virtual-interface** *number* **internal**	VAI に関連付けられたダウンストリーム VRF など、指定された VAI に関する内部情報を表示します。
Router# **show ip interface virtual-interface** *number*	VAI に関連付けられたダウンストリーム VRF など、指定された VAI に関する情報を表示します。
Router# **show ip route vrf** *vrf-name*	指定された VRF に関する IP ルーティング テーブルを表示します。 このコマンドは、ダウンストリーム VRF に導入されたユーザ単位ルートに関する情報を表示する場合に使用します。
Router# **show ip vrf**	関連付けられた各 VAI のダウンストリーム VRF など、ルータに設定されたすべての VRF に関する情報を表示します。
Router# **show ip vrf detail** *vrf-name*	VRF に関連付けられたすべての VAI など、指定された VRF に関する詳細情報を表示します。 *vrf-name* の値を指定しない場合、各 VRF に関連付けられたすべての VAI など、ルータに設定されたすべての VRF に関する詳細情報が表示されます。
Router# **show running-config interface** *type number*	アップストリームおよびダウンストリーム VRF の情報など、指定された VAI に関する情報を表示します。

例 4-13 に、インターフェイス virtual-access 3 に関する情報を表示する例を示します。

例 4-13　show running-config interface — virtual-access 3

```
Lipno# show running-config interface virtual-access 3

Building configuration...

Current configuration : 92 bytes
!
interface Virtual-Access3
 ip vrf forwarding U downstream D
 ip unnumbered Loopback2
end
```

例 4-14 に、インターフェイス virtual-access 4 に関する情報を表示する例を示します。

例 4-14　show running-config interface — virtual-access 4

```
Lipno# show running-config interface virtual-access 4

Building configuration...

Current configuration : 92 bytes
!
interface Virtual-Access4
 ip vrf forwarding U downstream D
 ip unnumbered Loopback2
end
```

例 4-15 に、D という名前のダウンストリーム VRF のルーティング テーブルを表示する例を示します。

例 4-15　show ip route vrf — Downstream

```
Lipno# show ip route vrf D

Routing Table: D
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     2.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
U       2.0.0.2/32 [1/0] via 2.8.1.1
S       2.0.0.0/8 is directly connected, Null0
U       2.0.0.5/32 [1/0] via 2.8.1.2
C       2.8.1.2/32 is directly connected, Virtual-Access4
C       2.8.1.1/32 is directly connected, Virtual-Access3
```

例 4-16 に、U という名前のアップストリーム VRF のルーティング テーブルを表示する例を示します。

例 4-16　show ip route vrf — Upstream

```
Lipno# show ip route vrf U


Routing Table: U
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS interarea
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 100.0.0.20 to network 0.0.0.0

     2.0.0.0/32 is subnetted, 1 subnets
C       2.0.0.8 is directly connected, Loopback2
B*   0.0.0.0/0 [200/0] via 100.0.0.20, 1w5d
```