CHAPTER 2

MPLS VPN の概念

この章では、MPLS の理解に役立つ概念について説明します。次の事項について説明します。

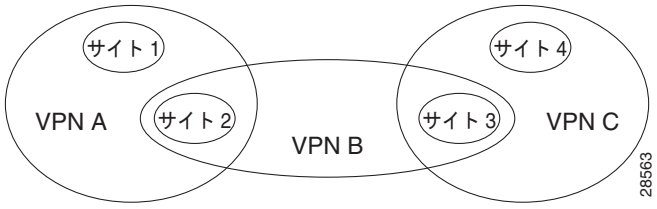
MPLS VPN

Virtual Private Network（VPN; バーチャル プライベート ネットワーク）は、簡単に言うと、同じルーティング テーブルを共有するサイトの集まりです。また、VPN は、プライベート ネットワークと同じ管理ポリシーが適用される共有インフラストラクチャ上で複数のサイトへのカスタマー接続が配置されたネットワークでもあります。VPN 内の 2 つのシステム間のパスとその特性もポリシーによって（全面的または部分的に）決定される場合があります。特定の VPN 内のシステムが別の VPN 内のシステムと通信できるかどうかもポリシーによって決まります。

MPLS VPN では、一般に VPN は MPLS プロバイダー コア ネットワークで相互接続されたサイトで構成されますが、同じサイト内でシステムごとに異なるポリシーを適用することもできます。ダイヤルイン接続のシステムにもポリシーを適用できます。ポリシーは、ダイヤルイン認証プロセスに基づいて選択されます。

一連のシステムを 1 つまたは複数の VPN に加入させることができます。VPN を構成するサイト（またはシステム）は、すべて同じ企業（イントラネット）に属していても、異なる企業（エクストラネット）に属していてもかまいません。また、すべて同じサービス プロバイダー バックボーンに接続されていることもあれば、異なるサービス プロバイダー バックボーンに接続されている場合もあります。

図 2-1　　サイトを共有する VPN



MPLS ベースの VPN は、ピア モデルに基づいてレイヤ 3 に作成されます。ピア モデルによって、従来の VPN よりスケーラビリティが向上し、構築や管理が容易になります。さらに、サービス プロバイダー バックボーンが各 MPLS VPN を安全なコネクションレス型 IP ネットワークとして認識するため、アプリケーションおよびデータのホスティング、ネットワーク商取引、テレフォニー サービスなどの付加価値サービスを特定の MPLS VPN に容易に追加し、運用できます。

MPLS VPN モデルは、各カスタマーの VPN に固有の VPN Routing and Forwarding（VRF; VPN ルーティング / 転送）テーブルを割り当てることによってトラフィックの分離を実行する真のピア VPN モデルです。そのため、VPN 内のユーザは外部のトラフィックを見ることができません。トラフィックの分離は、ネットワークに直接組み込まれるため、トンネリングや暗号化なしで行われます（VRF の詳細については、「VPN ルーティング / 転送テーブル」（P.2-3）を参照してください）。

サービス プロバイダーのバックボーンは、PE とそのプロバイダー ルータで構成されます。MPLS VPN では、特定の VPN のルーティング情報をその VPN に接続された PE ルータ*だけ*に配置できます。

MPLS VPN の特性

MPLS VPN には、次の特性があります。

- Multiprotocol Border Gateway Protocol（MP-BGP; マルチプロトコル ボーダー ゲートウェイ プロトコル）拡張を使用して、カスタマー IPv4 アドレス プレフィクスを一意の VPN-IPv4 Network Layer Reachability Information（NLRI; ネットワーク レイヤ着信可能性情報）値にエンコードします。NLRI は MP-BGP では宛先アドレスを表すため、NLRI は「1 つのルーティング単位」と見なされます。IPv4 MP-BGP では、NLRI は BGP4 ルーティング アップデートに含まれるネットワーク プレフィクスとプレフィクスの長さのペアを表します。
- 拡張 MP-BGP コミュニティ属性を使用して、カスタマー ルートの配布を制御します。
- 各カスタマー ルートには、ルートの始点となるプロバイダー エッジ ルータによって割り当てられる MPLS ラベルが関連付けられます。このラベルを利用して、データ パケットを正しい出力カスタマー エッジ ルータに転送します。データ パケットがプロバイダー バックボーンを越えて転送されるときには、2 つのラベルが使用されます。1 つめのラベルはパケットを適切な出力 PE に転送する役割を果たし、2 つめのラベルはその出力 PE がパケットを転送する方法を指定します。
- Cisco MPLS CoS および QoS メカニズムは、カスタマー データ パケット間のサービス差別化をもたらします。
- PE ルータと CE ルータ間のリンクでは、標準 IP フォワーディングが使用されます。

  PE は、各 CE をその CE で使用可能なルートだけが含まれるサイトごとの転送テーブルに関連付けます。

主要テクノロジー

MPLS ベースの VPN の構築を可能にする主要テクノロジーとして、次の 4 つがあります。

- PE 間の Multiprotocol Border Gateway Protocol（MP-BGP; マルチプロトコル ボーダー ゲートウェイ プロトコル）による CE ルーティング情報の伝送
- VPN ルート ターゲット拡張 MP-BGP コミュニティ属性に基づくルート フィルタリング
- MPLS フォワーディングによる PE 間の（サービス プロバイダーのバックボーンを越える）パケット伝送
- 1 つの PE に複数の VPN Routing and Forwarding（VRF; VPN ルーティング / 転送）インスタンスが存在

イントラネットとエクストラネット

VPN 内のすべてのサイトを同じ企業が所有している場合、その VPN は企業*イントラネット*です。VPN 内に複数の企業が所有するサイトがある場合、その VPN は*エクストラネット*です。1 つのサイトが複数の VPN に属することもできます。イントラネットとエクストラネットは、どちらも VPN と見なされます。

接続の基本単位はサイトですが、MPLS VPN アーキテクチャでは、接続をさらに細分化して制御できます。たとえば、サイトの特定のシステムだけに他のサイトへの接続を許可することが望ましい場合があります。つまり、1 つのサイトにおいて、一部のシステムはイントラネットと 1 つ以上のエクストラネットに追加でき、他のシステムはイントラネットだけに追加できるようにすることも可能です。

1 つの CE ルータが複数の VPN に属することは可能ですが、1 つのサイトには 1 つの CE ルータしか存在できません。1 つの CE ルータが複数の VPN に属している場合、それらの VPN のいずれか 1 つがプライマリ VPN と見なされます。一般に、CE ルータのプライマリ VPN は、その CE ルータのサイトがあるイントラネットです。PE ルータは、無制限の数のサイト内の CE ルータに接続でき、それらの CE ルータは同一の VPN に属していても複数の VPN に属していてもかまいません。堅牢性を確保するために、1 つの CE ルータを複数の PE ルータに接続できます。ある VPN に属する CE ルータに隣接する PE ルータは、その VPN に属します。

VPN ルーティング / 転送テーブル

VPN Routing and Forwarding（VRF; VPN ルーティング / 転送）テーブルは、MPLS VPN テクノロジーの主要な要素の 1 つです。VRF は PE にのみ存在します（Multi-VRF CE の場合を除く）。VRF はルーティング テーブル インスタンスであり、1 つの PE に複数の VRF が存在できます。1 つの VPN には、PE 上の 1 つまたは複数の VRF が存在できます。VRF には、特定のサイト群で使用可能なルートが含まれています。VRF には Cisco Express Forwarding（CEF; シスコ エクスプレス フォワーディング）テクノロジーが使用されているため、VPN は CEF 対応であることが必要です。

VRF には次の要素が関連付けられます。

- IP ルーティング テーブル
- Cisco Express Forwarding（CEF; シスコ エクスプレス フォワーディング）テクノロジーに基づく取得された転送テーブル
- 取得された転送テーブルを使用する一連のインターフェイス
- VRF に情報を渡す一連のルーティング プロトコルおよびルーティング ピア

各 PE に 1 つ以上の VRF が存在します。Prime Fulfillment ソフトウェアが適切な VRF でパケットの IP 宛先アドレスを検索するのは、そのパケットがその VRF に関連付けられたインターフェイスから直接到着した場合だけです。いわゆる「カラー」の MPLS ラベルは、宛先 PE に対し、パケットを正しい CE に送り、最終的にローカル ホスト マシンに転送できるように、VRF を調べて適切な VPN を確認するように指示します。

VRF には、対象となる 1 つまたは複数の VPN とトポロジ内の CE のロールに基づく名前が与えられます。VRF 名の形式は次のとおりです。

- ハブの VRF 名：`ip vrf V`*x*`:[`*VPN_name*`]`
- パラメータ *x* は、VRF 名を一意にするための番号です。

たとえば、Blue という VPN がある場合、ハブ CE の VRF には次のような名前が付けられます。

```
ip vrf V1:blue
```

Blue VPN のスポーク CE の VRF には次のような名前が付けられます。

```
ip vrf V1:blue-s
```

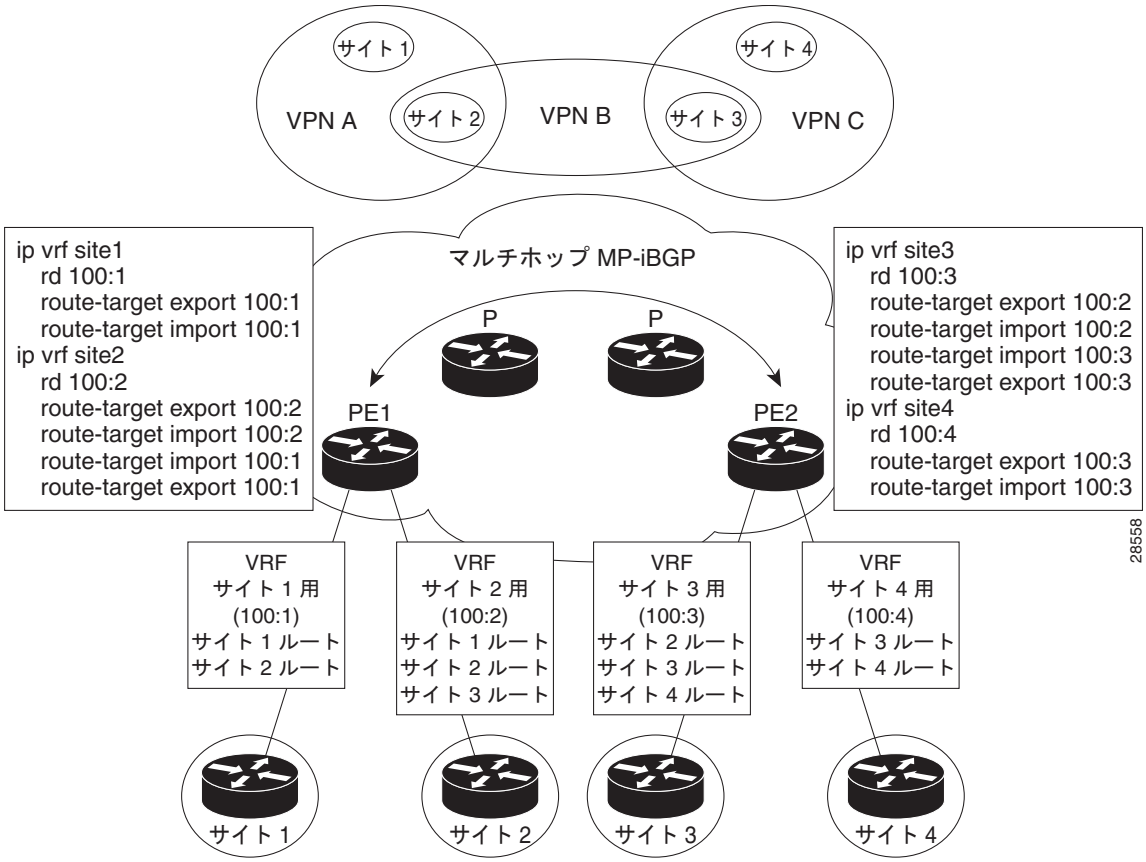
Green VPN 内のエクストラネット VPN トポロジの VRF には次のような名前が付けられます。

```
ip vrf V1:green-etc
```

このように、VRF 名から VPN 名とトポロジ タイプを特定できます。

図 2-2 は、4 つのサイトのうち 2 つの VPN のメンバであるサイトが 2 つあるネットワークにおいて、各サイトの VRF にどのルートが含まれているかを示しています。

図 2-2　複数の VPN に属するサイトの VRF



VRF 実装

VPN および VRF を実装するときには、次の点に留意してください。

- PE 上のローカル VRF インターフェイスは、従来の考え方では直接接続されたインターフェイスとは見なされません。たとえば、PE 上でファスト イーサネット インターフェイスを特定の VRF/VPN に追加した場合、**show ip route** コマンドを発行したときに、このインターフェイスは直接接続されたインターフェイスとして表示されません。このインターフェイスがルーティング テーブルに含まれていることを確認するには、**show ip route vrf** *vrf_name* コマンドを発行する必要があります。
- グローバル ルーティング テーブルと VRF ごとのルーティング テーブルは、それぞれ独立したエンティティです。Cisco IOS コマンドは、グローバル ルーティング テーブルのコンテキストで IP ルーティングに適用されます。たとえば、`show ip route` や他の EXEC レベルの show コマンド、および **ping**、**traceroute**、**telnet** などのユーティリティは、いずれもグローバル IP ルーティング テーブルを処理する、Cisco IOS ルーチンのサービスを呼び出します。

- CE ルータから標準 Telnet コマンドを発行して PE ルータに接続できます。ただし、PE から CE に接続するためには、その PE から次のコマンドを発行する必要があります。

  telnet *CE_RouterName* **/vrf** *vrf_name*

  同様に、**Traceroute** コマンドと **ping** コマンドも VRF のコンテキストで使用できます。

- MPLS VPN バックボーンは、EIGRP や OSPF など、MPLS 対応に設定された適切な Interior Gateway Protocol（IGP）に依存します。PE 上で **show ip route** コマンドを発行すると、PE 間の IGP-derived ルートが表示されます。それに対し、**show ip route vrf** *VRF_name* コマンドを発行すると、特定の VPN 内のカスタマー サイト間のルートが表示されます。

VRF インスタンス

VRF インスタンスの作成に使用するコンフィギュレーション コマンドは次のとおりです。

	コマンド	説明
ステップ 1	`Router#` **configure terminal** `Router(config)#`	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	`Router(config)#` **ip vrf** *vrf_name*	たとえば、**ip vrf** *CustomerA* は、VPN ルーティング テーブルと、CustomerA という関連する CEF テーブルを開始します。このコマンドは、VRF コンフィギュレーション サブモードを開始し、VRF に関連する変数を設定します。
ステップ 3	`Router(config-vrf)#` **rd** *RD_value*	8 バイトの Route Descriptor（RD; ルート記述子）または IP アドレスを入力します。PE は、IPv4 ルートの先頭に RD を追加してから、そのルートを MPLS VPN バックボーンに再配布します。
ステップ 4	`Router(config-vrf)#` **route-target import | export | both** *community*	VRF のルートターゲット情報を入力します。

独立 VRF オブジェクトの管理

Prime Fulfillment では、独立 VRF オブジェクトに VPN および VRF の情報を指定できます。このオブジェクトは、PE デバイスに配置され、さらに MPLS VPN サービス要求によって MPLS VPN リンクに関連付けられます。この機能の使用方法の詳細については、『*Cisco Prime Fulfillment User Guide 6.1*』を参照してください。

ルート識別子とルート ターゲット

MPLS ベースの VPN では、PE 間の通信に BGP を使用することにより、カスタマー ルートを円滑化します。これは、IPv4 アドレス以外のアドレスを伝送する、BGP の拡張機能によって可能となります。注目すべき拡張機能として、*Route Distinguisher*（RD; ルート識別子）があります。

Route Distinguisher（RD; ルート識別子）の目的は、プレフィクス値をバックボーン内で一意にすることです。同じ一連の Route Target（RT; ルート ターゲット）およびルーティング ポリシーの選択に使用される RT 以外のものに関連付けられたプレフィクスでは、同じ RD を使用する必要があります。対象となるコミュニティの関連付けは、Network Layer Reachability Information（NLRI; ネットワーク

着信可能性情報）とともに配信される Route Target（RT; ルート ターゲット）拡張コミュニティ属性に基づきます。RD 値は、他のプレフィクスとの競合を防ぐためにグローバルに一意な値である必要があります。

MPLS ラベルは BGP ルーティング アップデートの一部です。ルーティング アップデートには、アドレッシング情報と到着可能性情報も含まれています。RD が MPLS VPN ネットワーク内で一意である場合は、異なるカスタマーが一意でない IP アドレスを使用していても接続は正常に確立されます。

RD のためには、全体的なロールが同じであるすべての CE において、同じ名前、RD、および RT 値を持つ VRF を使用する必要があります。RD と RT は、BGP を実行する PE 間のルート交換に*のみ*使用されます。つまり、PE が MPLS VPN の処理を実行するためには、IPv4 ルートについて通常よりフィールド数が多いルーティング情報を交換する必要があります。そうした追加の情報には、RD や RT などが含まれます。

ルート識別子の値は Prime Fulfillment ソフトウェアによって選択されます。

- ハブ接続を持つ CE では、`bgp_AS:`*value* が使用されます。
- スポーク接続を持つ CE では、`bgp_AS:`*value* `+ 1` が使用されます。

各スポークでは、それぞれに固有の RD 値を使用して、CE 間の適切なハブおよびスポーク接続を確立します。そのため、Prime Fulfillment ソフトウェアは、プロビジョニングされたスポークごとに新しい RD を実装します。

Prime Fulfillment によってデフォルトのルート ターゲットが選択されますが、必要であれば、Prime Fulfillment ソフトウェアでルート ターゲットを定義するときに、自動的に割り当てられる RT 値を上書きできます。

ルート ターゲット コミュニティ

MPLS VPN は、VPN ルートターゲット拡張 MP-BGP コミュニティを使用して VPN ルーティング情報の配信を制御します。拡張 MP-BGP コミュニティは、8 オクテット構造の値です。MPLS VPN では、ルートターゲット コミュニティが次のように使用されます。

- MP-BGP に VPN ルートが挿入されると、そのルートに VPN ルートターゲット コミュニティのリストが関連付けられます。通常、このリストは、ルートを取得した VRF に関連付けられているコミュニティ値のエクスポート リストを基に作成されます。
- ルートターゲット コミュニティのインポート リストは、各 VRF に関連付けられています。このリストには、ルートをこの VRF にインポートしてもよいかどうかを判定するために照合する値が定義されています。

  たとえば、ある VRF のインポート リストが {A, B, C} である場合、コミュニティ値が A、B、C のいずれかである VPN ルートは、その VRF にインポートされます。

ルート ターゲット

VPN は、ルート ターゲットと呼ばれるサブセットで構成されます。ルート ターゲットは、VPN 内の CE が相互に通信する方法を示します。つまり、ルート ターゲットは VPN の論理トポロジを表します。Prime Fulfillment を使用すると、ハブとスポークまたはフル メッシュ ルート ターゲットを構築することにより、CE 間のさまざまな VPN トポロジを作成できます。ルート ターゲットは、複雑な VPN トポロジや CE 接続の作成を可能にする構築ブロックです。

最も一般的な VPN の形式は、*ハブアンドスポーク*と *フル メッシュ*です。

- ハブアンドスポーク形式のルート ターゲットでは、1 つまたは数台の CE がハブとして動作し、スポーク CE は、ハブとの間で、またはハブを介して通信し、相互に直接通信することはありません。
- フル メッシュ形式のルート ターゲットでは、各 CE が他のすべての CE と接続されます。

これらの基本的な 2 種類の VPN（フル メッシュとハブアンドスポーク）は、1 つのルート ターゲットで表すことができます。

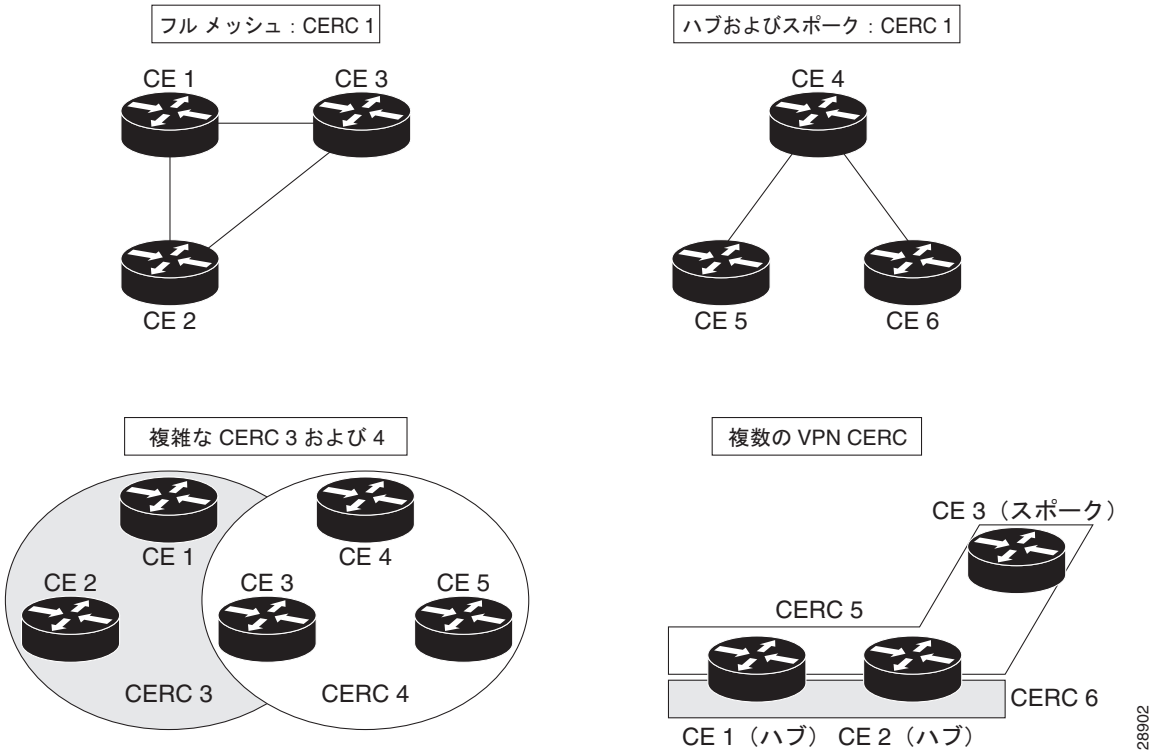
VPN を作成すると、Prime Fulfillment ソフトウェアにより、1 つのデフォルト ルート ターゲットが作成されます。したがって、高度なカスタマー レイアウト方法が必要となるまでは、新しいルート ターゲットを定義する必要はありません。それまでは、ルート ターゲットが VPN それ自体を表していると考えることができます。つまり、ルート ターゲットと VPN は同一のものです。何らかの理由で、ソフトウェアが選択したルート ターゲット値を変更する必要がある場合、その変更は Prime Fulfillment ソフトウェアでルート ターゲットを作成するときにのみ可能です。

きわめて複雑なトポロジを作成するには、CE 間の必要な接続をいくつかのグループに分割する必要があります。このとき、各グループをフル メッシュとハブアンドスポークのいずれかのパターンとします（各グループが 2 つの基本パターンのいずれかであれば、1 つの CE が一度に複数のグループに属していてもかまいません）。VPN 内の各サブグループに固有のルート ターゲットが必要です。1 つのグループだけに属している CE は、対応するルート ターゲットに参加します（必要な場合はスポークとして）。CE が複数のグループに属している場合は、プロビジョニングの実行時に [Advanced Setup] を選択することにより、その CE を 1 回のサービス要求で該当するすべてのグループに追加できます。この情報に基づいてプロビジョニング ソフトウェアが以降の処理を実行し、ルート ターゲット値と VRF テーブルを割り当てることにより、カスタマーの要求に合致した接続を提供します。トポロジ ツールを使用することで、ルート ターゲットのメンバシップと作成される VPN 接続を二重チェックできます。

Prime Fulfillment では、1 つのサイトに複数の CE が存在でき、同じ PE に複数のサイトを接続できます。ルート ターゲットには、それぞれ固有の Route Target（RT; ルート ターゲット）、Route Distinguisher（RD; ルート識別子）、および VRF 名があります。ルート ターゲットをプロビジョニングした後で、監査レポートを実行することにより、ルート ターゲットの配置を検証し、サービス要求によって作成されたトポロジを表示することを推奨します。この製品は、同一 VPN 内での複数ルート ターゲットのリンクをサポートしています。

図 2-3 に、Prime Fulfillment ルート ターゲットで使用できるトポロジの例を示します。

図 2-3　ルート ターゲット トポロジの例



ハブおよびスポークに関する考慮事項

ハブアンドスポーク MPLS VPN 環境では、スポーク ルータに固有の Route Distinguisher（RD; ルート識別子）が必要です。このような環境でハブ サイトを接続の中継点として使用するために、スポーク サイトがルートをハブにエクスポートします。スポークはハブと通信できますが、スポークが他のスポークへのルートを持つことはありません。

現在の MPLS VPN 実装により、スポーク VRF ごとに異なる RD を適用する必要があります。MP-BGP 選択プロセスは、同じ VRF にインポートする必要のあるすべてのルートと、その VRF の RD が同じであるすべてのルートを対象とします。選択プロセスが完了すると、最適なルートだけがインポートされます。この場合、最適なルートであってもインポートされないことがありえます。そのため、カスタマー側ではスポーク VRF ごとに異なる RD が必要です。

フル メッシュに関する考慮事項

各ルート ターゲットには、2 つの異なる RT と、ハブ RT およびスポーク RT がそれぞれ 1 つあります。フル メッシュ トポロジを作成するときには、必ずハブ RT を使用します。したがって、現在のフル メッシュ トポロジにスポーク サイトを追加する必要が生じたときには、ハブ サイトを再構成することなく簡単にスポーク サイトを追加できます。その場合には、既存のスポークを使用できます。これは、ハブアンドスポーク トポロジにフル メッシュ トポロジをリプロビジョニングする必要が生じることへの防止策となります。

MPLS VPN セキュリティ

この項では、MPLS VPN アーキテクチャのセキュリティ要件について説明します。ここでは、「外部」つまりインターネットや接続先の VPN からの攻撃に対するコア ネットワークの防御策に焦点を当てます。

（注）「内部」からの攻撃、つまりコア ネットワークへの論理アクセスまたは物理アクセスを有する者による攻撃に対する防御策については説明しません。内部からのアクセスによる攻撃を受ける可能性は、どのようなネットワークにもあるからです。

アドレス空間とルーティングの分離

MPLS VPN サービスの交差しない 2 つの VPN 間では、異なる VPN 間のアドレス空間が完全に独立していることを前提とします。これは、たとえば、交差しない 2 つの VPN はいずれも干渉のない 10/8 ネットワークを使用できる必要があることを意味します。ルーティングの観点から見ると、これは VPN 内の各エンド システムが固有のアドレスを持ち、そのアドレスへのすべてのルートが同じエンド システムに向かっていることを意味します。具体的には次のとおりです。

- VPN は、他のすべての VPN と同じアドレス空間を使用できる必要があります。
- VPN は、MPLS コアと同じアドレス空間を使用できる必要があります。
- 2 つの VPN 間のルーティングは独立している必要があります。
- VPN とコアとのルーティングは独立している必要があります。

アドレス空間の分離

セキュリティの観点では、基本的な要件は、特定の VPN 内のホスト a.b.c.d を宛先とするパケットが別の VPN またはコア内の同じアドレスを持つホストに到達しないようにすることです。

MPLS では、異なる VPN が同じアドレス空間を使用でき、それはプライベート アドレス空間でもかまいません。そのためには、各 IPv4 ルートに 64 ビットの Route Distinguisher（RD; ルート識別子）を追加し、VPN で一意のアドレスを MPLS コアでも一意にします。この「拡張」アドレスは *VPN-IPv4 アドレス*とも呼ばれます。したがって、MPLS サービスのカスタマーは、それぞれのネットワークで現在のアドレッシングを変更する必要がありません。

CE ルータと PE ルータの間でルーティング プロトコルを使用する場合は、1 つ例外があります（スタティック ルーティングでは問題になりません）。それは、CE ルータとピアになる PE ルータの IP アドレスです。PE ルータとの通信を可能にするためには、CE ルータ上のルーティング プロトコルでコア内のピア ルータのアドレスを設定する必要があります。このアドレスは、CE ルータから見て一意であることが必要です。サービス プロバイダーが CE ルータも Customer Premises Equipment（CPE; 顧客宅内機器）として管理する環境では、これをカスタマーに意識させないことが可能です。

ルーティングの分離

VPN 間でルーティングを分離することもできます。各 PE ルータには、接続されている VPN ごとに異なる Virtual Routing and Forwarding（VRF; 仮想ルーティング/転送）インスタンスがあります。PE ルータ上の各 VRF には、静的に設定されたルートまたは PE ルータと CE ルータの間で実行されるルーティング プロトコルによって、1 つの VPN からのルートが追加されます。結果的に各 VPN が異なる VRF を持つため、PE ルータ上の VPN 間で干渉は発生しません。

MPLS コアから他の PE ルータへの接続で、このルーティングの分離を実現するには、マルチプロトコル BGP に Route Distinguisher（RD; ルート識別子）などの一意の VPN 識別子を追加します。VPN ルートは、コアを越えて MP-BGP によって独占的に交換され、この BGP 情報はコア ネットワークには再配布されず、他の PE ルータにのみ再配布され、再び VPN 固有の VRF に追加されます。このように、MPLS ネットワークを越えるルーティングは VPN ごとに独立しています。

MPLS コア ネットワークを越えるアドレッシングとルーティングの分離により、MPLS は、ATM やフレーム リレーなどの同等のレイヤ 2 VPN と同じセキュリティを提供します。そのように設定しない限り、MPLS コアから他の VPN に侵入することはできません。

MPLS コア構造の隠蔽

MPLS コア ネットワークの内部構造（PE およびプロバイダー ルータ デバイス）は、外部ネットワーク（インターネットまたは接続されている VPN）から見える状態であってはなりません。この要件を満たしていなくてもセキュリティ問題につながるわけではありませんが、一般には、内部アドレッシングやネットワーク構造を外部から見えない状態にしておく方が好都合です。理想的なのは、内部ネットワークの情報を外部に公開しないことです。このことは、MPLS コアと同様にカスタマー ネットワークにも当てはまります。

たとえば、コア ルータに対するサービス拒否攻撃は、攻撃者が IP アドレスを知っている方がはるかに容易になります。アドレスは、わからない場合でも推測できますが、MPLS コア構造が隠されていれば、攻撃はきわめて困難になります。MPLS コアを同等のレイヤ 2 インフラストラクチャ（フレーム リレーや ATM など）と同じように不可視にすることが理想的です。

実際には、さまざまな追加のセキュリティ対策を講じる必要があります。特に重要となるのは、*十分なパケット フィルタリング*です。MPLS は、不要な情報を外部にはもちろん、カスタマー VPN にも公開しません。コア内のアドレッシングは、プライベート アドレスとパブリック アドレスのいずれかで行うことができます。VPN および潜在的にインターネットとのインターフェイスは BGP であるため、内

部情報を公開する必要はありません。PE と CE 間のルーティング プロトコルの場合、必要な情報は PE ルータのアドレスだけです。この情報を公開することが望ましくない場合は、PE と CE の間にスタティック ルーティングを設定できます。これにより、MPLS コアを完全に不可視の状態にできます。

MPLS クラウドへの到達可能性を確保するには、カスタマー VPN がルートを最低でも MPLS コアにアドバタイズする必要があります。これは情報を公開しすぎるように思えますが、MPLS コアが認識できる情報は、個々のホストではなくネットワーク（ルータ）に関するものであり、ある程度、抽象的です。また、VPN-only MPLS ネットワーク（つまり共有インターネット アクセスがない）では、これはカスタマーがある程度サービス プロバイダーを信頼することが求められる既存のレイヤ 2 モデルと同じです。フレーム リレーまたは ATM ネットワークにおいても、VPN に関するルーティング情報がコア ネットワーク上で可視になります。

共有インターネット アクセスのある VPN サービスでは、通常、サービス プロバイダーがそのアップストリームまたはピア プロバイダーにインターネットの利用を望むカスタマーのルートを通知します。

端的に言うと、インターネット アクセスを提供しない純粋な MPLS VPN サービスは、同等のフレーム リレーまたは ATM ネットワークと同様の高い情報隠蔽レベルを有し、アドレッシング情報は第三者やインターネットに公開されません。カスタマーが MPLS コアを介してインターネットにアクセスする場合は、通常のインターネット サービスの場合と同じアドレッシング構造を公開する必要があります。

インターネットとの相互接続がない MPLS ネットワークは、フレーム リレーまたは ATM ネットワークと同じものになります。MPLS クラウドからのインターネット アクセスを可能にするためには、サービス プロバイダーは最低でも 1 つの IP アドレス（ピアリング PE ルータのアドレス）を次のプロバイダー、つまり外部に公開する必要があります。

攻撃に対する防御力

他の VPN へ直接侵入することはできません。しかし、MPLS コアを攻撃し、そこから他の VPN への攻撃を試みることは可能です。MPLS コアに対する攻撃の基本的な方法として次の 2 つがあります。

- PE ルータを直接攻撃する。
- MPLS のシグナリング メカニズム（ほとんどの場合はルーティング）を攻撃する。

基本的な攻撃の種類には、正規のユーザがリソースを使用できなくなる *Denial of Service（DoS; サービス拒否）攻撃*と、リソースへの不正アクセスを目的とする*侵入攻撃*の 2 つがあります。

リソースへの不正アクセスを得る侵入攻撃については、基本的な防御方法として次の 2 つが挙げられます。

- 悪用される可能性のあるプロトコル（ルータへの Telnet など）のセキュリティを強化する。
- ネットワークのアクセス可能性をできるだけ低下させる。その手段としては、パケット フィルタリングと MPLS コア内の IP アドレスの隠蔽を組み合わせます。

サービス拒否攻撃は、最も簡単なケースでは 1 つの IP アドレスがわかっているだけでマシンを攻撃できるため、侵入攻撃より実行が容易です。このような攻撃に対して脆弱ではないことを検証する唯一の方法は、パケット フィルタリングと IP アドレスの ping によってマシンが到達可能ではないことを確認することです。

MPLS ネットワークは、両方の攻撃について、最低でも現在のレイヤ 2 ネットワークと同レベルの保護を提供する必要があります。

MPLS ネットワークの要素を攻撃する場合、まず必要となるのは、その要素、つまり要素の IP アドレスを突き止めることです。前の項で説明したように、MPLS コアのアドレッシング構造を外部に対して隠蔽することができます。これにより、攻撃者がコア内のルータの IP アドレスを突き止めることはできません。攻撃者がアドレスを推測し、そのアドレスにパケットを送信する可能性があります。ただし、MPLS のアドレス分離により、着信パケットはカスタマーのアドレス空間に属していると見なされます。そのため、IP アドレスを推測できたとしても、内部ルータに到達することはできません。これには 1 つだけ例外があります。それは PE ルータのピア インターフェイスです。

ルーティング プロトコルのセキュリティ保護

VPN と MPLS コア間のルーティングには、次の 2 つの設定方法があります。

1. **スタティック**。この場合、PE ルータには各 CE の背後にあるネットワークへのスタティック ルートが設定され、CE には VPN の他の部分に属するネットワークの PE ルータとのスタティック ルート（通常はデフォルト ルート）が設定されます。

   スタティック ルートは、PE ルータの IP アドレスと CE ルータのインターフェイス（serial0 など）のいずれかを接続先とすることができます。

   スタティック ルートの場合、CE ルータは PE ルータの IP アドレスを取得できませんが、何らかの方法で PE ルータに接続し、PE ルータのアドレスを推測して、そのアドレスで PE ルータを攻撃することは可能です。

   CE ルータから PE ルータへのスタティック ルートがあり、その接続先がインターフェイスである場合、CE ルータは、コア ネットワークの IP アドレスはもちろん、PE ルータの IP アドレスも取得する必要はありません。これには、多くの（静的な）設定が必要であるという短所がありますが、セキュリティの観点では他のケースより望ましいと言えます。

2. **ダイナミック**。ルーティング プロトコル（RIP、OSPF、BGP など）を使用して、各ピアリング ポイントにおいて CE と PE の間でルーティング情報を交換します。

他のケースでは、各 CE ルータが最低でも MPLS コア内の PE ルータのルータ ID（RID、ピア IP アドレス）を取得する必要があるため、攻撃の潜在的な標的となります。

実際には、Access Control List（ACL; アクセス コントロール リスト）を使用することにより、CE-PE インターフェイスを介した PE ルータへのアクセスを必要なルーティング プロトコルだけに制限できます。これにより、攻撃対象が BGP などの 1 つのルーティング プロトコルに限定されます。起こりうる攻撃として、大量ルートを送信し、PE ルータをルーティング アップデートであふれさせることがあります。これらの攻撃は、どちらも侵入攻撃ではなくサービス拒否攻撃につながる可能性があります。

このリスクを軽減するには、PE ルータにおいてルーティング プロトコルの安全性を可能な限り高める必要があります。これには、次のようにさまざまな方法があります。

- VRF を使用します。サービス プロバイダーは、VRF を使用することにより、カスタマーが VPN で使用できるルートの数をモニタし、制御できます。ルート数のしきい値（許容されるルート数の 80% など）を超えたときに、VRF が許容限界に近付いていることが syslog メッセージによってサービス プロバイダーに通知されるように設定できます。
- ACL を使用します。CE ルータからのルーティング プロトコルだけを受け入れ、それ以外からのルーティング プロトコルを拒否します。さらに、それ以外のアクセスは、各 PE インターフェイスのインバウンド ACL 内の PE ルータに対して許可してはなりません。

  ACL は、アクセスをルーティング プロトコルのポートだけに制限し、CE ルータからのルーティング プロトコルだけを許可するように設定する必要があります。
- 可能な場合は、ルーティング プロトコルに MD-5 認証を設定します。

  この設定は、BGP、OSPF、および RIP2 で可能です。これにより、パケットがカスタマーのネットワークのうち CE ルータ以外の部分からスプーフされる可能性がなくなります。この設定を行うためには、サービス プロバイダーとカスタマーがすべての CE ルータおよび PE ルータ間の共有秘密に合意する必要があります。ここで問題となるのは、すべての VPN カスタマーについて、この設定が必要になることです。セキュリティ要件が最も厳しいカスタマーについてのみ行ったのでは十分ではありません。

（注） Prime Fulfillment では、ルーティング プロトコルを使用する PE-CE リンクに MD-5 認証をプロビジョニングすることはできません。VPN カスタマーとサービス プロバイダーは、この設定を手動で行う必要があります。

ルーティング プロトコルの MD5 認証は、すべての PE-CE ピアで使用する必要があります。このようなサービス拒否攻撃の発生源は簡単に突き止めることができます。

- 可能であれば、この通信のセキュリティが向上するようにルーティング プロトコルのパラメータを設定します。

  たとえば、BGP では、ルーティング処理における対話の回数を制限する *dampening* を設定できます。また、可能な限り、VRF ごとに受け入れるルートの最大数も設定する必要があります。

簡単に言うと、ある VPN から他の VPN やコアに侵入することはできません。ただし、ルーティング プロトコルを利用して PE ルータにサービス拒否攻撃を仕掛けることは、理論的には可能です。これは、他の VPN に悪影響をもたらす可能性があります。そのため、PE ルータには、きわめて高いレベルのセキュリティ保護が必要であり、特に CE ルータとのインターフェイスには重点的な対策が必要です。

ラベル スプーフィング

前述のアドレスとルーティングの分離を前提とし、攻撃者は自らが所有していないラベルの付いたパケットを挿入することによって他の VPN へのアクセスを取得しようとする可能性があります。これを *ラベル スプーフィング*と呼びます。このような攻撃は、外部（別の CE ルータやインターネット）と MPLS コア内のどちらからも可能です。後者のケース（コア内からの攻撃）については、コア ネットワークが安全な状態で提供されることを前提としているため、ここでは説明しません。

MPLS ネットワーク内では、パケットは IP 宛先アドレスではなく先頭に PE ルータが付いたラベルに基づいて転送されます。攻撃者がパケットの送信元または宛先 IP アドレスを置き換える IP スプーフィング攻撃では、MPLS パケットのラベルをスプーフすることもできます。

CE ルータとそのピアリング PE ルータとのインターフェイスは IP インターフェイスであり、ラベルはありません。CE ルータは、MPLS コアを認識せず、宛先ルータだけを認識します。PE デバイスには、設定に基づいてラベルを選択し、それをパケットの先頭に追加するインテリジェント機能があります。この機能は、すべての PE ルータにおいて、CE ルータおよびアップストリーム サービス プロバイダーへの送信に対して実行されます。MPLS クラウドへのインターフェイスは、すべてラベルのない IP パケットを必要とします。

セキュリティ上の理由から、PE ルータは CE ルータからラベル付きのパケットを受け入れないことが必要です。Cisco ルータは、CE インターフェイスに到着したラベル付きのパケットをドロップするように設計されています。したがって、ラベルが受け入れられないため、偽のラベルを挿入することはできません。サービス プロバイダーが LDP を使用してラベルを配布している場合は、コアのピア ルータ間で MD5 認証を使用することによって追加のセキュリティを実装できます。

MPLS コアに送信されるパケットの IP アドレスがスプーフされる可能性は残ります。ただし、PE ルータでは厳格なアドレッシングの分離が行われ、各 VPN に固有の VRF があるため、IP アドレスがスプーフされたとしても、被害を受けるのはスプーフされたパケットの送信元の VPN だけです。つまり、VPN カスタマーが自らを攻撃する可能性があります。この場合、MPLS によってセキュリティ リスクが高まることはありません。

MPLS コアのセキュリティ保護

ここでは、セキュリティに配慮した MPLS ネットワークの設定に関する推奨事項と考慮事項を示します。

（注） ソリューション全体のセキュリティは、最も脆弱なリンクのセキュリティによって決まります。そのようなリンクとしては、PE と CE との最も脆弱な 1 つの相互接続、セキュリティで保護されていないアクセス サーバ、セキュリティで保護されていない TFTP サーバがあります。

信頼できるデバイス

PE および P デバイス、リモート アクセス サーバ、および AAA サーバは、信頼できるシステムとして扱われます。これには、施設の物理的セキュリティに始まり、アクセス コントロール、安全な設定管理、ストレージなどの問題を含めた強力なセキュリティ管理が必要となります。ネットワーク要素のセキュリティ対策については、資料が豊富にあるため、ここでは詳しく説明しません。

CE ルータは、通常、サービス プロバイダーの完全な管理下にはなく、「信頼できない」デバイスとして扱う必要があります。

PE-CE インターフェイス

PE ルータと CE ルータ間のインターフェイスは、MPLS ネットワークのセキュリティを確保するうえできわめて重要です。PE ルータは、可能な限り情報が公開されないように設定する必要があります。セキュリティの観点から考えると、最善のオプションは、CE ルータとのインターフェイスに番号を付けず、スタティック ルートを設定することです。

パケット フィルタ（アクセス コントロール リスト）は、CE ルータから PE ルータのピアリング インターフェイスへの 1 つのルーティング プロトコルだけを許可するように設定する必要があります。ルータおよび内部サービス プロバイダー ネットワークへの他のトラフィックは、すべて拒否します。これにより、対応するアドレス範囲に送信されるパケットがすべて PE ルータによってドロップされるため、PE および P ルータが攻撃される可能性がなくなります。唯一の例外は、ルーティングを目的とする PE ルータ上のピア インターフェイスです。PE ピア インターフェイスには、別個にセキュリティ対策を施す必要があります。

PE および P ルータでプライベート アドレス空間を使用する場合は、パケット フィルタリングに関するルールが適用されます。つまり、このアドレス範囲に送信されるパケットをすべてフィルタリングする必要があります。ただし、この範囲のアドレスはインターネット経由でルーティングしてはならないため、隣接するネットワークへの攻撃が制限されます。

ルーティング認証

すべてのルーティング プロトコルについて、CE およびインターネット接続への対応する認証オプションを設定する必要があります。具体的には、BGP、OSPF、および RIP2 です。ネットワーク内のピアリング関係は、すべて次のようにセキュリティを強化する必要があります。

- CE-PE リンク：BGP MD-5 認証を使用
- PE-P リンク：LDP MD5 認証を使用
- P-P

これにより、攻撃者がピア ルータをスプーフして偽のルーティング情報を送り込むことを防止できます。共有秘密がクリア テキストで含まれていることが多い（ルーティング プロトコル認証の場合など）コンフィギュレーション ファイルについては、安全な管理が特に重要となります。

CE-PE リンクの分離

複数の CE が共通のレイヤ 2 インフラストラクチャを使用して同じ PE ルータにアクセスする場合（イーサネット VLAN など）、CE ルータはパケットをその PE ルータとの接続を持つ別の VPN に属しているかのようにスプーフすることができます。ルーティング プロトコルのセキュリティを強化するだけでは、通常のパケットには影響しないため、十分ではありません。

この問題を回避するには、CE と PE の間に独立した物理接続を実装することを推奨します。さまざまな CE ルータと PE ルータの間にスイッチを配置することも可能ですが、CE と PE の各ペアを個別の VLAN に配置してトラフィックを分離することを強く推奨します。VLAN でスイッチを使用するとセ

キュリティは向上しますが、スイッチが攻撃を受ける可能性がまったくないわけではありません。したがって、この環境のスイッチは、信頼できるデバイスとして扱い、最高レベルのセキュリティ対策を施す必要があります。

LDP 認証

Label Distribution Protocol（LDP; ラベル配布プロトコル）も MPLS クラウドとの間での MD-5 認証によってセキュリティを強化できます。これにより、ハッカーが偽のルータを送り込んで LDP に参加させることを防止できます。

VPN 間の接続

MPLS は、VPN サービスにおいて VPN 間でのアドレスおよびルーティングの分離を可能にします。ただし、多くの環境では、VPN 内のデバイスが VPN の外部の宛先に到達できる必要があります。その目的としては、インターネット アクセスの確保や、2 つの企業が合併する場合などに 2 つの VPN を結合することなどがあります。MPLS は、完全な VPN 分離を実現するだけでなく、VPN の結合やインターネットへのアクセスも可能にします。

そのために、PE ルータにはさまざまなテーブルがあります。*ルーティング コンテキスト テーブル*は CE ルータに固有のテーブルで、その VPN からのルートだけが含まれています。このテーブルからルートが *VRF*（仮想ルーティング / 転送インスタンス）*ルーティング テーブル*に追加され、それを基に *VRF 転送テーブル*が計算されます。

分離された VPN の場合、VRF ルーティング テーブルには 1 つのルーティング コンテキストからのルートのみが含まれています。VPN を結合するときには、異なる VPN の複数のルーティング コンテキストが 1 つの VRF ルーティング テーブルに統合されます。これにより、2 つまたはそれ以上の VPN を 1 つの VPN に統合できます。この場合、結合するすべての VPN が相互に排他的なアドレッシング空間を保持している必要があります。つまり、アドレス空間全体が対象となるすべての VPN に固有のものであることが必要です。

VPN がインターネット接続を確立する場合にも同じ手順が使用されます。つまり、インターネット VRF ルーティング テーブル（デフォルト ルーティング テーブル）からインターネット アクセスを必要とする VPN の VRF にルートが追加されます。すべてのインターネット ルートを追加する代わりに、デフォルト ルートだけを追加することもできます。この場合、VPN とインターネットにはそれぞれ別個のアドレス空間が必要です。VPN では、他のすべてのアドレスがインターネットで発生するため、プライベート アドレス空間を使用する必要があります。

セキュリティの観点では、結合した VPN は 1 つの論理 VPN のように動作し、前述のセキュリティ メカニズムは結合した VPN と他の VPN の間で機能します。VPN を結合した場合、その内部に固有のアドレス空間が必要ですが、それ以降に追加した VPN でも干渉が発生することなく同じアドレス空間を使用できます。結合した VPN との間で送受信されるパケットを他の VPN に転送することはできません。MPLS のすべての分離機能は、他の VPN に関連して、結合した VPN にも適用されます。

2 つの VPN をこのように結合した場合、2 つの VPN が 1 つの VPN と同じように動作し、それぞれのホストは他方の VPN のホストに到達できます。標準 MPLS 機能では、結合した VPN 間において、分離、ファイアウォーリング、パケット フィルタリングは行われません。また、VPN が MPLS/BGP VPN メカニズムによってインターネット ルートを受け取る場合は、MPLS 機能に加えてファイアウォーリングまたはパケット フィルタリングを実装する必要があります。

MP-BGP セキュリティ機能

Prime Fulfillment MPLS ベースのネットワークのセキュリティは、MP-BGP と IP アドレス解決の組み合わせによって実現されます。さらに、サービス プロバイダーは、VPN が相互に分離されるように設定できます。

マルチプロトコル BGP は、マルチプロトコル拡張とコミュニティ属性によって何と何が通信できるかを定義するルーティング情報配布プロトコルです。VPN メンバシップは、VPN に入る論理ポートに依存します。VPN では、MP-BGP によって一意の Route Distinguisher（RD; ルート識別子）が割り当てられます（「ルート識別子とルート ターゲット」（P.2-5）を参照）。

エンド ユーザは RD を特定できないため、別のアクセス ポートからネットワークに入ってフローをスプーフすることはできません。事前に割り当てられたポートだけが VPN に参加できます。MPLS VPN では、MP-BGP が VPN に関する Forwarding Information Base（FIB; 転送情報ベース）を同じ VPN のメンバだけに配布することにより、論理 VPN トラフィック分離によるネイティブ セキュリティをもたらします。さらに、iBGP PE ルーティング ピアは、iBGP ピアリング関係を確立するときに MD5 シグニチャ オプションを使用して TCP セグメント保護を実行できるため、スプーフされた TCP セグメントが PE ルータ間の iBGP 接続ストリームに送り込まれる可能性がさらに低下します（MD5 シグニチャ オプションの詳細については、RFC 2385 を参照してください）。

VPN をプロビジョニングするときに特定の VPN に各インターフェイスを関連付けるのは、カスタマーではなくサービス プロバイダーです。ユーザは、正しい物理ポートまたは論理ポート上にあり、適切な RD を持っている場合にのみイントラネットまたはエクストラネットに参加できます。これにより、Cisco MPLS VPN に入ることは実質的に不可能となります。

コア内では、OSPF や IS-IS などの標準の Interior Gateway Protocol（IGP）によってルーティング情報が配布されます。プロバイダー エッジ ルータは、LDP を使用してラベルバインディング情報の伝送パスを確立します。外部（カスタマー）ルートのラベル バインディング情報を PE ルータに配布するときには、LDP ではなく 、配布済みの VPN IP 情報へのアクセスが容易な MP-BGP マルチプロトコル拡張が使用されます。

MP-BGP コミュニティ属性によって、到着可能性情報の範囲が制限されます。MP-BGP は、サービス プロバイダー ネットワーク内のすべてのエッジ ルータを更新するのではなく、特定の VPN に属するプロバイダー エッジ ルータだけに FIB テーブルをマッピングします。

IP アドレス解決によるセキュリティ

MPLS VPN ネットワークは、他のネットワークより IP ベースのカスタマー ネットワークと容易に統合できます。MPLS ベースのネットワークにはアプリケーションを認識する機能が組み込まれているため、加入者はイントラネット アプリケーションに変更を加えることなくシームレスにプロバイダー サービスとの相互接続を確立できます。各 VPN に固有識別子があるため、カスタマーは既存の IP アドレス空間を従来どおりに使用できます。

MPLS VPN どうしが互いを認識することはありません。VPN 間でのトラフィックの分離は、各 VPN の論理的に別個の転送テーブルと RD を使用して行われます。着信インターフェイスに基づいて、PE が VPN 内の有効な宛先だけが含まれる転送テーブルを選択します。エクストラネットを作成するには、プロバイダーが VPN 間の到達可能性を明示的に設定します。

PE の転送テーブルには、同じ VPN のメンバのアドレス エントリだけが含まれています。PE は、その転送テーブルに含まれていないアドレスに対する要求は拒否します。VPN ごとに論理的に別個の転送テーブルを実装することにより、各 VPN が共有インフラストラクチャ上に構築されたコネクションレス型プライベート ネットワークになります。

IP により、パケット ヘッダーのアドレスのサイズが 32 ビットに制限されます。VPN IP アドレスによってヘッダーの先頭に 64 ビットが追加され、ルーティング テーブルに従来の IP では転送できない拡張アドレスが作成されます。追加の 64 ビットはルート識別子によって定義され、生成されるルートは 96 ビットの一意のプレフィクスとなります。MPLS は、この問題を解決するためにトラフィックを

ラベルに基づいて転送します。そのため、MPLS を使用することにより、VPN IP ルートをラベルスイッチド パスにバインドできます。PE は、パケット ヘッダーではなくラベルを読み取ります。MPLS は、プロバイダーの MPLS コアを介して転送を管理します。ラベルは有効な宛先にのみ存在するため、これによって MPLS はセキュリティとスケーラビリティの両方をもたらします。

オーバーレイ モデルを使用して仮想回線を提供する場合、データ パケットの出力インターフェイスは、そのパケットの入力インターフェイスの機能でしかありません。そのパケットの IP 宛先アドレスによってバックボーン ネットワーク内のパスが決まることはありません。これにより、VPN において発着信する不正な通信を防止できます。

MPLS VPN では、特定のインターフェイス（またはサブインターフェイス）が受信するすべてのパケットが特定の VPN に属することを規定することにより、まずバックボーンが受信するパケットに特定の VPN が関連付けられます。次に、その VPN に関連付けられた転送テーブルでパケットの IP アドレスが検索されます。その転送テーブル内のルートは、受信されたパケットの VPN に固有のものです。

このように、入力インターフェイスによって出力インターフェイスの候補が決定され、その中からパケットの IP 宛先アドレスに基づいて出力インターフェイスが選択されます。これにより、VPN において発着信する不正な通信を防止できます。

VPN 分離の実現

VPN を他の VPN と適切に分離するためには、次の条件を満たさない限り、プロバイダー ルータが隣接する PE からラベル付きのパケットを受け入れないことが重要です。

- ラベル スタックの最上位のラベルがプロバイダー ルータによって PE デバイスに配布された。
- プロバイダー ルータが、そのラベルの使用によってパケットがバックボーンから出た後にスタックの下位のラベルと IP ヘッダーが検査されることを確認できる。

これらの制限は、パケットがその所属先の VPN 以外の VPN に入ることを防止するために必要です。

PE 内の VRF テーブルは、その PE デバイスに直接接続された CE から到着したパケットにのみ使用され、サービス プロバイダーのバックボーンに属する他のルータから到着したパケットのルーティングには使用されません。その結果、同じシステムへのルートが複数存在する可能性があり、その場合、パケットの伝送ルートは、そのパケットがどのサイトからバックボーンに入るかによって決定されます。したがって、IP ネットワークへのルートは、エクストラネットからのパケット（ファイアウォールに至るルート）とイントラネットからのパケットでは異なる場合があります。