Cisco Prime Fulfillment 動作理論ガイド 6.1

Cisco Prime Fulfillment Theory of Operations Guide 6.1

Text Part Number: OL-24388-01-J

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

Cisco Prime Fulfillment 動作理論ガイド 6.1

CONTENTS

このマニュアルについて

このガイドでは、Cisco Prime Fulfillment 6.1 の概要について説明します。Prime Fulfillment は、高速かつ費用対効果の高い IP サービスを実現するためのキャリアクラスのネットワークとサービス管理を実現します。

Prime Fulfillment を使用することで、迅速な展開機能とエラーのないプロビジョニング機能を備えた、完全な MPLS VPN サービス管理を実現できます。サービス オペレータは、Prime Fulfillment がインストールされているマシン 1 台で作業を開始し、Prime Fulfillment のマスター マシンが処理やモニタリングの負荷を軽減するために使用する処理サーバを追加できます。Prime Fulfillment のマスター マシンは、すべての処理サーバの制御およびモニタリングを行い、ロード バランシングとエラーのないプロビジョニングを実現します。

Prime Fulfillment によってパケットベース サービスの展開作業および管理作業が簡素化されて迅速化されるため、運用効率を高めながら、より短時間で成果に結び付けることができます。組織でのネットワーク展開するに対応した、エンドツーエンドのネットワーク管理ソリューションです。

対象読者

このマニュアルは、ネットワーク上の MPLS VPN、L2 VPN、TEM ソフトウェアおよび診断サービスの構成、プロビジョニング、管理を担当するネットワーク エンジニア、サービス オペレータ、ビジネス マネージャを対象にしています。ネットワーク マネージャおよびオペレータは、次の項目に精通している必要があります。

- インターネットワーキングで使用される基本的な概念と用語
- Layer 2 Virtual Private Network（L2VPN; レイヤ 2 バーチャル プライベート ネットワーク）、Virtual Private LAN Service（VPLS; 仮想専用 LAN サービス）、VPN、Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）、用語、およびテクノロジー
- ネットワーク トポロジおよびプロトコル

関連資料

Cisco Prime Fulfillment のマニュアル セットには、次の Web サイトからアクセスできます。

http://www.cisco.com/en/US/products/sw/netmgtsw/ps4748/tsd_products_support_series_home.html

または

http://www.cisco.com/go/isc

Cisco Prime Fulfillment 6.1 マニュアル セットには次のマニュアルが含まれます。

一般的なマニュアル（この順序で読むことを推奨します）

- 『*Cisco Prime Fulfillment Getting Started and Documentation Guide 6.1*』
  http://www.cisco.com/en/US/docs/net_mgmt/prime/fulfillment/6.1/roadmap/docguide.html
- 『*Release Notes for Cisco Prime Fulfillment 6.1*』
  http://www.cisco.com/en/US/docs/net_mgmt/prime/fulfillment/6.1/release/notes/relnotes.html
- 『*Cisco Prime Fulfillment Installation Guide 6.1*』
  http://www.cisco.com/en/US/docs/net_mgmt/prime/fulfillment/6.1/installation/guide/installation.html
- 『*Cisco Prime Fulfillment User Guide 6.1*』
  http://www.cisco.com/en/US/docs/net_mgmt/prime/fulfillment/6.1/user/guide/prime_fulfill.html
- 『*Cisco Prime Fulfillment 動作理論ガイド 6.1*』
  http://www.cisco.com/en/US/docs/net_mgmt/prime/fulfillment/6.1/theory/operations/guide/theory.html
- 『*Cisco Prime Fulfillment Third Party and Open Source Copyrights 6.1*』
  http://www.cisco.com/en/US/docs/net_mgmt/prime/fulfillment/6.1/third_party/open_source/copyright/Prime_Fulfillment_Third_Party_and_Open_Source_Copyrights61.pdf

API マニュアル

- 『*Cisco Prime Fulfillment API Programmer Guide 6.1*』
  http://www.cisco.com/en/US/docs/net_mgmt/prime/fulfillment/6.1/developer/guide/apipg.html
- 『*Cisco Prime Fulfillment API Programmer Reference 6.1*』
  http://www.cisco.com/en/US/docs/net_mgmt/prime/fulfillment/6.1/developer/reference/xmlapi.zip

（注） すべてのマニュアルは随時更新される*可能性があります*。更新されたすべてのマニュアルは、このマニュアルに記載されている URL で入手できます。

表記法

このガイドでは、次の表記法を使用しています。

書式

このガイドでは、次の書式を使用しています。

- ユーザによる入力および制御は**太字**で表記します。たとえば、「**1234** と入力」や「[Modify Scope] をクリック」のように記載します。
- オブジェクトの属性は*斜体*で表記します。たとえば、「*failover-safe-period* 属性」のように記載します。
- 章や項の相互参照は、青字で表記します。たとえば、「「表記法」（P.vi）を参照してください。」のように記載します。

ナビゲーションと画面

このガイドでは、ナビゲーションと画面について、次の表記法を使用しています。

- Windows システムでは、2 つボタン マウスを使用します。オブジェクトをドラッグ アンド ドロップするには、オブジェクトにカーソルを合わせて左のマウス ボタンをクリックして押したまま、オブジェクトを目的の位置までドラッグします。そして、ボタンを放します。
- Solaris システムでは、3 つボタン マウスを使用します。オブジェクトをドラッグ アンド ドロップするには、オブジェクトにカーソルを合わせて中央のマウス ボタンをクリックして押したまま、オブジェクトを目的の位置までドラッグします。そして、ボタンを放します。
- 画面表示は、使用しているシステムやブラウザによって、このガイドで示す内容とは多少異なる場合があります。
- Web UI ナビゲーション バーのラベルは、割り当てられているアドミニストレータ ロールの権限に応じて、IPv4 または IPv6 と表示されます。手順の説明を簡素化するため、このガイドでは、具体的な説明が必要になる場合を除き、メニュー バーのラベルは汎用的な名称で表しています。たとえば、[Address Space] メニューのラベルは、[Address Space v4] と表示される場合と、[Address Space v6] と表示される場合があります。手順説明では、[Address Space] とだけ示します。

記号

本文中に出てくる記号の意味は次のとおりです。

注意 「*要注意*」の意味です。潜在的なデータの破損や損失を警告しています。

（注） 「*注釈*」です。特筆すべき内容が記載されています。

ワンポイントアドバイス 「*時間を節約できる情報*」です。時間の節約につながる方法を紹介しています。

ヒント 「*役に立つ情報*」です。最適な処置について説明しています。

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

CHAPTER 1

レイヤ 2 VPN の概念

この章では、Prime Fulfillment レイヤ 2 VPN 概念の概要について説明します。内容は、次のとおりです。

レイヤ 2 用語の表記法

Prime Fulfillment のレイヤ 2 サービス プロビジョニングは、Layer 2 Virtual Private Network（L2VPN; レイヤ 2 バーチャル プライベート ネットワーク）サービス、FlexUNI/EVC サービス、および Virtual Private LAN Service（VPLS; 仮想専用 LAN サービス）で構成されます。この項では、これらのサービスに関して Prime Fulfillment および業界で一般に使用される用語を明確にします。

使用されている用語には、次の 3 種類があります。

- 現在の Metro Ethernet Forum（MEF; メトロ イーサネット フォーラム）用語
- 以前の MEF 用語
- Prime Fulfillment 用語（以前の MEF 用語に類似）

MEF 用語の表記法

一般に、L2VPN サービスでは、MEF は 4 つの一般的なイーサネット サービス タイプの構成概念をサポートします。

- Ethernet Line（E-Line; イーサネット回線）。ポイントツーポイントの Ethernet Virtual Circuit（EVC; イーサネット仮想回線）を提供します。
- Ethernet LAN（E-LAN; イーサネット LAN）。マルチポイントツーマルチポイントの EVC を提供します。
- PW コアを有効にした FlexUNI。EPL と EVPL を提供します。
- VPLS コアを有効にした FlexUNI。E-LAN と E-PLAN を提供します。

タイプごとに 2 つのイーサネット サービスを使用できます。これらは、User-to-Network Interface（UNI; ユーザネットワーク インターフェイス）で使用されるサービス ID によって次のように識別されます。

- ポート ベース。All-to-One バンドリング。これらは「専用」と呼ばれます。

- VLAN ベース。これらのサービスは多重化されています。EVC は VLAN ID によって識別されます。これらは「仮想専用」と呼ばれます。

表 1-1 に、上記の関係をまとめます。

表 1-1　イーサネット サービスの定義

サービス タイプ	ポートベース	VLAN ベース
E-Line	Ethernet Private Line（EPL; イーサネット専用回線）	Ethernet Virtual Private Line（EVPL; イーサネット仮想専用回線）
E-LAN	Ethernet Private LAN（EP-LAN; イーサネット専用 LAN）	Ethernet Virtual Private LAN（EVP-LAN; イーサネット仮想専用 LAN）

E-Line サービスと E-LAN サービスに加えて、レイヤ 2 では追加で次の 2 つのサービス タイプを使用できます。

- Frame Relay over MPLS（FRoMLS）
- ATM over MPLS（ATMoMPLS）

MEF はフレーム リレー フォーラムと統合されていますが、現在の MEF マニュアルには、これらのサービス タイプについての説明はありません。

以前は、レイヤ 2 サービスの MEF では、別の用語を使用していました。表 1-3 に、古い用語と最新の用語の対応付けを示します。

表 1-2　MEF イーサネット サービスの用語対応表

現在の MEF 用語	以前の MEF 用語
L2VPN over MPLS Core	
Ethernet Private Line（EPL; イーサネット専用回線）	イーサネット ワイヤ サービス（EWS）
Ethernet Virtual Private Line（EVPL; イーサネット仮想専用回線）	イーサネット リレー サービス（ERS）
ATM over MPLS（ATMoMPLS）	ATM over MPLS（ATMoMPLS）
Frame Relay over MPLS（FRoMPLS）	Frame Relay over MPLS（FRoMPLS）
VPLS over MPLS Core	
Ethernet Private LAN（EP-LAN; イーサネット専用 LAN）	イーサネット ワイヤ サービス（EWS）または イーサネット マルチポイント サービス（EMS）
Ethernet Virtual Private LAN（EVP-LAN; イーサネット仮想専用 LAN）	イーサネット リレー サービス（ERS）または イーサネット リレー マルチポイント サービス（ERMS）
VPLS over Ethernet Core	
Ethernet Private LAN（EP-LAN; イーサネット専用 LAN）	イーサネット ワイヤ サービス（EWS）
Ethernet Virtual Private LAN（EVP-LAN; イーサネット仮想専用 LAN）	イーサネット リレー サービス（ERS）

MEF の表記法についての詳細、およびメトロ イーサネット標準の有用な背景情報については、次の URL にある MEF Web サイトを参照してください。

http://metroethernetforum.org

特に、実用的なメトロ イーサネットの用語および定義については、MEF Web サイトの [Information Center] > [MEF Technical Specifications] に掲載されている資料『*Metro Ethernet Services Definitions Phase 2*』を参照してください。

MEF 用語とネットワーク テクノロジーの対応付け

MEF 用語は、サービスの外見上の特徴を説明します。つまり、User-to-Network Interface（UNI; ユーザネットワーク インターフェイス）デバイスを使用するカスタマーの立場から、サービスがどのように見えるかを説明する用語です。サービスを実装する方法について説明するものではありません。

これらのサービスの実装方法については、次の URL を参照してください。

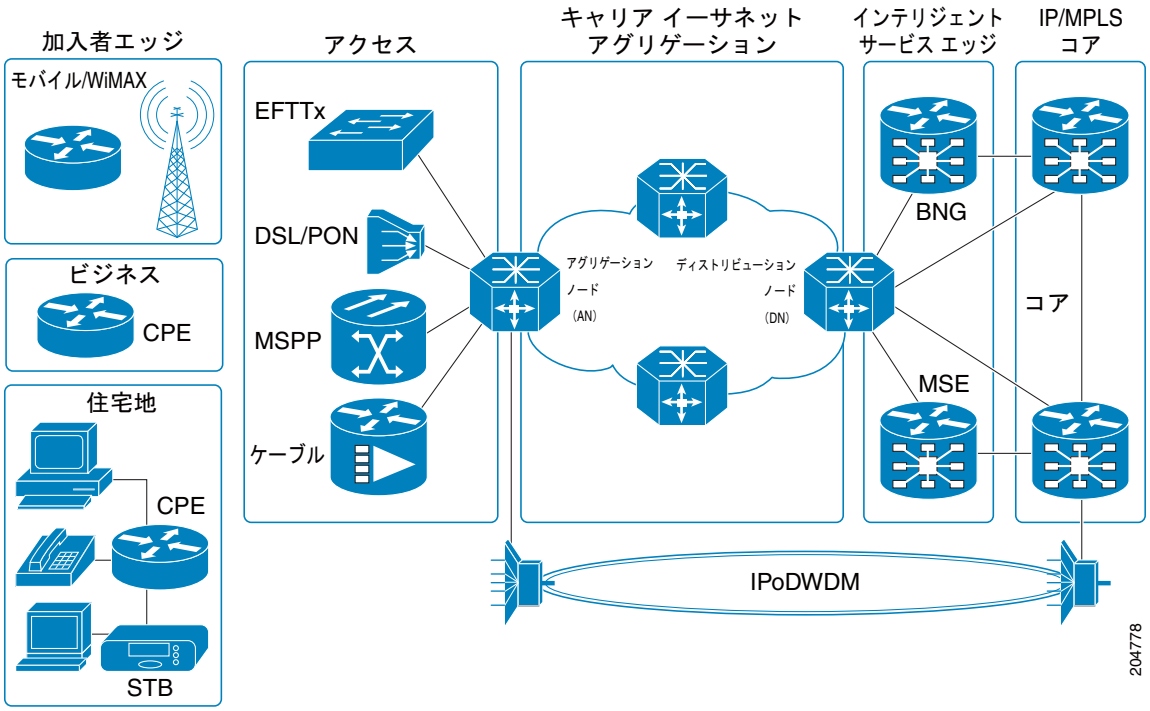
http://www.cisco.com/go/ce

特に、シスコ次世代 IP ネットワーク（NGN）キャリア イーサネット デザインに関する資料を参照してください。IP NGN キャリア イーサネット デザインは、各サービス固有の要件を満たすように最適化された、整合性のあるサービス配信を行うための、そのクラスで最高の実装を可能とする、Cisco IP NGN アーキテクチャの重要な要素を表しています。これは、ネットワーク アクセスから IP/MPLS コアに対する、エンドツーエンドのサービス転送の基盤です。このデザインにより、サービスとアプリケーション レイヤ コンポーネントが統合的に連携され、現在および将来のネットワーク サービス要件を満たすインテリジェントでスケーラブルな信頼性の高い集中型ネットワーク モデルを提供できるようになります。

IP NGN キャリア イーサネット デザイン（図 1-1 を参照）は、すべてのキャリア イーサネット プラットフォームに対して、プラットフォームに依存しないアーキテクチャおよびイーサネット ベースのサービス モデルを提供します。このデザインにより、サービス プロバイダーは高度な機能を備えた適切なネットワーキング テクノロジー（イーサネット、IP、MPLS、マルチキャスト、疑似回線、階層型プライベート仮想 LAN サービスなど）を駆使してサービス転送を最適化でき、ビジネスでの目標や Quality of Experience（QoE; ユーザ体感品質）での目標を達成できます。

（注）　現実のネットワーク実装では、スケーラブルなアーキテクチャのサブセットのみを実装することも考えられます。

図 1-1　　IP NGN キャリア イーサネット デザイン



Prime Fulfillment 用語とサポートされるネットワーク タイプ

ここでは、レイヤ 2 サービスおよびサポートされるネットワーク タイプで使用される Prime Fulfillment 用語について説明します。Prime Fulfillment では、次のサービス タイプをプロビジョニングできます。

- E-Line（EPL/EWS および EVPL/ERS）
- E-LAN（EP-LAN および EVP-LAN/ERMS）
- FRoMPLS
- ATMoMPLS

Prime Fulfillment では、イーサネット スイッチのみ（MPLS は未使用）で構成されるネットワーク上でのプロビジョニング イーサネット サービスもサポートします。これは、Prime Fulfillment 用語では「VPLS L2 コア」と呼ばれます。

（注）　E-Line サービスと E-LAN サービスでは、FlexUNI/EVC サービス ポリシー タイプの使用を推奨します（このガイドの、FlexUNI/EVC ポリシーを作成する方法とサービス要求の利用方法について説明する章を参照してください）。L2VPN と VPLS のサービス ポリシー タイプを使用してプロビジョニングされた既存サービスが存在することがあります。これらのサービスは現在もサポート対象で、そのサービス タイプとともに保守できますが、新しいサービスでは、必ず FlexUNI /EVC サービス ポリシー タイプを使用してください。ATM サービスと FRoMPLS サービスでは、以前と同様に、L2VPN サービス ポリシーを使用します。

Prime Fulfillment の GUI および本ユーザ ガイドには、これらのイーサネット サービスの命名規則について記載されています。この命名規則は、以前の MEF の表記法に合わせて設定されています。この表記法は、Prime Fulfillment の将来のリリースで改訂される予定です。参考として、MEF フォーラムで使用される同義語を表 1-3 にまとめます。

表 1-3　イーサネット サービス用語の対応付け

Prime Fulfillment 5.2 GUI および本ユーザ ガイドで使用される用語	現在の MEF での同義語
L2VPN over MPLS Core	
イーサネット ワイヤ サービス（EWS）	Ethernet Private Line（EPL; イーサネット専用回線）
イーサネット リレー サービス（ERS）	Ethernet Virtual Private Line（EVPL; イーサネット仮想専用回線）
ATM over MPLS（ATMoMPLS）	—
Frame Relay over MPLS（FRoMPLS）	—
VPLS over MPLS Core	
イーサネット ワイヤ サービス（EWS）またはイーサネット マルチポイント サービス（EMS）	Ethernet Private LAN（EP-LAN; イーサネット専用 LAN）
イーサネット リレー サービス（ERS）またはイーサネット リレー マルチポイント サービス（ERMS）	Ethernet Virtual Private LAN（EVP-LAN; イーサネット仮想専用 LAN）

表 1-3　イーサネット サービス用語の対応付け （続き）

Prime Fulfillment 5.2 GUI および本ユーザ ガイドで使用される用語	現在の MEF での同義語
VPLS over Ethernet Core	
イーサネット ワイヤ サービス（EWS）	Ethernet Private LAN（EP-LAN; イーサネット専用 LAN）
イーサネット リレー サービス（ERS）	Ethernet Virtual Private LAN（EVP-LAN; イーサネット仮想専用 LAN）

L2VPN サービス プロビジョニング

ここでは、MPLS コアを介してレイヤ 2 ポイントツーポイント接続を提供する Prime Fulfillment プロビジョニングの概要を説明します。シスコの Any Transport over MPLS（AToM）を使用すると、これらのサービスをサポートできます。同様に、これらの実装は次のようなサービス タイプをサポートします。

- イーサネット ワイヤ サービス（EWS）。このサービスに対応する MEF 用語は EPL です。
- イーサネット リレー サービス（ERS）。このサービスに対応する MEF 用語は EVPL です。
- ATM over MPLS（ATMoMPLS）
- Frame Relay over MPLS（FRoMPLS）

これらのサービスのポリシーを作成する方法とサービス要求については、本ガイドの他の章で説明しています。詳細については、次を参照してください。

- 「ポイントツーポイント イーサネット（EWS および ERS）（EPL および EVPL）」（P.1-5）
- 「ATM over MPLS（ATMoMPLS）」（P.1-10）
- 「Frame Relay over MPLS（FRoMPLS）」（P.1-11）

ポイントツーポイント イーサネット（EWS および ERS）（EPL および EVPL）

EWS サービスと ERS サービス（MEF 用語では、それぞれ「EPL」、「EVPL」と呼ばれます）は、Cisco メトロ イーサネットのサービスとともに提供されます。同じネットワーク アーキテクチャにより、さまざまなカスタマーに対する ERS（EPL）接続と EWS（EVPL）接続の両方の同時提供が可能となります。また、このメトロ イーサネット インフラストラクチャを使用して、上位レベルのサービス（IP ベースのバーチャル プライベート ネットワーキング、パブリック インターネット通信、Voice over IP、全アプリケーションの組み合わせなど）にアクセスすることもできます。

イーサネット ワイヤ サービス（EWS または EPL）

Ethernet Virtual Circuit（EVC; イーサネット仮想回線）は、物理的な 2 つの User-to-Network Interface（UNI; ユーザネットワーク インターフェイス）を接続します。この接続は、外観はカスタマー向けの仮想専用回線のように見えます。802.1Q-in-Q タグ スタック構成テクノロジーの実装により、VLAN の透過性とコントロール プロトコル トンネリングが提供されます。1 つの UNI で受信されたパケットは、他の対応する UNI に直接転送されます。

このサービスに対応する MEF 用語は EPL です。

イーサネット リレー サービス（ERS または EVPL）

Ethernet Virtual Circuit（EVC; イーサネット仮想回線）を使用すると、エンドポイントを論理的に接続することができますが、単一の UNI 上に複数の EVC が存在することになる場合があります。各 EVC は、802.1q VLAN タグ ID によって識別されます。ERS ネットワークは、イーサネット フレームがスイッチド ネットワーク上を横断するように動作します。また、特定のコントロール トラフィックは EVC の終端間では実行されません。ERS は、CE-VLAN タグが Data-Link Connection Identifier（DLCI; データリンク接続識別子）の役割を果たすフレーム リレーに類似しています。

このサービスに対応する MEF 用語は EVPL です。

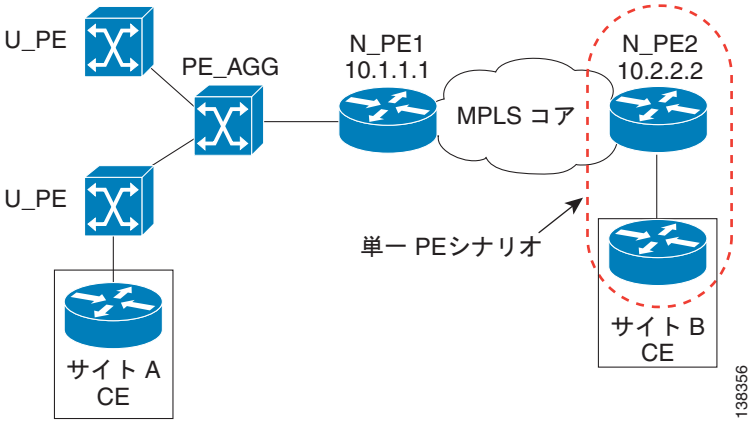
L2VPN Ethernet over MPLS（ERS および EWS）（EPL および EVPL）のトポロジ

Ethernet over MPLS（EoMPLS）はトンネリングのメカニズムで、これを使用してサービス プロバイダーはレイヤ 3 MPLS ネットワークを経由してレイヤ 2 トラフィックをトンネリングできます。重要なことは、EoMPLS はポイントツーポイント ソリューションのみを提供するという点です。

次の図に、EoMPLS の活用法の例を示します。イーサネット サービスは、2 つの方法でエンド ユーザに提供できます。

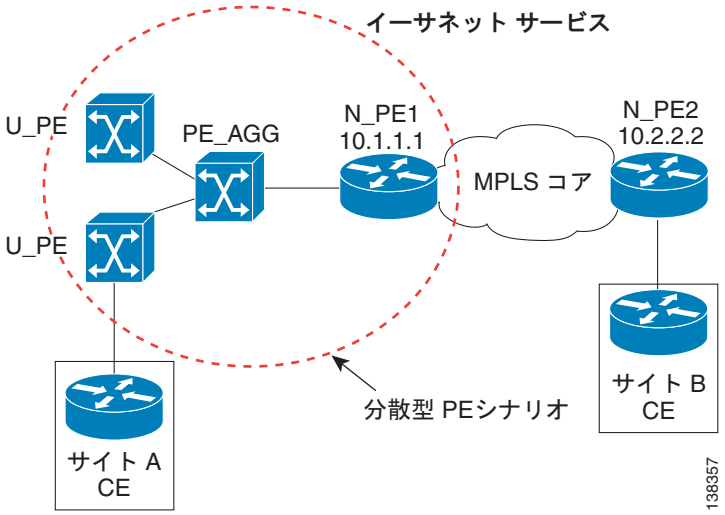
- 単一の PE シナリオでは、カスタマーは N-PE のイーサネット ポートに直接接続されます（図 1-2）。

図 1-2　単一の PE シナリオ



- 分散型 PE シナリオでは、エンド ユーザはアクセス ドメインを経由して N-PE に接続されます（図 1-3）。つまり、レイヤ 2 スイッチング環境は CE と N-PE の中間に位置することになります。

図 1-3　分散型 PE シナリオ



いずれのシナリオでも、VLAN は次のいずれかの方法で割り当てられます。

- Prime Fulfillment によって、ユーザが事前に定義した VLAN プールから自動的に割り当てられる。
- GUI または Northbound Interface（NBI）を使用して、ユーザによって手動で割り当てられる。

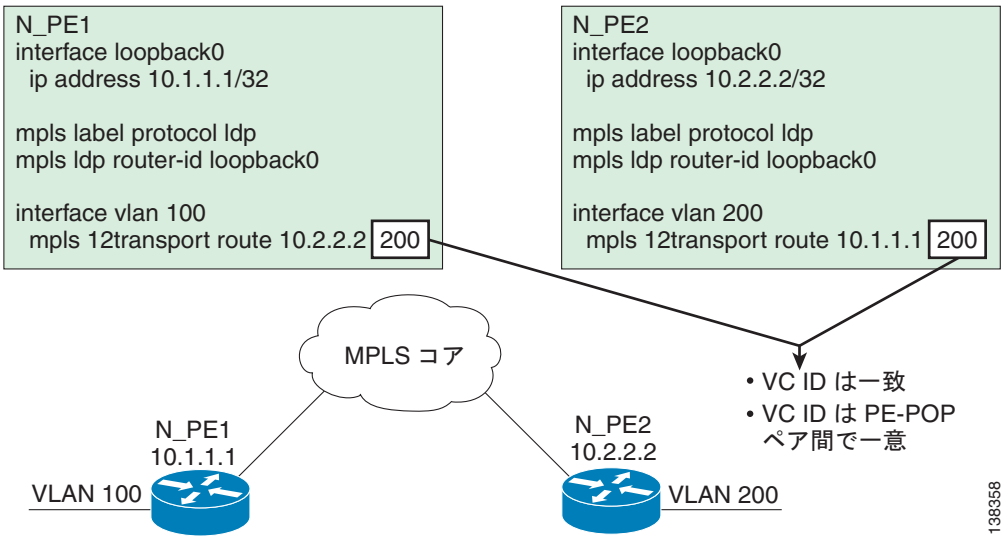
EoMPLS では、Prime Fulfillment はポイントツーポイント トンネルを作成し、リモート サイトに到達可能なピア N-PE ルータに対する EoMPLS トンネルを確立しようとします。リモート N-PE は、ループバック アドレスで識別されます。図 1-4 では、N-PE1 と N-PE2 にはループバック アドレスと同様に 10.1.1.1 と 10.2.2.2 が設定されます。図 1-4 では、サイト A には VLAN-100 が割り当てられ、サイト B には VLAN-200 が割り当てられます。VLAN は局部的な意味だけを持つ（N-PE で区切られるイーサネット アクセス ドメイン内でのみ有効な意味を持つ）ため、回線の両側に異なる VLAN ID を設定できます。

サイト A にサービスを提供する N-PE では、カスタマー向けのすべての L2 トラフィックを終端させるために VLAN インターフェイス（レイヤ 3 インターフェイス）が作成され、このインターフェイスに EoMPLS トンネルが設定されます。

（注）　この設定は、Cisco 7600 オプティカル サービス ルータに基づいて行われます。Cisco 7200 などの他のルータでは、異なる設定が行われます。

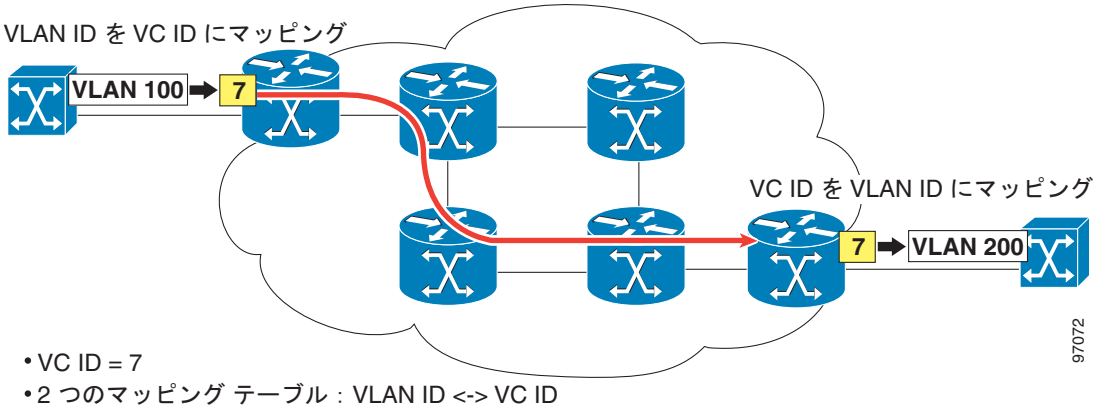
EoMPLS トンネルを定義する VC ID は 200 です（図 1-4 を参照）。

図 1-4　Ethernet over MPLS（EoMPLS）の設定



VC ID は、EoMPLS トンネルの両端で同一でなければならないことに注意してください。N-PE ごとに、EoMPLS トンネルに対する VLAN 間でマッピングが行われます（図 1-5 を参照）。

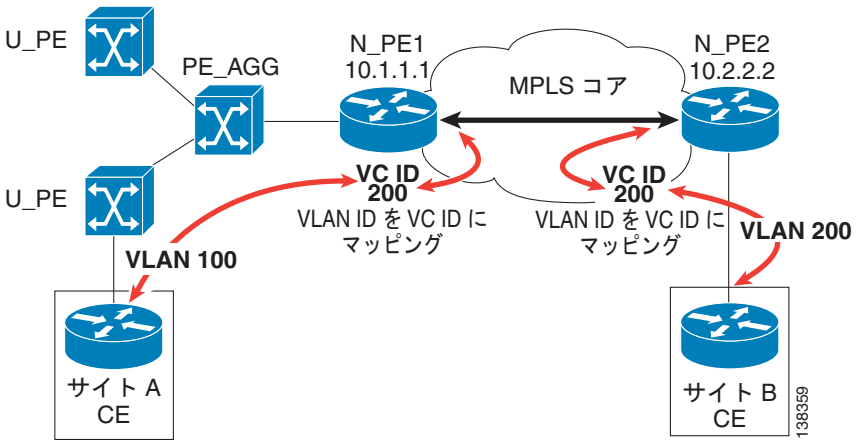
図 1-5　EoMPLS トンネル



接続全体では、マッピングは VLAN ID <-> VC ID <-> VLAN ID のように行われます。

この VLAN-VC ID マッピングにより、サービス プロバイダーはアクセス ドメイン内で同じ VLAN ID を使用できるようになります（図 1-6 を参照）。

図 1-6　VLAN-VC ID マッピング



各アクセス ドメインに割り当てられて使用される VLAN ID は、同じ ID にすることはできません。

ATM over MPLS（ATMoMPLS）

Cisco ATM over MPLS（ATMoMPLS）により、ATM Adaptation Layer 5（AAL5; ATM アダプテーション層 5）転送および Cell Relay over MPLS がサポートされます。

AAL5

AAL5 を使用すると、MPLS バックボーン経由で、さまざまなカスタマーから AAL5 PDU を転送できます。ATM AAL5 は、既存のレイヤ 3 サービスに加えてレイヤ 2 サービスを提供できるようにすることで、MPLS バックボーンの有用性を広げます。MPLS バックボーンの両端で Provider Edge（PE; プロバイダー エッジ）ルータを設定することで、MPLS バックボーン ネットワークを有効にし、AAL5 PDU を受け入れることができます。

MPLS 経由で AAL5 PDU を転送できるように、入力 PE ルータから出力 PE ルータへの仮想回線を設定します。この仮想回線により、1 台の PE ルータから別の PE ルータに AAL5 PDU が転送されます。各 AAL5 PDU は単一パケットとして転送されます。

Cell Relay over MPLS

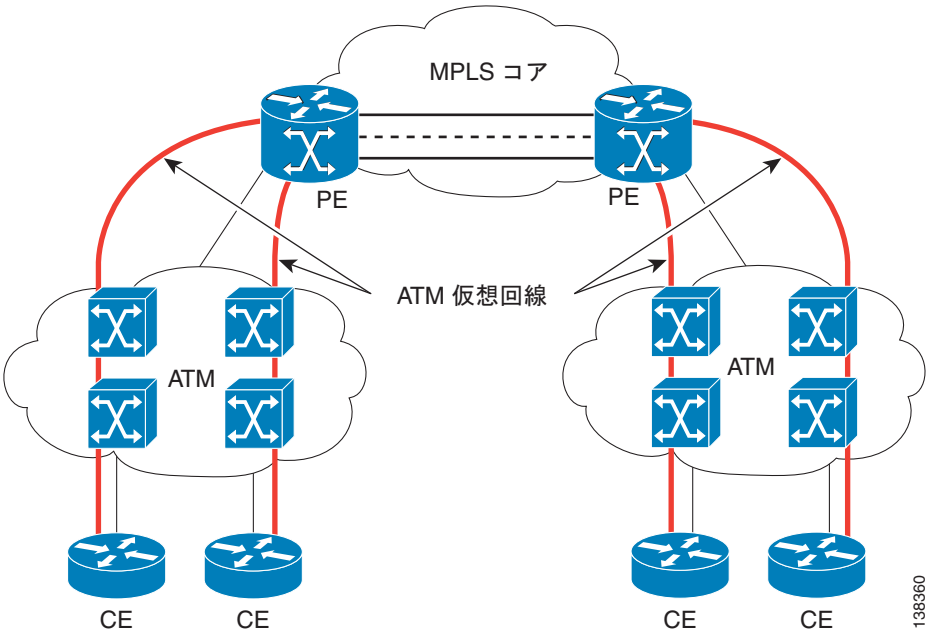
Cell Relay over MPLS を使用すると、MPLS バックボーン経由でさまざまなカスタマーから ATM セルを転送できます。ATM Cell Relay は、既存のレイヤ 3 サービスに加えてレイヤ 2 サービスを提供できるようにすることで、MPLS バックボーンの有用性を広げます。MPLS バックボーンの両端で Provider Edge（PE; プロバイダー エッジ）ルータを設定することで、MPLS バックボーン ネットワークを有効にし、ATM セルを受け入れることができます。

MPLS 経由で ATM セルを転送できるように、入力 PE ルータから出力 PE ルータへの仮想回線を設定します。この仮想回線により、1 台の PE ルータから別の PE ルータに ATM セルが転送されます。1 つの MPLS パケットには、1 つまたは複数の ATM セルを含めることができます。カプセル化タイプは AAL0 です。

ATMoMPLS のトポロジ

単一の PE シナリオのみがサポートされます（図 1-7 を参照）。

図 1-7　AAL5 および Cell Relay over MPLS の設定



Frame Relay over MPLS（FRoMPLS）

フレーム リレーに対応した Cisco AToM により、カスタマー フレーム リレー トラフィックを MPLS パケットにカプセル化し、目的の宛先に転送することができます。Cisco AToM を使用すると、サービス プロバイダーは、一般的なフレーム リレー プロビジョニングと比較して時間や手間をかけずに迅速に新しいサイトを追加できます。

Frame Relay over MPLS を使用して、サービス プロバイダーは MPLS バックボーン経由でフレーム リレーのフレームを転送できます。これにより、フレーム リレーの到達可能性が高まり、サービス プロバイダーは共通のパケット バックボーンを経由してフレーム転送を集約することができます。サービス プロバイダーは既存のフレーム リレー環境をパケット バックボーンと統合し、運用効率を高めたり、高速のパケット インターフェイスを実装して、フレーム リレー実装を拡張できます。

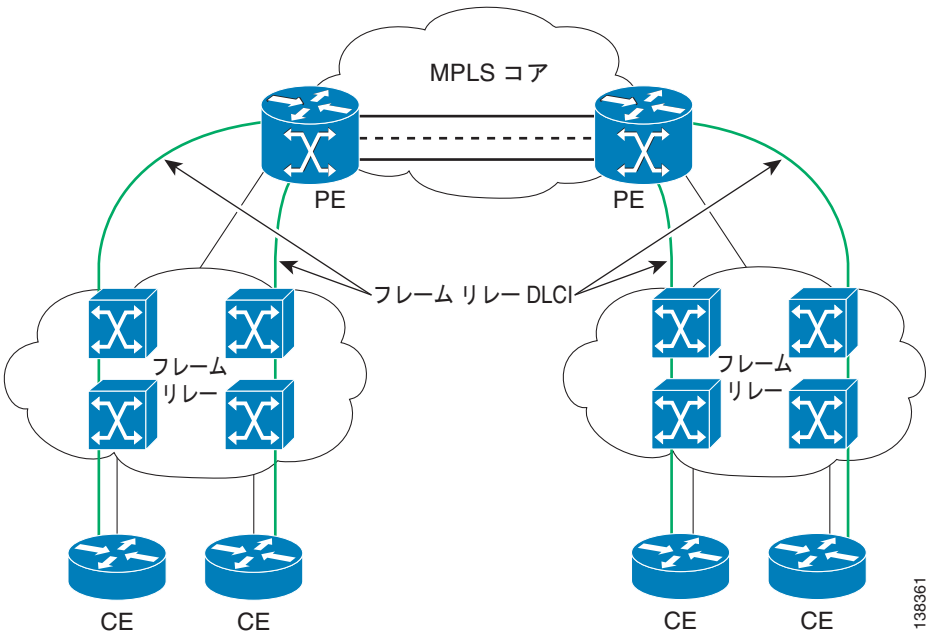
MPLS ネットワーク経由でフレーム リレーのフレームを転送することで、次のような数多くのメリットが得られます。

- フレーム リレー拡張サービス。
- より高速のバックボーン（OC-192 など）への集約による、フレーム リレー実装の拡張。
- 運用効率の向上。MPLS バックボーンは、既存の各種ネットワークおよびサービスを統合する単一のネットワークになります。

FRoMPLS のトポロジ

単一の PE シナリオのみがサポートされます（図 1-8 を参照）。

図 1-8　Frame Relay over MPLS



FlexUNI/EVC イーサネット サービス プロビジョニング

ここでは、Cisco Prime Fulfillment 6.1 における FlexUNI/EVC イーサネットおよび FlexUNI/EVC ATM インターワーキング サポートについて説明します。次の項目について説明します。

（注）　イーサネット（E-Line および E-LAN）サービスでは、FlexUNI/EVC ポリシーとサービス要求の使用を推奨します。FlexUNI/EVC 構文を使用してサービスのプロビジョニングを行っている場合、または今後その予定がある場合は、FlexUNI/EVC サービスを使用します。L2VPN および VPLS のサービス ポリシー タイプを使用してプロビジョニングした既存のサービスは、現在もサポートされており、そのサービス タイプとともに保守できます。ATM サービスと FRoMPLS サービスでは、以前と同様に、L2VPN サービス ポリシーを使用します。

概要

Flexible User Network Interface（FlexUNI; 柔軟性の高いユーザ ネットワーク インターフェイス）は、Prime Fulfillment でイーサネット サービスを作成するための一般的なアプローチとして使用されます。ハードウェアでサポートされる場合は、すべてのイーサネット プロビジョニングに使用可能です（FlexUNI/EVC をサポートするプラットフォームの詳細については、「Cisco Prime Fulfillment 6.1 での FlexUNI/EVC のプラットフォーム サポート」（P.1-14）を参照してください）。FlexUNI/EVC ポリシーは汎用的で柔軟性が高く、サービス デザイナーは従来の Prime Fulfillment L2VPN サービスや VPLS サービスを使用していた場合と比較してより高度なサービスを提供できます。

特定のラインカードには、Cisco IOS Ethernet Virtual Circuit（EVC; イーサネット仮想回線）構文をサポートするインターフェイスが備えられています。これらのインターフェイスの設定には、EVC インフラストラクチャ機能またはスイッチ ポート コマンドライン インターフェイス コマンド（クラス）を使用します。FlexUNI は、オプションで EVC CLI 構文/インフラストラクチャをサポートします。このことから、「FlexUNI ポリシー」と「サービス要求」は包括的な用語「FlexUNI/EVC」で表されます。ただし、FlexUNI/EVC ポリシーとサービス要求は新しい EVC 構文には関係していないことに注意してください。サービス エンドポイントでは、非 EVC 構文も使用できます。

FlexUNI/EVC インフラストラクチャを活用するサービスは多様であり、サービスの相違について明確な説明が可能であるとは限りません。これは、FlexUNI/EVC では、高い柔軟性を持ってこれらのサービスを提供しているためです。サービスの定義が難しくなっているのはこのためです。たとえば、従来の ERS は、プラットフォームのさまざまなクラスを使用して、さまざまな方法で提供することができました。

FlexUNI/EVC ポリシーと関連するサービス要求では、デバイス機能をサポートするための汎用的で柔軟性の高いサービスを構築します。このポリシーは、EVC アーキテクチャを使用して異なるサービスを提供するのに十分な柔軟性を備えています。これにより、サービス デザイナーは柔軟性の高い方法で大部分の EVC 機能を使用して、ハードウェア機能とプラットフォーム機能を対応付けることができます。

FlexUNI/EVC ポリシーを使用して、他の既存の Prime Fulfillment サービス要求タイプ（L2VPN や VPLS など）は作成せず、FlexUNI/EVC サービス要求のみを作成することができます。同様に、他の既存の Prime Fulfillment ポリシーは使用せず、FlexUNI/EVC ポリシーのみを使用して FlexUNI/EVC サービス要求を作成することもできます。

FlexUNI/EVC インフラストラクチャを使用すると、Carrier Ethernet（CE; キャリア イーサネット）展開では次のようなメリットを得られます。

- 柔軟性の高いフレーム マッチング。
- 柔軟性の高い VLAN タグ操作または変換。
- 同じポート上での複数のサービス。
- 柔軟性の高いサービス マッピング。
- VLAN スケーリングおよび局部的な意味を持つ VLAN。

FlexUNI/EVC は、次のような、さまざまなネットワーク構成をサポートします。

- イーサネット アクセスのプロビジョニング（N-PE 上での EVC 対応 EWS インターフェイスとして）。
- ブリッジ ドメイン内の 1 つまたは複数のポートにある単一の Cisco 7600 N-PE で終端するイーサネット アクセスの相互接続。
- VPLS サービスの複数の Cisco 7600 N-PE で終端するイーサネット アクセスの相互接続。
- FlexUNI/EVC サービスは、IOS XR を実行する Cisco ASR 9000 シリーズ ルータをサポートします。
- 既存のサービスをイーサネット アクセスと組み合わせたサービス（ERS/EWS インターワーキング サービスなど）。
- E-Line サービスのプロビジョニング。ここで、いずれかまたは両方の N-PE インターフェイスは FlexUNI です。

FlexUNI/EVC の機能

ここでは、Prime Fulfillment の FlexUNI/EVC ポリシーおよびサービス要求でサポートされる機能を要約して説明します。

- トポロジの選択：
  - 直接接続されたカスタマー エッジ デバイス（CE）。
  - イーサネット アクセス デバイス経由で接続された CE。
- プラットフォームの選択：
  - FlexUNI/EVC（すべての N-PE 上）。
  - FlexUNI/EVC（どの N-PE にもない）。
  - FlexUNI/EVC と古いインフラストラクチャの混在。展開したプラットフォームを継続してサポートするように、古いプラットフォームと新しいプラットフォームを共存させることができます。
- MPLS コアを経由した接続の選択（ブリッジ ドメインあり / なし）：
  - 疑似回線
  - VPLS
  - ローカル（ローカル接続）

- 柔軟性の高い VLAN 処理メカニズム（最大 2 つのレベルの VLAN タグを使用）：
  - サービス分類を行うための VLAN マッチング。外部 VLAN タグと内部 VLAN タグの両方をマッチングする機能、または広範な内部 VLAN タグをマッチングする機能を提供します。
  - VLAN 操作（ポップ外側タグ、ポップ内側タグ、プッシュ外側タグ、プッシュ内側タグ、VLAN 変換（1:1、2:1、1:2、2:2）など）。
- 柔軟性の高い転送オプション：
  - サービス インスタンス直下にある MPLS コアでの疑似回線の設定（E-Line のみ）。
  - Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）下にある MPLS コアでの疑似回線の設定（ブリッジ ドメインに関連付け）。

（注）　いずれの場合も、適切な VLAN 操作を疑似回線で実行できます。

  - 各種インターフェイスや VLAN から単一のブリッジ ドメインに対してトラフィックを関連付け（VPLS に対する適切な VLAN 操作を実行）。
  - 各種インターフェイスや VLAN から単一のブリッジ ドメインに対してトラフィックを関連付け（ローカル接続に対する適切な VLAN 操作を実行）。

Cisco Prime Fulfillment 6.1 での FlexUNI/EVC のプラットフォーム サポート

FlexUNI/EVC サービスは、次に説明するように、IOS と IOS XR の両方のプラットフォームでサポートされます。

IOS プラットフォームのサポート

FlexUNI/EVC サービスでは、次の IOS プラットフォームがサポートされています。

- IOS 12.2(33)SRB および SRC
- ES20 ラインカード（2x10GE および 20x1GE）
- Shared Port Adapter（SPA; 共有ポート アダプタ）インターフェイス プロセッサ 400（SIP-400）ラインカード、バージョン 2.0（2x1GE および 5x1GE）

（注）　このリリースでサポートされるハードウェア プラットフォームとソフトウェア プラットフォームの最新のリストについては、『*Cisco Prime Fulfillment Installation Guide 6.1*』を参照してください。

ES20 ラインカードおよび SIP-400 ラインカードのインターフェイスは、IOS EVC 構文をサポートします。

プラットフォームに関する 2 つのサンプル シナリオを、次に説明します。N-PE の UNI の特徴と FlexUNI 機能は相互依存の関係にはないことに注意してください。

例 1

FlexUNI/EVC サービス要求を使用すると、オペレータは、N-PE 上で EVC 対応インターフェイスまたは EVC 非対応インターフェイスを使用してリンクを追加できます。たとえば、オペレータは次の設定を行って、FlexUNI/EVC サービス要求（VPLS 接続を使用）に 3 つのリンクを追加できます。

- リンク 1 には、Cisco 7600 N-PE 上に Cisco 67xx インターフェイスと IOS 12.2 (33)SRB イメージがあります。

- リンク 2 には、Cisco 7600 N-PE 上に Cisco 67xx インターフェイスと IOS 12.2 (33)SRB イメージがあります。
- リンク 3 には、Cisco 7600 N-PE 上に ES20 ベースのインターフェイスと IOS 12.2 (33)SRB イメージがあります。

例 2

レイヤ 2 アクセス ノードに関する限り、U-PE と PE-AGG における UNI/NNI の設定に、N-PE の FlexUNI/EVC 機能の影響が及ぶことはありません。ただし、N-PE インターフェイスが実装されている Named Physical Circuit（NPC; 名前付き物理回線）を使用する場合で、FlexUNI/EVC を使用するように設定されているときは、従来の設定用にプロビジョニングすることはできません。このときにサービス要求を保存するとエラーが発生します。

ただし、N-PE インターフェイスが実装されている NPC を使用する場合で、FlexUNI/EVC を使用しないように設定されているときは、FlexUNI 設定用にプロビジョニングすることはできません。このときにサービス要求を保存するとエラーが発生します。

たとえば、FlexUNI/EVC サービス要求のリンクで、カプセル化に dot1Q を選択すると、そのインターフェイスでは、同じ U-PE/PE-AGG 上で他の L2 ERS/VPLS ERMS UNI を共有できます。

選択した NPC の一部である N-PE インターフェイスに（既存の L2VPN または VPLS サービス要求を使用して）非 FlexUNI/EVC 機能が設定されている場合、このインターフェイスに FlexUNI/EVC を設定することはできません。

（注）　カプセル化タイプとして「Dot1Q Tunnel」を選択している場合は、そのポートを他のサービスと共有することはできません。

IOS XR プラットフォーム サポート

FlexUNI/EVC サービスは、IOS XR を実行する Cisco ASR 9000 シリーズ ルータ上でサポートされます。

（注）　このリリースでサポートされるハードウェア プラットフォームとソフトウェア プラットフォームの最新のリストについては、『*Cisco Prime Fulfillment Installation Guide 6.1*』を参照してください。

IOS XR プラットフォームでは、次の FlexUNI/EVC 機能がサポートされています。

- E-Line 接続。ダイレクト リンクに ASR 9000 を追加すると、E-Line サービスでサポートされるのは DOT1Q カプセル化だけになります。NPC を設定した L2 アクセス ノードを使用すると、サポートされるすべてのカプセル化を使用できます。
- E-LAN 接続。
- 柔軟性の高いフレーム マッチング。
- 柔軟性の高い VLAN タグ操作/変換。
- VLAN スケーリングおよび局部的な意味を持つ VLAN。
- 同じ物理インターフェイス下で L2 サービスと L3 サービスを作成するための機能は、サブインターフェイスのみに限定されます。
- Cisco ASR 9000 デバイスのレイヤ 2 ポートはすべてトランク ポートであるため、サポートされるのはトランク ポートベースの設定のみとなります。

IOS XR プラットフォームでは、次の FlexUNI/EVC サービスはサポートされません。

- SVI 属性での N-PE 擬似回線はサポートされません。デバイス上で SVI インターフェイスを使用することはできません。このため、N-PE で UNI が設定されている場合、標準的な UNI およびポート セキュリティの設定のサポートは限定的なものとなります。
- インターフェイス コンフィギュレーションでは、xconnect コマンドは直接にはサポートされません。これらのコマンドは、IOS XR の別の階層でサポートされるようになりました。
- UNI を設定した N-PE デバイスでは、EWS サービスはサポートされません。Cisco ASR 9000 デバイスはルータであるため、レイヤ 2 ポートはすべてデフォルトのトランクになります。アクセス ポートを設定するオプションは存在しないため、アクセス ポートベースのサービスのサポートは限定的なものとなります。

（注）　特に記載のない限り、このガイドで説明する FlexUNI/EVC ポリシーおよびサービス要求の機能はすべて、IOS プラットフォームと IOS XR プラットフォームの両方に該当します。

FlexUNI/EVC が設定されたデバイスのロール

現在、Prime Fulfillment には U-PE、PE-AGG、および N-PE のデバイスがあります。FlexUNI/EVC ポリシーおよびサービス要求に対応するため、Prime Fulfillment の基本の PE デバイス ロールの関連付けは維持されます。Prime Fulfillment のこのリリースでは、PE ロールの割り当てに加えられた変更はありません。FlexUNI/EVC 機能を実装したデバイスで、Prime Fulfillment に既存のロール割り当てを変更する必要はありません。ただし、Prime Fulfillment での FlexUNI/EVC 機能は、N-PE 上にあるインターフェイスでのみサポートされ、PE-AGG や U-PE デバイスのインターフェイスではサポートされません。

（注）　Prime Fulfillment は、FlexUNI/EVC の Customer Edge（CE; カスタマー エッジ）デバイスをサポートしません。アクセス ポートに DSLAMS が含まれる場合、Prime Fulfillment ではサポートされないシスコ製以外のイーサネット デバイスや他のシスコ デバイス（ノードなど）は、Prime Fulfillment の処理対象ではありません。このような場合、Prime Fulfillment の観点から、最初に Prime Fulfillment が管理するデバイスのインターフェイスが UNI になります。

FlexUNI/EVC のトポロジ概要

ここでは、FlexUNI/EVC を使用してサポートされる、さまざまなトポロジの例を示します。「FlexUNI/EVC が設定されたデバイスのロール」（P.1-16）の最後に説明したように、Prime Fulfillment では、FlexUNI/EVC の機能を備えたカスタマー エッジ デバイス（CE）をサポートしません。次のようなさまざまなトポロジでの「CE」という言葉（「直接接続された CE」など）は、カスタマーまたはサードパーティのデバイスの N-PE への接続方法だけを指しています。FlexUNI/EVC が関与する場合、CE は Prime Fulfillment でサポートされません。また、Prime Fulfillment でサポートされないプロバイダー デバイスがアクセス回線で使用されている場合、そこが Prime Fulfillment のサポート対象範囲の境界となります。この境界を越えるデバイス（CE に向かうデバイス、サポートされないノードを含みます）は、Prime Fulfillment による管理は行われません。

CE 直接接続、FlexUNI/EVC 使用

この組み合わせでは、UNI は EVC の機能が設定された、サポートされるラインカード上のインターフェイスになります。Prime Fulfillment は、Prime Fulfillment の標準 UNI 機能（たとえば、ポート セキュリティ、ストーム コントロール、レイヤ 2 プロトコル トンネリング）は設定しません。これは、FlexUNI/EVC 対応ハードウェア上でコマンドがサポートされていないためです。オペレータは、テンプ

レートを使用して、プラットフォームでサポートされる関連パラメータを設定し、Prime Fulfillment では提供されない機能を実装できます。Prime Fulfillment が設定するのは、UNI 上で VLAN 操作や疑似回線、VPLS、またはローカル接続を使用できるサービス インスタンスだけです。このようなリンクを作成するときに NPC は必要ありません。NPC が必要になるのは、N-PE と CE の間にアクセス ノードがある場合に限られます。他の中間イーサネット アクセス ノードは、このトポロジでは使用しません。

CE 直接接続、FlexUNI/EVC なし

これは、Prime Fulfillment における、N-PE の UNI に類似しています。FlexUNI/EVC サービス要求を使用して、古い Cisco 7600 プラットフォーム（FlexUNI/EVC 機能のない N-PE インターフェイス）を使用したリンクを作成できますが、EVC サポートを使用して将来的に 1 つ以上のリンクを追加できます。これを行わず、Prime Fulfillment の既存の ERS/EWS/ERMS/EMS 機能を使用することも可能です。このようなリンクを作成するときに NPC は必要ありません。NPC が必要になるのは、N-PE と CE の間にアクセス ノードがある場合に限られます。他の中間イーサネット アクセス ノードは、このトポロジでは使用しません。

CE 直接接続なし、FlexUNI/EVC 使用

このトポロジには、次のコンフィギュレーションが伴います。

- CE が接続される U-PE または PE-AGG 上の UNI。
- イーサネット U-PE および PE-AGG
- CE 側に FlexUNI 対応のインターフェイスを備えた N-PE。

あらゆるサービス固有パラメータ（ポート セキュリティ、L2 プロトコル トンネリング、ストーム コントロールなど）を、これらの UNI（標準 UNI）で使用できます。U-PE および PE-AGG コンフィギュレーションにより、CLI が変更されることはありません。ただし、EVC コマンドを使用できるのは、N-PE 上だけです（CE 側のインターフェイス）。このようなリンクを作成するときには、NPC を使用します。

CE 直接接続なし、FlexUNI/EVC なし

このリンクは、既存の Prime Fulfillment 実装における接続回線とまったく同じです。また、既存の Prime Fulfillment サービスにある標準 UNI を備えています。このようなリンクを作成するときには、NPC を使用します。

コンフィギュレーションをチェックするときの留意事項

Prime Fulfillment は、FlexUNI/EVC サービス要求によって生成されたすべてのコンフィギュレーションについて、プロビジョニングを試行します。Prime Fulfillment は、CLI がプロビジョニングされている特定のデバイスとの互換性があるかどうかについて、事前のチェックは行いません。これは、時間の経過とともに変更される可能性のあるデバイス/プラットフォーム機能の柔軟性を確保するためです。したがって、サービス デザイナーまたはオペレータにとっては、FlexUNI/EVC ポリシーとサービス要求を慎重に作成することが重要です。

FlexUNI/EVC ATM イーサネット インターワーキング サービス プロビジョニング

Prime Fulfillment は、MPLS コアまたはローカル スイッチングで ATM およびイーサネット プロトコルを使用したサービスのインターワーキングをサポートします。ATM イーサネット インターワーキングは、次の機能を通してサポートされています。

- 「ATM イーサネット インターワーキング」タイプの FlexUNI/EVC ポリシーの作成。ATM イーサネット インターワーキング ポリシー タイプは、MPLS コア オプションの選択をサポートします。
  - Pseudowire
  - ローカル（ローカル接続）
- 単一の FlexUNI/EVC サービス要求を使用した ATM イーサネット インターワーキングのプロビジョニング。
- EVC と非 EVC 構文の組み合わせ。L2 構文と EVC 構文で構成される L2 回線の作成。
- サポートされるプラットフォーム
  - ATM インターワーキングは、ES-20 カードを備えた Cisco 7600 上でサポートされます。
  - IOS XR 3.7.3 と IOS XR 3.9 では、ASR 9000 デバイスがサポートされます。Cisco ASR 9000 には ATM インターフェイスはないため、Prime Fulfillment は ASR 9000 上で ATM インターフェイス用のインターワーキングをサポートしません。サポートされるのは、イーサネット インターフェイスだけです。

VPLS サービス プロビジョニング

VPLS サービスはマルチポイントです。MPLS またはイーサネット コアを介して、マルチポイント接続を提供します。同様に、これらの実装は次のようなサービス タイプをサポートします。

- VPLS over MPLS Core：
  - イーサネット ワイヤ サービス（EWS）。「EMS」または「イーサネット マルチポイント サービス」と呼ばれることもあります。このサービスに対応する MEF 用語は EP-LAN です。
  - イーサネット リレー サービス（ERS）。「ERMS」または「イーサネット リレー マルチポイント サービス」と呼ばれることもあります。このサービスに対応する MEF 用語は EVP-LAN です。
- VPLS over Ethernet Core：
  - イーサネット ワイヤ サービス（EWS）。このサービスに対応する MEF 用語は EP-LAN です。
  - イーサネット リレー サービス（ERS）。このサービスに対応する MEF 用語は EVP-LAN です。

これらのサービスのポリシーを作成する方法とサービス要求については、本ガイドの他の章で説明しています。

VPLS はマルチポイント レイヤ 2 VPN であり、EoMPLS ブリッジング技法によって 2 つ以上のカスタマー デバイスを接続します。VPLS EoMPLS は、MPLS-Based プロバイダー コアです。PE ルータが協同でコア内の所定の VPLS インスタンスにカスタマーのイーサネット トラフィックを転送しなければなりません。VPLS は基本的にユーザの観点からイーサネット スイッチをエミュレートします。すべての接続は、VPLS 内のピア接続で、直接通信を行います。アーキテクチャには、実質的に、分散型スイッチのアーキテクチャが採用されています。プロバイダー コアにより、複数の接続回線が結合されます。プロバイダー コアは、これらの複数の接続回線を接続する仮想ブリッジをシミュレートする必要があります。これを行うため、VPLS インスタンスに参加するすべての PE ルータにより、エミュレート VC が形成されます。

PE ルータ上では、VPLS インスタンスごとに Virtual Forwarding Instance（VFI; 仮想転送インスタンス）が作成されます。PE ルータでは、特定の VPLS インスタンスの VFI を検索して、パケットの転送先が決定されます。VFI は、特定の VPLS インスタンスの仮想ブリッジのように動作します。この VFI には、特定の VPLS に属する 2 本以上の接続回線を接続できます。PE ルータは、その VPLS インスタンス内にあるすべての他の PE ルータに対するエミュレート VC を構築し、これらのエミュレート VC を VFI に接続します。パケットの転送先の決定は、VFI に維持されているデータ構造に基づいて行われます。VPLS ドメイン内のすべての PE ルータは、エミュレート VC を構築するため、同じ VC-ID を使用します。この VC-ID は、VPLS VPN では「VPN-ID」とも呼ばれます。

詳細については、次を参照してください。

- 「MPLS-Based プロバイダー コアで使用するマルチポイント EWS（EP-LAN）」（P.1-19）
- 「MPLS-Based プロバイダー コアで使用するマルチポイント ERS（EVP-LAN）」（P.1-19）
- 「MPLS-Based VPLS 用のトポロジ」（P.1-19）

MPLS-Based プロバイダー コアで使用するマルチポイント EWS（EP-LAN）

マルチポイント EWS（MEF 用語では「EP-LAN」とも呼ばれます）を使用して、PE ルータは接続回線から受信したすべてのイーサネット パケット（タグ付き、タグなし、Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）など）を次のいずれかに転送します。

- 別の接続回線またはエミュレート VC（宛先 MAC アドレスが L2 転送テーブル（VFI）に見つかった場合）。
- 他のすべての接続回線および同じ VPLS インスタンスに属するエミュレート VC（宛先 MAC アドレスがマルチキャスト/ブロードキャスト アドレスであるか、L2 転送テーブルに見つからなかった場合）。

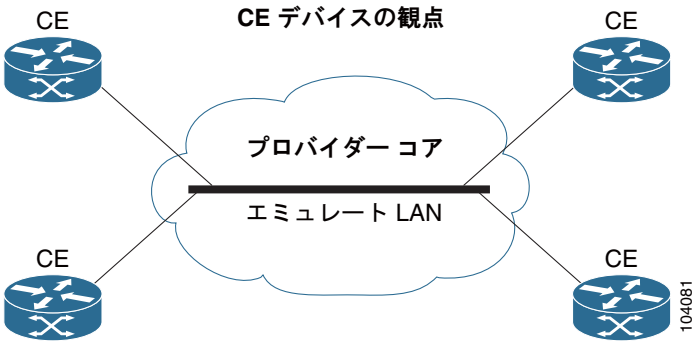
MPLS-Based プロバイダー コアで使用するマルチポイント ERS（EVP-LAN）

マルチポイント ERS（MEF 用語では「EVP-LAN」とも呼ばれます）を使用して、PE ルータは接続回線から受信した、特定の VLAN タグが設定されているすべてのイーサネット パケット（BPDU を除く）を他の接続回線またはエミュレート VC に転送します（宛先 MAC アドレスが L2 転送テーブル（VFI）に見つかった場合）。宛先 MAC アドレスが見つからないか、またはブロードキャスト/マルチキャスト パケットである場合は、他のすべての接続回線および同じ VPLS インスタンスに属するエミュレート VC に送信されます。VPLS ドメインの識別に使用される逆多重化 VLAN タグは、局部的な意味だけを持つものであるため、発信イーサネット インターフェイスまたはエミュレート VC にパケットを転送する前に削除されます。

MPLS-Based VPLS 用のトポロジ

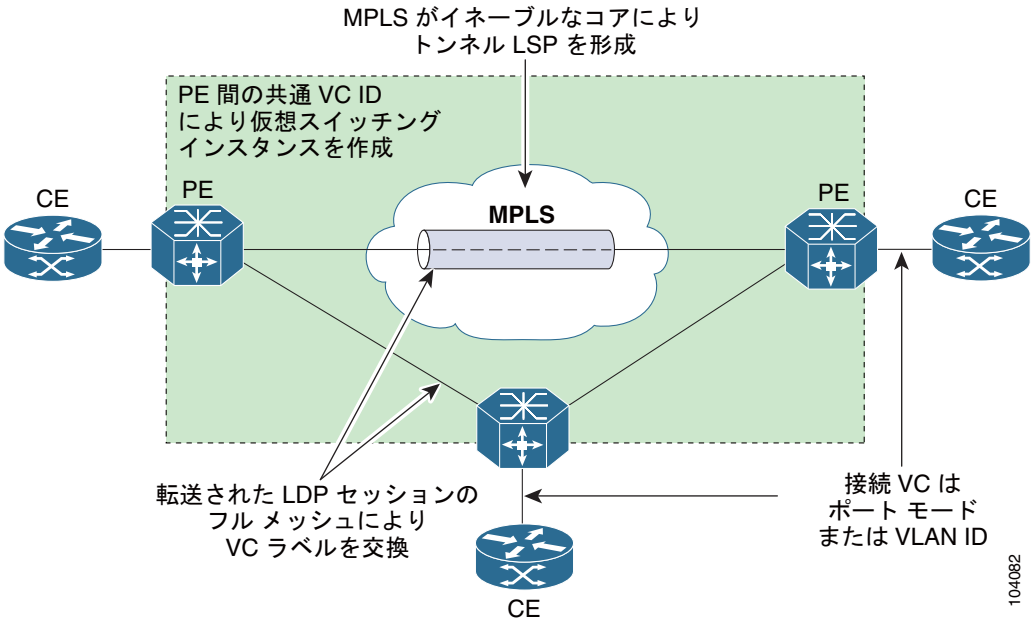
VPLS のトポロジは、カスタマーからは認識されません。すべての CE デバイスは、プロバイダー コアによってエミュレートされた論理ブリッジに接続されます。したがって、CE デバイスはエミュレートされた単一の LAN を認識することになります（図 1-9 を参照）。

図 1-9　MPLS-Based VPLS のトポロジ



PE ルータは、エミュレートされた仮想回線（VC）フル メッシュを作成し、CE デバイスで認識されるエミュレート LAN をシミュレートする必要があります。エミュレート VC のフル メッシュを形成することで、プロバイダー コアでの LAN のエミュレートのタスクが簡易化されます。LAN の 1 つの特性として、単一のブロードキャスト ドメインを維持することが挙げられます。つまり、ブロードキャスト、マルチキャスト、または不明なユニキャスト パケットがいずれかの接続回線で受信されると、パケットはその VPLS インスタンスに属する他のすべての CE デバイスに送信されます。これは、PE デバイスがパケットを他のすべての接続回線およびすべてのエミュレート回線に送信することで処理されます。このようなパケットは、エミュレート VC のフル メッシュを使用して、その VPLS インスタンスにある他のすべての PE デバイスに到達します（図 1-10 を参照）。

図 1-10　エミュレート VC のフル メッシュ



イーサネットベースの（L2）プロバイダー コアで使用する VPLS

イーサネットベースのプロバイダー コアを使用すると、カスタマー トラフィックの転送はコア内で簡単に行うことができます。イーサネットベースのプロバイダー コアに使用される VPLS はマルチポイント レイヤ 2 VPN で、802.1Q-in-Q タグ スタック構成テクノロジーを使用して 2 台以上のカスタマー デバイスを接続します。VPLS は基本的にユーザの観点からイーサネット スイッチをエミュレートします。すべての接続は、VPLS 内のピア接続で、直接通信を行います。アーキテクチャには、実質的に、分散型スイッチのアーキテクチャが採用されています。

イーサネットベースのプロバイダー コアに使用される VPLS の詳細については、次を参照してください。

- 「イーサネットベースのプロバイダー コアで使用するマルチポイント EWS（EP-LAN）」（P.1-21）
- 「イーサネットベースのプロバイダー コアで使用するマルチポイント ERS（EVP-LAN）」（P.1-21）
- 「イーサネットベースの VPLS 用のトポロジ」（P.1-21）

イーサネットベースのプロバイダー コアで使用するマルチポイント EWS（EP-LAN）

マルチポイント EWS（MEF 用語では「EP-LAN」とも呼ばれます）は、ポイントツーポイント イーサネット セグメントをエミュレートするサービスです。EWS サービスは、特定の User-to-Network Interface（UNI; ユーザネットワーク インターフェイス）で受信されたすべてのフレームをカプセル化し、そのコンテンツには関係なく、これらのフレームを単一の出力 UNI に転送します。このサービスの処理は、タグなしフレームまたは VLAN タグ付きフレームに EWS を使用できること、およびこのサービスはすべてのフレームに対して透過的であることを意味します。EWS サービスはカスタマー フレーム内にある VLAN タグを認識しないため、このサービスでは「All-to-One」バンドリングの概念が採用されています。

イーサネットベースのプロバイダー コアで使用するマルチポイント ERS（EVP-LAN）

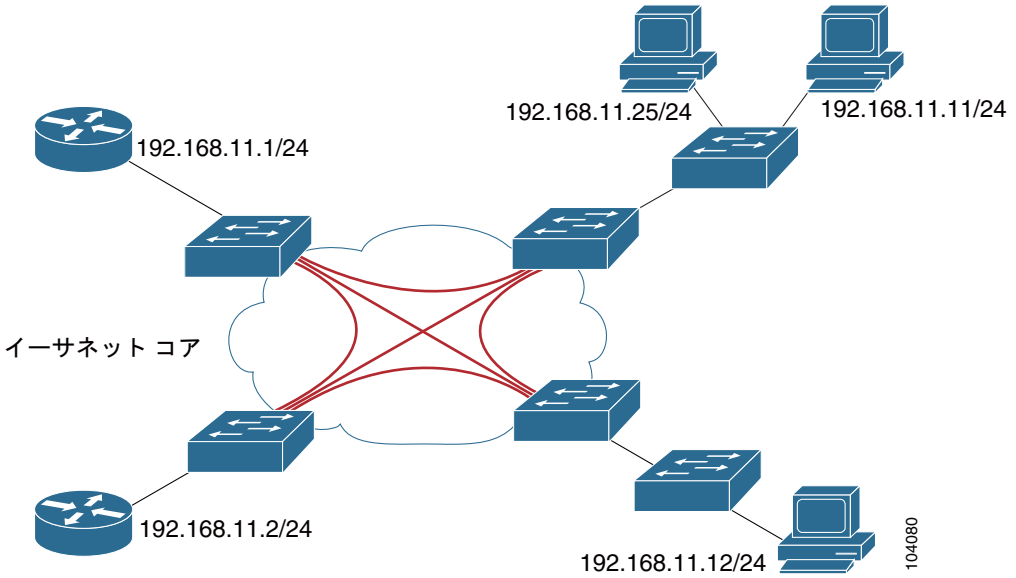
マルチポイント ERS（MEF 用語では「EVP-LAN」とも呼ばれます）は、VLAN インデックスを使用してサイト間の仮想回線を識別することで、既存のフレーム リレー ネットワークによって提供される接続をモデル化します。ただし、ERS は、サービス プロバイダーの実装およびカスタマーの VLAN インデックスの受け入れ状況（サービス プロバイダーによって左右されます）によって、はるかに高いレベルの QoS 機能を提供します。また、ERS サービス多重化機能により、単一インターフェイスでの多数の仮想インターフェイスのサポートが可能となるため、企業の所有コストが低減されます。

イーサネットベースの VPLS 用のトポロジ

イーサネットベースの VPLS はマルチポイント接続モデルを接続することから、EWS（EP-LAN）および ERS（EVP-LAN）のポイントツーポイント L2VPN 定義とは異なります。VPLS サービスでは、インターフェイスまたは VLAN を特定のポイントツーポイント疑似回線にマッピングすることはしませんが、代わりに、仮想イーサネット スイッチの動作をモデル化します。VPLS はカスタマーの MAC アドレスを使用して、対象 EWS（EP-LAN）のサービス プロバイダーのネットワーク内にある正しい出力 UNI にフレームを転送します。

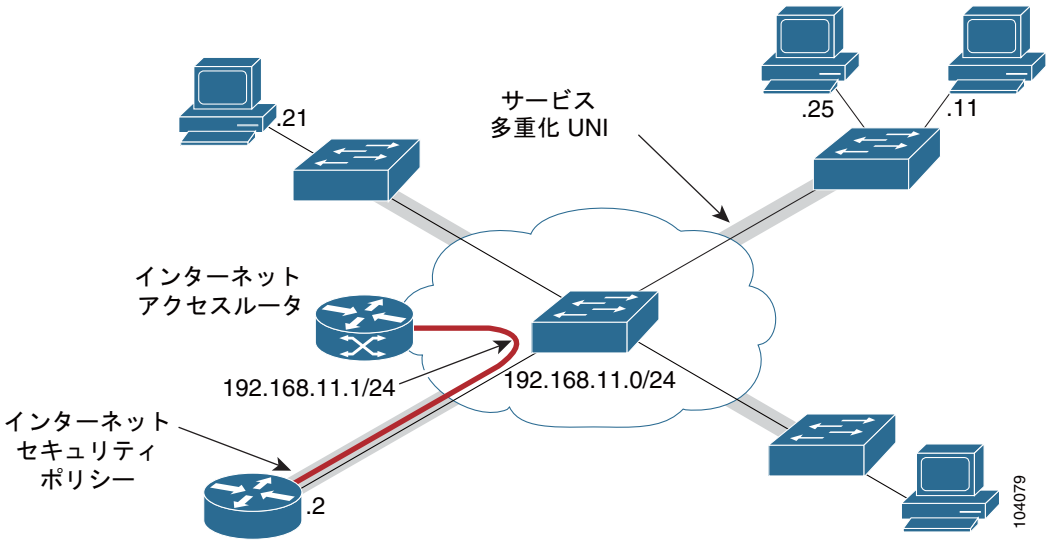
EWS（EP-LAN）サービスは、イーサネット スイッチのサービス属性をエミュレートし、送信元 MAC を学習して、不明なフラッディング ブロードキャストとマルチキャスト フレームのインターフェイスの関連付けを行います。図 1-11 に、EWS（EP-LAN）VPLS トポロジを示します。

図 1-11　VPLS EWS のトポロジ



イーサネット リレー サービス（ERS または EVP-LAN）は、EWS およびサービス多重化の Any-to-Any 接続特性を提供します。この組み合わせにより、カスタマーのイントラネット接続と 1 つ以上の追加の EVC をサポートする単一の UNI の構築が可能となり、外部ネットワーク、ISP、またはコンテンツ プロバイダーに接続できるようになります。図 1-12 に、ERS（EVP-LAN）VPLS マルチポイント トポロジを示します。

図 1-12　VPLS ERS（EVP-LAN）マルチポイント トポロジ



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。

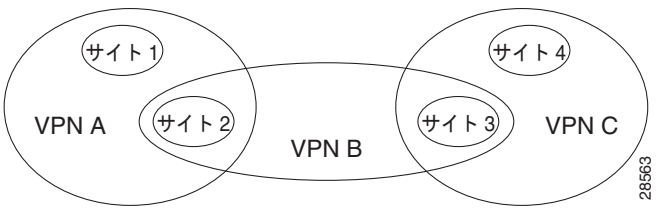
MPLS VPN

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
```

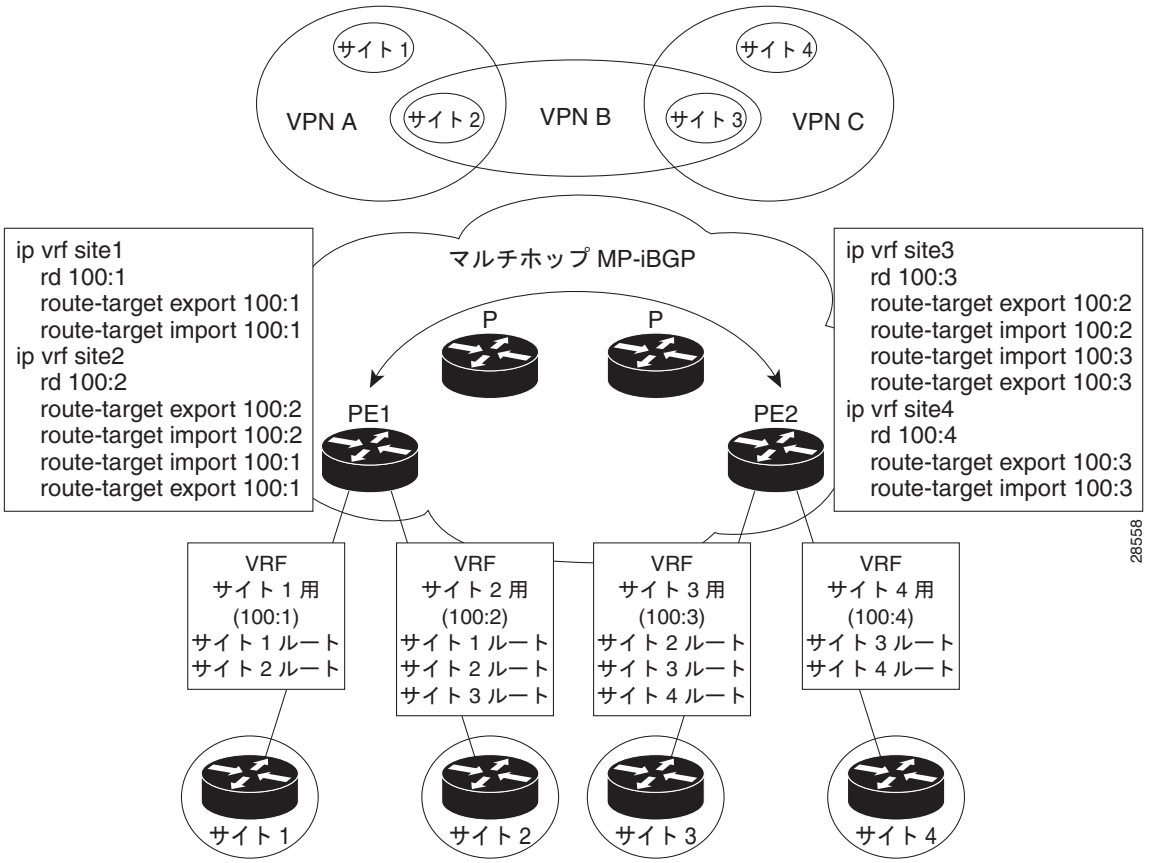
Green VPN 内のエクストラネット VPN トポロジの VRF には次のような名前が付けられます。

```
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。

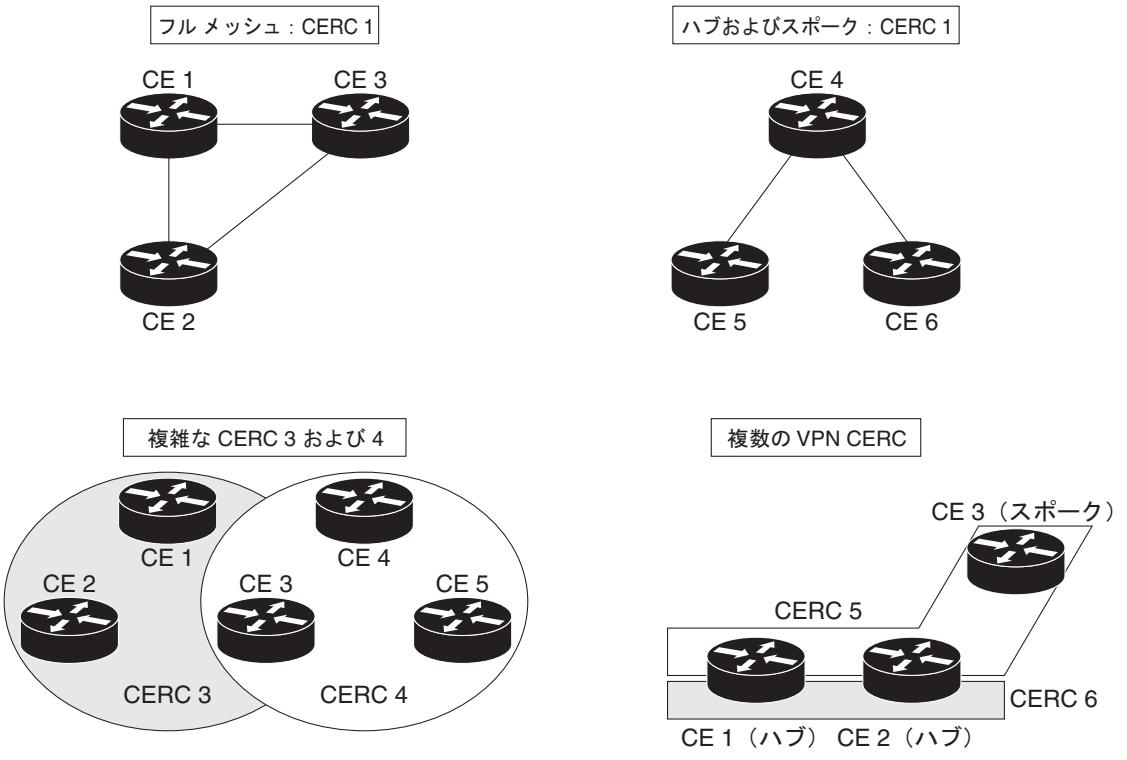
VPN を作成すると、Prime Fulfillment ソフトウェアにより、1 つのデフォルト ルート ターゲットが作成されます。したがって、高度なカスタマー レイアウト方法が必要となるまでは、新しいルート ターゲットを定義する必要はありません。それまでは、ルート ターゲットが VPN それ自体を表していると考えることができます。つまり、ルート ターゲットと VPN は同一のものです。何らかの理由で、ソフトウェアが選択したルート ターゲット値を変更する必要がある場合、その変更は Prime Fulfillment ソフトウェアでルート ターゲットを作成するときにのみ可能です。

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。

CHAPTER 3

トラフィック エンジニアリング管理の概念

この章では、Cisco Prime Fulfillment およびこのガイドで使用する概念について概説します。この章では、次の項について説明します。

Prime FulfillmentTEM の概要

TEM は、Prime Fulfillment のトラフィック エンジニアリング管理モジュールです。トラフィックの Service Level Agreement（SLA; サービス レベル契約）に基づく保証の提供を目的として Multiprotocol Label Switching Traffic Engineering（MPLS TE; マルチプロトコル ラベル スイッチング）プライマリ トンネルおよびバックアップ トンネルを管理するためのツールです。TEM は、帯域幅保護管理とネットワーク検出の機能を提供し、MPLS TE の設定をサポートします。また、高度なプライマリ パス計算ツールや要素保護のためのバックアップ トンネル計算機能など、多くの強力な計画ツールが含まれています。

予測可能性の要件、QoS 要件に適合するトラフィック フロー、および保証帯域幅による迅速な復旧をサポートするための MPLS TE メカニズムを搭載しており、厳格な SLA パフォーマンス基準（アベイラビリティ、遅延、ジッター）を確実に満たします。

Prime Fulfillment の機能

Prime Fulfillment は、次のような各種の MPLS TE プライマリ トンネル管理機能を提供します。

- Tunnel Audit：トンネルの変更後に不一致を検出します。
- Tunnel Admission：新しいトンネルをネットワークに受け入れます。
- Tunnel Repair：ネットワークやサービスの変更後にトンネルの不一致を解決します。
- Network Grooming：ネットワーク全体の利用を最適化します。

さらに、Prime Fulfillment は次のような Prime Fulfillment 機能との連携および統合も実現します。

- サービス アクティベーション フォーカス
- 他の Prime Fulfillment モジュールとの統合
- データの永続化
- ユーザ インテントのロギング
- サービス状態管理
- サービス監査
- Web ベースの GUI
- Role Based Access Control（RBAC; ロール ベース アクセス コントロール）

Prime Fulfillment TEM の基礎

Prime Fulfillment の機能を理解するためには、いくつかの主要な概念について把握する必要があります。

Managed/Unmanaged プライマリ トンネル

Prime Fulfillment では、Managed トンネルの概念が TE 計画作業の中心を成します。

次のような違いを理解する必要があります。

- Managed TE トンネル：
  - （設定 / 保持）優先順位 0
  - 0 以外の RSVP 帯域幅
  - 最初のパス オプションが明示パス
  - 自動帯域幅には最大値が必要
- Unmanaged トンネル：その他すべてのトンネル

Prime Fulfillment の Graphical User Interface（GUI; グラフィカル ユーザ インターフェイス）には、Managed トンネルと Unmanaged トンネルを操作するための別個のエントリ ポイントがあります。

Conformant/Non-Conformant トンネル

Conformant トンネルと Non-Conformant トンネルについて理解することは、Prime Fulfillment を効率的に使用するために不可欠です。

Prime Fulfillment では、Conformant トンネルのみ作成できます。Non-conformant トンネルは、TE 検出プロセスを介して導入できます（ユーザ ガイドの Chapter 36, “TE Network Discovery” を参照）。

Conformant/Non-Conformant トンネルの定義

Prime Fulfillment の設計では、Conformant トンネルと Non-Conformant トンネルが次のように厳格に区別されています。

- Conformant トンネル : Prime Fulfillment の TE 管理パラダイム（下記を参照）を満たす正常に動作するトンネルです。Managed トンネルは Conformant トンネルにのみなることができます。優先順位が 0 以外である Unmanaged トンネルも Conformant トンネルになることがあります。ただし、Conformant トンネルは必ずしも Managed トンネルではありません。

  接続保護トンネルは、トンネル帯域幅が 0 で、バックアップ帯域幅が無制限であり、最初のパス オプションが「exclude address」である場合は、Conformant = true とマークされます。BW Protected 設定では、トンネルのバックアップ帯域幅が 0 以外に設定され、ストリクト パス オプション 1 が選択されている必要があります。

- Non-Conformant トンネル : Prime Fulfillment の帯域幅保証を満たす能力に影響する可能性のある TE トンネルです。自動帯域幅に最大帯域幅が未設定、プリエンプションの可能性、ダイナミック パスなど、未知の帯域幅要件が原因で発生することがあります。優先順位が 0 である Unmanaged トンネルも Non-Conformant トンネルになることがあります。

  次に、Non-Conformant トンネルの例を示します。

  - 設定および保持優先順位が 0 で、最初のパス オプションが明示パスであるが、帯域幅は 0 であるトンネル
  - 設定および保持優先順位が 0 で、帯域幅は 0 以外であるが、最初のパス オプションがダイナミック パスであるトンネル
  - 設定および保持優先順位が 0 で、明示パス オプションが 1 であり、自動帯域幅の最大値が定義されていないトンネル
  - Conformant = false とマークされた接続保護トンネルは、バックアップ トンネルのために予約されており、トンネル帯域幅 0、無制限のバックアップ帯域幅、最初のパス オプション「exclude address」のいずれも設定されていません。

  上記のトンネルは、なぜ Non-Conformant なのでしょうか。Prime Fulfillment は、設定および保持優先順位が 0 であるトンネルをすべて管理し、それらが通過するリンクがいずれも十分な帯域幅を持ち、アフィニティが一致、TE ポリシーに定義された遅延または FRR 制約に違反しないことを確認するからです。

  ただし、トンネルのパスがダイナミック パスであるか、トンネルが必要とする帯域幅の量が定義されていない場合、Prime Fulfillment はトンネルの管理に必要な情報を得られないため、そのトンネルを Non-Conformant とマークします。すべての Non-Conformant トンネルは [TE Unmanaged Primary Tunnels SR] ウィンドウに表示されます。

Non-Conformant トンネルの管理

Non-Conformant トンネルは、SLA 違反の原因となる可能性があるだけでなく、Managed トンネルに悪影響（帯域幅を奪うなど）を与えるおそれもあることを理解しておくことが重要です。

ただし、Non-Conformant トンネルが検出されたときには、警告が記録されます。Prime Fulfillment は、Non-Conformant トンネルを追跡して廃棄します。

したがって、Conformant トンネルの方が望ましいと言えます。Conformant トンネルによって、システムは Managed トンネルの帯域幅保証を提供できます。Unmanaged Non-Conformant トンネルは、必要な帯域幅を提供したりしなかったりするため、帯域幅保証は提供されません。

Non-Conformant トンネルがある場合は、設定および保持優先順位を 0 以外の値に変更する（Managed トンネルに対するプリエンプション処理を実行できないようにするため）か、Managed トンネルに移行させてツールが適切な明示パスを検出できるようにします。

複数の同時実行ユーザ

以前のリリースでは、TEM は単一の GUI ユーザしかサポートしていませんでした。本リリースは、ブラウジング、更新、プロビジョニングのいずれの操作においても複数の同時実行ユーザをサポートします。

Managed トンネルと Unmanaged トンネルの同時使用

複数ユーザ機能が TEM にどのように実装されているかを理解するためには、Managed トンネルと Unmanaged トンネルの違いを理解することが重要です。これについては、F-2 ページの「Managed/Unmanaged プライマリ トンネル」を参照してください。

複数ユーザのサポートに関しては、Managed トンネルと Unmanaged トンネルの処理方法に大きな違いがあります。

- Managed トンネルは、すべて SR によってカプセル化されます。SR の操作により、Router Generator サーバによるパス計算の後にスナップショット内のすべてのオブジェクトが最適化される可能性があります。
- Unmanaged トンネルの場合、SR はトンネルヘッド エンド ルータとして定義されます。そのため、Unmanaged トンネルには、いくつかの制限があります。たとえば、2 人のユーザが同じデバイスで同時にプロビジョニングすることはできません。
- TEM は、Unmanaged トンネル SR が同じデバイスで同時にプロビジョニングすることを許可しませんが、Unmanaged トンネル SR による複数のデバイスでの同時プロビジョニングはサポートします。
- Managed トンネルは、すべて各 TE プロバイダーの共有 Managed TE トンネル SR 内に存在します。Unmanaged トンネルの場合は、ヘッド デバイスごとに別個の Unmanaged TE トンネル サービス要求が作成されます。TEM は、1 つの TE プロバイダーにつき複数の SR をサポートします。

複数の TEM ユーザが TEM でブラウジングおよびプロビジョニングを実行できます。最大 20 人までの同時ユーザがサポートされ、そのうちの 7 人までがプロビジョニング タスクを実行できます。

以前は、Managed と Unmanaged の両方のプライマリ トンネルがすべて TE プロバイダーごとに 1 つの TE トンネル SR に存在していました。現在は、Managed トンネルへの複数の同時変更を可能にするために、TE トンネル SR が TE プロバイダーあたり 1 つの Managed トンネル SR とヘッド TE ルータあたり 1 つの Unmanaged トンネル SR に分割されています。

同じ SR で並行プロビジョニングを行うことはできませんが、Unmanaged トンネルについては SR がルータ レベルで存在するため、Unmanaged トンネルを同時に複数のルータにプロビジョニングすることができます。

ロッキング メカニズム

Unmanaged トンネルをプロビジョニングすると、そのトンネルのヘッド TE ルータがロックされます。ロックされていることは、[TE Nodes] ウィンドウの [System Lock Status] 列で確認できます。ロッキングによって、プロビジョニング タスクが完了し、TE ルータのロックが解除されるまで、他のユーザはそのルータにどのような種類のトンネルも配置できなくなります。

ロッキング メカニズムは、バックアップ トンネル、リソース SR、リンク削除、TE トラフィック アドミッションなどの Prime Fulfillment 機能にも適用されます。リソース SR には、明示パスの削除/編集、保護要素の削除、SRLG の削除/編集などが含まれます。

リンク削除の場合、一定レベルのインテリジェンス機能が組み込まれています。ユーザまたは Prime Fulfillment によって再ルーティングまたは削除できるトンネルが存在せず、TE 関連オブジェクトだけが残っている場合、リンクを削除するためには、ユーザによる介入が必要となります。このとき、削除対象として選択されたインターフェイスを保護するバックアップ トンネルがある場合は、バックアップ トンネルを配置する操作の実行中、ロッキング メカニズムが働きます。TE リンクの削除の詳細については、ユーザ ガイドの Deleting TE Links, page 37-5 を参照してください。

発生する可能性のあるエラーについては、ユーザ ガイドの Locking Operation Errors, page 42-10 を参照してください。

Managed プライマリ トンネルまたはバックアップ トンネルをプロビジョニングすると、そのトンネルに関連付けられている TE プロバイダーがロックされます。ロックされていることは、[TE Provider] ウィンドウの [System Lock Status] 列で確認できます。TE プロバイダー レベルのロックによって、トンネルがどの TE ルータを起点としているかに関係なく、別のユーザがその TE プロバイダーでトンネルを変更することを防止できます。

Managed トンネルおよびバックアップ トンネルのロッキング メカニズムと Unmanaged トンネルのロッキング メカニズムが異なるのは、Managed トンネルとバックアップ トンネルがすべての制約を満たす最適なルートを見つけるためにパス生成アルゴリズムを使用し、そのアルゴリズムが、ルーティング決定基準として、TE トポロジとそこに含まれるすべてのトンネルの安定したグローバル ビューを必要とするからです。これを実現する唯一の方法は、一度に 1 人のユーザだけが変更を実行できるようにすることです。

Prime Fulfillment のロッキング メカニズムを管理する方法の詳細については、ユーザ ガイドの Managing the Locking Mechanism, page 42-9 を参照してください。

複数の OSPF 領域

Prime Fulfillment は、複数の Open Shortest Path First（OSPF）内での TE トンネルの検出、管理、プロビジョニングをサポートします。

Prime Fulfillment の管理対象となるのは、OSPF 領域の範囲内にあるプライマリ TE トンネルとバックアップ TE トンネルだけです。複数の OSPF 領域にまたがる検出および作成はサポートしていません。

Prime Fulfillment では、OSPF 領域は TE プロバイダーによって表されます。領域を TE プロバイダーに割り当てた後で変更することはできません。1 つの Prime Fulfillment プロバイダーに複数の TE プロバイダーを関連付けることができます。

TE 検出に適したデバイス

複数の OSPF 領域があるネットワークでは、各 OSPF 領域が TE プロバイダーで表されるため、OSPF 領域内のどのルータでも TE 検出に使用できます。1 つのプロバイダーに属する複数の TE プロバイダー（複数の OSPF 領域）を使用することにより、複数の領域にまたがる L3VPN のプロビジョニングが可能になります。

（注）　Prime Fulfillment は、複数の領域にまたがる TE トンネル（ある領域にヘッド ルータがあり、別の領域にテール ルータがあるトンネル）を検出またはプロビジョニングしません。

複数の領域があるネットワークを検出するためには、TE 検出を使用して各領域を順に検出する必要があります（ユーザ ガイドの Chapter 36, “TE Network Discovery” を参照）。シード ノードは、Area Border Router（ABR; エリア境界ルータ）を含め、領域内のどのデバイスでもかまいません。

TE 検出と TE 領域 ID

TE 検出には TE プロバイダーが関連付けられ、各 TE プロバイダーには領域が割り当てられます。この領域は TE プロバイダーの作成プロセスで割り当てられます（ユーザ ガイドの Creating a TE Provider, page 35-8 を参照）。この領域は単純な整数値またはドット付き 10 進表記（領域 0.6.0.0 など）です。

TE プロバイダー オブジェクトは、作成時の指定または検出時の自動入力によって対象とする領域を認識し、ドット表記と 10 進表記の変換に対応します。デフォルトはネットワークで使用されている表記です。

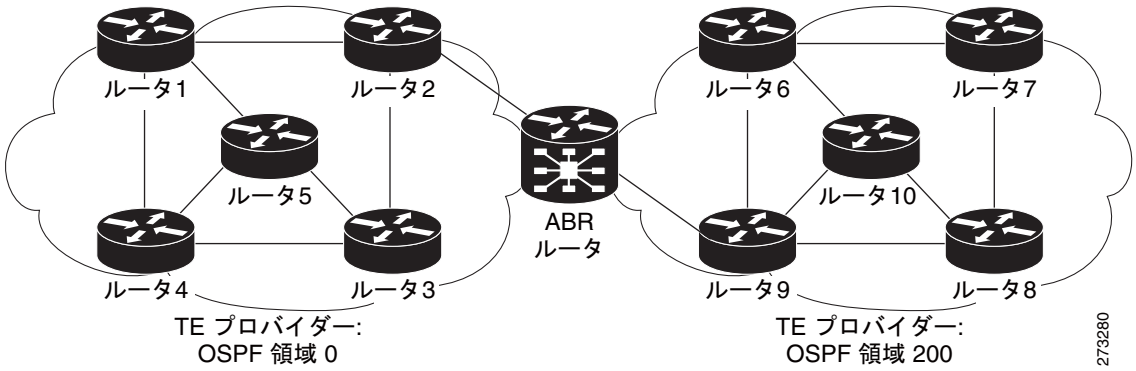
選択した TE プロバイダーがある領域に対して検出を実行すると、その領域に関連付けられたすべてのトンネルおよび明示パスが Prime Fulfillment データベースにインポートされます。領域単位の検出の実行手順については、ユーザ ガイドの Managing Per Area Discovery, page 36-5 を参照してください。

複数の OSPF 領域があるネットワークの例

TE プロバイダー内の TE ルータを複数のリージョン（地域など）に割り当てることにより、デバイスを論理的な基準に基づいてリージョンにグループ化できます。また、Prime Fulfillment ではリージョンに基づくフィルタリングが可能です。オブジェクトを特定のリージョンに割り当てるには、検出の実行後、[Inventory] > [Provider Devices] から手動で行います。PE デバイスのリージョンは、[Select Region] ポップアップ ウィンドウで変更できます。

次の図 3-1 に示す例では、2 つの TE プロバイダーがそれぞれ 1 つの Prime Fulfillment プロバイダー内に作成され、視覚化された 1 つの OSPF 領域を担当します。

図 3-1　　複数の OSPF 領域があるネットワーク



TE の管理方法については、ユーザ ガイドの Creating a TE Provider, page 35-8 を参照してください。

帯域幅プール

各 TE 対応のインターフェイスの帯域幅には、ネストされた複数の帯域幅プールが割り当てられます。現在、IOS は、グローバル プールとサブ プールという 2 種類の帯域幅プールをサポートしています。

帯域幅プールについての理解を深めるために、図 3-2 を参照してください。

図 3-2　　帯域幅プール

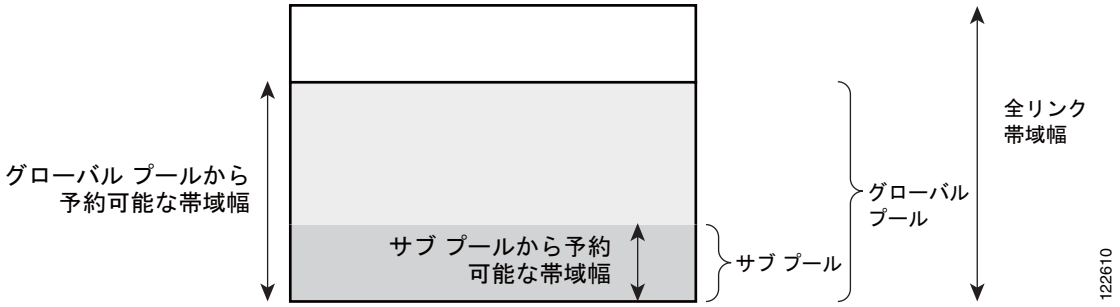


図 3-2 に示すように、サブ プールはグローバル プール内にネストされています。したがって、プライマリ トンネルがサブ プールから帯域幅を予約すると、同じ帯域幅がグローバル プールでも予約されます。

サブ プールでの帯域予約（プライマリ トンネル）は、合計でサブ プールのサイズを超えてはなりません。同様に、グローバル プールでの帯域予約は、合計でグローバル プールのサイズを超えてはなりません。

計画ツール

ここでは、トラフィック エンジニアリングされたネットワークの改善計画を What-If シナリオを基づいて評価するためのツールについて説明します。

計画ツールには、次の機能が含まれます。

- プライマリ計画ツール：
  - Tunnel Audit：トンネルまたはリソースの変更が提案されているかどうかにかかわらず、既存のネットワークのプライマリ配置に不一致がないかどうか調べます。
  - Tunnel Placement：通常は、新しいトンネルに使用します。Tunnel Placement では、新しいルートを生成できます。この機能は、それまでパスがなく、配置することが必要なトンネルに使用できます。
  - Tunnel Repair：Tunnel Audit の実行後（問題が検出された場合）に実行します。Tunnel Repair には再ルーティング機能があり、トンネルの移動に使用できます。
  - Grooming：ネットワーク全体を対象とする最適化ツールです。トンネルの属性が変更されていない場合にのみ使用できます。
- 保護計画ツール：
  - Audit SR：手動で追加、変更、削除されたバックアップ トンネルについて、配置前に保護の状態を調べます。
  - Compute Backup：選択されたネットワーク要素に最適なバックアップ トンネルを自動的に計算します。
  - Audit Protection：選択された要素の保護を既存のバックアップ トンネルの観点から監査します。

これらの計画ツールは Prime Fulfillment に完全に統合されており、次のような GUI のさまざまな場所から使用できます。

- TE Protected Elements（Compute Backup および Audit Protection）
- Create Managed TE Tunnel（Tunnel Audit、Tunnel Placement、Tunnel Repair、Grooming）
- Create TE Backup Tunnel（Audit SR）

接続保護（CSPF）バックアップ トンネル

TEM によって作成される帯域幅保護のバックアップ トンネルに加え、一連の CSPF-routed バックアップ トンネルも Prime Fulfillment 内に作成できます。CSPF-routed バックアップ トンネルは、[TE Protection SR] ウィンドウで管理します。

接続保護バックアップ トンネルは「exclude-address」明示パスを使用します。この明示パスは [TE Explicit Path List] ウィンドウで作成します。exclude address パスは、パスが使用するホップではなくパスが回避するホップを示す点で strict パスと異なります。どのパスが最適であるかはルータ上の CSPF アルゴリズムによって決定されますが、このアルゴリズムには exclude address パス設定のホップを使用できないという制約があります。この種のパスは、特にバックアップ トンネルで役に立ちます。exclude address パスが回避する必要のあるインターフェイスは、バックアップ トンネルの保護対象である可能性があるからです。

Prime Fulfillment では、これらのバックアップ トンネルに無制限のバックアップ帯域幅が設定されます。無制限とは帯域幅が保証されないことを意味しますが、障害発生時に使用可能な最大限の帯域幅が使用されます。そのため、帯域幅保護は実質的にベスト エフォートです。ただし、接続は保証されます。接続保護バックアップ トンネルは、帯域幅保護バックアップ トンネルへの追加または代替として使用できます。

帯域幅保護バックアップ トンネルと接続保護バックアップ トンネルには、次のような違いがあります。

- 帯域幅保護バックアップ トンネルの最初のパス オプションはストリクト明示パスであるのに対し、接続保護バックアップ トンネルの最初のパス オプションは exclude address 明示パスです。
- 帯域幅保護バックアップ トンネルにはバックアップ帯域幅が定義されているのに対し、接続保護バックアップ トンネルでは無制限のバックアップ帯域幅がベスト エフォート方式で使用されます。
- 帯域幅保護バックアップ トンネルは、最適なバックアップ トンネルを生成して既存のトンネルが要素を完全に保護することを確認するルート ジェネレータ アルゴリズムに渡されるのに対し、接続保護バックアップ トンネルはルート ジェネレータ アルゴリズムに渡されないため、トンネルが目的を果たしていることをユーザが確認する必要があります。

クラスベース トンネル選択

マルチプロトコル ラベル スイッチング トラフィック エンジニアリング Class-Based Tunnel Selection（CBTS; クラスベース トンネル選択）を使用すると、同一トンネル ヘッド エンドと同一テール エンド間でさまざまな TE トンネルに、さまざまな Class of Service（CoS; サービス クラス）値を指定して、トラフィックを動的にルーティングおよび転送できます。パケットの CoS 値は EXP ビット内にあります。8 個の EXP ビットがあり、0 ～ 7 の番号が付いています。

同一ヘッド エンドから同一テール エンドへの TE（または DS-TE）トンネルは、複数の CoS 値を持つように設定できます。設定後、CBTS は、次の要件を満たすトンネルに各パケットを動的にルーティングして転送します。

- 標準の自動ルートまたはスタティック ルートを使用してトラフィック アドミッションの対象として選択されている。
- EXP ビットがパケットの EXP ビットと一致している。

したがって、CBTS は、TE トンネルへの直接のトラフィック アドミッションではなく、トラフィックが TEM でサポートされる自動ルートまたはスタティック ルート メカニズムによってトンネルに入る前に満たす必要のある追加の基準です。

CBTS は DS-TE トンネル経由でダイナミック ルーティングを行い、設定が最小限で済むので、大規模なネットワークにおいて DS-TE の配置が大幅に軽減されます。CBTS は、すべての CoS 値をさまざまな種類のトンネルに配布できます。

CBTS 機能には次の制限があります。

- 1 つの宛先について、同じテール エンドで終端するトンネルを使用してすべての CoS 値が伝送されます。すべての CoS 値がトンネルで伝送されるか、またはトンネルでまったく値が伝送されないかのいずれかです。したがって、1 つの宛先について、一部の CoS 値を DS-TE トンネルでマッピングし、その他の CoS 値を Shortest Path First（SPF; 最短パス優先）Label Distribution Protocol（LDP; ラベル配布プロトコル）または SPF IP パスでマッピングすることはできません。
- CBTS では、複数のトンネルで特定の EXP 値のロードバランスを図ることはできません。2 つ以上のトンネルが特定の experimental（EXP）値を伝送するように設定されている場合、CBTS はその中から 1 つのトンネルを選択して、この EXP 値を伝送します。
- Any Transport over MPLS（AToM）、MPLS TE Automesh、または Label-Controlled（LC）-ATM では、CBTS の動作はサポートされません。

グローバル スタティック ルートを使用してトンネルへのトラフィック アドミッションが行われ、特定の宛先に対し、管理上の重みが同じであるトンネルが複数ある場合は、CBTS 属性がトンネルの選択基準となります（上記の CBTS でのロードバランスに関する説明を参照してください）。

ポリシーベース トンネル選択

マルチプロトコル ラベル スイッチング トラフィック エンジニアリング Policy-Based Tunnel Selection（PBTS; ポリシーベース トンネル選択）を使用すると、トラフィックを同一トンネル ヘッド エンドと同一テール エンド間でさまざまな TE トンネルにポリシーに基づいて動的にルーティングおよび転送できます。ルーティング アルゴリズムは、フォワーディング ルックアップの前にヘッドエンド ルータの入力インターフェイスで実行されます。

Prime Fulfillment の PBTS 実装では、トラフィックはインターフェイス コマンド policy-class を使用して特定の TE トンネルに転送されます。CBTS は IOS デバイスを対象としていますが、PBTS は IOS XR デバイス用に厳密に設計されています。

CBTS と同じように、PBTS は、TE トンネルへの直接のトラフィック アドミッションではなく、トラフィックが TEM でサポートされる自動ルートまたはスタティック ルート メカニズムによってトンネルに入る前に満たす必要のある追加の基準です。

（注）　Prime Fulfillment は、ポリシー クラスをプロビジョニングするわけではなく、トンネルに既存のポリシー クラスを関連付けるだけです。そのためには、policy-class 属性を 1 ～ 7 の値に設定します。

CBTS の詳細については、「クラスベース トンネル選択」（P.3-8）を参照してください。

PBTS および IOS XR の一般的な情報については、
http://www.cisco.com/en/US/docs/ios_xr_sw/iosxr_r3.7/mpls/configuration/guide/gc37te.html#wp1325561
を参照してください。

CHAPTER 4

Prime Diagnostics の概要

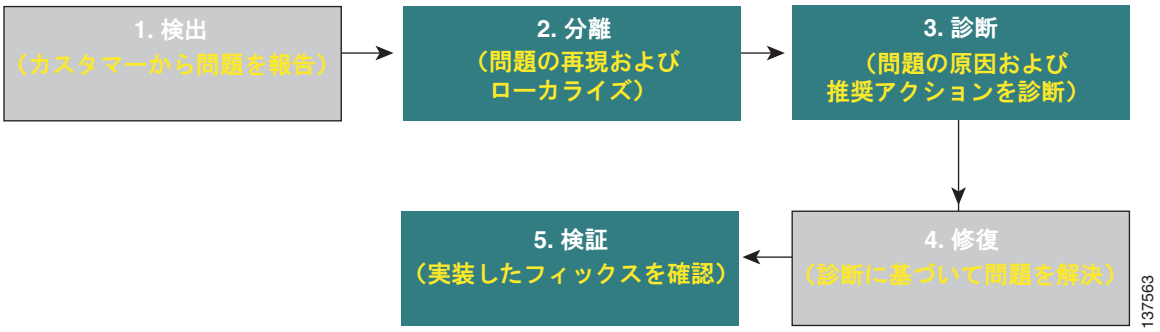
Prime Diagnostics は自動化されたワークフローベースのネットワーク管理アプリケーションで、Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）VPN における問題の診断やトラブルシューティングを行います。このアプリケーションは、MPLS に関連するネットワーク停止の診断に要する時間を削減するための機能を提供します。多くの場合、時間単位から分単位に短縮されます。MPLS アクセス、エッジ、およびコア ネットワーク全体にわたるネットワーク障害シナリオの分析に基づいて、診断が行われます。この診断は、サービス プロバイダー、および企業が自ら展開した MPLS VPN ネットワークの両方で同様に実行されます。Network Operations Center（NOC; ネットワーク オペレーション センター）は技術者をサポートします。本製品以降は、第 2 次および第 3 次のサポートも受けることができるようになりました。Prime Diagnostics は、オプションで、Prime Fulfillment MPLS VPN プロビジョニング コンポーネントと統合できます。MPLS VPN の中核となる問題を診断するには、Label-Switched Path（LSP; ラベルスイッチド パス）ping および LSP traceroute など、MPLS のオペレーションおよびメンテナンス（OAM）機能をサポートする Cisco IOS ソフトウェア リリースおよび IOS XR ソフトウェア リリースが必要です。

障害の発見やトラブルシューティングを効果的に行うため、次の 5 つのステップを踏みます。

1. 検知
2. 分離
3. 診断
4. 修復
5. 検証

Prime Diagnostics は、エンド ユーザが VPN サービスの問題を報告する、反応的な状況をサポートするように設計されています。これは、基本的に、図 4-1 の「診断」のステップに該当します。ルータ デバイスに加えられた変更を徹底して自ら管理し、それを行うための社内手順を定めているプロバイダーが多いため、「修復」機能はサポートされません。

図 4-1　反応的な障害ライフサイクル



（注）　Prime Diagnostics が実行するのは、ステップ 2、3、および 5 です。ステップ 1 と 4 は手動で実行する必要があります。

Prime Diagnostics は、「分離」、「診断」、および「検証」のステップを重点的に扱います。ネットワークでの障害の分離および診断、障害の発生したデバイスの特定、適切なデバイス ステータスのチェック、および障害発生の考えられる理由を特定するための設定を行うための貴重な機能を提供します。また、Prime Diagnostics は、デバイス設定に加えた変更によって問題が解決されたことを検証するため、テストを再実行する機能も提供します。

この機能は、Prime Fulfillment の他のモジュール（VPN プロビジョニングまたはトラフィック エンジニアリング管理など）に依存することなく、単独で使用できます。また、他の Prime Fulfillment モジュールを使用する Prime Fulfillment インストールで使うこともできます。MPLS VPN プロビジョニング機能を使用する場合、トラブルシューティングのスターティング ポイントとしてカスタマー データおよび VPN データを使用して、接続をテストするエンドポイント（カスタマー エッジ デバイスなど）を特定できます。

Prime Diagnostics は、トラブルシューティングだけでなく、VPN ポストプロビジョニング チェックにも使用できます。VPN を展開した後、手動でまたは Prime Fulfillment VPN プロビジョニング機能を使用して接続テストを実行し、VPN が正常にプロビジョニングされているかどうかを検証できます。

（注）　Prime Diagnostics は、トラブルシューティング中に基本的な設定やルーティングの変更を行う機能はサポートしていません。Prime Diagnostics の実行中、オペレータが加えた変更やルータのコントロール プレーンを使用して加えた変更は、実際のトラブルシューティングには反映されません。このような変更が加えられた場合、Prime Diagnostics で正しい障害シナリオや観察の結果が得られるとは限りません。

IPv6

Internet Assigned Numbers Authority（IANA）が管理する IPv4 アドレス フリー プールが残り少なくなってきています。シスコは、この事態に対応するため、IPv6 アドレス指定を採用しています。

Prime Diagnostics は、IPv4 と IPv6 の両方のアドレスを備えるデバイスの設定および選択をサポートします。Prime Diagnostics では、接続回線が次に該当する場合に MPLS VPN サービスのトラブルシューティングを行うことができます。

- IPv6 アドレス指定を使用する場合
- デュアルスタックの IPv4/IPv6 アドレス指定を使用する場合

デュアルスタックは、同じインターフェイス上に IPv4 と IPv6 の両方を共存させるための技術です。（永続的にではないにせよ）長期にわたり、インターネット上に IPv6 ノードと IPv4 ノードが混在することになります。このため、IPv4 ノードを大規模に展開している企業では、IPv4 から IPv6 への移行を成功させることがとても重要です。たとえば、単一のインターフェイスを、IPv4 アドレスと IPv6 アドレスの両方を持つように設定できます。「デュアルスタック」と呼ばれるあらゆる要素（プロバイダー エッジやカスタマー エッジ ルータなど）は、IPv4 だけでなく、IPv6 アドレス指定およびルーティング プロトコルも実行します。

（注）　Prime Diagnostics がサポートするのは、グローバル ユニキャスト IPv6 アドレスだけです。グローバル ユニキャスト アドレスの機能は、131.107.1.100 のような IPv4 ユニキャスト アドレスと類似しています。つまり、これらのアドレスは、従来型の、公的にルーティング可能なアドレスであると言えます。グローバル ユニキャスト アドレスには、グローバル ルーティング プレフィクス、サブネット ID、およびインターフェイス ID が含まれます。

表 4-1　一般的なユニキャスト アドレス構造

フィールド	ネットワーク プレフィクス	サブネット	インターフェイス ID
Bits	48	16	64

（注）　Prime Diagnostics では、接続回線エンドポイントが IPv6 と IPv6 の場合、IPv4 と IPv4 の場合のいずれにおいてもテストを起動できます。両方のアドレス指定を混在させることはできません。

IPv6 アドレスでテストを開始する場合の詳細については、『Cisco Prime Fulfillment User Guide 6.1』を参照してください。

APPENDIX A

MPLS サービス要求の状態移行

この章では、MPLS のサービス要求の状態移行について説明します。

表 A-1 および表 A-2（P.A-2）に、Prime Fulfillment サービス要求の状態移行の順序を示します。最初の列にサービス要求の開始状態、見出し行にサービス要求が移行する状態を示します。

たとえば、表 A-1 を使用して「Pending」のサービス要求の状態を「Functional」の状態まで追跡するには、最初の列で「**Pending**」を探し、見出しが「**Functional**」の列まで右に移動します。「Pending」から「Functional」までサービス要求の状態を順に見ていくと、正しい順序での監査を行わなければならないことを理解できます。

表 A-1 に、「*Requested*」から「*Lost*」までのサービス要求の移行を示します。

表 A-1　Prime Fulfillment サービス要求の状態移行順序（パート 1）

サービス要求状態	Requested	Pending	Failed Audit	Deployed	Functional	Lost
Requested	「Requested」への移行なし	サービス要求展開中	「Failed Audit」への移行なし	「Deployed」への移行なし	「Functional」への移行なし	「Lost」への移行なし
Pending	「Requested」への移行なし	サービス要求展開中	「Audit」不成功	「Audit」成功	正しい順序での監査成功	「Lost」への移行なし
Failed Audit	「Requested」への移行なし	サービス要求再展開中	「Failed Audit」への移行なし	「Audit」成功	正しい順序での監査成功	「Lost」への移行なし
Deployed	「Requested」への移行なし	サービス要求再展開中	「Failed Audit」への移行なし	「Audit」成功	正しい順序での監査成功	監査が見つかりません
Functional	「Requested」への移行なし	サービス要求再展開中	「Failed Audit」への移行なし	「Deployed」への移行なし	正しい順序での監査成功	監査が見つかりません
Lost	「Requested」への移行なし	サービス要求再展開中	「Failed Audit」への移行なし	「Audit」成功	正しい順序での監査成功	監査が見つかりません
Broken	「Requested」への移行なし	サービス要求再展開中	「Failed Audit」への移行なし	「Deployed」への移行なし	正しい順序での監査成功	監査が見つかりません
Invalid	「Requested」への移行なし	サービス要求再展開中	サービス要求エラーによる再展開	「Deployed」への移行なし	「Functional」への移行なし	「Lost」への移行なし
Failed Deploy	「Requested」への移行なし	サービス要求再展開中	サービス要求の再展開に失敗しました。コンフィグレットをダウンロードできません。	「Deployed」への移行なし	「Functional」への移行なし	「Lost」への移行なし
Closed	「Requested」への移行なし	「Pending」への移行なし	「Failed Audit」への移行なし	「Deployed」への移行なし	「Functional」への移行なし	「Lost」への移行なし

表 A-2 に、「*Broken*」から「*Closed*」までのサービス要求の移行を示します。

表 A-2　Prime Fulfillment サービス要求の状態移行順序（パート 2）

サービス要求状態	Broken	Invalid	Failed Deploy	Closed
Requested	「Broken」への移行なし	サービス要求展開エラー	展開に失敗しました	「Closed」への移行なし
Pending	「Route audit」不成功正しいコンフィグレットです。	サービス要求エラーによる再展開	サービス要求の再展開に失敗しました。コンフィグレットをダウンロードできません。	サービス要求の削除成功
Failed Audit	「Route audit」不成功正しいコンフィグレットです。	サービス要求エラーによる再展開	サービス要求の再展開に失敗しました。コンフィグレットをダウンロードできません。	「Closed」への移行なし
Deployed	「Route audit」不成功正しいコンフィグレットです。	サービス要求エラーによる再展開	サービス要求の再展開に失敗しました。コンフィグレットをダウンロードできません。	「Closed」への移行なし
Functional	「Route audit」不成功正しいコンフィグレットです。	サービス要求エラーによる再展開	サービス要求の再展開に失敗しました。コンフィグレットをダウンロードできません。	「Closed」への移行なし
Lost	「Route audit」不成功正しいコンフィグレットです。	サービス要求エラーによる再展開	サービス要求の再展開に失敗しました。コンフィグレットをダウンロードできません。	「Closed」への移行なし
Broken	「Route audit」不成功正しいコンフィグレットです。	サービス要求エラーによる再展開	サービス要求の再展開に失敗しました。コンフィグレットをダウンロードできません。	「Closed」への移行なし
Invalid	「Broken」への移行なし	サービス要求エラーによる再展開	サービス要求の再展開に失敗しました。コンフィグレットをダウンロードできません。	「Closed」への移行なし
Failed Deploy	「Broken」への移行なし	サービス要求再展開エラー	サービス要求の再展開に失敗しました。コンフィグレットをダウンロードできません。	「Closed」への移行なし
Closed	「Broken」への移行なし	「Invalid」への移行なし	「Failed Deploy」への移行なし	「Closed」への移行なし

INDEX

O

P

T

V

あ

い

え

か

く

け

さ

し

せ

た

て

と

に

は

ふ

ほ

ま

め

も

よ

ら

り

る

ろ