CHAPTER 13

MPLS/VPN のサポート

このモジュールでは、サービス コントロール MPLS/VPN サポートの概要を説明します。また、MPLS/VPN の設定とモニタリングに関するさまざまな手順についても説明します。

MPLS/VPN ネットワークのサービス コントロール ソリューションの概要

MPLS/VPN ネットワークは非常に複雑で、多数のルーティング プロトコル、および多数の異なるレベルのアドレッシングとコントロールが含まれています。また、各種の VPN で重複 IP アドレス（プライベート IP）が使用されることもあります。

SCE プラットフォームは、異なる VPN から発信された同一 IP アドレスを識別し、パケットに付加された MPLS ラベルに基づいて、IP アドレスをサブスクライバにマップします。この処理では、システムのあらゆるレベルで各種のメカニズムが使用されます。

MPLS/VPN 環境で SCE プラットフォームを運用するには、次の前提および要件が満たされている必要があります。

- MPLS/VPN アーキテクチャが、RFC-2547 に準拠している。
- 特殊タイプのカプセル化として、RFC-3032 に記述されている MPLS shim header over Ethernet を使用する。
- 2 つのレベルの MPLS ラベルがある。
  - 外部ラベル — サービス プロバイダーの MPLS コア ネットワーク上での転送に使用。
  - 内部ラベル（BGP ラベル）— 各エッジ ルータに接続された VPN の識別に使用。通常、BGP プロトコルによって制御されます。
- 1 つの VPN のすべての IP アドレスが、単一サブスクライバとして処理される。
- MPLS/VPN ソリューションに、SCE プラットフォームと SM が含まれている。SM は、サービス プロバイダー ネットワークの PE ルータの BGP ピアとして動作し、SCE プラットフォームと通信して、BGP 情報をサブスクライバ情報として渡します。

（注）　MPLS/VPN ソリューションでは、MPLS/VPN サブスクライバと非 VPN サブスクライバを同時にサポートできます（「非 VPN サブスクライバ」[p.13-5] を参照）。

定義および略語

次に、重要な用語と略語についての定義を示します。

表 13-1　MPLS/VPN の用語または略語

用語または略語	定義
PE（プロバイダー エッジ ルータ）	サービス プロバイダー ネットワークのエッジにあるルータ。PE ルータは、顧客に接続して、VPN を保守します。
P（プロバイダー ルータ）	サービス プロバイダー ネットワークのコアにあるルータ。P ルータは、VPN に関係なく、MPLS パケットだけを転送します。
VPN（バーチャル プライベート ネットワーク）	サービス コントロールでは、VPN は特定のサイトに常駐する VPN の一部になります。これは、ソリューションのサブスクライバです。
BGP LEG	SM サーバに常駐するソフトウェア モジュールで、BGP 関連のログイン イベントを生成します。BGP LEG は、BGP ルータ（PE）と通信し、SM ソフトウェアに関連するアップデート情報を渡します。SM ソフトウェアは、アップデートされた VPN サブスクライバ用に SCE プラットフォームへのログイン イベントを生成します。
アップストリーム	PE ルータから発信され、P ルータに送信されるトラフィック。
ダウンストリーム	P ルータから発信され、PE ルータに送信されるトラフィック。
RD（ルート識別子）	異なる VRF からの同じネットワーク / マスク（VPN A からの 10.0.0.0/8 と VPN B からの 10.0.0.0/8 など）を個別に識別するために使用します。
RT（ルート ターゲット）	ポリシーのインポートおよびエクスポートを制御し、顧客用の任意の VPN トポロジを構築するために、ルーティング プロトコルによって使用されます。
VRF（Virtual Routing and Forwarding インスタンス）	インターフェイス単位のルーティング テーブルを構築するためのメカニズム。各 PE は、接続先の各サイトに 1 つずつ、多数の VRF を保持します。これにより、プライベート IP の固有性が確保されます。

MPLS/VPN サポートのサービス コントロールにおける課題

- プライベート IP アドレスのフローは、MPLS ラベルを除き、すべて同じになります。
- MPLS ラベルは各方向で異なりますが、一致している必要があります。
- 1 つの VPN 全体を、単一サブスクライバとしてアカウントする必要があります。特定の VPN に属すフローの検出方法が問題です。
- ダウンストリーム方向には、外部ラベルがありません。内部ラベルおよび PE の MAC アドレスから VPN 情報を認識できる必要があります。

MPLS/VPN サポートの動作

サービス コントロールは、MPLS/VPN サポートを動作させるために、2 つのメカニズムをサポートしています。

- フロー検出 — SCE プラットフォームの処理で、フローを識別するために、アップストリームとダウンストリームのトラフィックを照合します。
- サブスクライバの検出 — SM の処理で、サブスクライバ エンティティを識別するために、ダウンストリーム ラベルと VPN を照合します。
- フロー検出（p.13-3）
- サブスクライバの検出（p.13-3）
- サービス コントロール MPLS/VPN ソリューションの動作（p.13-4）

フロー検出

フロー検出は、同じフローに属すパケットを判別するプロセスです。これは、最初の 2 つの課題に関連しています。

- プライベート IP アドレスのフローは、MPLS ラベルを除き、すべて同じになります。
- MPLS ラベルは各方向で異なりますが、一致している必要があります。

フロー検出は、MPLS ではパケットのラベルが各方向で個別に付けられることを考慮し、SCOS のフロー識別方式である 基本 5 タプルを拡張した MPLS ラベルに基づいています。

MPLS トラフィックは単方向なので、SCE プラットフォームは、次の情報を使用して、各方向を個別に分類します。

- ダウンストリーム — BGP ラベルおよび PE の MAC アドレス（分類に関連するラベルは 1 つだけです）。

  ダウンストリームのラベルは、コントロール プレーン（BGP）から学習されます。
- アップストリーム — 外部ラベル、BGP ラベル、および P ルータの MAC アドレスの組み合わせ（分類に関連するラベルは 2 つです）。

  アップストリームのラベルは、データ プレーンから学習されます。

サブスクライバの検出

- VPN サブスクライバの概要（p.13-3）
- SM およびサブスクライバの検出（p.13-3）

VPN サブスクライバの概要

他の運用モードと同様に、MPLS/VPN では、各フローは特定のサブスクライバに属しています。VPN サブスクライバは、VPN サービスに対して料金を支払うサービス プロバイダーの顧客です。VPN 顧客のトラフィックはすべて、サービス コントロール用の単一 VPN サブスクライバとして集約されます。

SM およびサブスクライバの検出

VPN サブスクライバを分割するネットワーク設定は、SM によって制御されます。ネットワーク全般で、VPN を最も詳細に示す値は、RT（ルート ターゲット）または RD（ルート識別子）のどちらかです。

- 管理者は、選択した属性（RT または RD）に基づいて VPN サブスクライバが検出されるように SM を設定します。

- ネットワーク オペレータは、SCE プラットフォームに、RT 値と VPN サブスクライバ名のマッピングを提供します。

Subscriber Manager（SM）サーバの関連モジュールは、BGP-LEG です。BGP-LEG は、MPLS ラベル上の情報を取得するために、BGP ネイバーフッドに追加します。ローカル PE は、BGP-LEG を BGP ピアとして追加するように設定します。

- BGP-LEG は、PE から、VPN 単位で割り当てられたラベルとともに MP-BGP メッセージを取得し、SM モジュールに転送します。

SM は、MPLS ラベルと VPN サブスクライバのマッピングによって、各 SCE プラットフォームをアップデートします。

サービス コントロール MPLS/VPN ソリューションの動作

サービス コントロール MPLS/VPN ソリューションの動作：要約

- SM に、管理対象となる VPN を設定します。

  VPN は、RD/RT および PE によって識別されます。
- BGP-LEG により、MPLS ラベルを使用して SM をアップデートします。
- SM は、VPN のダウンストリーム MPLS ラベルを付加して、VPN サブスクライバを SCE プラットフォームにプッシュします。
- SCE プラットフォームは、PE MAC アドレスを解決して、新しい情報をテーブルに反映します。
- SCE プラットフォームが、P MAC アドレスを含むアップストリーム ラベルを取得します。
- SCE プラットフォームにより、VPN サブスクライバに標準サービス（BW 管理、レポートなど）が提供されます。

MPLS/VPN ソリューションでの SCE プラットフォームのタスク

- アップストリーム ラベルとダウンストリーム ラベルを一致させます。
  - ダウンストリーム ラベルと VPN サブスクライバのマッピングを、SM から受信します。
  - アップストリーム ラベルを、データ プレーンから学習します。
- PE の MAC アドレスを使用して、異なる PE のダウンストリーム ラベルを識別します。
- ラーニングが終了すると、各フローが、いずれかの VPN サブスクライバに属すフローとして分類されます。
- SCE プラットフォームでは、ネットワーク フロー用の SCA-BB アプリケーションの実行によりフローが VPN サブスクライバごとに分類されるので、サブスクライバ単位のサービス コントロールおよびレポートを提供できます。

MPLS/VPN ソリューションでの BGP LEG のタスク

- BGP LEG は、SM サーバ上で実行されるソフトウェア モジュールです。
- LEG は、PE のリストにより、BGP セッションを維持します。
- セッションが確立されると、LEG は PE から SM モジュールに、MP-BGP ルート アップデートを伝播します。

MPLS/VPN ソリューションでの SM のタスク

- VPN は、VPN サブスクライバとして SM データベースに保管されます。

- VPN サブスクライバは、VPN サイトのグループです。
- 各 VPN サイトは、次の情報によって定義されます。
  - PE ルータのループバック インターフェイスの IP アドレス
  - PE ルータ内で VPN を識別する RD または RT
- SM は BGP LEG からアップデート情報を受信し、新しい MPLS ラベルを使用して VPN サブスクライバ情報をアップデートします。
- MPLS アップデートを取得する関連 SCE プラットフォームは、VPN サブスクライバ ドメインによって定義されます。

サービス コントロール MPLS/VPN の概念

非 VPN サブスクライバ

MPLS/VPN ソリューションでは、MPLS/VPN サブスクライバと非 VPN（標準 IP）サブスクライバを同時にサポートできますが、次の制限および要件があります。

- SM を「プッシュ」モードで実行する必要があります。
- 非 VPN サブスクライバには、MPLS/VPN マッピングを適用できません。
- VLAN サブスクライバを、MPLS/VPN サブスクライバと同時にサポートすることはできません。

一般的な MPLS/VPN ネットワークでは、どの VPN にも属さないトラフィックには、ルーティングに使用されるアップストリーム方向の 1 つの MPLS ラベルだけが付加されます。これらのフローは、ダウンストリーム方向では最後から 2 番めのホップになるので、ラベルは付加されません。

SCE プラットフォームは、1 つまたは複数のアップストリーム ラベルを使用し、ダウンストリームのラベルを使用しないという定義によって、非 VPN フローを識別します。これらのフローの分類およびトラフィック プロセッサのロード バランシングは、ラベルではなく、IP ヘッダーに基づいて実行されます。

このプロセスは、これらのフローが使用するアップストリーム ラベルの学習を必要とし、前述したフロー検出メカニズムを使用して実行されます（「フロー検出」[p.13-3] 参照）。

未知 VPN のバイパス

MPLS ネットワークでは、多数の VPN が SCE プラットフォームを経由し、サービス コントロール機能を必要とする VPN は、そのなかの少数に過ぎないことがあります。そのため、SCE プラットフォームで、管理対象ではない VPN を認識する必要があります。

- SCE プラットフォームは、SM に設定されていないすべての VPN を自動的にバイパスします。
- SCE プラットフォームによってバイパスされる VPN には、どのサービスも提供されません。

57,344 の異なるラベル数の制限値には、バイパスした VPN のラベルも含まれることに注意してください。

アップストリームおよびダウンストリームの両方で、バイパスされた各 VPN エントリは、設定時間（10 分間）の経過後、データベースから削除されます。削除したエントリがトラフィックで引き続き使用されている場合には、再学習されます。したがって、ルータが異なる VPN 用にラベルを再使用した場合でも、データベースはクリーンな状態になります。

show bypassed VPNs — **show bypassed VPNs** コマンドの出力に、各ラベルのエージ（学習されてからの経過時間）が表示されます。

その他の MPLS パターンのサポート

MPLS/VPN ソリューションは、MPLS/VPN ネットワークで DPI サービスを提供するように設計されています。これらのネットワークでは、VPN のコントロール プレーンとして BGP プロトコルが使用され、ルーティング用に LDP プロトコルが使用されます。複雑なネットワークでは、MPLS インフラストラクチャが、VPN およびルーティングだけでなく、Traffic Engineering（TE; トラフィック エンジニアリング）や、より優れたフェールオーバーなどの他の機能にも使用されます。これらの機能は通常、PE の VRF 単位でイネーブルに設定されます。

サービス コントロール MPLS/VPN ソリューションでは、他の MPLS 関連機能を使用する VPN はサポートされません。MPLS-TE または MPLS-FRR（Fast Reroute）などの機能は、サポートされません。これらの機能がイネーブルである VPN は、システムで自動的にバイパスできますが、サービス対象の VPN として SM に設定することはできません。これらの VPN を SM に設定すると、ラベル エイリアスにより、VPN が不正に分類されることがあります。

次に、SCE プラットフォームでサポートされるラベルの組み合わせを示し、各組み合わせがプラットフォーム上でどのように解釈されるのかについて説明します。

- 1 つまたは複数のアップストリーム ラベル、ダウンストリーム ラベルなし：

  非 VPN として認識されます（「非 VPN サブスクライバ」[p.13-5] 参照）。

  SCE プラットフォームは、後続の IP フローを非 VPN フローとして処理し、ラベルを無視します。
- 1 つのアップストリーム ラベル、1 つのダウンストリーム ラベル：

  P ルータがアップストリームの最終ホップであった VPN トラフィックとして認識されます。

  ダウンストリーム ラベルは、通常の場合と同様に BGP ラベルとして処理されます。BGP ラベルが SM に設定されていれば、フローは適正なサブスクライバに割り当てられます。設定されていなければ、バイパスされた VPN として処理されます。
- 2 つのアップストリーム ラベル、1 つのダウンストリーム ラベル：

  システムの一般的な設定です。2 つのアップストリーム ラベルは、BGP ラベルと LDP ラベルです。ダウンストリーム ラベルは、BGP だけです。
- 3 つ以上のアップストリーム ラベル、または 2 つ以上のダウンストリーム ラベル：

  他の MPLS 関連機能がイネーブルに設定されている VPN の組み合わせです。これらの VPN はサポートされないので、SM に設定すべきではありません。ただし、SCE プラットフォームで、サービスを提供せずに、これらの VPN をバイパスさせることができます。この場合、他の VPN のサービスには影響しません。

VPN 識別子（RD または RT）

VPN サブスクライバを識別するには、Route Distinguisher（RD; ルート識別子）または Route Target（RT; ルート ターゲット）のいずれかを使用できます。VPN サブスクライバの識別に最適な属性を決定し、それに応じてシステムを設定する必要があります。設定はすべてのサブスクライバに対してグローバルに適用されるので、同じ属性によってすべてのサブスクライバを識別できる必要があります。

プロバイダーに接続している各顧客の明確な VPN ルートを識別するには、通常、RD が使用されます。したがって、ほとんどの場合、RD はネットワーク上のサブスクライバの有効な識別子になります。RD は、ターゲット VRF ではなくローカル VRF の識別子なので、共通の中央エンティティ（中央銀行、事故通報システム、湾務局など）に情報を転送する VPN サイト間の識別に使用できます。

RT は、宛先 VPN サイトを定義するために使用されます。宛先ルートに基づく VPN サブスクライバの定義は直観的ではありませんが、状況によっては簡単に定義できる場合もあります。たとえば、中央銀行と通信するすべての VPN サイトを単一サブスクライバとして処理するような場合には、RT を VPN 識別子として使用できます。

この設定はグローバルであることに注意してください。したがって、ある時点で、VPN サブスクライバを RD で定義する必要が生じた場合、他のすべての VPN サブスクライバも、同様に RD で定義する必要があります。初回の配置を設計するときに、この点を考慮する必要があります。

サービス コントロール MPLS/VPN の要件

トポロジ

次に、MPLS/VPN サポートの一般的なトポロジの要件を示します。

- SCE プラットフォームは、ネットワークの P ルータ（プロバイダー MPLS コア ルータ）と PE（プロバイダー エッジ ルータ）の中間に配置します。
- SCE プラットフォームのサブスクライバ側は、PE ルータに対して接続します。
- SCE プラットフォームのネットワーク側は、P ルータに対して接続します。
- SM に BGP LEG をインストールし、ネットワーク上の任意の場所に配置します。

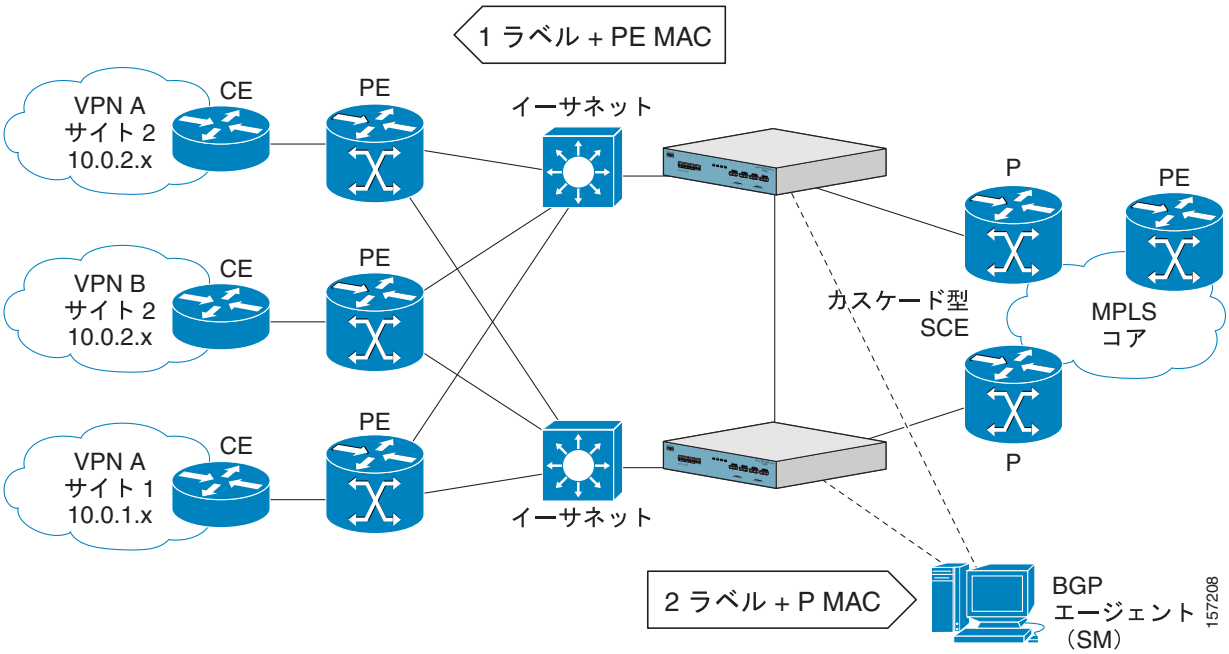
  SM は、管理 IP を使用して SCE プラットフォームと通信します。

カスケード型インストレーション：

- 2 台の SCE プラットフォームを、カスケード インターフェイスを介して相互に接続します。
- P および PE 間とのデータ リンクを、上述のように、各 SCE プラットフォームの他方のインターフェイスを介して接続します。
  - 各 SCE プラットフォームのサブスクライバ側は、PE ルータに対して接続します。
  - 各 SCE プラットフォームのネットワーク側は、P ルータに対して接続します。

次の図に、一般的なカスケード型インストレーションを示します。

図 13-1　一般的な MPLS/VPN インストレーション



容量

システムのサポート容量は、次のとおりです。

- MPLS/VPN サブスクライバ数、最大 2015
- 異なるラベル数、最大 57,344（アップストリーム、ダウンストリーム、バイパスされた VPN のラベルを含む）
- 各 SCE プラットフォームの PE 数、最大 256
- 各 PE のインターフェイス数、最大 4

制限

相互に排他的なシステム モード

システムで MPLS/VPN モードを実行している場合、次のモードはサポートされません。

- 他のトンネリング モード（MPLS/TE、L2TP、VLAN など）
- TCP バイパスの確立
- DDoS
- フロー フィルタ TOS ルール — MPLS/VPN 機能をアクティブにすると、フロー フィルタ モードは自動的に tunnel-id に切り替わります。この機能を非アクティブにしても、フロー フィルタ モードは tunnel-id のままです。

  これにより、簡単に MPLS/VPN の設定を実行できます。TOS/Tunnel-ID モードを一貫性のある正しい設定にするために、tunnel-id モードの実行中は TOS ベース ルールの設定はできません。逆の場合も同じです。

MPLS ラベル数

- 固有の VPN サイトは、BGP ラベルだけに基づいて選択される必要があります。BGP ラベルは、最も内側のラベルでなければなりません。

- MPLS/VPN　ソリューションでは、各種のラベルの組み合わせがサポートされます。その他の MPLS パターンのサポートを参照してください。
- MPLS-TE または MPLS-FRR などの他の MPLS 関連機能がイネーブルに設定されている VPN は、サポートされません。

サブスクライバ関連の制限

現在のソリューションには、次のサブスクライバ関連の制限があります。

- SM は、プッシュ モードで動作するように設定する必要があります。
- VLAN サブスクライバは使用できません。
- 次の両方の条件に適合する場合、同じ VPN の 2 つのサイトを単一サブスクライバとして集約する必要があります。
  - 両方とも、同じ SCE プラットフォームに接続している。
  - 両方とも、同じアップストリーム ラベルおよび P ルータを使用して共通のリモート サイトと通信する。

TCP 関連の要件

- アップストリーム TCP フロー数 — 各時間範囲で、各 PE-PE ルート上のサブスクライバ側から十分な TCP フローがオープンされる必要があります。サブスクライバ側からの TCP フロー数が多いほど、メカニズムの精度は高くなります。

MPLS/VPN サポートの設定方法

MPLS 環境の設定

MPLS/VPN サポートを実現するには、環境を正しく設定する必要があります。具体的には、次の設定が必要です。

- 他のすべてのトンネリング プロトコルを、デフォルト モードに設定する必要があります。
- VLAN サポートをデフォルト モードに設定する必要があります。
- MPLS 自動ラーニング メカニズムをイネーブルにする必要があります。
- 実行コンフィギュレーションのチェック方法（p.13-10）
- MPLS 環境の設定方法（p.13-10）

実行コンフィギュレーションのチェック方法

実行コンフィギュレーションを調べ、トンネリング プロトコルまたは VLAN サポートにユーザが設定した値が存在せず、すべてがデフォルト モードであることを確認してください。

ステップ 1　SCE# プロンプトで、`show running-config` と入力し、Enter キーを押します。

実行コンフィギュレーションを表示します。

ステップ 2　VLAN または L2TP 設定が表示されていないことを確認します。

MPLS 環境の設定方法

VLAN またはトンネリング サポートがデフォルト モードになっている場合には、次の作業のうち、不要な手順を省略してかまいません。

要約ステップ

1. SCE(config if)# プロンプトで、`default vlan` と入力し、Enter キーを押します。
2. SCE(config if)# プロンプトで、`no IP-tunnel` と入力し、Enter キーを押します。
3. SCE(config if)# プロンプトで、`MPLS VPN auto-learn` と入力し、Enter キーを押します。

詳細なステップ

ステップ 1　SCE(config if)# プロンプトで、`default vlan` と入力し、Enter キーを押します。

VLAN サポートをデフォルト モードに設定します。

ステップ 2　SCE(config if)# プロンプトで、`no IP-tunnel` と入力し、Enter キーを押します。

他のすべてのトンネリング プロトコルのサポートをディセーブルにします。

（注）　トンネリング モードを変更するには、トンネル マッピングを使用しているすべてのサブスクライバをクリアする必要があります。SM との接続がダウンしている場合には、**no subscriber all with-tunnel-mappings** CLI コマンドを使用します。

ステップ 3　SCE(config if)# プロンプトで、`MPLS VPN auto-learn` と入力し、Enter キーを押します。

MPLS 自動ラーニング メカニズムをイネーブルにします。

MPLS/VPN サポートの SCE プラットフォームの設定方法

MPLS/VPN サポートの SCE プラットフォームの設定について

MPLS/VPN サポートの SCE プラットフォームの設定には、3 つの主要な手順があります。

1. MPLS トンネリング環境を正しく設定し、他のすべてのトンネリング プロトコルをディセーブルにし、VLAN サポートもディセーブルにします（「MPLS 環境の設定方法」[p.13-10] を参照）。
2. すべての PE ルータを定義し、MAC 解決に必要な関連インターフェイスの IP アドレスを指定します（「PE ルータの定義方法」[p.13-11] 参照）。
3. MAC リゾルバを設定します（「MAC リゾルバの設定方法」[p.13-13] 参照）。

PE ルータの定義方法

オプション

次のオプションを使用できます。

- **PE-ID** — PE ルータを識別する IP アドレス
- **Interface-IP** — PE ルータのインターフェイス IP アドレス。MAC 解決に使用します。
  - 各 PE ルータに最低 1 つのインターフェイス IP アドレスを定義する必要があります。
  - 1 つの PE ルータに複数のインターフェイス IP アドレスを定義できます。
  - PE ルータの複数の IP インターフェイスが同じ MAC アドレスを共有している場合には、1 つの PE インターフェイスを設定するだけで十分です。
- **vlan** — 各インターフェイス IP に、任意に VLAN タグを指定できます。

VLAN タグが異なっていても、2 つのインターフェイスに同じ IP アドレスを定義することはできません。この設定を試みても、既存の PE インターフェイスの VLAN タグ情報がアップデートされるだけです。

PE ルータの追加方法

MPLS/VPN サブスクライバを管理している各 PE を、次の CLI コマンドを使用して定義する必要があります。

ステップ 1　SCE(config if)# プロンプトに、`MPLS VPN PE-ID` *pe-id* `interface-IP` *interface-ip* `[vlan` *vlan*`][Interface-IP` *interface-ip* `[vlan` *vlan*`]]` を入力して、Enter キーを押します。

オプションの VLAN タグとオプションの追加 IP アドレスとともに PE ルータを定義します。

PE ルータの削除方法

- PE ルータの削除について（p.13-12）
- 指定 PE ルータの削除方法（p.13-12）
- 全 PE ルータの削除方法（p.13-12）
- PE ルータからの指定インターフェイスの削除方法（p.13-13）

PE ルータの削除について

これらのコマンドでは、1 つまたはすべての定義済み PE ルータを削除します。

次の事項に注意してください。

- MPLS マッピングを保持している PE ルータは、削除できません。ルータを削除する前に、そのルータを使用している VPN をログアウトする必要があります。
- PE ルータの最後のインターフェイスを削除すると、ルータそのものが削除されます。したがって、最後のインターフェイスを削除する場合には、関連 VPN をログアウトする必要があります。
- 同様に、no PE-Database コマンドを使用する場合には、事前にすべての MPLS VPN をログアウトする必要があります。このコマンドでは、すべての PE ルータが削除されるからです。

指定 PE ルータの削除方法

ステップ 1　SCE(config if)# プロンプトで、`no MPLS VPN PE-ID` *pe-id* を入力し、Enter キーを押します。

指定した PE ルータを削除します。

全 PE ルータの削除方法

ステップ 1　SCE(config if)# プロンプトで、`no MPLS VPN PE-Database` と入力し、Enter キーを押します。

すべての設定済 PR ルータを削除します。

PE ルータからの指定インターフェイスの削除方法

ステップ 1　SCE(config if)# プロンプトで、`no MPLS VPN PE-ID` *`pe-id`* `interface-IP` *`interface-ip`* を入力し、Enter キーを押します。

PE ルータ定義から指定インターフェイスを削除します。PE ルータ自体は削除されません。

MAC リゾルバの設定方法

MAC リゾルバについて

MAC リゾルバを使用すると、SCOS で、特定の IP アドレスに関連付けられている MAC アドレスを検索できます。SCE プラットフォームを MPLS/VPN モードで運用するには、PE ルータ インターフェイスの IP アドレスが対応する MAC アドレスに変換されるように、MAC リゾルバを設定する必要があります。

MPLS/VPN モードでは、標準 ARP プロトコルではなく MAC リゾルバが必要になります。ARP は管理インターフェイスで使用されますが、MPLS/VPN は、ARP には含まれていない SCE プラットフォームのトラフィック インターフェイスを使用するからです。

MAC リゾルバのデータベースには、解決するクライアントにより登録された IP アドレスが保管されます。ルータの IP アドレスをデータベースに追加、およびデータベースから削除するには、次のいずれかのモードを使用します。

- ダイナミック モード（デフォルト）

  このモードでは、システムは設定された PE インターフェイスの ARP メッセージを待ち受け、ARP メッセージの MAC アドレスにより情報をアップデートします。ダイナミック モードを使用する場合、設定は不要です。

  - 利点：PE インターフェイスの MAC アドレスが変更されても、問題はありません。
  - 欠点：特定のネットワーク トポロジで、MAC 解決のコンバージェンス タイムがかなり長くなることがあります。

- スタティック モード

  このモードでは、各 PE ルータの MAC アドレスを、ユーザが明示的に定義する必要があります。

  - 利点：IP アドレスのコンバージェンスに初期遅延が生じません。
  - 欠点：PE インターフェイスは、ARP アップデートによって自動アップデートされません。したがって、MAC アドレスがオンザフライで変更された場合、自動的にはサポートされません。

  ただし、スタティックに設定した MAC アドレスの場合、MAC アドレスの変更が検出されると、ユーザ ログ メッセージが表示されます。これにより、オペレータは新しいアドレスを設定できます。

2 つのモードは同時に使用できるので、一部の PE ルータだけをスタティックに設定し、他の PE ルータはダイナミックに解決する、ということもできます。

MAC リゾルバの詳細については、『*Cisco Service Control Engine Software Configuration Guide*』を参照してください。

オプション

次のオプションを使用できます。

- **ip address** — データベースに追加、またはデータベースから削除する IP アドレス エントリ
- **vlan tag** — IP アドレスを伝播する VLAN を識別するための VLAN タグ（適用する場合）
- **mac address** — IP アドレスに割り当てる MAC アドレス、xxxx.xxxx.xxxx 形式

スタティック IP アドレスの追加方法

ステップ 1　SCE(config if)# プロンプトで、`mac-resolver arp` *ip_address* `[vlan` *vlan_tag*`]` *mac_address* を入力し、Enter キーを押します。

指定された IP アドレスと MAC アドレスのペアを MAC リゾルバ データベースに追加します。

スタティック IP アドレスの削除方法

ステップ 1　SCE(config if)# プロンプトで、`no mac-resolver arp` *ip_address* `[vlan` *vlan_tag*`]` *mac_address* を入力し、Enter キーを押します。

指定された IP アドレスと MAC アドレスのペアを MAC リゾルバ データベースから削除します。

MAC リゾルバのモニタ方法

このコマンドでは、MAC リゾルバのデータベースに現在登録されている、すべての IP アドレスおよび対応 する MAC アドレスのリストを表示します。

ステップ 1　SCE# プロンプトで、`show interface linecard 0 mac-resolver arp` と入力し、Enter キーを押します。

MAC リゾルバのデータベースに現在登録されている、すべての IP アドレスおよび対応する MAC アドレスのリストを表示します。

MPLS/VPN サポートの SM の設定方法

MPLS/VPN サポートの SM の設定

MPLS/VPN サポートの SM を設定するには、次の 2 つの主要手順を実行します。

ステップ 1　*p3sm.cfg* コンフィギュレーション ファイルを編集し、SM が MPLS-VPN の識別に使用する BGM メッセージのフィールドを指定します。

「SM コンフィギュレーション ファイルの編集方法」（p.13-15）を参照してください。

ステップ 2　BGP LEG をインストールし設定します。

『*Cisco SCM SM MPLS/VPN BGP LEG Reference Guide*』を参照してください。

SM コンフィギュレーション ファイルの編集方法

SM が MPLS-VPN を識別するために使用する BGP メッセージのフィールドを指定するには、SM コンフィギュレーション ファイルの *p3sm.cfg* を設定する必要があります。

- MPLS/VPN サポートの SM の設定方法（p.13-15）
- MPLS/VPN サポートのトラブルシューティング用 SM の設定方法（p.13-15）

MPLS/VPN サポートの SM の設定方法

ステップ 1　*p3sm.cfg* コンフィギュレーション ファイルに、次のセクションを追加します。

```
# The following parameter enables SM operation with MPLS-VPN support.
[MPLS-VPN]
# The following parameter determines field in the BGP messages that should be used
# for MPLS-VPN identification, in correlation to the MPLS-VPN mappings that were
# previously set to the SM.
# possible values: "rd" or "rt".
# (default: rt)
vpn_id=rt
```

MPLS/VPN サポートのトラブルシューティング用 SM の設定方法

BGP LEG インストレーションのトラブルシューティングを容易にするために、オプション パラメータを設定できます。このパラメータをオンにすると、BGP LEG から受信したメッセージの詳細なロギングが有効になります。このオプションは、トラブルシューティングが必要な場合にのみ使用し、通常のシステム運用時はオフにしておいてください。

ステップ 1　*p3sm.cfg* コンフィギュレーション ファイルに、次のセクションを追加します。

```
# The following parameter turns on detailed logging of messages received from the BGP
LEG
# should be changed to true only during troubleshooting
# (default: false)
log_all=true
```

MPLS/VPN サポートの管理方法

SNMP による MPLS/VPN サポートの管理方法

MPLS/VPN 自動学習の SNMP サポートは、2 つの方法で提供されます。

- MIB 変数
- SNMP トラップ
- MPLS/VPN の MIB オブジェクト（p.13-16）
- MPLS/VPN トラップ（p.13-16）

MPLS/VPN の MIB オブジェクト

mplsVpnAutoLearnGrp MIB オブジェクト グループ（pcubeSEObjs 17）に、MPLS/VPN 自動学習に関する情報が含まれています。

mplsVpnAutoLearnGrp のオブジェクトは、次の情報を提供します。

- 最大マッピング数
- 現在許可されているマッピング数

詳細については、『*Cisco Service Control Engine Software Configuration Guide*』の「Proprietary MIB Reference」を参照してください。

MPLS/VPN トラップ

1 つの MPLS/VPN 関連トラップがあります。

- *mplsVpnTotalHWMappingsThresholdExceeded*（pcubeSeEvents 45）

システムのハードウェア MPLS/VPN マッピングの使用率が 80% に到達すると、リソース不足をオンラインで通知するために、ユーザ ログに警告メッセージが表示され、この SNMP トラップが送信されます。

しきい値を超えると、100 のマッピング数が追加されるごとに、この警告とトラップの両方が送信されます。

SCE プラットフォーム CLI による MPLS/VPN サポートのモニタ方法

以下のセクションでは、SCE プラットフォーム CLI で実行可能な機能について説明しています。

サブスクライバ マッピングの表示方法

サブスクライバ マッピングを表示するには、次のビューア コマンドを使用します。これらのコマンドにより、次の情報が表示されます。

- 指定したサブスクライバのすべての MPLS/VPN マッピング
- 指定したサブスクライバの MPLS/VPN マッピング数
- 指定したダウンストリーム マッピング（PE ループバック IP アドレスおよび BGP ラベル）がマップされているサブスクライバ
- 指定したサブスクライバのすべての MPLS/VPN マッピング表示方法（p.13-17）
- 指定したサブスクライバの MPLS/VPN マッピング数のみの表示方法（p.13-17）
- 指定したダウンストリーム マッピングのあるサブスクライバ名の表示方法（p.13-18）
- 非 VPN フローに属するアップストリーム ラベルのマッピングの表示方法（p.13-18）

指定したサブスクライバのすべての MPLS/VPN マッピング表示方法

ステップ 1　SCE# プロンプトに、`show interface linecard 0 subscriber name` *name* `mappings` を入力して、Enter キーを押します。

mappings キーワードを指定すると、MPLS/VPN マッピング情報だけが表示されます。このキーワードを指定しないと、マッピングを含むすべてのサブスクライバ情報が表示されます。

指定したサブスクライバのすべての MPLS/VPN マッピングの表示：例

```
SCE# show interface linecard 0 subscriber name  SubscriberX_1122334455 mappings
Subscriber 'SubscriberX_1122334455' mappings:
Downstream MPLS Mappings:
PE-ID = 1.1.1.1 Mpls Label = 30
PE-ID = 1.1.1.1 Mpls Label = 256
PE-ID = 1.1.1.1 Mpls Label = 2
PE-ID = 1.1.1.1 Mpls Label = 3
PE-ID = 1.1.1.1 Mpls Label = 4
=====>Total Downstream Mappings: 5
Upstream MPLS Mappings:
Upstream MPLS label: (MAC = 00:50:04:b9:c8:a0 BGP label = 0x14, LDP Label = 0xa)
=====>Total Upstream Mappings: 1
```

指定したサブスクライバの MPLS/VPN マッピング数のみの表示方法

ステップ 1　SCE# プロンプトに、`show interface linecard 0 subscriber name` *name* `mappings |include Total` を入力して、Enter キーを押します。

指定したサブスクライバの MPLS/VPN マッピング数のみの表示：例

```
SCE# show interface linecard 0 subscriber name  SubscriberX_1122334455 mappings
Subscriber 'SubscriberX_1122334455' mappings:
=====>Total Downstream Mappings: 5
=====>Total Upstream Mappings: 1
```

指定したダウンストリーム マッピングのあるサブスクライバ名の表示方法

ステップ 1　SCE# プロンプトに、`show interface linecard 0 subscriber mapping MPLS-VPN PE-ID` *pe-id* `BGP-label` *label* を入力し、Enter キーを押します。

非 VPN フローに属するアップストリーム ラベルのマッピングの表示方法

ステップ 1　SCE# プロンプトで、`show interface linecard 0 MPLS-VPN non-VPN-mappings` と入力し、Enter キーを押します。

サブスクライバ マッピングのクリア方法

このコマンドでは、指定した VPN サブスクライバについて、学習されたすべてのアップストリーム ラベルを削除します。

ステップ 1　SCE（config if）# プロンプトで、`no subscriber name` *name* `mapping upstream mpls all` を入力し、Enter キーを押します。

このコマンドを使用すると、ラベルのエージングが早期に終了します。マッピングをクリアすると、再学習が実行されます。ほとんどの場合、ラベルはクリアされたあと、すぐに再学習されます。したがって、このコマンドを使用すると、標準エージング時間が経過するまで待機せずに、マッピングをアップデートできます。

サブスクライバ カウンタのモニタ方法

MPLS/VPN マッピングに関連するカウンタを含むサブスクライバ カウンタを表示するには、次のビューア コマンドを使用します。

- サブスクライバ カウンタについて（p.13-18）
- サブスクライバ カウンタのモニタリング：例（p.13-19）

サブスクライバ カウンタについて

MPLS/VPN サブスクライバをイネーブルにすると、基本的なサブスクライバ カウンタに加え、次の関連カウンタが表示されます。

- MPLS/VPN サブスクライバ：
  - 現在の MPLS/VPN サブスクライバ数
  - MPLS/VPN サブスクライバの最大数

  MPLS/VPN サブスクライバは全般サブスクライバ カウンタにカウントされますが、全般サブスクライバの最大数が MPLS/VPN サブスクライバに適用されるわけではありません。MPLS/VPN サブスクライバの最大数は、これより少なくなります。
- MPLS/VPN マッピング：
  - 現在使用されている MPLS/VPN マッピング数
  - MPLS/VPN マッピングの最大数

これらの値は、MPLS/VPN サブスクライバが使用しているマッピングだけでなく、マッピングの総数を示していることに注意してください。バイパスされた VPN も、MPLS/VPN マッピングを使用します。

ステップ 1　SCE# プロンプトに、**show interface linecard 0 subscriber db counters** と入力して、Enter キーを押します。

サブスクライバ カウンタのモニタリング：例

```
SCE#show interface linecard 0 subscriber db counters
Current values:
===============
Subscribers: 2 used out of 99999 max.
Introduced subscribers: 2.
Anonymous subscribers: 0.
Subscribers with mappings: 2 used out of 99999 max.
IP mappings: 0 used.MPLS/VPN subscribers are enabled. MPLS/VPN mappings: 2 used out of
57344 max.  MPLS/VPN subscribers: 2 used out of 2015 max.
Subscribers with open sessions: 0.
Subscribers with TIR mappings: 0.
Sessions mapped to the default subscriber: 0.
Peak values:
============
Peak number of subscribers with mappings: 2
Peak number occurred at: 14:56:55 ISR MON November 7 2005
Peak number cleared at: 13:29:39 ISR MON November 7 2005
Event counters:
===============
Subscriber introduced: 2.
Subscriber pulled: 0.
Subscriber aged: 0.
Pull-request notifications sent: 0.
State notifications sent: 0.
Logout notifications sent: 0.
Subscriber mapping TIR contradictions: 0
```

（注）　MPLS/VPN サポートをイネーブルにすると、サブスクライバの最大数は、実際には最初の回線の最大数ではなく、MPLS/VPN 加入者線（2015）の最大数になります。

MPLS/VPN カウンタのモニタ方法

MPLS/VPN 情報を表示するには、次のビューア コマンドを使用します。

- MPLS/VPN カウンタのモニタリング：例（p.13-20）

ステップ 1　SCE# プロンプトで、`show interface linecard 0 mpls vpn` と入力し、Enter キーを押します。

MPLS/VPN カウンタのモニタリング：例

```
SCE#show interface linecard 0 mpls vpn
MPLS/VPN auto-learn mode is enabled.
MPLS/VPN subscribers: 0 used out of 2015 max
Total HW MPLS/VPN mappings utilization: 0 used out of 57344 max
MPLS/VPN mappings are divided as follows:
    downstream VPN subscriber mappings: 0
    upstream VPN subscriber mappings: 0
    non-vpn upstream mappings: 0
    downstream bypassed VPN mappings: 0
    upstream bypassed VPN mappings: 0
```

PE ルータのモニタ方法

PE ルータをモニタするには、次のビューア コマンドを使用します。これらのコマンドにより、次の情報が表示されます。

- 現在定義されているすべての PE ルータの設定
- 指定した PE ルータの設定
- 現在定義されているすべての PE ルータの設定表示方法（p.13-20）
- 指定した PE ルータの設定表示方法（p.13-20）

現在定義されているすべての PE ルータの設定表示方法

ステップ 1　SCE# プロンプトで、`show interface linecard 0 MPLS VPN PE-Database` と入力し、Enter キーを押します。

指定した PE ルータの設定表示方法

ステップ 1　SCE# プロンプトで、`show interface linecard 0 MPLS VPN PE-Database PE-ID` *`pe-id`* を入力し、Enter キーを押します。

バイパスされた VPN のモニタ方法

- バイパスされている現在の VPN の表示方法（p.13-20）
- バイパスされているすべての学習済の VPN の表示方法（p.13-21）

バイパスされている現在の VPN の表示方法

ステップ 1　SCE# プロンプトで、`show interface linecard 0 MPLS VPN Bypassed-VPNs` と入力し、Enter キーを押します。

バイパスされているすべての学習済の VPN の表示方法

ステップ 1　SCE# プロンプトで、`clear interface linecard 0 MPLS VPN Bypassed-VPNs` と入力し、Enter キーを押します。

非 VPN マッピングのモニタ方法

- 非 VPN マッピングの表示方法（p.13-21）
- 学習済のすべての非 VPN マッピングの削除方法（p.13-21）

非 VPN マッピングの表示方法

ステップ 1　SCE# プロンプトで、`show interface linecard 0 MPLS-VPN non-VPN-mappings` と入力し、Enter キーを押します。

学習済のすべての非 VPN マッピングの削除方法

ステップ 1　SCE# プロンプトで、`clear interface linecard 0 MPLS VPN non-VPN-mappings` と入力し、Enter キーを押します。

SM CLU による MPLS/VPN サポートの管理方法

SM の CLU では、次の操作を実行できます。

- 指定したサブスクライバ（VPN）の MPLS/VPN マッピングの追加、削除、表示
- SM データベースからの、すべての MPLS/VPN マッピングのクリア
- オプション（p.13-21）
- 個々のサブスクライバの MPLS/VPN マッピングの管理方法（p.13-22）
- サブスクライバの MPLS/VPN マッピングのモニタ方法（p.13-22）
- SM データベース MPLS/VPN マッピングの管理方法（p.13-22）

オプション

サブスクライバの MPLS/VPN マッピングを管理するには、**p3subs** ユーティリティを使用します。

次のオプションを使用できます。

- **Subscriber-Name** — サブスクライバとして追加されたときに VPN に割り当てられたサブスクライバ名
- **RT@PE-IP** — サブスクライバ /VPN に割り当てられたマッピング。カンマを使用して、複数のマッピングを指定できます。
  - **RT** = ASN:n 表記または IP:n 表記を使用して指定された、VPN のルート ターゲット。

  ルート ターゲットの代わりに、ルート識別子が指定されていることもあります。

－ PE-IP = VPN に接続されている PE ルータのループバック IP

個々のサブスクライバの MPLS/VPN マッピングの管理方法

p3subs

ステップ 1　シェル プロンプトから、次の一般形式でコマンドを入力します。**p3subs** *operation*--subscriber= *Subscriber-Name***--mpls-vpn=** *RT@PE-IP* `[--additive-mapping]`

次の表に、マッピングの管理に関するすべての **p3subs** 処理を示します。

表 13-2　p3subs マッピング 処理

処理	説明
--set	サブスクライバを追加 / アップデートします。マッピングが存在する場合には、additive-mapping オプションを使用しない限り、既存のマッピングと置換されます。
--remove-all-mappings	指定したサブスクライバのすべてのマッピングを削除します。
--remove-mappings	指定したサブスクライバの、指定したマッピングを削除します。

表 13-3　p3subs のマッピング オプション

オプション	説明
--additive-mapping	既存のマッピングに指定したマッピングを追加します（このオプションを使用しない場合、既存のマッピングが置換されます）。set 処理と併用します。

サブスクライバの MPLS/VPN マッピングのモニタ方法

ステップ 1　シェル　プロンプトから、次のコマンドを入力します。**p3subs　--show-all-mappings　--subscriber=** *Subscriber-Name*

SM データベース MPLS/VPN マッピングの管理方法

ステップ 1　シェル プロンプトから、次のコマンドを入力します。**p3subsdb --remove-all-mpls-vpn**