



MPLS 機能の設定

この章では、MGX 8850 の Route Processor Module (RPM-XF; ルート プロセッサ モジュール) で使用する Multiprotocol Label Switching (MPLS; マルチプロトコル ラベル スイッチング) と Virtual Private Network (VPN; バーチャル プライベート ネットワーク) の機能を説明します。この章の内容は次のとおりです。

- [MPLS の概要](#)
- [MGX 8850 の MPLS の設定](#)
- [VPN の概要](#)
- [VPN の動作原理](#)
- [VPN の設定](#)
- [マルチキャスト VPN](#)
- [MPLS LDP](#)
- [RPM-XF でのマルチ VC のサポート](#)

この章では、MGX 8850 Release 5.1 シェルフで RPM-XF の MPLS 機能を使用して、Edge Label Switch Router (ELSR; エッジ ラベル スイッチ ルータ) または Label Switch Controller (LSC; ラベル スイッチ コントローラ) として設定する方法を説明します。

MPLS については、『*Cisco MPLS Controller Software Configuration Guide*』を参照してください。MPLS コマンドと VPN コマンドについては、『*Cisco MPLS VPN Feature Guide*』を参照してください。

MPLS の概要

ここでは、MPLS について説明し、MGX 8850 スイッチで RPM-XF が ELSR または LSC として果たす役割について説明します。

パケットの転送に使用するラベルは、Label Distribution Protocol (LDP; ラベル配布プロトコル) または Tag Distribution Protocol (TDP; タグ配布プロトコル) を使用してネゴシエートされます。その際、RPM-XF は、IP パケットを受信しラベルを付ける、エッジ LSR として動作します。ATM セルベース モードでは、RPM-XF は LSC としても機能し、MPLS ネットワークでのラベルの配布を制御することができます。ただし、RPM-XF カードは、同時に ELSR および LSC として機能することはできません。

MPLS の動作には、2つのモードがあります。

- パケットベース
- ATM セルベース

RPM-XF GigE または POS のパケットベース MPLS の動作と設定は、IOS ルータのパケットベース MPLS の動作と設定に似ています。PVC のパケットベース MPLS の設定は、RPM-PR の設定に似ています。この章では、主に ATM セルベース MPLS の動作を説明し、RPM-XF でのパケットベース MPLS についても簡単に説明します。

ATM MPLS

MPLS では、レイヤ 2 (データ リンク レイヤ) スwitチングのパフォーマンスと仮想回線機能が、レイヤ 3 (ネットワーク レイヤ) のルーティング機能によるスケーラビリティと統合されます。この統合により、サービス プロバイダーは、既存のネットワーク インフラストラクチャを活用しながら、成長を管理するソリューションを配信し、さまざまなサービスを提供することが可能になります。

MGX 8850 は、ラベル スイッチ コントローラ (LSC) 機能をサポートします。この機能を使用して、LVC を ATM スイッチ内の個々の ATM インターフェイスに直接設定できます。LVC は MPLS シグナリングの直接の制御下で確立されます。それぞれの LVC は、MPLS ラベルの個々の値に対応します。

RPM-XF は MPLS による VPN をサポートします。MPLS VPN の運用では、RPM-XF は Provider Edge (PE; プロバイダー エッジ) ルータとして動作します。PE ルータ機能は、VPN のルーティング情報を伝送するために、MPLS エッジ LSR 機能と、マルチプロトコル拡張を備えた Border Gateway Protocol v4 (BGP v4) の機能を組み合わせたものです。

MGX 8850 スイッチでの MPLS

MPLS は、MGX 8850 プラットフォームにおいて、レイヤ 2 管理コストをかけずに、IP ソリューションを実現します。IP over ATM とは対照的に、MPLS では、お客様のネットワーク管理コストと運用コストが削減されます。さらに、フレームリレーまたは ATM と同レベルのプライバシーが守られます。

RPM-XF がエッジ LSR としてどのように動作して MPLS フィーダ機能をサポートするかについては、「[システム ブロック図](#)」(P. 9-4) を参照してください。

MPLS の機能

RPM-XF は、次の機能をサポートしています。

- MPLS アプリケーション
 - MPLS VPN
 - マルチ VC を含む MPLS COS
- MGX 8850 シェルフでの RPM-XF によるエッジ LSR 機能
 - 通常のインターフェイスおよび PVP (VP トンネル) LC-ATM インターフェイスでの ATM セルベース MPLS
 - PVC パケットベース MPLS



(注) RPM-XF スイッチ インターフェイスは 2000 の PVC、4000 の LVC、および 240 の PVP をサポートできます。

- MGX 8850 シェルフでの RPM-XF による LSC 機能
 - 通常の XtagATM インターフェイス
 - VP トンネル ベースの XtagATM インターフェイス
 - LSC の MPLS COS



(注) 同じ RPM-XF 上での LSC と ELSR の使用はサポートされません。



(注) RPM-XF の ELSR は、LSC の冗長性をサポートしません。

- RPM-XF Gigabit Ethernet (MGX-1GE) での MPLS
- OC-12 Packet Over SONET (MGX-1OC12POS-IR) での MPLS
- サポートされるプロトコル
 - OSPF
 - IS-IS
 - MPLS LDP
 - BGP (BGP、RIPv2、OSPF、および PE-CE リンクのスタティック ルートが VPN 追加を提供)



(注) RPM-XF は、最大 2000 個の Interface Descriptor Block (IDB; インターフェイス記述子ブロック) をサポートできます。

- RPM-XF 切り替えによる 1:N 冗長機能

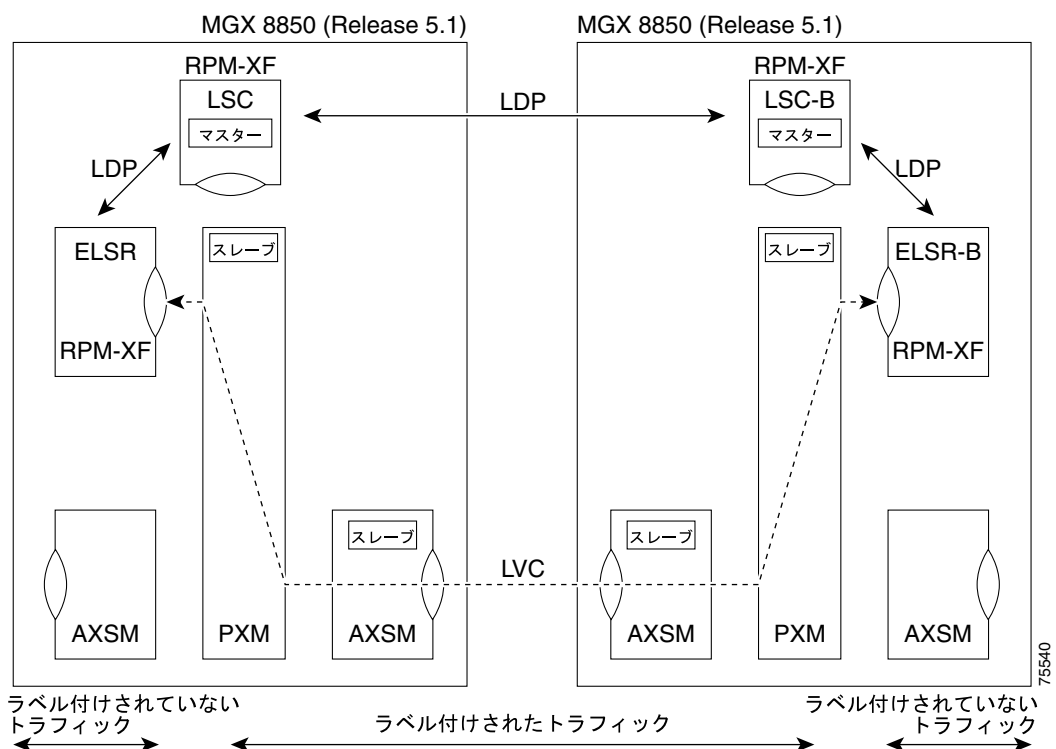
システム ブロック図

次のシステムブロック図（図 9-1 参照）は、RPM-XF を ELSR および LSC として配置してセルベース MPLS を実現する一般的な構成を示しています。この図は、2 台の MGX 8850（Release 5.1）ノードを表し、各ノードには RPM-XF LSC と RPM-XF ELSR が 1 つずつあります。以降に、図右側の MGX 8850（Release 5.1）での RPM-XF LSC と RPM-XF ELSR の設定例を示します。



(注) MGX 8850（Release 5.1）ノードの RPM-XF LSC/ELSR と PXM1 ベース MGX 8850/8250/8230 ノードの RPM-PR ELSR 間の相互運用もサポートされます。詳細については、『Cisco MGX Route Processor Module (RPM-PR) Installation and Configuration Guide』を参照してください。

図 9-1 ELSR と LSC を設定した RPM-XF のある MGX 8850



MPLS COS のサポート

ここでは、Service Class Template (SCT; サービス クラス テンプレート) への MPLS Class of Service (CoS; サービス クラス) のマッピングについて説明します。SCT は AXSM カードで使用するテンプレートであり、デフォルトの VC パラメータと QoS パラメータを設定可能にします。SCT は RPM-XF でサポートされません。RPM-XF では、固定のデフォルト VC パラメータと QoS パラメータを使用します。

MGX 8850 で MPLS をサポートするように設定するには、サービス クラス テンプレート 4 または 5 を AXSM カードに設定し、サービス クラス テンプレート 5 を AXSM-E カードに設定する必要があります。



(注) RPM-XF は、MPLS および PNNI サービス タイプに対し変更不可能なデフォルトの VC パラメータと QoS 設定のセットに従うので、SCT は必要ありません。

MGX 8850 の MPLS の設定

ここでは、MGX 8850 スイッチで MPLS をサポートするための、RPM-XF、PXM45、および AXSM カードの設定手順を説明します。

MPLS をサポートするための手順を次に示します。

- RPM-XF LSC を設定するために、MPLS コントローラを PXM45 に追加します。
- RPM-XF を LSC として設定します。
- MPLS 用に AXSM ポートを追加し割り当てます。
- RPM-XF を ELSR として設定します。
- AXSM ポートと RPM-XF ELSR ポートを LSC の XTagAtm インターフェイスにマッピングします。
- 基本的な LSC の動作を行うように RPM-XF を設定します。詳細については、次の URL を参照してください。
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftlsc.htm#xtocid20>
- Cisco BPX スイッチに接続するために RPM-XF LSC のネットワーク設定を行います。詳細については、次の URL を参照してください。
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftlsc.htm#95055>
- 簡易 PVC ベースのパケット MPLS のネットワーク設定を行います。詳細については、次の URL を参照してください。
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftlsc.htm#xtocid26>

PXM45 への MPLS コントローラの追加と RPM-XF LSC の設定

RPM-XF LSC (図 9-1 の LSC-B) に MPLS サービスを設定する場合、まず MPLS コントローラを PXM45 に追加します。これは、PXM45 へ PNNI コントローラを追加する手順と似ています (第 6 章を参照)。MPLS コントローラを追加するには、次の手順に従います。

ステップ 1 スイッチの CLI にアクセスして、**addcontroller** コマンドを入力します。

```
MGX8850.7.PXM.a>addcontroller <cntrlrId> i <cntrlrType> <slot> [cntrlrName]
```

パラメータ	説明
<i>cntrlrId</i>	範囲は 1 ~ 20 です。 1 は PAR 用に、 2 は PNNI 用に、 3 は LSC 用に予約されています。
<i>i</i>	内部
<i>cntrlrType</i>	1 は PAR 用に、 2 は PNNI 用に、 3 は LSC 用に予約されています。
<i>slot</i>	RPM-XF LSC スロット。範囲は 1 ~ 6 と 9 ~ 14 です。
<i>cntrlrName</i>	コントローラの名前を指定するオプションのフィールド

この例を次に示します。

```
MGX8850.7.PXM.a>addcontroller 5 i 3 5 LSC-5
```

パラメータ	説明
<i>cntrlrId</i>	5
<i>i</i>	i = 内部
<i>cntrlrType</i>	3 = LSC
<i>slot</i>	5 = スロット 5 に挿入されている RPM-XF LSC
<i>cntrlrName</i>	LSC-5

ステップ 2 `cc` コマンド、`cc 5` を入力して、RPM-XF カードに移動します。

ステップ 3 次の例に示すようにコマンドを入力して RPM-XF を LSC として設定します。

```
RPM-XF>enable
Password:
RPM-XF#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
RPM-XF(config)#interface loopback0
RPM-XF(config-if)#ip address 28.28.28.28 255.255.255.255
RPM-XF(config-if)#interface switch1
RPM-XF(config-if)#no ip address
RPM-XF(config-if)#label-control-protocol vsi id 5
RPM-XF(config-if)#switch partition 5 5
RPM-XF(config-if-swpart)#ingress-percentage-bandwidth 10 100
RPM-XF(config-if-swpart)#egress-percentage-bandwidth 10 100
RPM-XF(config-if-swpart)#vpi 0 50
RPM-XF(config-if-swpart)#vci 32 10000
RPM-XF(config-if-swpart)#connection-limit 1 10000
```



(注) VSI コントローラ ID は、上記のステップで入力した `addcontroller` コマンド ID と同じにする必要があります。

MPLS 用の AXSM NNI ポートの追加および割り当て

次の手順では、MPLS 用に NNI ポートを AXSM カードに追加して割り当てます。

ステップ 1 `cc` コマンドを入力して、AXSM カードに移動します。

```
MGX8850.7.a>cc 1
```

ステップ 2 次の例に示すように `cnfcdsct` コマンドを入力して、PNNI と MPLS 用に AXSM カードサービス クラス テンプレート (SCT) を設定します。

```
MGX8850.1.AXSM.a>cnfcdsct 4
```



(注) 4 = ポリシング有効、5 = ポリシング無効 (ATM Forum サービス タイプ)

ステップ 3 **upln** コマンドを入力して、追加する回線を始動します。

```
MGX8850.1.AXSM.a>upln 1.1
```

ステップ 4 **addport** コマンドを入力して、ポートを追加します。

```
addport <ifNum> <bay.line> <guaranteedRate> <maxRate> <sctID> <ifType> [vpiNum]
```

パラメータ	説明
<i>ifNum</i>	1 ~ 60 の数値
<i>bay.line</i>	バック カードの <i>bay</i> (ベイ) を表すポート位置。1 は上部、2 は下部 <i>line</i> は、バックカードに固有です。
<i>guaranteedRate</i>	セル / 秒単位の仮想速度
<i>maxRate</i>	最大速度は、接続により次のように異なります。 OC48 : 50 ~ 5651320 OC12 : 50 ~ 1412830 OC3 : 50 ~ 353207 T3 : 50 ~ 96000 (PLCP) または 104268 (ADM) E3 : 50 ~ 80000
<i>sctID</i>	ポート SCT ID。範囲は 0 ~ 255。デフォルトのファイルは 0、MPLS は 4 または 5 を使用します。
<i>ifType</i>	1 は uni 用、2 は nni 用、3 は vnmi 用
<i>vpiNum</i>	インターフェイスを仮想トランクとして設定するために使用します。範囲は 1 ~ 4095

この例を次に示します。

```
MGX8850.1.AXSM.a>addport 1 1.1 353207 353207 4 0
```

ステップ 5 **addpart** コマンドを入力して、上記で追加したポートを割り当てます。

```
addpart <ifNum> <partId> <cntlId> <egrminbw> <egrmaxbw> <ingminbw> <ingmaxbw>  
<minVpi> <maxVpi> <minVci> <maxVci> <minConns> <maxConns>
```

パラメータ	説明
<i>ifNum</i>	1 ~ 60 の数値
<i>partId</i>	パーティション識別子。1 ~ 5 の数値を入力します。
<i>cntlId</i>	コントローラ識別子。1 ~ 20 の数値を入力します。 1 は PAR 用に、2 は PNNI 用に、3 は LSC 用に予約されています。
<i>egrminbw</i>	出力帯域幅の保証割合 (単位: インターフェイス帯域幅の 0.0001%)
<i>egrmaxbw</i>	出力帯域幅の最大割合 (単位: インターフェイス帯域幅の 0.0001%)
<i>ingminbw</i>	入力帯域幅の保証割合 (単位: インターフェイス帯域幅の 0.0001%)
<i>ingmaxbw</i>	入力帯域幅の最大割合 (単位: インターフェイス帯域幅の 0.0001%)
<i>minVpi</i>	最小 VPI 値。0 ~ 4095 の数値を入力します。 (UNI インターフェイスの場合 0 ~ 255)

パラメータ	説明
<i>maxVpi</i>	最大 VPI 値。0 ~ 4095 の数値を入力します。 (UNI インターフェイスの場合 0 ~ 255)
<i>minVci</i>	最小 VCI 値。32 ~ 65535 の数値を入力します。
<i>maxVci</i>	最大 VCI 値。32 ~ 65535 の数値を入力します。
<i>minConns</i>	保証される接続数。0 ~ <i>portgroup</i> の最大接続数までの値です (<i>portgroup</i> については、 dspe を参照)。
<i>maxConns</i>	最大接続数。0 ~ <i>portgroup</i> の最大接続数までの値です (<i>portgroup</i> の詳細については、 dspe を参照)。

この例を次に示します。

```
MGX8850.1.AXSM.a>addpart 1 2 5 500000 500000 500000 500000 0 1500 32 65535 4000 4000
```

ステップ 6 **dspe** コマンドを入力して、新しく追加したパーティションを表示してその設定を確認します。

```
MGX8850.1.AXSM.a > dspe
if part Ctlr egr egr ingr ingr min max min max min max
Num ID ID GuarBw MaxBw GuarBw MaxBw vpi vpi vci vci conn conn
      (.0001%) (.0001%) (.0001%) (.0001%)
-----
  1  2  5 500000 500000 500000 500000  0 1500  32 65535 4000 4000
```

RPM-XF をエッジ ラベル スイッチ ルータとして設定

ラベル スイッチ コントローラ (LSC) を設定した MGX 8850 Release 5.1 シェルフで、RPM-XF をエッジ ラベル スイッチ ルータ (ELSR) として設定することもできます。これを [図 9-1](#) に ELSR B として示しています。次の手順に従ってこの機能を設定します。

ステップ 1 RPM-XF のグローバル設定動作モードで、次のコマンドを入力します。

```
RPMELSR (config)#interface loopback0
RPMELSR (config-if)#ip address 192.168.3.11 255.255.255.255
```

ステップ 2 次のコマンドを入力して、MPLS パーティションを設定します。

```
RPMELSR (config)#int switch1
RPMELSR (config-if)#switch partition 5 5
RPMELSR (config-if)#ingress-percentage-bandwidth 10 100
RPMELSR (config-if)#egress-percentage-bandwidth 10 100
RPMELSR (config-if)#vpi 100 100
RPMELSR (config-if)#vci 32 65535
RPMELSR (config-if)#connection-limit 1 10000
```


ステップ 3 次のコマンドを入力して、MPLS サブインターフェイスを作成します。

```
RPMELSR (config)#interface switch1.11 mpls
RPMELSR (config-if)#ip unnumbered loopback0
RPMELSR (config-if)#mpls ip
RPMELSR (config-if)#mpls atm control-vc 100 32
RPMELSR (config-if)#mpls atm vpi 100 vci-range 33-65535
```



(注) LSC への RPM-XF ELSR パーティションが 0 以外の vpi 範囲である場合、mpls サブインターフェイスの下に **mpls atm control-vc** と **mpls atm vpi** 文を設定する必要があります。LSC の Xtagatm インターフェイスの下にも同じ文を設定する必要があります。

vp トンネルを使用している場合は、control vc を設定する必要はありません。詳細については、「[LSC の XTagATM インターフェイスへの AXSM ポートおよび ELSR ポートのマッピング](#)」の項を参照してください。



(注) RPM-XF では、デフォルトで Cisco Express Forwarding (CEF ; Cisco エクスプレス転送) が有効になっているため、**ip cef** コマンドを使用する必要はありません。

LSC の XTagATM インターフェイスへの AXSM ポートおよび ELSR ポートのマッピング

次のコマンドを RPM-XF LSC (図 9-1 の LSC-B) に入力して、前述の手順で設定した AXSM ポートと ELSR ポートをこの LSC にマッピングします。

ステップ 1 **cc** コマンド、**cc 5** を入力して、RPM-XF LSC カードに切り替えます。

ステップ 2 **enable** とパスワードを入力します。

```
RPMLSC>enable
Password:
```

ステップ 3 **config t** と入力して、グローバル設定モードに切り替えます。

```
RPMLSC#config t
Enter configuration commands, one per line. End with CNTL/Z.
```

ステップ 4 次の AXSM ポート 1.1 の例に示すように、**interface XTagATM**、**ip**、**extended-port**、および **mpls** コマンドを入力して、AXSM ポートへの通信を確立します。

```
RPMLSC (config)#interface XTagATM1111
RPMLSC (config-if)#ip unnumbered Loopback0
RPMLSC (config-if)# extended-port Switch1 descriptor "1:1.1:1"
RPMLSC (config-if)# mpls ip
```

ステップ 5 次の例に示すように、ELSR (図 9-1 では ELSR-B) に対し **interface XTagATM**、**ip**、**extended-port**、および **mpls** コマンドを入力します。

```
RPLMSC(config)#interface XTagATM4122
RPLMSC(config-if)#ip unnumbered loopback0
RPLMSC(config-if)#extended-port Switch1 descriptor "4:1.2:2"
RPLMSC(config-if)#mpls ip
RPLMSC(config-if)#mpls atm control-vc 100 32
RPLMSC(config-if)#mpls atm vpi 100 vci-range 33-65535
```



(注) **extended-port Switch1 descriptor** *<slot:bay.line:port>* は、XTagATM インターフェイスが示す拡張スイッチ ポートの位置を識別します。RPM-XF では、記述子は、*<slot>:1.2:2* の形式です。*<slot>* は、RPM-XF カードの論理スロットです。

VPN の概要

Virtual Private Network (VPN; バーチャルプライベートネットワーク) は、専用私設網の外観、機能、および効用を備えています。MPLS の VPN 機能によって、専用のアドレッシング、アクセス制御、およびサイト間のサービス レベルの保証を実装し、Cisco IOS ネットワークに、スケーラブルな IPv4 レイヤ 3 VPN バックボーン サービスを展開できます。

VPN はさまざまなサービス プロバイダーのネットワークでサポートされているため、ラベル付きパケットは、RPM-PR または RPM-XF のエッジ LSR からこれらのネットワークを経由して他の RPM-PR または RPM-XF のエッジ LSR へと転送されます。VPN サービスにより、公衆インフラストラクチャに複数の私設ネットワーク環境が作成されます。サービス プロバイダーは VPN を使用して、クライアントごとに個別化した私設ネットワーク サービスを、公衆インフラストラクチャを利用することによって、セキュリティで保護された IP 環境で提供することができます。

MPLS VPN の詳細については、次の URL を参照してください。

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t5/vpn.htm>

MPLS VPN 拡張の詳細については、次の URL を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t7/vpn_en.htm#xtocid151250

必要条件

効果的な VPN の要件は、次のとおりです。

- **プライバシー** : すべての IP VPN サービスは、共有 (公衆) ネットワーク インフラストラクチャ上でのプライバシーを保証します。その最もよく知られているソリューションは暗号化トンネルです。IP VPN サービスは、専用のアドレッシングを提供する必要があります。お客様の私設ネットワーク内のアドレスは、グローバル レベルで一意である必要はありません。
- **スケーラビリティ** : IP VPN サービスは、何十万というサイトをユーザが利用できるように拡張が容易である必要があります。IP VPN サービスはまた、サービス プロバイダーが、サービスへのアクセスを制御するための、管理ツールとしての役割を果たす必要もあります。たとえばこのアクセス管理機能として、データ サービスや音声サービスの非公開ユーザグループなどがあります。アクセス制御により、ネットワーク内の特権プログラム、プロセス、または他のシステムのパフォーマンスが制限されます。
- **柔軟性** : IP VPN サービスは、どのようなトラフィック パターンにも対応する必要があり、しかも、新しいサイトを素早く受け入れ、各種のメディアでユーザを接続し、新しいイントラネット アプリケーションの転送と帯域幅の要求に応じられる必要があります。
- **予測可能なパフォーマンス** : IP VPN サービスによってサポートされるイントラネット アプリケーションは、さまざまな CoS を必要とします。カスタマー サイト間で、サービス レベルのパフォーマンスを保証する必要があります。たとえば、モバイルユーザのリモート接続には広範囲の接続性が必要です。また、支店間での対話型イントラネット アプリケーションには持続的なパフォーマンスの保証が必要です。

MPLS VPN の機能

MPLS 向けの VPN 機能は、IP VPN の機能より優れており、Cisco IOS ネットワークは、次のような拡張の容易な IPv4 レイヤ 3 VPN バックボーン サービスを展開することができます。

- **コネクションレス型サービス**：MPLS VPN は、コネクションレス型です。MPLS VPN は、ネットワーク プライバシーを保証する上でトンネルや暗号化を必要としないため、複雑さが低減されています。
- **集中型サービス**：レイヤ 3 における VPN は、ユーザをイントラネット サービスに専用接続し、1 つの VPN で表されるユーザ グループに合わせてカスタマイズされたサービスを柔軟に配送することができます。VPN では、VPN 内でのマルチキャスト、QoS、および電話サポートなどの IP サービスを配送するとともに、コンテンツと Web ホスティングのような集中型サービスも同様に配送します。サービスの組み合わせは、個々のお客様向けにカスタマイズすることができます。
- **スケーラビリティ**：MPLS ベースの VPN は、レイヤ 3 コネクションレス型アーキテクチャを使用しており、拡張が非常に容易です。
- **セキュリティ**：MPLS VPN は、コネクション型 VPN と同じセキュリティ レベルを提供します。1 つの VPN からのパケットが、間違えて別の VPN に送信されることはありません。プロバイダー ネットワークのエッジで、着信パケットは正しい VPN に向かいます。バックボーンでは、VPN トラフィックの独立が維持されます。



(注) PER のスプーフィングは、着信パケットが IP パケットであり、VPN タグによって一意に識別されるインターフェイスまたはサブインターフェイス上で受信されるため、ほとんど不可能です。

- **作成の簡単さ**：MPLS VPN は、コネクションレス型です。そのため、簡単に、イントラネットとエクストラネットにサイトを追加すること、および非公開ユーザ グループを作成することができます。各サイトは、複数のグループのメンバーになることができます。
- **柔軟なアドレッシング**：MPLS VPN は、アドレスのパブリック ビューとプライベート ビューを提供するので、お客様は、独自の未登録アドレス、つまりプライベート アドレスを使用することができます。また、Network Address Translation (NAT; ネットワーク アドレス変換) なしに、公衆 IP 網を通して自由に通信することができます。
- **簡単な移行**：MPLS VPN は、IP、ATM、フレーム リレー、およびハイブリッド ネットワークを含む複数のネットワーク アーキテクチャ上で構築することができます。Customer Edge (CE; カスタマー エッジ) ルータで MPLS をサポートする上で特別な要件はありません。

サポートされているプラットフォーム

Cisco 3600 シリーズ ルータを含むすべての Cisco ルータ、RPM-PR または RPM-XF を搭載した MGX 8850 マルチサービス スイッチ、Cisco 6400 シリーズ ルータ、およびその他のいくつかのデバイスが、VPN をサポートしています。LSR 機能を備えたプラットフォームはすべて、バックボーンで稼働することができます。また、LightStream 1010 ATM スイッチ、Catalyst 8540 MSR、BPX 8650 マルチサービス スイッチも VPN をサポートします。MPLS 機能を備えていない ATM スイッチも、PVC や PVP を介して MPLS を伝送できるため使用できます。

VPN の動作原理

各 VPN は、1 つ以上の VPN Routing/Forwarding instance (VRF ; VPN ルーティング / 転送インスタンス) に関連付けられています。この VRF では、1 台の PE ルータに接続されている 1 つのカスタマー サイトについて VPN を 1 つ定義します。VRF テーブルの構成要素は、次のとおりです。

- IP ルーティング テーブル
- 導出 Cisco Express Forwarding (CEF; Cisco エクスプレス転送) テーブル
- 転送テーブルを使用するインターフェイスのセット
- 転送テーブルに登録する事項を決定する規則とルーティング プロトコル変数のセット

MPLS 用 VPN

1 つのカスタマー サイトを、複数の VPN のメンバーにすることができます。ただし、1 つのサイトが関連付けられる VRF は、1 つに限られます。1 つのカスタマー サイトの VRF には、関連する VPN からそのサイトへの利用可能なルートすべてを定義します。

各 VRF の IP ルーティング テーブルと CEF テーブルは、パケット転送情報を格納します (この 2 つのテーブルを合わせたものは、MPLS で使用されている Forwarding Information Base (FIB; 転送情報ベース) に似ています)。論理的に無関係なルーティング テーブルと CEF テーブルのセットが、各 VRF について作成されます。この 2 つのテーブルによって、パケットが、当該 VPN から外部に転送されるのを防ぐと同時に、VPN の外側からパケットが、VPN の内部のルータに転送されるのも防ぐことができます。

VPN ルートターゲット コミュニティとエクスポート リストおよびインポート リスト

VPN ルーティング情報の配布は、VPN ルートターゲット コミュニティを使用して制御されます。VPN ルートターゲット コミュニティは、Border Gateway Protocol (BGP; ボーダーゲートウェイ プロトコル) の拡張コミュニティによって実装されています。配布は、次のように行われます。

- VPN ルートは、BGP に投入されると、VPN ルートターゲット コミュニティのリストに関連付けられます。このリストは、当該 VPN ルートの情報のある VRF に関連するエクスポート リストを通して設定されます。
- 各 VRF には、ルートターゲット コミュニティのインポート リストが関連付けられています。このインポート リストには、当該ルートを VPN ルーティング インスタンスにインポートするのが妥当であると判断するために、VRF テーブルで確認すべき値を定義しています。たとえば、当該 VRF のインポート リストに、コミュニティ区別子 A、B、および C がある場合、A、B、または C を伝送する VPN ルートすべてが VRF にインポートされます。

iBGP による VPN ルーティング情報の配布

PER (プロバイダー エッジ ルータ) は、IP プレフィックスを、CE ルータの静的設定、BGP セッション、RIP、または OSPF を通じて入手します。次に、PER は、8 バイトのルート区別子を IP プレフィックスに結合して、VPN-IPv4 (vpng4) プレフィックスを生成します。この VPN-IPv4 アドレスは、各 VPN サイト内でホストを一意に識別します。これは、グローバルには一意でない IP アドレス (未登録のプライベート IP アドレス) を使用しているサイトであっても同様です。VPN-IPv4 プレフィックスの作成に使用されるルート区別子は、PER 上の設定コマンドによって指定します。

BGP は、VPN-IPv4 アドレスを使用して、サービス プロバイダー ネットワーク内にある各 VPN のネットワーク到着可能性情報を配布します。BGP は、ルーティング テーブルを構築または保守したときに、ルーティング メッセージを、IP ドメイン内 (内部 BGP つまり iBGP)、または IP ドメイン間 (外部 BGP つまり eBGP) に配布します。

BGP は、拡張アドレスを取り扱うために、BGP マルチプロトコル拡張を使用して、vpn4 情報を伝えます。RFC 2283 の『*Multiprotocol Extensions for BGP-4*』を参照してください。BGP は、到着可能性情報 (VPN-IPv4 アドレスとして表される) を PE ルータ間で伝えます。ある VPN の到着可能性情報は、その VPN のメンバーだけに伝えられます。BGP マルチプロトコル拡張によって、VPN ルーティング情報の有効な配布先が識別されます。

ラベル転送

MPLS は、各 VRF の IP ルーティング テーブルと CEF テーブルに格納されているルーティング情報に基づき、拡張 VPN-IPv4 アドレスを使用して、パケットを送信先に転送します。

これを実現するため、MPLS ラベルが、各カスタマー ルートに関連付けられます。PE ルータは、ルート発信元のラベルを割り当て、データ パケットが正しい CE ルータに向かうようにします。プロバイダーのバックボーンを通るタグ転送は、ダイナミック IP パスまたはトラフィック エンジニアリングされたパスに基づいて行われます。

お客様のデータ パケットは、バックボーンを通して転送される時、次の 2 つのレベルのラベルが付けられます。

- 最初のラベルによって、パケットは正しい PE ルータに向けられます。
- 2 番目のラベルでは、PE ルータがどのようにパケットを転送するかが決まります。

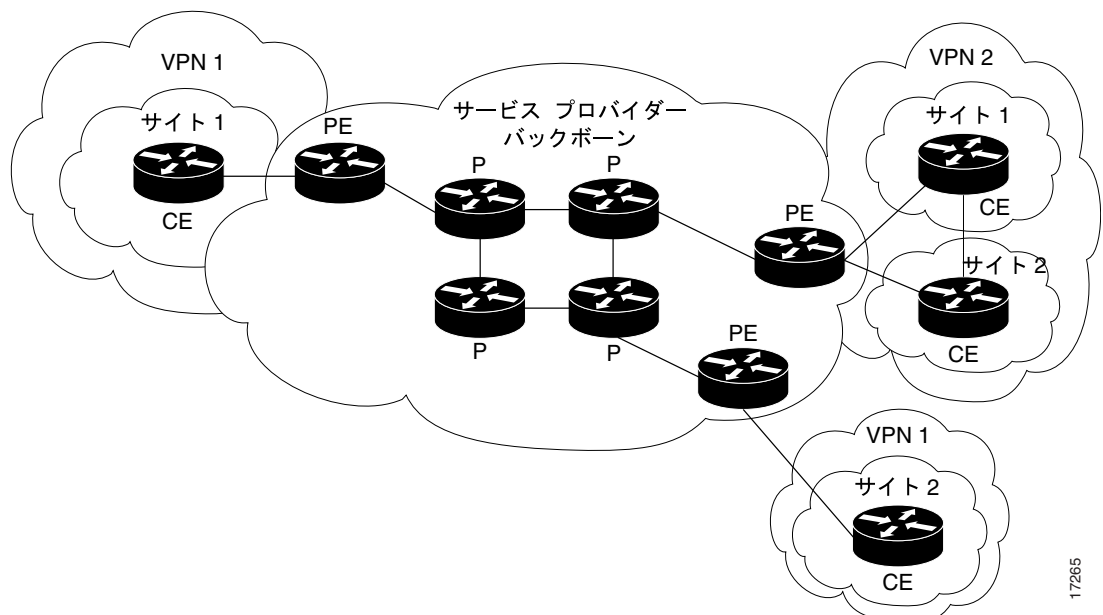
PE ルータでは、それぞれの CE ルータが使用可能なルートのセットだけを含む転送テーブルと、その CE ルータとが関連付けられます。

VPN トポロジーの例

VPN には、カスタマー デバイスが CE ルータに接続されて配置されています。このカスタマー デバイスは、この VPN を使用してデータを交換します。PE ルータだけが、この VPN を認識しています。

例として、サービス プロバイダー (P) のバックボーン ネットワーク、サービス プロバイダー エッジ (PE) ルータ、およびカスタマー エッジ (CE) ルータがある VPN を図 9-2 に示します。

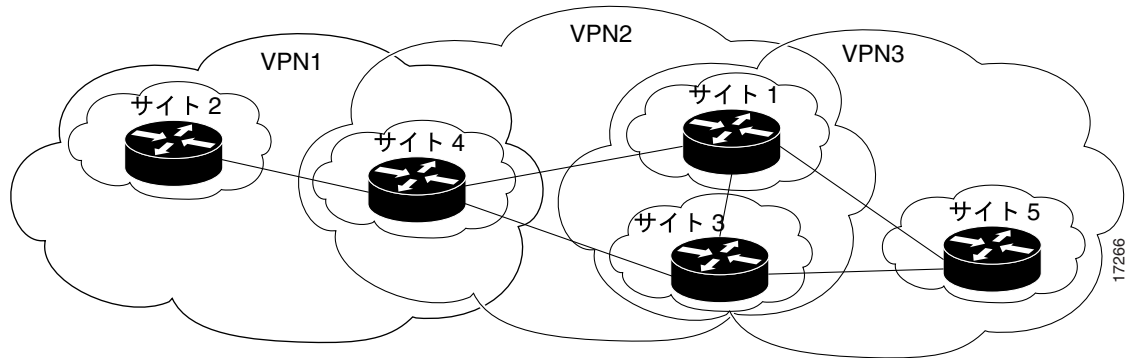
図 9-2 サービス プロバイダー (P) バックボーン ネットワークがある VPN



17265

5箇所のカスタマー サイトと通信する3つのVPNを図9-3に示します。サイト1、3、4は、2つのVPNのメンバーであることに注目してください。

図9-3 カスタマー サイトと通信するVPN



VPN の設定

ここでは、VPN の運用を行うための RPM-XF の設定方法を説明します。最初に、VPN 設定の前提条件を示し、次に設定手順を説明します。

VPN 動作の前提条件

VPN 動作の設定には、ネットワークが次の Cisco IOS サービスを実行していることが必要です。

- CEF スイッチング。タグ転送可能なすべてのルータで必要です。
- すべての PE（プロバイダー エッジ）ルータ間の MPLS 接続性。すべての P ルータ（プロバイダー バックボーンルータ）が VPN サービスまたは MPLS を提供する必要があります。
- VPN コード付き MPLS。VPN PE ルータ（エッジ サービス ルータ）のあるすべてのプロバイダー ルータで必要です。
- BGP。VPN サービスを提供するすべてのルータで必要です。

次の作業をすべて完了してから、VPN 動作を設定してください。

- Cisco エクスプレス転送（CEF）を起動します（CEF は、デフォルトで RPM-XF で有効です）。
- MPLS を設定します。
- VPN ルーティング情報を配布するために、BGP をプロバイダー ルータ間で有効にします。

VPN 動作の設定

ここでは、ルーティング プロトコルを設定し、VPN 用に VRF を作成する方法を説明します。作業に使用するコマンドの詳細は、「[MPLS COS のサポート](#)」を参照してください。次の 4 つの作業を行って、ネットワーク内に VPN を設定し、確認してください。

1. VRF を設定し、インターフェイスを VRF に関連付けます。
2. プロバイダー ルータ間に BGP を設定して、VPN ルーティング情報を配布できるようにします。
3. インポート ルートとエクスポート ルートを設定して、ルーティング情報の配布を制御できるようにします。
4. VPN 動作を確認します。

VRF の設定

VRF を作成するには、プロバイダーのエッジルータで次の手順を実行してください。

ステップ 1 VRF 設定モードに入り、これ以降のステップでコマンドを適用する VRF を指定します。

```
RPM(config)# ip vrf vrf-name
```

ステップ 2 名前と 8 バイトのルート区別子を割り当てて、インスタンスを定義します。

```
RPM(config-vrf)# rd route-distinguisher
```

ステップ 3 インターフェイスを VRF に関連付けます。

```
RPM(config-if)# ip vrf forwarding vrf-name
```


ステップ 4 BGP を PE と VRF CE の間で使用する場合は、BGP パラメータを VRF CE セッション用に設定します。

```
RPM(config-router)# address-family ipv4 vrf name
RPM(config-router-af)# aggregate-address
RPM(config-router-af)# auto-summary
RPM(config-router-af)# default-information originate
RPM(config-router-af)# default-metric ...
RPM(config-router-af)# distance ...
RPM(config-router-af)# distribute-list ...
RPM(config-router-af)# network ...
RPM(config-router-af)# neighbor ...
RPM(config-router-af)# redistribute ...
RPM(config-router-af)# synchronization
RPM(config-router-af)# table-map...
```



(注) CE ルータから BGP 経由で入手したアドレスが、PE ルータ上で、VPN IPv4 アドレスとして正しく処理されているかどうかを確認するには、CE 近接ルータをまったく設定しない状態で **no bgp default ipv4-activate** コマンドを入力します。「[BGP の設定](#)」のステップ 2 とステップ 3 を参照してください。

ステップ 5 RIP を PE と VRF CE の間で使用する場合は、RIP パラメータを設定します (VRF アドレス ファミリ サブモードで)。



(注) **auto-summary** と **synchronization** のデフォルト設定は、VRF アドレス ファミリ サブモードでは、オフになっています。

```
RPM(config-router)# address-family ipv4 vrf name
RPM(config-router-af)# auto-summary
RPM(config-router-af)# default-information originate
RPM(config-router-af)# default-metric ...
RPM(config-router-af)# distance ...
RPM(config-router-af)# network ...
RPM(config-router-af)# offset-list ...
RPM(config-router-af)# redistribute ...
```

ステップ 6 アドレス ファミリ設定モードを終了します。

```
RPM(config-router-af)# exit-address-family
```

ステップ 7 スタティック ルートを VRF 用に設定します。

```
RPM(config)# ip route [vrf vrf-name] destination <interface> ip_address
```

BGP の設定

ボーダーゲートウェイプロトコル (BGP) ルータ アドレス ファミリを設定するには、セッションを定義し、ルーティングプロトコル用のグローバル変数を設定した後、PE ルータにおいて次の手順を設定モードで実行してください。

ステップ 1 BGP アドレス ファミリを設定します。

```
RPM(config-router)# address-family {ipv4 | vpnv4}[unicast | multicast]
```

ステップ 2 BGP セッションを定義します。

```
RPM(config-router-af)# neighbor address | peer-group} remote-as as-number
RPM(config-router-af)# neighbor address | peer-group} update-source interface
RPM(config-router-af)# neighbor peer-group peer-group
RPM(config-router-af)# neighbor address peer-group peer-group
```

ステップ 3 **no bgp default ipv4-activate** コマンドを入力して BGP セッションを起動し、すべての近接ルータへのアドレスファミリ IPv4 の自動アドバタイズメントを禁止します。

このコマンドは、CE ルータとの BGP セッションを確立する PE 上で実行する必要があります。特定の近接ルータに対して、IPv4 プレフィックスのアドバタイズメントを有効にするには、IPv4 のアドレスファミリ モードに入り、その近接ルータに対して、コマンド **neighbor...activate** を使用します。

```
RPM(config-router)# no bgp default ipv4-activate
```

特定のアドレスファミリに対しては、**neighbor... activate** を入力します。

```
RPM(config-router-af)# [no] neighbor address |peer-group} activate
```

ステップ 4 オプションの BGP グローバル コマンドを実行します。これは、すべてのアドレスファミリに影響します。

```
RPM(config-router)# bgp always-compare-med
RPM(config-router)# bgp bestpath ...
RPM(config-router)# bgp client-to-client reflection
RPM(config-router)# bgp cluster-id ...
RPM(config-router)# bgp confederation ...
RPM(config-router)# bgp default local-Xference ...
RPM(config-router)# bgp deterministic-med ...
RPM(config-router)# bgp fast-external-falover ...
RPM(config-router)# bgp log-neighbor-changes
RPM(config-router)# bgp redistribute-internal
RPM(config-router)# bgp router-id ...
RPM(config-router)# timers bgp ...
```

ステップ 5 BGP 設定コマンドをアドレス ファミリ IPv4 に対して入力します。

IOS の以前のバージョンでサポートされている BGP 設定コマンドはすべて、アドレス ファミリ IPv4 ユニキャストでも有効です。この BGP 設定コマンドは、すべての IPv4 インスタンスか、またはデフォルトの IPv4 ルーティング テーブルに影響します。下位互換性に考慮して、これらのコマンドは、ルータ設定モードでも、または `ipv4` ユニキャストのアドレス ファミリ モードでも入力できるようになっています。**no bgp default ipv4-activate** コマンドの説明については、ステップ 3 を参照してください。

```
RPM(config-router)# bgp ...
```

ステップ 6 BGP 設定コマンドをアドレス ファミリ VPNv4 に対して入力します。

```
RPM(config-router)# bgp dampening ...
RPM(config-router)# neighbor ...
RPM(config-router)# neighbor address | peer-group}activate
```

ステップ 7 iBGP を、VPNv4 Network Layer Reachability Information (NLRI; ネットワーク レイヤ到着可能性情報) を交換するように (PE ルータとルート リフレクタの間または PE ルータ間で) 設定するには、まず iBGP BGP セッションを定義します。



(注) VPN パケットが、PE ルータ間で正しくタグ転送されているか確認するには、近接ルータ アドレスと更新元インターフェイスのループバック アドレスを指定します。

```
RPM(config-router)# neighbor address remote-as as-number
RPM(config-router)# neighbor address update-source interface
```

ステップ 8 VPNv4 NLRI のアドバタイズメントを起動します。

```
RPM(config-router)# address-family vpnv4
RPM(config-router-af)# neighbor address activate
```

eiBGP ロード シェアリングの実行

External and Internal Border Gateway Protocol (eiBGP; 外部および内部ボーダーゲートウェイ プロトコル) ロード シェアリングは、ボーダーゲートウェイ プロトコル (BGP) を拡張したもので、カスタマー エッジルータとプロバイダー エッジルータの間のパラレル リンク上でロード シェアリングを実現します。この機能により、サービス プロバイダーは MPLS コア ネットワーク内のパラレルパスにカスタマー トラフィックの負荷を分散できます。

BGP 上でロード シェアリングを実行するには、トラフィックが、自律システム (AS) 間の複数のパス上のゲートウェイ ルータによって振り分けられるように設定する必要があります。この機能を実装するには、次の CLI コマンドを使用します。

コマンド	説明
maximum-path <nums>	<p>EiBGP パラレルルートの最大数を設定します。</p> <p>たとえば、次のように設定します。</p> <pre>bgpbox-zenith-CE1(config)#router bgp 4 bgpbox-zenith-CE1(config-rout)#maximum-paths 3 bgpbox-zenith-CE1(config-rout)#end</pre>
show ip bgp	<p>このコマンドは、マルチパスを表示するように拡張されました。</p> <p>各マルチパスは、「multipath」として示されます。</p> <p>ベストパスは、「multipath」および「bestpath」として示されます。</p> <p>出力には、有効になっているマルチパスの種類も示されます。</p> <p>たとえば、次のように入力します。</p> <pre>bgpbox-zenith-CE1#sh ip bgp 141.22.0.0 BGP routing table entry for 141.22.0.0/16, version 18 Paths: (2 available, best #1) Multipath: eBGP Advertised to non peer-group peers: 7.0.76.9 100 5 7.0.76.2 from 7.0.76.2 (100.0.0.2) Origin IGP, localpref 100, valid, external, multipath, best 100 5 7.0.76.9 from 7.0.76.9 (100.0.0.9) Origin IGP, localpref 100, valid, external, multipath</pre>

インポート ルートとエクスポート ルートの設定

VRF ルート ターゲット拡張コミュニティとインポート ルート マップを設定するには、PE ルータにおいて、次の手順を設定モードで実行してください。

ステップ 1 VRF 設定モードに入り、VRF を指定します。

```
RPM(config)# ip vrf vrf-name
```

ステップ 2 指定した拡張コミュニティからルーティング情報をインポートします。

```
RPM(config-vrf)# route-target import community-distinguisher
```

ステップ 3 ルーティング情報を、指定した拡張コミュニティにエクスポートします。

```
RPM(config-vrf)# route-target export community-distinguisher
```

ステップ 4 設定する VRF に、指定したルート マップを関連付けます。

```
RPM(config-vrf)# import map route-map
```

VRF のチェック

VPN の設定内容を確認するには、次の手順を実行します。

- ステップ 1** 定義されている VRF のセット、および各 VRF に関連しているインターフェイスを表示します。

```
RPM# show ip vrf
```

- ステップ 2** 設定されている VRF の詳細情報、たとえばインポート コミュニティ リストとエクスポート コミュニティ リストなどを表示します。

```
RPM# show ip vrf detail
```

- ステップ 3** VRF の IP ルーティング テーブルを表示します。

```
RPM# show ip route vrf vrf-name
```

- ステップ 4** VRF に関連付けられているルーティング プロトコル情報を表示します。

```
RPM# show ip protocols vrf vrf-name
```

- ステップ 5** VRF に関連付けられている CEF 転送テーブルを表示します。

```
RPM# show ip cef vrf vrf-name
```

- ステップ 6** インターフェイスに関連付けられている VRF テーブルを表示します。次のコマンドのどちらかを使用します。

```
RPM# show ip interface interface-number  
RPM# show cef interface interface-number
```

- ステップ 7** VPNv4 NLRI 情報を表示します。

キーワード **all** を指定すると、データベース全体が表示されます。キーワード **rd** では、指定したルート区別子に一致する NLRI が表示されます。キーワード **vrf** では、指定した VRF を持つ NLRI が表示されます。他のすべてのキーワードおよび引数の後に、キーワード **tags** を指定すると、VPNv4 NLRI によって配布されるタグのリストが表示されます。

```
RPM # show ip bgp vpnv4 all [tags]  
RPM # show ip bgp vpnv4 rd route-distinguisher [tags]  
RPM # show ip bgp vpnv4 vrf vrf-name [tags]
```

- ステップ 8** このルータによってアドバタイズされる VRF ルートに対応するタグ転送エントリを表示します。

```
RPM # show mpls forwarding vrf vrf-name [prefix mask/length] [detail]
```

ステップ 9 ping または traceroute も使用できます。

```
RPM # ping vrf vpn 1.1.1.1
```

1.1.1.1 は送信先アドレスです。

ステップ 10 次の telnet コマンドを入力して、VRF をチェックします。

```
telnet 1.1.1.1 /vrf vpn
```

マルチキャスト VPN

マルチキャスト VPN には、マルチキャスト トンネリングを使用して MPLS-VPN 内にマルチキャスト トラフィックを伝送する機能が用意されています。1 つの MPLS-VPN エンドポイントから、MPLS-VPN 内の他のすべての宛先エンドポイントにマルチキャスト パケットを送信できます。

マルチキャスト VPN は、次の機能をサポートします。

- MPLS フレームベースのカプセル化
- PIM-SM および PIM-SSM コア モード
- 最大 384 個の mVRF
- ATM、POS、および GIGE インターフェイス
- ポイントツーポイント ATM サブインターフェイス

マルチキャスト VPN は、次のコマンドをサポートしません。

- ip multicast rate-limit
- ip multicast multipath

表 9-1 で、マルチキャスト VPN で使用するいくつかの用語を説明します。

表 9-1 マルチキャスト VPN の用語

用語	説明	説明
VPN	バーチャル プライベート ネットワーク	
mVPN	マルチキャスト バーチャル プライベート ネットワーク	ネイティブ マルチキャストをサポートする MPLS-VPN
VRF	VPN ルーティング / 転送テーブル	PE で VPN 用ユニキャストルーティングテーブルを保持します。
mVRF	マルチキャスト VPN ルーティング / 転送テーブル	PE の VPN 用マルチキャストルーティングテーブル
MDT	マルチキャスト配布ツリー	各マルチキャスト ドメインで P (プロバイダー) ネットワークに組み込まれたマルチキャスト ツリー
Default-MDT	デフォルトのマルチキャスト配布ツリー	すべての mVRF がこのツリーに属します。PIM 制御トラフィック、低帯域幅送信元、密モードのフラグディングで使用します。
Data-MDT	データ マルチキャスト配布ツリー	高帯域幅送信元でオンデマンドで作成され、対象でない PE への複製を回避します。

マルチキャスト VPN の動作

マルチキャスト VPN は、マルチキャスト トンネリングを使用して MPLS-VPN 内でのマルチキャスト トラフィックをサポートする機能です。マルチキャスト VPN では、MPLS をプロバイダー ネットワークにまたがるマルチキャスト トラフィックの伝送機能としては使用しません。

CE ルータ (カスタマー エッジルータ) は、マルチキャスト パケット (C パケット (カスタマー パケット)) を PE ルータ (プロバイダー エッジルータ) に送信します。PE ルータは、GRE-IP ヘッダーか IP-IP ヘッダーのいずれかを追加することによって P パケット (プロバイダー パケット) を作成します。次に、PE ルータは、この P パケットを、マルチキャスト処理を使用して 1 つ以上の P ルータ (プロバイダー ルータ) に送信します。

マルチキャスト ドメインはマルチキャストを有効にした VRF (mVRF) の集まりで、ドメイン内の mVRF はマルチキャスト トラフィックを互いに送信することができます。マルチキャスト VPN マッピングは、GRE を使用して C パケットを P パケットにカプセル化することで行われます。

MPLS-VPN の 1 つのセグメントから発信されたカスタマー マルチキャスト パケット (C パケット) は、次のように、MPLS-VPN の別のセグメントに送信されます。

1. CE ルータが C パケットを PE ルータに送信します。
2. PE ルータは、GRE-IP ヘッダーを追加することによってプロバイダー マルチキャスト パケット (P パケット) を作成し、その P パケットを、マルチキャスト処理を使用して 1 つ以上の P ルータに送信します。P パケット内の宛先 IP アドレスには、その MPLS-VPN (VRF) 用に設定されたマルチキャスト アドレスが含まれます。
3. P ルータは、マルチキャスト処理を使用してプロバイダー ネットワーク内で P パケットを転送します。転送は、P パケット内のマルチキャスト アドレスに基づいて行われます。
4. MPLS-VPN セグメントに関連するその他の PE ルートは P パケットを受信し、トンネル ヘッダーを削除し、C パケットをマルチキャスト処理を使用してその MPLS-VPN セグメントに関連する CE ルートに転送します。転送は、C パケット内のマルチキャスト アドレスに基づいて行われます。

マルチキャスト VPN の設定例

```
ip vrf coke
  rd 1:1
  route-target export 1:1
  route-target import 1:1
  mdt default 232.0.0.1
  mdt data 232.0.1.0 0.0.0.255 threshold 500
!
ip pim sparse-mode
```

IP マルチキャスト

IP マルチキャストでは、1 つの送信元から複数の宛先に情報を送信します。データグラムの 1 つのコピーが送信元から送信されると、各受信装置で複製が作成されます。

IP マルチキャストは、通常の IP パケットです。ただし、マルチキャスト宛先アドレスを使用します。宛先アドレスの範囲は 224.0.0.0 ~ 239.255.255.255 (D クラス) です。送信元はグループアドレスを送信し、宛先はそのグループアドレスを傍受します。

マルチキャスト トラフィックは、マルチキャスト配布ツリーを使用して転送されます。このツリーには、次の 2 種類があります。

- 送信元ツリー
- 共有ツリー

パケットは、IP マルチキャスト ステートを使用して送信元ツリーから共有ツリーに送られます。IP マルチキャスト ステートによって、ツリーのパケット配布の転送エントリが形成されます。このステートは、送信元アドレス (根) とマルチキャスト ストリームの宛先グループからなります。

送信元ツリーは、(S, G) で表されます。これは、特定のグループ (Group) の特定の送信元 (Source) を表します。共有ツリーは (*, G) で表されます。これは、特定のグループ (Group) のすべての送信元 (*) を表します。

マルチキャスト トラフィックは、最短パスを使用して送信元 (根) から受信側 (葉) に搬送されます。ランデブー ポイントのルータは多くのマルチキャスト グループを処理します。受信側は、ランデブー ポイントに接続され送信元について学習します。送信元はランデブー ポイントに送信し、ランデブー ポイントは受信側に転送します。

マルチキャスト プロトコル

RPM-XF は次のマルチキャスト モードをサポートします。

- 密モード プロトコル：フラッド (Flood) とプルーン (Prune)
 - Distance Vector Multicast Routing Protocol (DVMRP; ディスタンス ベクター マルチキャスト ルーティング プロトコル)
 - Protocol Independent Multicast (PIM-DM; プロトコル独立型マルチキャスト)：レガシー
- 疎モード プロトコル：ジョイン (Join) とプルーン (Prune)
 - Core Based Trees (CBT; コア ベース ツリー)
 - プロトコル独立型マルチキャスト (PIM-SM)
PIM-SM は、最も広く使用されているマルチキャスト プロトコルであり、RPF チェックに既存のユニキャスト テーブルを使用します。
- リンク ステート プロトコル
 - Multicast Open Shortest Path First (MOSPF)

SP コアでサポートされるマルチキャスト プロトコル

コアの IOS では、PIM ベースのプロトコルだけがサポートされます。Cisco IOS では、次の PIM モードがサポートされています。

- PIM Bidirectional (PIM-BIDIR; 双方向 PIM)
- PIM 送信元固有マルチキャスト (PIM-SSM)
- PIM 疎モード (PIM-SM)
- ゼニス社でサポートされている PIM のモード
- PIM 送信元固有マルチキャスト (PIM-SSM)
- PIM 疎モード (PIM-SM)

マルチキャスト モード

- PIM 密モード
 - フラッドとプルーンの動作：送信元ツリーだけを使用するレガシー アプリケーション用 プッシュ モデルであり、展開されることはほとんどありません。
- PIM 疎モード
 - ジョインとプルーンの動作：共有ツリーを使用するプル モデルですが、送信元ツリーに切り替えることができます。
- 双方向 PIM
 - PIM-SM と同じ原理で動作しますが、すべてのトラフィックで BIDIR (双方向) 共有ツリーを使用します。
- 送信元固有マルチキャスト (SSM)
 - (S, G) 送信元ツリーを常に使用し、RP (ランデブー ポイント) は不要です。受信側には S/W (ソフトウェア) が必要で、最後のホップルータには IGMPv3 などのインテリジェンスが必要です。

送信元固有マルチキャスト

送信元固有マルチキャスト (SSM) では、プロバイダー エッジ (PE) ルータを MDT の送信元ツリーに直接接続できます。ネットワーク内にランデブー ポイントは必要ありません。ランデブー ポイントは障害ポイントとなる可能性があり、送信元固有マルチキャストの追加のオーバーヘッドとなります。

送信元固有マルチキャストは、共有ツリーと双方向ツリーを使用します。ただし、PE ルータの各 mVPN には送信元とグループ (S, G) ステートが 1 つずつ必要です。たとえば、5 台の PE ルータがあり、それぞれが 1 つの mVRF RED を維持している場合は、5 つの (S, G) エントリが必要です。

SSM の設定例

```
ip pim ssm range Data-MDT-Range
!
ip access-list standard Data-MDT-Range
permit 239.192.10.0 0.0.0.255
```

mVPN 転送の動作

ここでは、mVPN 転送の動作について説明します。

CE からの C パケットの転送は、次のように行われます。

1. C パケットが、VRP を設定した PE インターフェイスに到着します。
2. mVRF (FIB インデックス) が暗黙的に識別されます。
3. C 送信元で通常の RPF チェックが行われます。

(*G) または (S,G) エントリを探すために検索が行われます。送信元 IP アドレス、マルチキャストグループ アドレス、および FIB インデックスを使用して検索が行われます。PXF は、検索に少なくとも 1 つのコンテキスト (新しいワーク) を使用します。

4. 一致しない場合、パケットは RP にパントされます。これにより IOS はそのグループの (*G)/(S,G) エントリを作成します。
5. C パケットは、一致した (*G)/(S,G) エントリの o リスト内の各カスタマー ネットワーク インターフェイスへ複製されます。

PXF は、各複製につき 1 つのフィードバックを使用します。o リストに MTI が含まれる場合、C パケットは P パケットにカプセル化されます。送信元は PE BGP ピア アドレスで、宛先は MDT グループ アドレスです。カプセル化されたパケットは、その MDT グループのグローバル (*G)/(S,G) エントリの o リストのすべての o/g (outgoing) インターフェイスへ複製されます。PXF は、それらの各複製につき 2 つのフィードバックを使用します。

6. PXF は最後の 1 つのフィードバックをクリーンアップ用に取り込みます。

P ネットワークからの P パケットの転送

7. P パケットは通常のマルチキャストとして P ネットワーク上で転送されます。
8. グローバル インターフェイスは P パケットを送信し、その MDT グループの (S, G) または (*, G) エントリを検索します。
9. P 送信元 (PE ピア) で通常の RPF チェックが行われます。PXF は、チェックに少なくとも 1 つのコンテキスト (新しいワーク) を使用します。
10. P パケットは o リストの個々のインターフェイスへ複製されます。この時点では、これはグローバル mroute テーブルの P/PE インターフェイスとなります。

11. PXF は、各複製につき 1 つのフィードバックを取り込みます。発信インターフェイス リストに mVRF i/f (インターフェイス) がある場合、P パケットのカプセルは解除されます。MDT グループからターゲット mVRF が抽出されます。これは、PXF クライアントによってすでに PXF でプログラミングされています。
12. ターゲット mVRF では、パケット内部の送信元およびグループ アドレスを使用して検索が行われます。これで、少なくとも 1 つのフィードバックが取り込まれます。一致しない場合、パケットは廃棄されます。これは、該当する受信者がいないことを意味します。
13. 次に、C パケットは、mVRF の一致したエントリの o リストに複製されます。PXF は、各複製につき 1 つのフィードバックを取り込みます。
14. 最後に、クリーンアップ用に 1 つのフィードバックが必要です。

VRF の設定例

```

ip multicast-routing vrf CustomerB

ip vrf CustomerB
 rd 101:1

 route-target export 101:1

 route-target import 101:1

 mdt default 238.1.1.1

 mdt data 238.1.2.0 0.0.0.255 threshold 1

interface Switch1.56 point-to-point
 ip vrf forwarding CustomerB
 ip address 156.1.1.10 255.255.255.0
 ip pim sparse-mode

02:05:15: %LINEPROTO-5-UPDOWN:Line protocol on Interface Tunnel0, changed state to up

pop20-slot10#sh int tunnel0
Tunnel0 is up, line protocol is up
Hardware is Tunnel Interface is unnumbered.
Using address of Loopback0 (10.10.10.10)
MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec, reliability 255/255, txload 112/255,
rxload 1/255 Encapsulation TUNNEL, loopback not set Keepalive not set Tunnel source
10.10.10.10 (Loopback0), destination 238.1.1.1 Tunnel protocol/transport GRE/IP
Multicast, key disabled, sequencing disabled Tunnel TTL 255 Checksumming of packets
disabled, fast tunneling enabled

PE 1# show ip pim vrf CustomerB interface
Address          Interface          Ver/  Nbr  Query DR   DR
                  Mode  Count Intvl Prior
156.1.1.10       Switch1.56         v2/SD 1    30    1   0.0.0.0
10.10.10.10      Tunnel0            v2/SD 2    30    1  10.10.10.10

PE 1#sh ip mroute
IP Multicast Routing TableFlags:
  D - Dense, S - Sparse, B - Bidir Group,
  s - SSM Group, C - Connected, L - Local,
  P - Pruned, R - RP-bit set, F - Register flag,
  T - SPT-bit set, J - Join SPT, M - MSDP created entry,
  X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
  U - URD, I - Received Source Specific Host Report, Z - Multicast Tunnel
  Y - Joined MDT-data group, y - Sending to MDT-data group
Outgoing interface flags:
H - Hardware switched Timers: Uptime/Expires Interface state: Interface, Next-Hop
or VCD, State/Mode

(10.10.10.10, 238.1.2.0), 00:28:43/00:03:28, flags: FTZ Incoming interface:
Loopback0, RPF nbr 0.0.0.0 Outgoing interface list: Switch1.2,
Forward/Sparse-Dense, 00:27:43/00:03:18 Switch1.7, Forward/Sparse-Dense,
00:28:43/00:03:18

(10.10.10.10, 238.1.1.1), 21:29:48/00:01:24, flags: FTZ Incoming interface:
Loopback0, RPF nbr 0.0.0.0 Outgoing interface list: Switch1.7,
Forward/Sparse-Dense, 18:14:59/00:03:25 Switch1.2, Forward/Sparse-Dense,
21:29:48/00:02:56

```

MPLS LDP

MPLS Label Distribution Protocol (LDP; ラベル配布プロトコル) により、複数のサービス レベルをサポートする、拡張が非常に容易で柔軟な IP バーチャルプライベート ネットワーク (VPN) を構築できます。LDP は、基になる Interior Gateway Protocol (IGP; 内部ゲートウェイ プロトコル) ルーティング プロトコルにより選択されたルートにラベルを割り当てることで、MPLS ネットワークにおいてホップごとに配布する標準的な方法、つまりダイナミック ラベル配布方式を提供します。その結果得られたラベル付きのパスは、Label Switch Path (LSP; ラベル スイッチ パス) と呼ばれ、MPLS バックボーンを介して特定の送信先にラベルトラフィックを転送します。これらの機能により、サービス プロバイダーは、マルチベンダ MPLS ネットワークを介して Cisco MPLS ベースの IP VPN と IP+ATM サービスを実装できます。

LDP は、シスコのプリスタンダードな Tag Distribution Protocol (TDP; タグ分配プロトコル) のスーパーセットであり、通常のルーティング パスで転送する MPLS もサポートします。LDP と TDP が共有する機能では、ネットワーク ルーティング プラットフォーム間のプロトコル交換パターンは同じです。LDP と TDP でサポートされる機能の両プロトコルでの主な違いは、プロトコルメッセージの符号化など、それぞれの細かい実装の違いです。

LDP と TDP の両方のプロトコルをサポートする Cisco IOS の今回のリリースにより、既存のネットワークを TDP 稼働環境から LDP 稼働環境へ移行することが可能になります。したがって、任意のルータ プラットフォームで LDP と TDP を同時に実行できます。選択したルーティング プロトコルは、直接接続の近隣ルータに対してはインターフェイスごとに設定でき、間接接続 (ターゲット) 近隣ルータに対してはセッションごとに設定できます。さらに、MPLS ネットワークの LSP は、一部のホップでは LDP で、その他のホップでは TDP でサポートできます。

設定作業、TDP から LDP へのネットワークの移行、およびコマンド リファレンス マニュアルなどの詳細については、次の URL にある Cisco IOS Release 12.2T の『MPLS Label Distribution Protocol』を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ldp_221t.htm#xtocid212130



(注)

CWM での LDP または TDP のサポート予定はありません。

RPM-XF でのマルチ VC のサポート

この機能では、RPM-XF で送信先ごとに複数の Label Switched Path (LSP; ラベル スイッチドパス) の開始をサポートし、異なるサービス クラス (COS) を提供できます。4 つの MPLS COS に対応して、4 つの LVC が作成されます。MPLS COS 機能により、ネットワーク管理者は、MPLS が有効なネットワークを介して IP パケットを転送するための幅広い要件を満たすことができます。

マルチ VC 機能は、RPM-XF eLSR で有効にします。RPM-XF eLSR は、内部で RM7000A MIPS 処理エンジン内に 4 つのキューを作成し、4 MPLS COS のための QoS を提供します。各 MPLS COS への帯域幅の割り当ては、IOS Modular QoS CLI から設定でき、RPM-XF eLSR で設定された MPLS パーティションを基に計算されます。

RPM-XF eLSR へ到着したラベルのない IP パケットは、IP 優先順位ビット設定に基づいて異なる MPLS COS に分類されます。このパケットの MPLS COS 分類を基に、正しい LVC がラベルインポジションとパケットの転送に使用されるようになります。その後、パケットは、対応する RM7000A MIPS 処理エンジン キューである COS キューにキューイングされます。

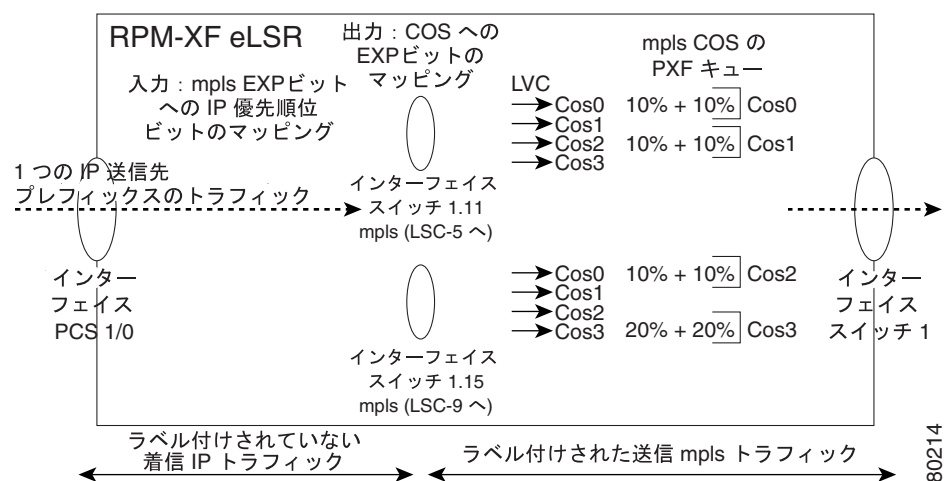
次の例は、モジュラ QoS を使用した一般的な multi-vc モードの設定を示します。

RPM-XF eLSR でのマルチ VC の設定

図 9-4 に、マルチ VC 機能を有効にした、RPM-XF eLSR のトラフィック フローの例を示します。ラベルのない着信 IP パケットは、着信 POS インターフェイスを介して送信されます。POS インターフェイスに設定された入力サービスポリシーにより、各パケットの IP 優先順位ビットが MPLS EXP ビットにマッピングされます。各 MPLS EXP ビットは、MPLS COS にマッピングされます。このパケット MPLS COS に従って、4 つの LVC のうちの 1 つ (cos-map を使用して、送信先 IP プレフィックスごとに作成される LVC 数を制御可能) が、ラベルインポジションとパケット転送に使用されます。パケットに正しいラベルが付けられると、パケットは対応する COS キューの最後にキューイングされ、RPM-XF ATM インターフェイス スイッチ 1 から送信されます。

図 9-4 は、図 9-1 に示したシステム ブロック図を基に作成されています。次の図の RPM-XF eLSR は、図 9-1 の ELSR-B です。以降の設定に関する説明も、この例を基に構築されています。

図 9-4 マルチ VC 設定



(注) マルチ VC は RPM-XF のエッジ LSR だけで設定する必要があります。

次の設定例では、RPM-XF eLSR で行う 5 つの基本手順を示します。

- IP 優先順位を MPLS EXP ビットにマッピングするようにポリシー マップを設定します。
- 入力サービス ポリシーを入力インターフェイスに関連付けます。
- 帯域幅を各 MPLS COS キューに割り当てるように出力サービス ポリシーを設定します。
- 出力サービス ポリシーを出力 MPLS インターフェイスに関連付けます。
- MPLS パーティションを出力 MPLS インターフェイスに結合します (RPM-XF 固有に新規追加)。

次の例は、RPM-XF でのマルチ VC の設定方法を示します。

```

! Zenith-ELSR

class-map match-all IP_PREC0
match ip precedence 0 4
class-map match-all IP_PREC1
match ip precedence 1 5
class-map match-all IP_PREC2
match ip precedence 2 6
class-map match-all IP_PREC3
match ip precedence 3 7
!
class-map match-all COS_0
  match mpls experimental 0 4
class-map match-all COS_1
  match mpls experimental 1 5
class-map match-all COS_2
  match mpls experimental 2 6
class-map match-all COS_3
  match mpls experimental 3 7
!
policy-map set_EXP0
class IP_PREC0
set mpls experimental 0
policy-map set_EXP1
class IP_PREC1
set mpls experimental 1
policy-map set_EXP2
class IP_PREC2
set mpls experimental 2
policy-map set_EXP3
class IP_PREC3
set mpls experimental 3
!
policy-map COS_0123
class COS_0
  bandwidth percent 20
class COS_1
  bandwidth percent 20
class COS_2
  bandwidth percent 20
class COS_3
  bandwidth percent 40
!
interface Switch1
  no ip address
  switch partition 8 8
  ingress-percentage-bandwidth 50 100
  egress-percentage-bandwidth 50 100
  vpi 140 145
  vci 32 65535
  connection-limit 8000 8000
!
  switch auto_synch off
!
interface Switch1.14 mpls
ip unnumbered Loopback1
service-policy output COS_0123
mpls ip
mpls atm switch-partition 8
mpls atm multi-vc
mpls atm control-vc 140 32
mpls atm vpi 140-145 vci-range 33-65535
!

```


次の例は、IP 優先順位を MPLS EXP ビットにマッピングするポリシー マップの設定方法を示します。

```
class-map match-all IP_PREC0
  match ip precedence 0 4
class-map match-all IP_PREC1
  match ip precedence 1 5
class-map match-all IP_PREC2
  match ip precedence 2 6
class-map match-all IP_PREC3
  match ip precedence 3 7
!

policy-map set_EXP0123
  class IP_PREC0
    set mpls experimental 0
  class IP_PREC1
    set mpls experimental 1
  class IP_PREC2
    set mpls experimental 2
  class IP_PREC3
    set mpls experimental 3
!
```

次の例は、入力サービス ポリシーを入力インターフェイスに接続する方法を示します。

```
int POS1/0
  service-policy input set_EXP0123
!
```

次の例は、帯域幅を各 MPLS COS キューに割り当てるように入力サービス ポリシーを設定する方法を示します。

```
class-map match-all COS_0
  match mpls experimental 0 4
class-map match-all COS_1
  match mpls experimental 1 5
class-map match-all COS_2
  match mpls experimental 2 6
class-map match-all COS_3
  match mpls experimental 3 7
!

policy-map COS_0123
  class COS_0
    bandwidth percent 20
  class COS_1
    bandwidth percent 20
  class COS_2
    bandwidth percent 20
  class COS_3
    bandwidth percent 40
!
```

次の例は、出力サービス ポリシーを出力 MPLS インターフェイスに接続し、MPLS パーティションを出力 MPLS インターフェイスに結合する方法を示します。

```
interface switch1.11 mpls
  service-policy output COS_0123
  mpls atm switch-partition 5
!
```



(注) 図 9-1 の ELSR-B の設定例では、switch-partition 5 と interface switch1.11 が、マルチ VC 機能のないセルベース MPLS を有効にするように設定されています。上記の例は、マルチ VC 機能を有効にするために必要な追加コマンドを示しています。