IPv4 マルチキャスト VPN サポート

- 「mVPN の前提条件」（P.49-1）
- 「mVPN に関する制約事項」（P.49-1）
- 「mVPN について」（P.49-3）
- 「mVPN のデフォルト設定」（P.49-11）
- 「mVPN の設定方法」（P.49-11）
- 「mVPN の設定例」（P.49-27）

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

mVPN の前提条件

なし。

mVPN に関する制約事項

- 「一般的な制約事項」（P.49-2）
- 「mVPN with L3VPN over mGRE の制約事項」（P.49-3）

一般的な制約事項

- マルチキャスト ドメインのすべての PE ルータでは、mVPN 機能をサポートする Cisco IOS ソフトウェア イメージを実行する必要があります。P ルータおよび CE ルータには、mVPN をサポートするための要件がありません。
- すべてのバックボーン ルータでは、IPv4 マルチキャスト トラフィックのサポートをイネーブルにする必要があります。
- マルチキャスト トラフィックをサポートするすべてのルータでは、ボーダー ゲートウェイ プロトコル（BGP）ルーティング プロトコルを設定して動作させる必要があります。BGP 拡張コミュニティをイネーブルにしないと（**neighbor send-community both** コマンドまたは **neighbor send-community extended** コマンドを使用）、ネットワークにおける MDT の使用がサポートされません。
- スイッチが PE として動作しており、Time-To-Live（TTL）値が 2 であるカスタマー ルータからマルチキャスト パケットを受信した場合、そのパケットは、カプセル化されて mVPN リンクを横断して転送される代わりにドロップされます。mVPN リンクの反対側の PE がこのようなパケットを正常にドロップするので、トラフィック フローは影響されません。
- コア マルチキャスト ルーティングが SSM を使用する場合は、データ Multicast Distribution Tree（MDT）グループおよびデフォルト マルチキャスト配信ツリー（MDT）グループを IPv4 アドレスの SSM 範囲内で設定する必要があります。
- BGP ピアリングの更新送信元インターフェイスは、ルータで設定されているすべての BGP ピアリングで同一でないと、デフォルト MDT は適切に設定されません。BGP ピアリングにループバック アドレスを使用する場合は、ループバック アドレスで PIM sparse モードをイネーブルにする必要があります。
- BGP ピアリング インターフェイスとして使用されるループバック インターフェイスで **ip mroute-cache** コマンドをイネーブルにしないと、分散マルチキャスト スイッチングは、それをサポートするプラットフォームで機能しません。このようなインターフェイスでは、**no ip mroute-cache** コマンドを*設定しないでください*。
- dense モード マルチキャスト フローにはフラッディングとプルーニングという性質があり、データ MDT の周期的な始動および分解という結果になるので、データ MDT は VRF PIM dense モード マルチキャスト ストリームで作成されません。
- 送信元情報が使用できないので、VRF PIM 双方向モードではデータ MDT が作成されません。
- mVPN では複数の BGP ピアリング更新送信元がサポートされず、これを設定すると、mVPN Reverse Path Forwarding（RPF）チェックが中断することがあります。mVPN トンネルの送信元 IPv4 アドレスは、BGP ピアリング更新送信元に使用される最高の IPv4 アドレスによって決まります。この IPv4 アドレスが、リモート PE ルータを含む BGP ピアリング アドレスとして使用される IPv4 アドレスでない場合、mVPN は適切に機能しません。
- MDT トンネルではユニキャスト トラフィックが搬送されません。
- mVPN が MPLS VPN ネットワークのインフラストラクチャを使用する場合、MPLS タグやラベルは、VPN 上のマルチキャスト トラフィックに適用できません。
- デフォルト MDT で設定されている各 mVRF は、ユーザに表示される外部 VLAN に加えて、3 つの非表示 VLAN（カプセル化、カプセル化解除、インターフェイスに 1 つずつ）を使用します。つまり各ルータでは、絶対最大値の 1,000 mVRF がサポートされます。（MDT が設定されていない mVRF では 1 つの内部 VLAN が使用されるので、未使用 mVRF を削除して VLAN 割り当てを維持する必要があります）。

- MPLS VPN ネットワークに VRF のネットワークがすでに含まれている場合は、そのネットワークを削除したり再作成したりしなくても、mVRF トラフィックをサポートできます。その代わりに次の手順に示すように **mdt default** コマンドおよび **mdt data** コマンドを設定し、VRF 上でマルチキャスト トラフィックをイネーブルにしてください。
- 特定 VPN 接続をサポートする各 PE ルータでは、同一 mVRF を設定する必要があります。
- 特定 mVRF をサポートする各 PE ルータは、同じ **mdt default** コマンドで設定する必要があります。

mVPN with L3VPN over mGRE の制約事項

- 15.1(1) SY よりも前のリリースでは、mVPN with L3VPN over mGRE が設定されている場合、スーパーバイザ エンジンのポート、または CFC のあるスイッチング モジュールのポートには、IPv4 ルーティングを設定しないでください。（CSCtr05033）
- RP へのユニキャスト パスがスーパーバイザ エンジンのポートを使用しないことを確認してください。さらに VSS モードで、RP へのユニキャスト パスが CFC のあるスイッチング モジュールのポートを使用しないことを確認してください。（CSCts43614）
- GRE トンネルの宛先アドレスおよび送信元アドレスが mGRE トンネルと同じである場合、GRE トンネルはルートキャッシュが切り替えられます。
- フラグメンテーションが必要なパケットは、ルートキャッシュが切り替えられます。
- L3VPN プロファイルをいったん削除して後で戻す場合、**clear ip bgp** *neighbor_ip_address* **soft** コマンドを使用して、ボーダー ゲートウェイ プロトコル（BGP）をクリアする必要があります。
- mGRE トンネルが作成されると、ダミー トンネルも作成されます。
- BGP コンフィギュレーションのアップデート元で使用されるループバックまたは IP アドレスは、L3VPN プロファイルの送信元と同じである必要があります。
- mGRE は、ステートフル スイッチオーバー（SSO）には対応していません。ただし、mGRE と SSO の両方が共存します。
- ハードウェア内で、すべての GRE オプションがサポートされているわけではありません（GRE 拡張ヘッダーや GRE キーなど）。
- トンネル上では、複数の同一 VLAN（インターネット制御メッセージ プロトコル（ICMP）リダイレクト）のチェックはサポートされていません。
- トンネル上では、ユニキャスト リバース パス転送（uRPF）や BGP ポリシー アカウントなどの機能はサポートされていません。

mVPN について

- 「mVPN の概要」（P.49-4）
- 「マルチキャスト ルーティング、転送、マルチキャスト ドメイン」（P.49-4）
- 「Multicast Distribution Tree（MDT）」（P.49-4）
- 「Multicast Tunnel Interface」（P.49-7）
- 「mVPN の PE ルータ ルーティング テーブルのサポート」（P.49-8）
- 「Multicast Distributed Switching サポート」（P.49-9）
- 「ハードウェア処理の IPv4 マルチキャスト」（P.49-9）

- 「mVPN with L3VPN over mGRE について」（P.49-9）

mVPN の概要

mVPN は仮想化されたプロバイダー ネットワーク（たとえば、MPLS または mGRE トンネルなど）全体で IPv4 マルチキャスト トラフィックを伝送する標準機能です。mVPN は、VPN を介してワイヤ速度でマルチキャスト トラフィックを転送するのに、IPv4 マルチキャスト トラフィックに対する PFC ハードウェア サポートを使用します。mVPN では、レイヤ 3 IPv4 VPN 上における IPv4 マルチキャスト トラフィックのサポートが、既存の IPv4 ユニキャスト サポートに追加されます。

mVPN では、VPN ルーティング / 転送（VRF）インスタンスごとにマルチキャスト パケットのルーティングおよび転送が行われ、サービス プロバイダー バックボーンを横断して VPN トンネルでマルチキャスト パケットが送信されます。

mVPN は、フル メッシュのポイントツーポイント GRE トンネルの代替手段です。簡単に拡張できるソリューションではなく、カスタマーに提供される粒度に制限があります。

マルチキャスト ルーティング、転送、マルチキャスト ドメイン

mVPN では、VPN ルーティング / 転送テーブルにマルチキャスト ルーティング情報が追加されます。プロバイダー エッジ（PE）ルータがマルチキャスト データまたは制御パケットをカスタマー エッジ（CE）ルータから受信すると、マルチキャスト VRF（mVRF）の情報に従って転送が実行されます。

それぞれの mVRF では、特定 VRF インスタンスに必要となるルーティング情報および転送情報が維持されます。mVRF の作成と設定は既存 VRF と同じ方法で行われますが、それぞれの mVRF ではマルチキャスト ルーティングもイネーブルになります。

マルチキャスト ドメインは、MPLS ネットワークで相互にマルチキャスト トラフィックを送信できるホストのセットで構成されます。たとえば、特定タイプのマルチキャスト トラフィックをすべてのグローバルな従業員に送信するカスタマーのマルチキャスト ドメインは、そのエンタープライズと関連するすべての CE ルータから構成されます。

Multicast Distribution Tree（MDT）

mVPN 機能では、少なくとも 1 つの Multicast Distribution Tree（MDT）がマルチキャスト ドメインごとに確立されます。MDT では、さまざまな PE ルータに存在する同一 mVRF の相互接続に必要となる情報が提供されます。

mVPN では、次の 2 つの MDT タイプがサポートされます。

- デフォルト MDT：特定マルチキャスト ドメインのすべての PE ルータ間における PIM 制御メッセージおよび低帯域幅ストリームの永続チャネルです。デフォルト MDT におけるすべてのマルチキャスト トラフィックは、ドメインのその他すべての PE ルータに複製されます。各 PE ルータは、ドメインのその他すべての PE ルータから、論理的に PIM ネイバー（1 ホップ先）と見なされます。
- データ MDT：これはオプションです。イネーブルにするとダイナミックに作成され、フルモーション ビデオなど、すべての PE ルータに送信する必要がない高帯域幅送信用に最適なパスが提供されます。これにより、PE ルータ間において高帯域幅トラフィックのオンデマンド転送が可能になるので、作成されるすべての高帯域幅ストリームですべての PE ルータがフラッディングされなくなります。

データ MDT を作成するため、バックボーンにマルチキャスト ストリームを定期的に転送する各 PE ルータは、各デフォルト MDT で送信されるトラフィックを次のように定期的に検査します。

1. 各 PE ルータはマルチキャスト トラフィックを定期的にサンプル抽出して（ソフトウェア スイッチングの場合は約 10 秒ごと、ハードウェア スイッチングの場合は 90 秒ごと）、マルチキャスト ストリームが設定しきい値を超えているかどうかを判断します （ストリームのサンプル抽出タイミングにより、最悪の場合は、高帯域幅ストリームが検出されるまでに最大 180 秒かかることがあります）。

   （注） データ MDT は、VRF マルチキャスト ルーティング テーブル内で、（S,G）マルチキャスト ルート エントリ専用に作成されます。（*,G）エントリ用には作成されません。

2. 特定マルチキャスト ストリームが定義済みしきい値を超えた場合、送信側 PE ルータは、その特定マルチキャスト トラフィック用にデータ MDT をダイナミックに作成します。
3. 送信側 PE ルータは、その他の PE ルータに DATA-MDT JOIN 要求（ポート 3232 へのユーザ データグラム プロトコル（UDP）メッセージ）を送信し、新しいデータ MDT について通知します。
4. 受信側 PE ルータは VRF ルーティング テーブルを調べて、このデータ ストリームの受信に関係するカスタマーがいるかどうかを判断します。そのようなカスタマーがいる場合、受信側 PE ルータは PIM プロトコルを使用し、この特定データ MDT グループの PIM JOIN メッセージ（グローバル テーブル PIM インスタンス）を送信してストリームを受け入れます。このストリームのカスタマーがいないルータは、カスタマーがあとでそのストリームを要求したときのため、情報をキャッシュします。
5. 送信側 PE ルータは、DATA-MDT JOIN メッセージ送信の 3 秒後、高帯域幅マルチキャスト ストリームをデフォルト MDT から削除し、新しいデータ MDT で送信し始めます。
6. 送信側 PE ルータは、マルチキャスト ストリームが定義済みしきい値を超え続ける限り、60 秒ごとに DATA-MDT JOIN メッセージの送信を続けます。ストリームが 60 秒より長くしきい値を下回った場合、送信側 PE ルータは DATA-MDT JOIN メッセージの送信を停止し、ストリームをデフォルト MDT に戻します。
7. 受信側ルータは、3 分より長く DATA-MDT JOIN メッセージを受信しなかった場合、デフォルト MDT のキャッシュ情報と期限切れにします。

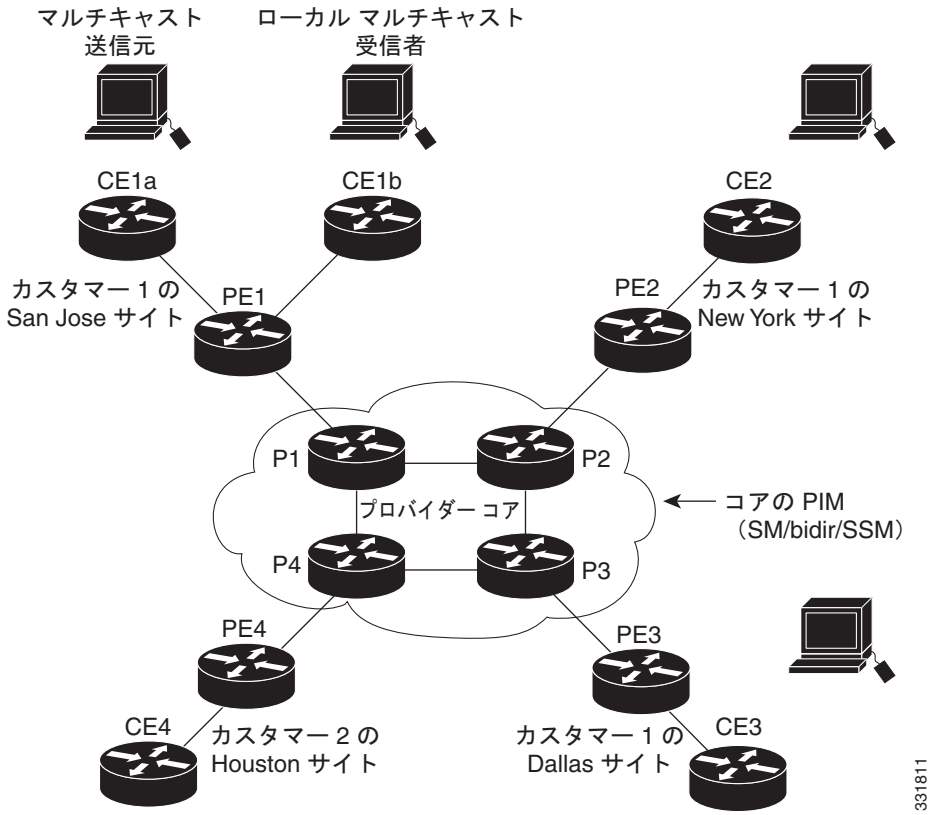
データ MDT では高帯域幅の送信元が VPN 内部で許可されますが、MPLS VPN コアでの最適トラフィック転送が確保されます。

次の例のサービス プロバイダーには、San Jose、New York、Dallas にオフィスがあるマルチキャスト カスタマーがいます。San Jose サイトは、単方向マルチキャスト プレゼンテーションを送信しています。サービス プロバイダー ネットワークでは、このカスタマーと関連する 3 つすべてのサイト、および別のエンタープライズ カスタマーの Houston サイトがサポートされます。

エンタープライズ カスタマーのデフォルト MDT は、プロバイダーのルータ P1、P2、P3、およびその関連 PE ルータから構成されています。PE4 は、MPLS コアのその他のルータに相互接続されていますが、別のカスタマーと関連しているので、デフォルト MDT の一部ではありません。

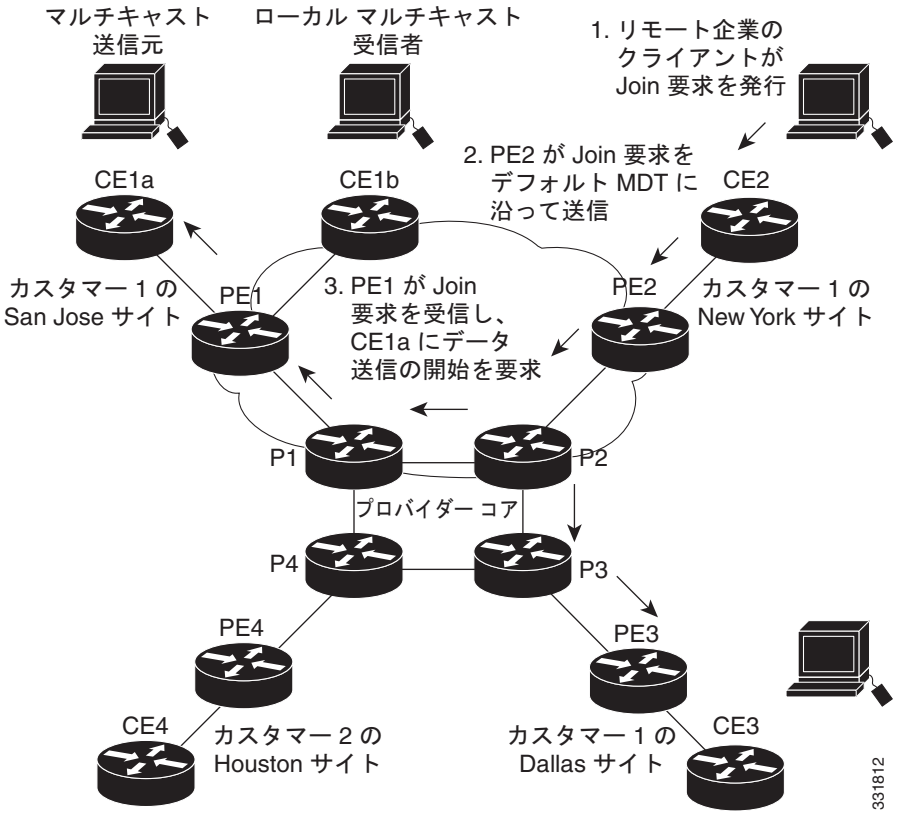
図 49-1 は、San Jose の外側でマルチキャスト ブロードキャストに加入するユーザがいない場合、つまりデフォルト MDT でデータが流れない場合のネットワークの状況を示しています。各 PE ルータはデフォルト MDT 上にあるその他の PE ルータとの PIM 関係を維持し、直接接続している PE ルータとの PIM 関係も維持します。

図 49-1　デフォルト マルチキャスト配信ツリーの概要



New York の従業員がマルチキャスト セッションに加入した場合、ニューヨーク サイトに関連する PE ルータは Join 要求を送信します。この Join 要求は、マルチキャスト ドメインのデフォルト MDT に流れます。マルチキャスト セッション送信元（PE1）と関連する PE ルータは、この要求を受信します。図 49-2 は、PE ルータが、マルチキャスト送信元（CE1a）と関連する CE ルータに要求を転送する方法を示しています。

図 49-2　データ MDT の初期化



CE ルータ（CE1a）は関連 PE ルータ（PE1）にマルチキャスト データを送信し始め、PE ルータは、マルチキャスト データが帯域幅しきい値を超えているためにデータ MDT を作成する必要があることを認識します。PE1 はデータ MDT を作成し、データ MDT に関する情報を含むデフォルト MDT を使用してすべてのルータにメッセージを送信します。

約 3 秒後、PE1 は、データ MDT を使用してその特定ストリームのマルチキャスト データを送信し始めます。この送信元に関係するレシーバは PE2 だけにいるので、PE2 だけがデータ MDT に加入してデータ MDT でトラフィックを受信します。

Multicast Tunnel Interface

PE ルータは、マルチキャスト ドメインのマルチキャスト VRF（mVRF）ごとに Multicast Tunnel Interface（MTI）を作成します。mVRF はトンネル インターフェイスを使用してマルチキャスト ドメインにアクセスし、mVRF とグローバル mVRF を接続するコンジットを提供します。

ルータの場合、MTI はクラス D マルチキャスト アドレスを含むトンネル インターフェイスです（**interface tunnel** コマンドで作成）。この mVRF 用にデフォルト MDT で設定したすべての PE ルータは論理ネットワークを作成し、この論理ネットワークでは、各 PE ルータが、マルチキャスト ドメインにあるその他すべての PE ルータの PIM ネイバー（1 ホップ先）として表示されます。この場合、各ルータ間の物理的な距離は関係ありません。

mVRF を設定すると、MTI は自動的に作成されます。BGP ピアリング アドレスは MTI インターフェイス送信元アドレスとして割り当てられ、PIM プロトコルは各 MTI で自動的にイネーブルになります。

ルータは、ネットワークのカスタマー側からマルチキャスト パケットを受信すると、着信インターフェイスの VRF を使用して、受信する mVRF を判断します。次にルータは、GRE カプセル化を使用してパケットをカプセル化します。ルータは、パケットをカプセル化するとき、送信元アドレスを BGP ピアリング インターフェイスの送信元アドレスに、デフォルト MDT のマルチキャスト アドレス、またはデータ MDT の送信元アドレス（設定されている場合）に宛先アドレスを設定します。次にルータは、適切な数の MTI インターフェイスで転送するために、必要に応じてパケットを複製します。

ルータは、MTI インターフェイスでパケットを受信すると、宛先アドレスを使用して適切なデフォルト MDT またはデータ MDT を識別し、適切な mVRF を識別します。次にパケットのカプセル化を解除し、必要なだけ複製して適切なインターフェイスに転送します。

（注）
- mVPN MTI は、Cisco ルータで一般的に使用されるその他のトンネル インターフェイスと異なり、ポイントツーポイント インターフェイスではなく、LAN インターフェイスとして分類されます。MTI インターフェイスは設定可能でありませんが、**show interface tunnel** コマンドを使用してそのステータスを表示できます。
- MTI インターフェイスは、VPN トンネル上のマルチキャスト トラフィックに排他的に使用されます。
- このトンネルは、ユニキャストでルーティングされたトラフィックを搬送しません。

mVPN の PE ルータ ルーティング テーブルのサポート

mVPN フィーチャをサポートする各 PE ルータは、次のルーティング テーブルを使用して、VPN トラフィックおよび mVPN トラフィックを正しくルーティングします。

- デフォルト ルーティング テーブル：すべての Cisco ルータで使用される標準ルーティング テーブル。このテーブルには、バックボーン トラフィック、および非 VPN ユニキャスト トラフィックとマルチキャスト トラフィック（総称ルーティング カプセル化（GRE）マルチキャスト トラフィックを含む）に必要なルートが含まれています。
- VPN ルーティング/転送（VRF）テーブル：VRF インスタンスごとに作成されるルーティング テーブル。プロバイダー ネットワークの VPN 間でユニキャスト トラフィックをルーティングします。
- マルチキャスト VRF（mVRF）テーブル：VRF インスタンスごとに作成されるマルチキャスト ルーティング テーブルおよびマルチキャスト ルーティング プロトコル インスタンス。ネットワークのマルチキャスト ドメインでマルチキャスト トラフィックをルーティングします。このテーブルには、マルチキャスト ドメインへのアクセスに使用される Multicast Tunnel Interface も含まれます。

Multicast Distributed Switching サポート

mVPN では、インターフェイス単位および VRF 単位でマルチキャストをサポートするため、Multicast Distributed Switching（MDS）がサポートされます。MDS を設定するときには、ループバック インターフェイスも含めたすべてのインターフェイスに **no ip mroute-cache** コマンドが設定されていないことを確認する必要があります。

ハードウェア処理の IPv4 マルチキャスト

Cisco IOS Release 15.1SY では、VPN トラフィック上の IPv4 マルチキャスト用にハードウェア アクセラレーションがサポートされ、RP CPU の使用率を上げずにワイヤ速度で適切な VPN にマルチキャスト トラフィックが転送されます。

カスタマー VRF では、PFC のハードウェア アクセラレーションは、PIM dense（デンス）、PIM スパース、PIM 双方向、PIM Source-Specific Multicast（SSM）モードのマルチキャスト トラフィックをサポートします。

サービス プロバイダー コアでは、PFC のハードウェア アクセラレーションは、PIM スパース、PIM 双方向、PIM SSM モードのマルチキャスト トラフィックをサポートします。サービス プロバイダー コアの場合は、PFC ハードウェア アクセラレーションは PIM dense モードでマルチキャスト トラフィックをサポートしません。

mVPN with L3VPN over mGRE について

- 「概要」（P.49-9）
- 「ルート マップ」（P.49-10）
- 「トンネル エンドポイントの検出およびフォワーディング」（P.49-10）
- 「トンネルの非カプセル化」（P.49-10）
- 「トンネルの送信元」（P.49-11）

（注）　詳細については、「mVPN with L3VPN over mGRE の設定」（P.49-23）を参照してください。

概要

リリース 15.0(1) SY1 以降では、Multicast Virtual Private Network with Layer 3 Virtual Private Network over multipoint Generic Routing Encapsulation (mVPN with L3VPN over mGRE) をサポートします。mVPN with L3VPN over mGRE は標準 IP 専用ネットワークによって接続されている各ネットワーク間で VPN 接続を提供します。mGRE トンネルは、IP ネットワークをオーバーレイし、PE デバイスを接続して、IP コア経由の L3 PE ベースの VPN サービスの展開をサポートする VPN に転送します。

（注）
- mGRE は、ポイントツーマルチポイント モデルなので、各 PE デバイスを相互接続するうえでフル メッシュ構造の GRE トンネルは不要です。
- マルチキャストおよびユニキャスト トラフィックは、個別のトンネル、マルチキャスト用に MDT、およびユニキャスト用に mGRE を使用します。

ルート マップ

デフォルトでは、VPN ユニキャスト トラフィックの送信に LSP が使用されます。mVPN with L3VPN over mGRE 機能では、ユーザ定義のルート マップが使用されて、mGRE トンネルを介して到達可能な VPN プレフィックスと、LSP を使用して到達可能な VPN プレフィックスが決定されます。ルート マップは、VPNv4 および VPNv6 アドレス ファミリのアドバタイズメントに適用されます。ルート マップでは、VPN トラフィックのカプセル化方式の決定に Next Hop Tunnel Table が使用されます。

mGRE トンネルを経由してルーティングされるトラフィックは、代替アドレス空間を使用します。したがって、mGRE トンネルでのトラフィックのカプセル化によって、すべてのネクスト ホップに到達します。mGRE トンネルを使用するように特定のルートを設定するには、ルート マップにそのルートに対するエントリの設定が必要です。その新しいエントリによって、代替アドレス空間に対して、そのルートのネットワーク層到着可能性情報（NLRI）が再マッピングされます。あるルートのルート マップ内に再マッピング エントリが存在しない場合、そのルート上のトラフィックは LSP を介して転送されます。

mVPN with L3VPN over mGRE 機能は、代替アドレス空間を自動的にプロビジョニングします。この空間は通常、トンネルカプセル化された仮想ルーティングおよび転送（VRF）インスタンスに保持されます。アドレス空間を介して到達可能なトラフィックが確実にすべて mGRE トンネル内でカプセル化されるように、トンネル外への単一のデフォルト ルートが自動的にインストールされます。また、ルート マップ上にデフォルト トンネルも自動的に作成されます。デフォルト ルート マップは、適切な BGP アップデートに添付できます。

トンネル エンドポイントの検出およびフォワーディング

mVPN with L3VPN over mGRE 機能は、ネットワーク内のリモート PE を検出できなければならず、リモート PE のトンネル フォワーディング情報を構築できる必要があります。リモート PE が無効となったことが検出され、その PE のトンネル フォワーディング情報が削除されるようにする必要もあります。

入力 PE によって BGP を介して VPN アドバタイズメントが受信される場合、その入力 PE によってルート ターゲット属性（VRF に入力されます）および、アドバタイズメントからの MPLS VPN ラベルが使用され、その結果、プレフィックスと適切なお客様が関連付けられます。入力されたルートのネクスト ホップが、アドバタイズメントの NLRI に設定されます。

アドバタイズされたプレフィックスには、システム内のリモート PE に関する情報が（NLRI の形式で）格納され、PE では、この情報が使用されて、NLRI がアクティブまたは非アクティブになったときシステムに通知されます。システムでは、この通知が使用されて、PE フォワーディング情報がアップデートされます。

この機能によって、新しいリモート PE の通知が受信されると、Tunnel Endpoint Database にその情報が追加され、トンネル インターフェイスに関連付けられた隣接が作成されます。この隣接の説明として、カプセル化に関する情報、およびカプセル化されたパケットを新しいリモート PE に送信するために必要なその他の処理に関する情報が記述されています。

この機能によって、トンネル カプセル化 VRF に隣接情報が示されます。VPN NLRI が VRF 内のルートに（ルート マップを使用して）再マッピングされると、隣接に対して NLRI がリンクされ、これによりトンネルに VPN がリンクされます。

トンネルの非カプセル化

出力 PE が mVPN with L3VPN over mGRE 機能を使用するトンネル インターフェイスからパケットを受信すると、PE は VPN ラベルのタグ付きパケットを作成するために、パケットのカプセル化を解除し、パケットを転送します。

トンネルの送信元

mVPN with L3VPN over mGRE 機能では、大量のエンドポイント（リモート PE）を持つシステムの設定に、mGRE トンネルとして設定された単一のトンネルが使用されます。トンネルカプセル化パケットの送信元を特定するために、システムによってトンネル送信元情報が使用されます。

送信（入力）PE では、VPN パケットがトンネルに送信されるときのトンネル宛先は NLRI です。受信（出力）PE では、トンネル送信元は、mGRE トンネルでカプセル化されたパケットが受信されるアドレスです。そのため、出力 PE では、パケットの宛先がローカル PE からの NLRI と一致している必要があります。

mVPN のデフォルト設定

なし。

mVPN の設定方法

- 「Multicast VPN ルーティング / 転送インスタンスの設定」（P.49-11）
- 「マルチキャスト VRF ルーティングの設定」（P.49-17）
- 「mVPN をサポートするマルチキャスト ルーティング用インターフェイスの設定」（P.49-20）
- 「mVPN with L3VPN over mGRE の設定」（P.49-23）

（注）　この設定タスクでは、マルチキャスト トラフィックを送受信するすべてのルータで BGP がすでに設定されていて動作していることを想定しています。BGP 拡張コミュニティをイネーブルにしないと（**neighbor send-community both** コマンドまたは **neighbor send-community extended** コマンドを使用）、ネットワークにおける MDT の使用がサポートされません。

Multicast VPN ルーティング / 転送インスタンスの設定

- 「VRF エントリの設定」（P.49-12）
- 「ルート識別子の設定」（P.49-12）
- 「ルートターゲット拡張コミュニティの設定」（P.49-12）
- 「デフォルト MDT の設定」（P.49-13）
- 「データ MDT の設定（任意）」（P.49-14）
- 「データ MDT ロギングのイネーブル化」（P.49-14）
- 「設定例」（P.49-15）
- 「VRF 情報の表示」（P.49-15）

VRF エントリの設定

VRF エントリを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# configure terminal`	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`	VRF ルーティング テーブル エントリおよび Cisco Express Forwarding（CEF; シスコ エクスプレス フォワーディング）テーブル エントリを設定し、VRF コンフィギュレーション モードを開始します。
ステップ 3	`Router(config-vrf)# do show ip vrf vrf_name`	設定を確認します。

次に、blue という名前の VRF を設定し、設定を確認する例を示します。

```
Router# configure terminal
Router(config)# ip vrf blue
Router(config-vrf)# do show ip vrf blue
Name                              Default RD          Interfaces
  blue                              <not set>
```

ルート識別子の設定

ルート識別子を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config-vrf)# rd route_distinguisher`	VPN IPv4 プレフィックスのルート識別子を指定します。
ステップ 2	`Router(config-vrf)# do show ip vrf vrf_name`	設定を確認します。

ルート識別子の設定時には、次のうちいずれかの形式でルート識別子を入力してください。

- 16 ビット AS 番号：32 ビット番号（101:3）
- 32 ビット IPv4 アドレス：16 ビット番号（192.168.122.15:1）

次に、ルート識別子として 55:1111 を設定し、設定を確認する例を示します。

```
Router(config-vrf)# rd 55:1111
Router(config-vrf)# do show ip vrf blue
Name                              Default RD          Interfaces
blue                              55:1111
```

ルートターゲット拡張コミュニティの設定

ルートターゲット拡張コミュニティを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config-vrf)# route-target [import | export | both] route_target_ext_community`	ルートターゲット拡張コミュニティを VRF 用に設定します。
ステップ 2	`Router(config-vrf)# do show ip vrf detail`	設定を確認します。

ルートターゲット拡張コミュニティの設定時には、次に注意してください。

- **import**：ターゲット VPN 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。
- **export**：ターゲット VPN 拡張コミュニティにルーティング情報をエクスポートします。
- **both**：インポートおよびエクスポートを行います。
- *route_target_ext_community*：48 ビット ルートターゲット拡張コミュニティを VRF に追加します。以下のいずれかの形式で番号を入力します。
  - 16 ビット AS 番号：32 ビット番号（101:3）
  - 32 ビット IPv4 アドレス：16 ビット番号（192.168.122.15:1）

次に、インポートおよびエクスポートのルートターゲット拡張コミュニティとして 55:1111 を設定し、設定を確認する例を示します。

```
Router(config-vrf)# route-target both 55:1111
Router(config-vrf)# do show ip vrf detail
VRF blue; default RD 55:1111; default VPNID <not set>
VRF Table ID = 1
  No interfaces
  Connected addresses are not in global routing table
  Export VPN route-target communities
    RT:55:1111
  Import VPN route-target communities
    RT:55:1111
  No import route-map
  No export route-map
CSC is not configured.
```

デフォルト MDT の設定

デフォルト MDT を設定するには、次の作業を行います。

コマンド	目的
`Router(config-vrf)# mdt default group_address`	デフォルト MDT を設定します。

デフォルト MDT を設定する際、次の情報に注意してください。

- *group_address* は、デフォルト MDT グループのマルチキャスト IPv4 アドレスです。このアドレスは mVRF コミュニティの識別子として動作します。この同一グループ アドレスで設定したすべてのプロバイダー エッジ（PE）ルータはグループのメンバになり、メンバは、グループの他のメンバが送信した PIM 制御メッセージおよびマルチキャスト トラフィックを受信します。
- これと同じデフォルト MDT を各 PE ルータで設定しないと、PE ルータは、この特定 mVRF のマルチキャスト トラフィックを受信できません。

次に、デフォルト MDT として 239.1.1.1 を設定する例を示します。

```
Router(config-vrf)# mdt default 239.1.1.1
```

データ MDT の設定（任意）

任意のデータ MDT を設定するには、次の作業を行います。

コマンド	目的
Router(config-vrf)# **mdt data** *group_address wildcard_bits* [**threshold** *threshold_value*] [**list** *access_list*]	（任意）マルチキャスト アドレスの指定範囲にデータ MDT を設定します。

任意のデータ MDT の設定時には、次に注意してください。

- *group_address1*：マルチキャスト グループ アドレス。アドレスは 224.0.0.1 ～ 239.255.255.255 の範囲にすることができますが、デフォルト MDT に割り当てたアドレスと重複させることはできません。
- *wildcard_bits*：可能なアドレス範囲を作成するために、マルチキャスト グループ アドレスに適用されるワイルドカード ビット マスク。これにより、各 mVRF がサポートできるデータ MDT の最大数を制限できます。
- **threshold** *threshold_value*：（任意）しきい値をキロビット単位で定義します。このしきい値を超えると、マルチキャスト トラフィックはデフォルト MDT からデータ MDT に切り替わります。*threshold_value* パラメータの範囲は 1 ～ 4294967 キロビットです。
- **list** *access_list*：（任意）このトラフィックに適用するアクセス リスト名または番号を指定します。

次に、データ MDT を設定する例を示します。

```
Router(config-vrf)# mdt data 239.1.2.0 0.0.0.3 threshold 10
```

データ MDT ロギングのイネーブル化

データ MDT ロギングをイネーブルにするには、次の作業を行います。

コマンド	目的
Router(config-vrf)# **mdt log-reuse**	（任意）データ MDT が再利用されるたびに Syslog メッセージを生成することで、データ MDT 再利用情報の記録をイネーブルにします。データ MDT が頻繁に再利用される場合は、**mdt data** コマンドで使用されるワイルドカード ビット マスクのサイズを増やして、データ MDT の許可数を増やす必要があります。

次に、データ MDT ロギングをイネーブルにする例を示します。

```
Router(config-vrf)# mdt log-reuse
```

設定例

次のコンフィギュレーション ファイルからの抜粋は、VRF の範囲の典型的な VRF 設定を示しています。表示を簡素にするため、先頭の VRF および末尾の VRF だけを示します。

```
!
ip vrf mvpn-cus1
 rd 200:1
 route-target export 200:1
 route-target import 200:1
 mdt default 239.1.1.1
!
ip vrf mvpn-cus2
 rd 200:2
 route-target export 200:2
 route-target import 200:2
 mdt default 239.1.1.2
!
ip vrf mvpn-cus3
 rd 200:3
 route-target export 200:3
 route-target import 200:3
 mdt default 239.1.1.3
!
...

ip vrf mvpn-cus249
 rd 200:249
 route-target export 200:249
 route-target import 200:249
 mdt default 239.1.1.249
 mdt data 239.1.1.128 0.0.0.7
```

VRF 情報の表示

スイッチで設定されているすべての VRF を表示するには、**show ip vrf** コマンドを使用します。

```
Router# show ip vrf

  Name                              Default RD          Interfaces
  green                             1:52                GigabitEthernet6/1
  red                               200:1               GigabitEthernet1/1
                                                        GigabitEthernet3/16
                                                        Loopback2

Router#
```

すべての mVRF 用に現在設定されている MDT に関する情報を表示するには、**show ip pim mdt** コマンドを使用します。次に、このコマンドの典型的な出力例を示します。

```
Router# show ip pim mdt

  MDT Group       Interface   Source                  VRF
* 227.1.0.1       Tunnel1     Loopback0               BIDIR01
* 227.2.0.1       Tunnel2     Loopback0               BIDIR02
* 228.1.0.1       Tunnel3     Loopback0               SPARSE01
* 228.2.0.1       Tunnel4     Loopback0               SPARSE02
```

（注）　特定トンネル インターフェイスに関する情報を表示するには、**show interface tunnel** コマンドを使用します。トンネル インターフェイスの IPv4 アドレスは、mVRF のデフォルト MDT のマルチキャスト グループ アドレスです。

特定 VRF のルーティング情報を表示するには、**show ip route vrf** コマンドを使用します。

```
Router# show ip route vrf red

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

Gateway of last resort is not set

     2.0.0.0/32 is subnetted, 1 subnets
C       2.2.2.2 is directly connected, Loopback2
     3.0.0.0/32 is subnetted, 1 subnets
B       3.3.3.3 [200/0] via 3.1.1.3, 00:20:09
C    21.0.0.0/8 is directly connected, GigabitEthernet3/16
B    22.0.0.0/8 [200/0] via 3.1.1.3, 00:20:09

Router#
```

特定 mVRF のマルチキャスト ルーティング テーブルおよびトンネル インターフェイスに関する情報を表示するには、**show ip mroute vrf** コマンドを使用します。次に、BIDIR01 という名前の mVRF の典型的な出力例を示します。

```
Router# show ip mroute vrf BIDIR01

IP Multicast Routing Table
Flags: 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
(*, 228.1.0.1), 00:16:25/stopped, RP 10.10.10.12, flags: SJCF
  Incoming interface: Tunnel1, RPF nbr 10.10.10.12, Partial-SC
  Outgoing interface list:
    GigabitEthernet3/1.3001, Forward/Sparse-Dense, 00:16:25/00:02:49, H
(6.9.0.100, 228.1.0.1), 00:14:13/00:03:29, flags: FT
  Incoming interface: GigabitEthernet3/1.3001, RPF nbr 0.0.0.0, RPF-MFD
  Outgoing interface list:
    Tunnel1, Forward/Sparse-Dense, 00:14:13/00:02:46, H

Router#
```

（注）　この例では、**show ip mroute vrf** コマンドによって、VRF が使用している MDT Tunnel Interface（MTI）が Tunnel1 であることが示されます。

マルチキャスト VRF ルーティングの設定

- 「IPv4 マルチキャスト ルーティングのグローバルなイネーブル化」（P.49-17）
- 「IPv4 マルチキャスト VRF ルーティングのイネーブル化」（P.49-17）
- 「PIM VRF RP アドレスの指定」（P.49-18）
- 「PIM VRF 登録メッセージ送信元アドレスの設定（任意）」（P.49-18）
- 「MSDP ピアの設定（任意）」（P.49-18）
- 「マルチキャスト ルートの最大数の設定（任意）」（P.49-19）
- 「設定例」（P.49-20）
- 「IPv4 マルチキャスト VRF ルーティング情報の表示」（P.49-20）

（注）　マルチキャスト トラフィックの送受信を行うすべてのルータでは、BGP を設定して動作させる必要があります。BGP 拡張コミュニティをイネーブルにしないと（**neighbor send-community both** コマンドまたは **neighbor send-community extended** コマンドを使用）、ネットワークにおける MDT の使用がサポートされません。

IPv4 マルチキャスト ルーティングのグローバルなイネーブル化

IPv4 マルチキャスト ルーティングをグローバルにイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# configure terminal`	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 multicast-routing`	IPv4 マルチキャスト ルーティングをグローバルにイネーブルにします。

次に、IPv4 マルチキャスト ルーティングをグローバルにイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# ip multicast-routing
```

IPv4 マルチキャスト VRF ルーティングのイネーブル化

IPv4 マルチキャスト VRF ルーティングをイネーブルにするには、次の作業を行います。

コマンド	目的
`Router(config)# ip multicast-routing vrf` *vrf_name* `[distributed]`	IPv4 マルチキャスト VRF ルーティングをイネーブルにします。

IPv4 マルチキャスト VRF ルーティングをイネーブルにするときは、次の情報に注意してください。

- *vrf_name*：マルチキャスト ルーティングの特定 VRF を指定します。*vrf_name* は、「Multicast VPN ルーティング/転送インスタンスの設定」（P.49-11）で示しているように、前に作成された VRF を参照するようにします。
- **distributed**：（任意）Multicast Distributed Switching（MDS）をイネーブルにします。

次に、IPv4 マルチキャスト VRF ルーティングをイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# ip multicast-routing vrf blue
```

PIM VRF RP アドレスの指定

PIM VRF ランデブー ポイント（RP）を指定するには、次の作業を行います。

コマンド	目的
Router(config)# **ip pim vrf** *vrf_name* **rp-address** *rp_address* [*access_list*] [**override**] [**bidir**]	PIM RP IPv4 アドレスを指定します（sparse PIM ネットワークの場合必須）。

PIM VRF RP アドレスの指定時には、次の情報に注意してください。

- **vrf** *vrf_name*：（任意）使用する特定 VRF インスタンスを指定します。
- *rp_address*：PIM RP ルータのユニキャスト IP アドレス。
- *access_list*：（任意）RP のマルチキャスト グループを定義するアクセス リストの番号または名前。
- **override**：（任意）RP アドレスが競合する場合は、この特定 RP により、Auto-RP で学習した RP を上書きします。
- **bidir**：（任意）*access_list* 引数で指定したマルチキャスト グループが双方向モードで動作することを指定します。このオプションを指定しない場合、グループは PIM sparse モードで動作します。
- できるだけ双方向モードを使用してください。スケーラビリティがより適切になります。

次に、PIM VRF RP アドレスを指定する例を示します。

```
Router(config)# ip pim vrf blue rp-address 198.196.100.33
```

PIM VRF 登録メッセージ送信元アドレスの設定（任意）

PIM VRF 登録メッセージ送信元アドレスを設定するには、次の作業を行います。

コマンド	目的
Router(config)# **ip pim vrf** *vrf_name* **register-source** *interface_type interface_number*	（任意）PIM VRF 登録メッセージ送信元アドレスを設定します。登録メッセージの送信元としてループバック インターフェイスを設定できます。

次に、PIM VRF 登録メッセージ送信元アドレスを設定する例を示します。

```
Router(config)# ip pim vrf blue register-source loopback 3
```

MSDP ピアの設定（任意）

Multicast Source Discovery Protocol（MSDP）ピアを設定するには、次の作業を行います。

コマンド	目的
Router(config)# **ip msdp vrf** *vrf_name* **peer** {*peer_name* | *peer_address*} [**connect-source** *interface_type interface_number*] [**remote-as** *ASN*]	（任意）MSDP ピアを設定します。

MSDP ピアの設定時には、次の情報に注意してください。

- **vrf** *vrf_name*：使用する特定 VRF インスタンスを指定します。
- {*peer_name* | *peer_address*}：MSDP ピア ルータのドメイン ネーム システム（DNS）名または IP アドレス。
- **connect-source** *interface_type interface_number*：プライマリ アドレスが TCP 接続の送信元 IP アドレスとして使用されるインターフェイスのインターフェイス名および番号。
- **remote-as** *ASN*：（任意）MSDP ピアの自律システム番号。これは表示専用です。

次に、MSDP ピアを設定する例を示します。

```
Router(config)# ip msdp peer router.cisco.com connect-source gigabitethernet 1/1 remote-as
109
```

マルチキャスト ルートの最大数の設定（任意）

マルチキャスト ルートの最大数を設定するには、次の作業を行います。

コマンド	目的
`Router(config)# ip multicast vrf vrf_name route-limit limit [threshold]`	（任意）マルチキャスト トラフィックに追加できるマルチキャスト ルートの最大数を設定します。

ルートの最大数の設定時には、次の情報に注意してください。

- **vrf** *vrf_name*：指定した VRF のルート制限をイネーブルにします。
- *limit*：追加できるマルチキャスト ルートの数。範囲は 1 ～ 2147483647 であり、デフォルトは 2147483647 です。
- *threshold*：（任意）警告メッセージが発生する前に追加できるマルチキャスト ルートの数。有効範囲は、1 から *limit* パラメータの値までです。

次に、マルチキャスト ルートの最大数を設定する例を示します。

```
Router(config)# ip multicast vrf blue route-limit 200000 20000
```

IPv4 マルチキャスト ルート フィルタリングの設定（任意）

IPv4 マルチキャスト ルート フィルタリングを設定するには、次の作業を行います。

コマンド	目的
`Router(config)# ip multicast mrinfo-filter access_list`	（任意）アクセス リストで IPv4 マルチキャスト ルート フィルタリングを設定します。*access_list* パラメータは、アクセス リストの名前または番号にすることができます。

次に、IPv4 マルチキャスト ルート フィルタリングを設定する例を示します。

```
Router(config)# ip multicast mrinfo-filter 101
```

設定例

次のコンフィギュレーション ファイルからの抜粋は、VRF の範囲でマルチキャスト ルーティングをサポートするために必要となる最低限の設定を示しています。表示を簡素にするため、先頭の VRF および末尾の VRF だけを示します。

```
!
ip multicast-routing
ip multicast-routing vrf lite
ip multicast-routing vrf vpn201
ip multicast-routing vrf vpn202

...

ip multicast-routing vrf vpn249
ip multicast-routing vrf vpn250


...

ip pim rp-address 192.0.1.1
ip pim vrf lite rp-address 104.1.1.2
ip pim vrf vpn201 rp-address 192.200.1.1
ip pim vrf vpn202 rp-address 192.200.2.1

...

ip pim vrf vpn249 rp-address 192.200.49.6
ip pim vrf vpn250 rp-address 192.200.50.6
...
```

IPv4 マルチキャスト VRF ルーティング情報の表示

特定 mVRF の既知の PIM ネイバーを表示するには、**show ip pim vrf neighbor** コマンドを使用します。

```
Router# show ip pim vrf 98 neighbor

PIM Neighbor Table
Neighbor          Interface                Uptime/Expires    Ver   DR
Address                                                            Prio/Mode
40.60.0.11        Tunnel96                 00:00:31/00:01:13 v2    1 / S
40.50.0.11        Tunnel96                 00:00:54/00:00:50 v2    1 / S

Router#
```

mVPN をサポートするマルチキャスト ルーティング用インターフェイスの設定

- 「マルチキャスト ルーティング設定の概要」（P.49-21）
- 「インターフェイスでの PIM の設定」（P.49-21）
- 「IPv4 VRF 転送用インターフェイスの設定」（P.49-22）
- 「設定例」（P.49-22）

マルチキャスト ルーティング設定の概要

IPv4 マルチキャスト トラフィック用に使用されているすべてのインターフェイスでは、Protocol Independent Multicast（PIM）を設定する必要があります。VPN マルチキャスト環境では、最低でも次のインターフェイスのすべてで PIM をイネーブルにする必要があります。

- バックボーンに接続されているプロバイダー エッジ（PE）ルータの物理インターフェイス
- BGP ピアリングに使用されているループバック インターフェイス
- sparse PIM ランデブー ポイント（RP）ルータ アドレスの送信元として使用されているループバック インターフェイス

マルチキャスト トラフィックを転送する予定のインターフェイスと mVRF を関連付ける必要もあります。

マルチキャスト トラフィックの送受信を行うすべてのルータでは、BGP を設定して動作させる必要があります。BGP 拡張コミュニティをイネーブルにしないと（**neighbor send-community both** コマンドまたは **neighbor send-community extended** コマンドを使用）、ネットワークにおける MDT の使用がサポートされません。

インターフェイスでの PIM の設定

インターフェイスで PIM を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router# configure terminal`	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)# interface type {slot/port | number}`	指定したインターフェイスに対してインターフェイス コンフィギュレーション モードを開始します。
ステップ 3	`Router(config-if)# ip pim {dense-mode | sparse-mode | sparse-dense-mode}`	インターフェイスで PIM をイネーブルにします。

インターフェイスでの PIM の設定時には、次の情報に注意してください。

- 次のうちいずれかのインターフェイス タイプを使用できます。
  - バックボーンに接続されているプロバイダー エッジ（PE）ルータの物理インターフェイス
  - BGP ピアリングに使用されているループバック インターフェイス
  - スパース PIM ネットワーク RP アドレスの送信元として使用されるループバック インターフェイス
- PIM モードは次のとおりです。
  - **dense-mode**：動作の dense モードをイネーブルにします。
  - **sparse-mode**：動作の sparse モードをイネーブルにします。
  - **sparse-dense-mode**：マルチキャスト グループで RP ルータが定義されている場合は sparse モード、RP ルータが定義されていない場合は dense モードをイネーブルにします。
- バックボーンに接続されているすべての PE ルータの物理インターフェイス、および BGP ピアリングに使用されるか RP アドレス指定の送信元として使用されるすべてのループバック インターフェイスには、**sparse-mode** を使用してください。

次に、物理インターフェイス上で PIM sparse モードを設定する例を示します。

```
Router# configure terminal
Router(config)# interface gigabitethernet 10/1
Router(config-if)# ip pim sparse-mode
```

次に、ループバック インターフェイス上で PIM sparse モードを設定する例を示します。

```
Router# configure terminal
Router(config)# interface loopback 2
Router(config-if)# ip pim sparse-mode
```

IPv4 VRF 転送用インターフェイスの設定

IPv4 VRF 転送用インターフェイスを設定するには、次の作業を行います。

コマンド	目的
`Router(config-if)# ip vrf forwarding vrf_name`	（任意）指定した VRF ルーティング テーブルおよび転送テーブルをインターフェイスと関連付けます。指定しない場合、インターフェイスのデフォルトはグローバル ルーティング テーブルの使用になります。 **（注）** インターフェイスでこのコマンドを入力すると、IP アドレスが削除されるので、IP アドレスを再設定してください。

次に、VRF blue 転送用インターフェイスを設定する例を示します。

```
Router(config-if)# ip vrf forwarding blue
```

設定例

次のコンフィギュレーション ファイルからの抜粋は、単一 mVRF 上でマルチキャスト トラフィックをイネーブルにするインターフェイス設定、および関連 mVRF 設定を示しています。

```
ip multicast-routing vrf blue
ip multicast-routing

ip vrf blue
 rd 100:27
 route-target export 100:27
 route-target import 100:27
 mdt default 239.192.10.2

interface GigabitEthernet1/1
 description blue connection
 ip vrf forwarding blue
 ip address 192.168.2.26 255.255.255.0
 ip pim sparse-mode

interface GigabitEthernet1/15
 description Backbone connection
 ip address 10.8.4.2 255.255.255.0
 ip pim sparse-mode

ip pim vrf blue rp-address 192.7.25.1
ip pim rp-address 10.1.1.1
```

mVPN with L3VPN over mGRE の設定

- 「L3VPN カプセル化プロファイルの設定」（P.49-23）（必須）
- 「BGP およびルート マップの設定」（P.49-24）（必須）

（注）　詳細については、「mVPN with L3VPN over mGRE について」（P.49-9）を参照してください。

L3VPN カプセル化プロファイルの設定

（注）　この設定では、IPv6、MPLS、IP、およびレイヤ 2 トンネル プロトコル バージョン 3（L2TPv3）のような転送プロトコルも使用できます。

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	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 3	**l3vpn encapsulation ip** *profile-name* **例：** `Router(config)# l3vpn encapsulation ip tunnel encap`	L3 VPN カプセル化コンフィギュレーション モードを開始し、トンネルを作成します。
ステップ 4	**transport ipv4 [source** *interface-type interface-number***]** **例：** `Router(config-l3vpn-encap-ip)# transport ipv4 source loopback 0`	（任意）IPv4 送信元モードを指定して、送信元インターフェイスを定義します。 • **transport ipv4 source** *interface-type interface-number* コマンドを使用する場合、指定した送信元アドレスが、PE によってアドバタイズされた BGP アップデートにおけるネクスト ホップとして使用されていることを確認します。 • このコマンドを使用しない場合、**bgp update source** または **bgp next-hop** コマンドが、トンネル送信元として自動的に使用されます。
ステップ 5	**protocol gre [key** *gre-key***]** **例：** `Router(config-l3vpn-encap-ip)# protocol gre key 1234`	GRE をトンネル モードとして指定し、GRE キーを設定します。

	コマンドまたはアクション	目的
ステップ 6	**end** **例：** `Router(config-l3vpn-encap-ip)# end`	L3 VPN カプセル化コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 7	**show l3vpn encapsulation ip** *profile-name* **例：** `Router# show l3vpn encapsulation ip tunnel encap`	（任意）プロファイルの状態および基本となるトンネル インターフェイスを表示します。

BGP およびルート マップの設定

BGP およびルート マップを設定するには、次の作業を実行します。次の手順では、ルート マップをアプリケーション テンプレートにリンクし、アップデートがルート マップを介してフィルタ処理されるように BGP VPNv4 と VPNv6 の交換を設定することも可能です。

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	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 3	**router bgp** *as-number* **例：** `Router(config)# router bgp 100`	他の BGP ルータに接続されたルータを特定する自律システムの番号を指定し、転送されるルーティング情報にタグ付けし、ルータ コンフィギュレーション モードを開始します。
ステップ 4	**bgp log-neighbor-changes** **例：** `Router(config-router)# bgp log-neighbor-changes`	BGP ネイバー リセットのロギングをイネーブルにします。
ステップ 5	**neighbor** *ip-address* **remote-as** *as-number* **例：** `Router(config-router)# neighbor 209.165.200.225 remote-as 100`	BGP ネイバー テーブルまたはマルチプロトコル BGP ネイバー テーブルにエントリを追加します。
ステップ 6	**neighbor** *ip-address* **update-source** *interface name* **例：** `Router(config-router)# neighbor 209.165.200.225 update-source loopback 0`	BGP セッションが、TCP 接続の動作インターフェイスを使用できるようにします。

	コマンドまたはアクション	目的
ステップ 7	**address-family ipv4** **例：** `Router(config-router)# address-family ipv4`	アドレス ファミリ コンフィギュレーション モードを開始し、IPv4 アドレス プレフィックスを使用するルーティング セッションを設定します。
ステップ 8	**no synchronization** **例：** `Router(config-router-af)# no synchronization`	IGP を待たずにネットワーク ルートをアドバタイズするよう、Cisco IOS ソフトウェアをイネーブルにします。
ステップ 9	**redistribute connected** **例：** `Router(config-router-af)# redistribute connected`	1 つのルーティング ドメインから別のルーティング ドメインにルートを再配布し、送信元プロトコルによって認識されたルート、および、送信元プロトコルが実行されているインターフェイスを介して接続されているプレフィックスを、ターゲット プロトコルで再配布できるようにします。
ステップ 10	**neighbor** *ip-address* **activate** **例：** `Router(config-router-af)# neighbor 209.165.200.225 activate`	BGP ネイバーとの情報交換をイネーブルにします。
ステップ 11	**no auto-summary** **例：** `Router(config-router-af)# no auto-summary`	自動サマライズをディセーブルにし、サブプレフィックス ルーティング情報をクラスフル ネットワーク境界間で送信します。
ステップ 12	**exit** **例：** `Router(config-router-af)# exit`	アドレス ファミリ コンフィギュレーション モードを終了します。
ステップ 13	**address-family vpnv4** **例：** `Router(config-router)# address-family vpnv4`	アドレス ファミリ コンフィギュレーション モードを開始して、標準 VPNv4 アドレス プレフィックスを使用する、BGP などのルーティング セッションを設定します。
ステップ 14	**neighbor** *ip-address* **activate** **例：** `Router(config-router-af)# neighbor 209.165.200.225 activate`	BGP ネイバーとの情報交換をイネーブルにします。
ステップ 15	**neighbor** *ip-address* **send-community both** **例：** `Router(config-router-af)# neighbor 209.165.200.225 send-community both`	標準コミュニティと拡張コミュニティの両方のコミュニティ属性が、BGP ネイバーに送信されるように指定します。
ステップ 16	**neighbor** *ip-address* **route-map** *map-name* **in** **例：** `Router(config-router-af)# neighbor 209.165.200.225 route-map SELECT_UPDATE_FOR_L3VPN in`	名前付きルート マップを受信ルートに適用します。

	コマンドまたはアクション	目的
ステップ 17	**exit** **例：** `Router(config-router-af)# exit`	アドレス ファミリ コンフィギュレーション モードを終了します。
ステップ 18	**address-family vpnv6** **例：** `Router(config-router)# address-family vpnv6`	アドレス ファミリ コンフィギュレーション モードを開始して、VPNv6 アドレス プレフィックスを使用する、BGP などのルーティング セッションを設定します。
ステップ 19	**neighbor** *ip-address* **activate** **例：** `Router(config-router-af)# neighbor 209.165.200.252 activate`	BGP ネイバーとの情報交換をイネーブルにします。
ステップ 20	**neighbor** *ip-address* **send-community both** **例：** `Router(config-router-af)# neighbor 209.165.200.252 send-community both`	標準コミュニティと拡張コミュニティの両方のコミュニティ属性が、BGP ネイバーに送信されるように指定します。
ステップ 21	**neighbor** *ip-address* **route-map** *map-name* **in** **例：** `Router(config-router-af)# neighbor 209.165.200.252 route-map SELECT_UPDATE_FOR_L3VPN in`	名前付きルート マップを受信ルートに適用します。
ステップ 22	**exit** **例：** `Router(config-router-af)# exit`	アドレス ファミリ コンフィギュレーション モードを終了します。
ステップ 23	**route-map** *map-tag* **permit** *position* **例：** `Router(config-router)# route-map SELECT_UPDATE_FOR_L3VPN permit 10`	ルート マップ コンフィギュレーション モードを開始し、1 つのルーティング プロトコルから別のルーティング プロトコルへルートを再配布する条件を定義します。 • **redistribute** ルータ コンフィギュレーション コマンドによって、指定されたマップ タグが使用され、このルート マップが参照されます。複数のルート マップで同じマップ タグ名を共有できます。 • このルート マップの一致基準が満たされている場合は、set アクションの制御に従ってルートが再配布されます。 • 一致基準が満たされないと、同じマップ タグを持つ次のルート マップが検査されます。あるルートが、同じ名前を共有するルート マップ セットの一致基準のいずれをも満たさない場合、そのセットによる再配布は行われません。 • *position* 引数は、同じ名前で設定済みのルート マップのリストに新しいルート マップが入る位置を示します。

	コマンドまたはアクション	目的
ステップ 24	**set ip next-hop encapsulate l3vpn** *profile-name* **例：** `Router(config-route-map)# set ip next-hop encapsulate l3vpn my profile`	ルート マップの match 句を渡す出力 IPv4 パケットは、トンネルのカプセル化のため、VRF に送信されます。
ステップ 25	**set ipv6 next-hop encapsulate l3vpn** *profile-name* **例：** `Router(config-route-map)# set ip next-hop encapsulate l3vpn tunnel encap`	ルート マップの match 句を渡す出力 IPv6 パケットは、トンネルのカプセル化のため、VRF に送信されます。
ステップ 26	**exit** **例：** `Router(config-route-map)# exit`	ルート マップ コンフィギュレーション モードを終了し、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 27	**exit** **例：** `Router(config)# exit`	グローバル コンフィギュレーション モードを終了します。

mVPN の設定例

- 「デフォルト MDT だけの mVPN 設定」（P.49-27）
- 「デフォルト MDT およびデータ MDT を含む mVPN 設定」（P.49-29）
- 「mVPN with L3VPN over mGRE 設定の確認」（P.49-33）
- 「mVPN with L3VPN over mGRE の設定シーケンス」（P.49-33）

デフォルト MDT だけの mVPN 設定

次のコンフィギュレーション ファイルからの抜粋は、3 つの mVRF の mVPN 設定に関連する行を示しています。（必須 BGP 設定は表示されていません）。

```
!
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
service compress-config
!
hostname MVPN Router
!
boot system flash slot0:
logging snmp-authfail
!
ip subnet-zero
!
no ip domain-lookup
ip host tftp 223.255.254.238
!
ip vrf mvpn-cus1
```

```
 rd 200:1
 route-target export 200:1
 route-target import 200:1
 mdt default 239.1.1.1
!
ip vrf mvpn-cus2
 rd 200:2
 route-target export 200:2
 route-target import 200:2
 mdt default 239.1.1.2
!
ip vrf mvpn-cus3
 rd 200:3
 route-target export 200:3
 route-target import 200:3
 mdt default 239.1.1.3
!
ip multicast-routing
ip multicast-routing vrf mvpn-cus1
ip multicast-routing vrf mvpn-cus2
ip multicast-routing vrf mvpn-cus3
ip multicast multipath
frame-relay switching
mpls label range 4112 262143
mpls label protocol ldp
mpls ldp logging neighbor-changes
mpls ldp explicit-null
mpls traffic-eng tunnels
mpls tdp discovery directed-hello accept from 1
mpls tdp router-id Loopback0 force
platform flow ip destination
no platform flow ipv6
platform rate-limit unicast cef glean 10 10
platform qos
platform cef error action freeze

...

vlan internal allocation policy ascending
vlan access-log ratelimit 2000
!
vlan 2001-2101,3501-3700,4001,4051-4080,4093
!
!
!
interface Loopback0
 ip address 201.252.1.14 255.255.255.255
 ip pim sparse-dense-mode
!
interface Loopback1
 ip address 209.255.255.14 255.255.255.255
!
interface Loopback10
 ip vrf forwarding mvpn-cus1
 ip address 210.101.255.14 255.255.255.255
!
interface Loopback11
 ip vrf forwarding mvpn-cus1
 ip address 210.111.255.14 255.255.255.255
 ip pim sparse-dense-mode
!
interface Loopback12
 ip vrf forwarding mvpn-cus1
 ip address 210.112.255.14 255.255.255.255
```

```
...

!
interface GigabitEthernet3/3
 mtu 9216
 ip vrf forwarding mvpn-cus3
 ip address 172.10.14.1 255.255.255.0
 ip pim sparse-dense-mode
!

...

!
interface GigabitEthernet3/19
 ip vrf forwarding mvpn-cus2
 ip address 192.16.4.1 255.255.255.0
 ip pim sparse-dense-mode
 ip igmp static-group 229.1.1.1
 ip igmp static-group 229.1.1.2
 ip igmp static-group 229.1.1.4
!
interface GigabitEthernet3/20
 ip vrf forwarding mvpn-cus1
 ip address 192.16.1.1 255.255.255.0
 ip pim sparse-dense-mode
!
...
```

デフォルト MDT およびデータ MDT を含む mVPN 設定

次の設定例には、デフォルト MDT とデータ MDT の両方で設定された 3 つの mVRF が含まれています。mVPN 設定に関連する設定だけを表示しています。

```
...
!
ip vrf v1
 rd 1:1
 route-target export 1:1
 route-target import 1:1
 mdt default 226.1.1.1
 mdt data 226.1.1.128 0.0.0.7 threshold 1
!
ip vrf v2
 rd 2:2
 route-target export 2:2
 route-target import 2:2
 mdt default 226.2.2.1
 mdt data 226.2.2.128 0.0.0.7
!
ip vrf v3
 rd 3:3
 route-target export 3:3
 route-target import 3:3
 mdt default 226.3.3.1
 mdt data 226.3.3.128 0.0.0.7
!
ip vrf v4
 rd 155.255.255.1:4
 route-target export 155.255.255.1:4
 route-target import 155.255.255.1:4
 mdt default 226.4.4.1
```

```
 mdt data 226.4.4.128 0.0.0.7
!
ip multicast-routing
ip multicast-routing vrf v1
ip multicast-routing vrf v2
ip multicast-routing vrf v3
ip multicast-routing vrf v4
mpls label protocol ldp
mpls ldp logging neighbor-changes
mpls tdp router-id Loopback1
platform ip multicast replication-mode ingress
platform ip multicast bidir gm-scan-interval 10
no platform flow ip
no platform flow ipv6
platform cef error action freeze
!

...

vlan internal allocation policy ascending
vlan access-log ratelimit 2000
!
!
interface Loopback1
 ip address 155.255.255.1 255.255.255.255
 ip pim sparse-mode
!
interface Loopback11
 ip vrf forwarding v1
 ip address 155.255.255.11 255.255.255.255
 ip pim sparse-dense-mode
!
interface Loopback22
 ip vrf forwarding v2
 ip address 155.255.255.22 255.255.255.255
 ip pim sparse-mode
!
interface Loopback33
 ip vrf forwarding v3
 ip address 155.255.255.33 255.255.255.255
 ip pim sparse-mode
!
interface Loopback44
 ip vrf forwarding v4
 ip address 155.255.4.4 255.255.255.255
 ip pim sparse-mode
!
interface Loopback111
 ip vrf forwarding v1
 ip address 1.1.1.1 255.255.255.252
 ip pim sparse-dense-mode
 ip ospf network point-to-point
!
interface GigabitEthernet1/1
 description Gi1/1 - 155.50.1.155 255.255.255.0 - peer dut50 - mpls
 mtu 9216
 ip address 155.50.1.155 255.255.255.0
 ip pim sparse-mode
 mpls ip
!
interface GigabitEthernet1/2
 ip vrf forwarding v1
 ip address 155.1.2.254 255.255.255.0
 ip pim sparse-mode
```

```
!
interface GigabitEthernet1/3
 description Gi1/3 - 185.155.1.155/24 - vrf v1 stub peer 185.Gi1/3
 ip vrf forwarding v1
 ip address 185.155.1.155 255.255.255.0
 ip pim sparse-mode
!

...

!
interface GigabitEthernet1/48
 ip vrf forwarding v1
 ip address 157.155.1.155 255.255.255.0
 ip pim bsr-border
 ip pim sparse-dense-mode
!
interface GigabitEthernet6/1
 no ip address
 shutdown
!
interface GigabitEthernet6/2
 ip address 9.1.10.155 255.255.255.0
 media-type rj45
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 11 vrf v1
 router-id 155.255.255.11
 log-adjacency-changes
 redistribute connected subnets tag 155
 redistribute bgp 1 subnets tag 155
 network 1.1.1.0 0.0.0.3 area 155
 network 155.255.255.11 0.0.0.0 area 155
 network 155.0.0.0 0.255.255.255 area 155
 network 157.155.1.0 0.0.0.255 area 0
!
router ospf 22 vrf v2
 router-id 155.255.255.22
 log-adjacency-changes
 network 155.255.255.22 0.0.0.0 area 155
 network 155.0.0.0 0.255.255.255 area 155
 network 157.155.1.0 0.0.0.255 area 0
!
router ospf 33 vrf v3
 router-id 155.255.255.33
 log-adjacency-changes
 network 155.255.255.33 0.0.0.0 area 155
!
router ospf 1
 log-adjacency-changes
 network 155.50.1.0 0.0.0.255 area 0
 network 155.255.255.1 0.0.0.0 area 155
!
router bgp 1
 bgp router-id 155.255.255.1
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 175.255.255.1 remote-as 1
 neighbor 175.255.255.1 update-source Loopback1
 neighbor 185.255.255.1 remote-as 1
 neighbor 185.255.255.1 update-source Loopback1
```

```
 !
 address-family vpnv4
 neighbor 175.255.255.1 activate
 neighbor 175.255.255.1 send-community extended
 neighbor 185.255.255.1 activate
 neighbor 185.255.255.1 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf v4
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family ipv4 vrf v3
 redistribute ospf 33
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family ipv4 vrf v2
 redistribute ospf 22
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family ipv4 vrf v1
 redistribute ospf 11
 no auto-summary
 no synchronization
 exit-address-family
!
ip classless
ip route 9.255.254.1 255.255.255.255 9.1.10.254
no ip http server
ip pim bidir-enable
ip pim rp-address 50.255.2.2 MCAST.MVPN.MDT.v2 override bidir
ip pim rp-address 50.255.3.3 MCAST.MVPN.MDT.v3 override bidir
ip pim rp-address 50.255.1.1 MCAST.MVPN.MDT.v1 override bidir
ip pim vrf v1 spt-threshold infinity
ip pim vrf v1 send-rp-announce Loopback11 scope 16 group-list MCAST.GROUP.BIDIR bidir
ip pim vrf v1 send-rp-discovery Loopback11 scope 16
ip pim vrf v1 bsr-candidate Loopback111 0
ip msdp vrf v1 peer 185.255.255.11 connect-source Loopback11
ip msdp vrf v1 cache-sa-state
!
!
ip access-list standard MCAST.ANYCAST.CE
 permit 2.2.2.2
ip access-list standard MCAST.ANYCAST.PE
 permit 1.1.1.1
ip access-list standard MCAST.BOUNDARY.VRF.v1
 deny   226.192.1.1
 permit any
ip access-list standard MCAST.GROUP.BIDIR
 permit 226.192.0.0 0.0.255.255
ip access-list standard MCAST.GROUP.SPARSE
 permit 226.193.0.0 0.0.255.255
ip access-list standard MCAST.MVPN.BOUNDARY.DATA.MDT
 deny   226.1.1.128
 permit any
ip access-list standard MCAST.MVPN.MDT.v1
 permit 226.1.0.0 0.0.255.255
ip access-list standard MCAST.MVPN.MDT.v2
 permit 226.2.0.0 0.0.255.255
```

```
ip access-list standard MCAST.MVPN.MDT.v3
 permit 226.3.0.0 0.0.255.255
ip access-list standard MCAST.MVPN.RP.v4
 permit 227.0.0.0 0.255.255.255
!
access-list 1 permit 226.1.1.1
access-list 2 deny   226.1.1.1
access-list 2 permit any
...
```

mVPN with L3VPN over mGRE 設定の確認

設定が正しく動作していることを確認する例を次に示します。

エンドポイントの作成

トンネルのエンドポイントが作成されているかどうかを確認します。

```
Router# show tunnel endpoints tunnel 0

 Tunnel0 running in multi-GRE/IP mode

 Endpoint transport 209.165.200.251 Refcount 3 Base 0x2AE93F0 Create Time 00:00:42
   overlay 209.165.200.254 Refcount 2 Parent 0x2AE93F0 Create Time 00:00:42
```

隣接

対応する隣接が作成されているかどうかを確認します。

```
Router# show adjacency tunnel 0

   Protocol Interface                 Address
  IP       Tunnel0                   209.165.200.251(4)
  TAG      Tunnel0                   209.165.200.251(3)
```

プロファイルの状態

show l3vpn encapsulation *profile-name* コマンドを使用して、アプリケーションの基本的な状態に関する情報を取得できます。このコマンドの出力には、基本となるトンネルの詳細が表示されます。

```
Router# show l3vpn encapsulation ip tunnel encap

    Profile: tunnel encap
    transport ipv4 source Auto: Loopback0
    protocol gre
    Tunnel Tunnel0 Created [OK]
    Tunnel Linestate [OK]
    Tunnel Transport Source (Auto) Loopback0 [OK]
```

mVPN with L3VPN over mGRE の設定シーケンス

次に、mVPN with L3VPN over mGRE の設定シーケンスの例を示します。

```
vrf definition Customer A
 rd 100:110
 route-target export 100:1000
 route-target import 100:1000
 !
address-family ipv4
 exit-address-family
```

```
 !
address-family ipv6
 exit-address-family
!
!
ipv6 unicast-routing
!
l3vpn encapsulation ip sample_profile_name
 transport ipv4 source loopback 0
!
!
interface Loopback0
  ip address 209.165.200.252 255.255.255.224
  ip router isis
!
interface gigabitethernet 1/1
 vrf forwarding Customer A
 ip address 209.165.200.253 255.255.255.224
 ipv6 address 3FFE:1001::/64 eui-64
!
router bgp 100
 bgp log-neighbor-changes
 neighbor 209.165.200.254 remote-as 100
 neighbor 209.165.200.254 update-source Loopback0
 !
address-family ipv4
  no synchronization
  redistribute connected
  neighbor 209.165.200.254 activate
  no auto-summary
 exit-address-family
 !
address-family vpnv4
  neighbor 209.165.200.254 activate
  neighbor 209.165.200.254 send-community both
  neighbor 209.165.200.254 route-map SELECT_UPDATE_FOR_L3VPN in
 exit-address-family
 !
address-family vpnv6
  neighbor 209.165.200.254 activate
  neighbor 209.165.200.254 send-community both
  neighbor 209.165.200.254 route-map SELECT_UPDATE_FOR_L3VPN in
 exit-address-family
 !
address-family ipv4 vrf Customer A
  no synchronization
  redistribute connected
 exit-address-family
 !
address-family ipv6 vrf Customer A
  redistribute connected
  no synchronization
 exit-address-family
!
!
route-map SELECT_UPDATE_FOR_L3VPN permit 10
set ip next-hop encapsulate sample_profile_name
set ipv6 next-hop encapsulate sample_profile_name
```

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する