MPLS VPN over mGRE

MPLS VPN over mGRE 機能では、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マルチプロトコル ラベル スイッチング（MPLS）接続を可能にすることによって、通信事業者が MPLS をサポートしていなければならないという要件を克服しています。これにより、MPLS Label Switched Path（LSP; ラベル スイッチド パス）が、総称ルーティング カプセル化（GRE）トンネルを使用して、ルーティング エリア、自律システム、および Internet Service Provider（ISP; インターネット サービス プロバイダー）を横断することが可能になります。Multipoint GRE（mGRE; マルチポイント GRE）を介して MPLS VPN を設定すると、標準ベースの IP コアを使用して、Layer-3（L3; レイヤ 3）プロバイダー エッジ（PE）ベースのバーチャル プライベート ネットワーク（VPN）サービスを導入できます。これにより、オーバーレイ方式を使用しないで VPN サービスをプロビジョニングできます。

mGRE トンネルを設定して、IP バックボーンをオーバーレイするマルチポイント トンネル ネットワークを作成できます。このオーバーレイによって、VPN トラフィックを転送するために各 PE ルータ同士が接続されます。さらに、MPLS VPN を mGRE を介して設定すると、標準ベースの IP コアを使用して、L3 PE ベースの VPN サービスを導入できます。これにより、オーバーレイ方式を使用しないで VPN サービスをプロビジョニングできます。MPLS VPN over mGRE が設定されると、システムでは、PE 間の VPN ラベル IPv4 および IPv6 パケットのカプセル化に IPv4 ベースの mGRE トンネルが使用されます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、「MPLS VPN over mGRE の機能情報」（P.15）を参照してください。

プラットフォーム サポートと Cisco ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

内容

- 「MPLS VPN over mGRE の前提条件」（P.2）
- 「MPLS VPN over mGRE の制約事項」（P.2）
- 「MPLS VPN over mGRE について」（P.3）
- 「MPLS VPN over mGRE の設定方法」（P.5）
- 「MPLS VPN over mGRE の設定例」（P.11）
- 「その他の参考資料」（P.13）
- 「MPLS VPN over mGRE の機能情報」（P.15）

MPLS VPN over mGRE の前提条件

mGRE トンネルを使用して MPLS VPN を設定する前に、MPLS VPN が設定されていて、正しく動作していることを確認してください。MPLS VPN の設定については、『Configuring MPLS Layer 3 VPNs』モジュールを参照してください。

MPLS VPN over mGRE の制約事項

- MPLS VPN over mGRE は、ES-40 ライン カードおよび SIP 400 ライン カードがコアに面したカードとして使用されている Cisco 7600 シリーズ ルータ上でサポートされています。
- トンネルリングされたタグ トラフィックは、MPLS VPN over mGRE がサポートされているライン カードを介してルータに入る必要があります。
- 各 PE ルータでサポートされるトンネル コンフィギュレーションは 1 つだけです。
- MPLS VPN over mGRE では、VPN 間におけるマルチキャスト トラフィックの転送はサポートされていません。
- GRE トンネルの宛先アドレスおよび送信元アドレスが mGRE と同じである場合、トンネルによって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によって、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 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。
- mGRE とマルチキャスト配信ツリー（MDT）トンネルを同一のループバック アドレスを使用して設定できません。

MPLS VPN over mGRE 機能の制限事項は、次のとおりです。

- 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（Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）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、Unicast Reverse Path Forwarding（uRPF; ユニキャスト リバース パス転送）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。

MPLS VPN over mGRE について

- 「MPLS VPN over mGRE」（P.3）

MPLS VPN over mGRE

GRE とは、ポイントツーポイント トンネリング プロトコルの 1 つであり、2 つのピアがトンネルのエンドポイントとなります。GRE は、ネットワーク層のパケットを IP トンネリング パケット内にカプセル化するように設計されています。mGRE は、GRE と類似したプロトコルですが、トンネルの片方は単一のエンドポイントで、それがトンネルのもう片方にある複数のエンドポイントに接続されています。mGRE トンネルによって、同じ VPN に接続された各支社間が共通のリンクを使用できるようになります。mGRE は、ポイントツーマルチポイント モデルなので、各 MPLS VPN 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。

MPLS は、広く採用されている VPN インターネット アーキテクチャです。MPLS では、ネットワーク内のすべてのコア ルータで MPLS がサポートされていることが必要です。この機能は、サービス プロバイダーがバックボーン キャリアを使用して接続を提供しているネットワークで有用です。

MPLS VPN over mGRE 機能では、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 MPLS 接続を可能にすることによって、通信事業者が MPLS をサポートしていなければならないという要件を克服しています。これにより、MPLS LSP が、GRE トンネルを使用して、ルーティング エリア、自律システム、および ISP を横断することが可能になります。

MPLS VPN を mGRE を介して設定すると、標準ベースの IP コアを使用して、L3 PE ベースの VPN サービスを導入できます。これにより、LSP やラベル配布プロトコル（LDP）を使用しないで VPN サービスをプロビジョニングできます。システムでは、PE 間の VPN ラベル IPv4 および IPv6 パケットのカプセル化に IPv4 ベースの mGRE トンネルが使用されます。

また、MPLS VPN over mGRE 機能によって、既存の MPLS VPN LSP カプセル化テクノロジーを、MPLS VPN over mGRE と同時に導入し、特定のトラフィックをルーティングするために使用されるカプセル化方式が自動的に決定されるようにすることも可能です。入力 PE ルータによって、パケットがリモート PE ルータに送信されるときに使用されるカプセル化テクノロジーが決定されます。

ここでは、MPLS VPN over mGRE 機能に関する次の項目について説明します。

- 「ルート マップ」（P.4）
- 「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.4）
- 「トンネルの非カプセル化」（P.4）
- 「トンネルの送信元」（P.5）
- 「IPv6 VPN」（P.5）

ルート マップ

デフォルトでは、VPN トラフィックの送信に LSP が使用されます。MPLS VPN 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 プレフィクスと、LSP を使用して到達可能な VPN プレフィ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ネクスト ホップ トンネル テーブルが使用されます。

mGRE トンネルを介してトラフィックをルーティングするため、mGRE トンネル内でトラフィックをカプセル化することによって到達されるすべてのネクスト ホップを示す代替アドレス空間が自動的に作成されます。mGRE トンネルを使用する特定のルートを設定するには、ユーザが、そのルートのエントリをルート マップに追加します。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 Network Layer Reachability Information（NLRI; ネットワーク層到着可能性情報）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。

ユーザが MPLS VPN over mGRE を設定すると、代替アドレス空間が自動的にプロビジョニングされ、通常の場合、トンネルカプセル化 Virtual Routing and Forwarding（VRF）インスタンス内に保持されます。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。ユーザは、このデフォルト ルート マップを、適切な BGP アップデートに対応付けることが可能です。

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

MPLS VPN over mGRE 機能が正しく機能するように、システム内のリモート PE が検出でき、それらのリモート PC のトンネル フォワーディング情報が作成できるようにする必要があります。また、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。

システムによって、新しいリモート PE の通知が受信されると、トンネル エンドポイント データベースにその情報が追加され、これを契機として、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 に送信するために実行される必要のあるその他の処理に関する情報が記述されています。

この隣接情報は、トンネル カプセル化 VRF に入力されます。ユーザが（ルート マップを使用して）VRF 内のルートに VPN NLRI を再マッピングすると、その NLRI が隣接に対してリンクされ、その結果、VPN がトンネルにリンクされます。

トンネルの非カプセル化

MPLS VPN over mGRE 機能を使用するトンネル インターフェイスからのパケットを入力 PE が受信すると、その PE によってパケットが非カプセル化され、VPN ラベル タグ付きパケットが作成されて、MPLS Forwarding（MFI）コードにそのパケットが送信されます。

トンネルの送信元

MPLS VPN 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。

IPv6 VPN

アドバタイジング PE ルータのアドレスが IPv6 である場合、（PE 間のネットワークには関係なく）NLRI のアドレスも IPv6 である必要があります。各 PE 間のネットワークが IPv4 ベースである場合、::FFFF:IPv4-PE-address という形式の IPv4 射影アドレスが使用されて、アドバタイジング PE の IPv6 アドレスが作成されます。受信 PE によって、VPN タグ IPv6 プレフィクスのネクスト ホップが、IPv6 NLRI に埋め込まれた IPv4 アドレスに設定されます。これにより、PE によって、VPNv4 トラフィックをマッピングするのと同じ方法で、VPNv6 トラフィックを LSP または mGRE トンネルにリンクすることが可能になります。

PE によって VPNv6 アップデートが受信されると、そのアップデートが IPv6 ルート マップに適用されます。MPLS VPN over mGRE 機能では、Tunnel_Encap VRF におけるネクスト ホップ情報の設定に IPv6 ルート マップが使用されます。

MPLS VPN over mGRE の設定方法

MPLS VPN over mGRE トンネルを配置するには、VRF インスタンスを作成し、L3 VPN カプセル化をイネーブルおよび設定し、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 の交換を設定します。

MPLS VPN over mGRE を配置するための設定手順は、次の各項で説明します。

- 「L3VPN カプセル化プロファイルの設定」（P.5）（必須）
- 「BGP およびルート マップの設定」（P.7）（必須）

L3VPN カプセル化プロファイルの設定

ここでは、L3VPN カプセル化プロファイルを設定する方法を説明します。

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

手順の概要

1. **enable**
2. **configure terminal**
3. **l3vpn encapsulation ip** *profile-name*
4. **transport ipv4** [**source** *interface-type interface-number*]

5. **protocol gre** [**key** *gre-key*]
6. **end**
7. **show l3vpn encapsulation ip** *profile-name*

手順の詳細

	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。 • プロンプトが表示されたら、パスワードを入力します。
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。
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。

手順の概要

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **bgp log-neighbor-changes**
5. **neighbor** *ip-address* **remote-as** *as-number*
6. **neighbor** *ip-address* **update-source** *interface-name interface-number*
7. **address-family ipv4**
8. **no synchronization**
9. **redistribute connected**
10. **neighbor** *ip-address* **activate**
11. **no auto-summary**
12. **exit**
13. **address-family vpnv4**
14. **neighbor** *ip-address* **activate**
15. **neighbor** *ip-address* **send-community both**
16. **neighbor** *ip-address* **route-map** *map-name* **in**
17. **exit**
18. **address-family vpnv6**
19. **neighbor** *ip-address* **activate**
20. **neighbor** *ip-address* **send-community both**
21. **neighbor** *ip-address* **route-map** *map-name* **in**
22. **exit**
23. **route-map** *map-tag* **permit** *position*
24. **set ip next-hop encapsulate l3vpn** *profile-name*
25. **set ipv6 next-hop encapsulate l3vpn** *profile-name*
26. **exit**
27. **exit**

手順の詳細

	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。 • プロンプトが表示されたら、パスワードを入力します。
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。
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。

	コマンドまたはアクション	目的
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。
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。

	コマンドまたはアクション	目的
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。
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。

	コマンドまたはアクション	目的
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。

MPLS VPN over mGRE の設定例

- 「例：MPLS VPN over mGRE 設定の確認」（P.11）
- 「例：MPLS VPN over mGRE の設定シーケンス」（P.12）

例：MPLS VPN 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。

Cisco Express Forwarding（CEF; シスコ エクスプレス フォワーディング）スイッチング

CEF スイッチングが想定どおりに動作しているかどうかを確認します。

```
Router# show ip cef vrf Customer_A tunnel 0

209.165.200.250/24
    nexthop 209.165.200.251 Tunnel0 label 16
```

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]
```

例：MPLS VPN over mGRE の設定シーケンス

次に、MPLS VPN 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
!
!
ip cef
!
ipv6 unicast-routing
ipv6 cef
!
!
l3vpn encapsulation ip sample profile name
 transport source loopback 0
 protocol gre key 1234
!
!
 interface Loopback0
  ip address 209.165.200.252 255.255.255.224
  ip router isis
!
interface Serial2/0
 vrf forwarding Customer A
 ip address 209.165.200.253 255.255.255.224
 ipv6 address 3FFE:1001::/64 eui-64
 no fair-queue
 serial restart-delay 0
!
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
```

その他の参考資料

関連資料

関連項目	参照先
MPLS レイヤ 3 VPN の設定	『*Cisco IOS Multiprotocol Label Switching Configuration Guide*』
マルチポイント GRE トンネルを使用したダイナミック レイヤ 3 VPN	『*Cisco IOS Interface and Hardware Component Configuration Guide*』
シスコ エクスプレス フォワーディング	『*Cisco IOS IP Switching Configuration Guide*』
総称ルーティング カプセル化	『*Cisco IOS Interface and Hardware Component Configuration Guide*』

標準

標準	タイトル
なし	—

MIB

MIB	MIB リンク
IETF-PPVPN-MPLS-VPN-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2547	『*BGP/MPLS VPNs*』
RFC 2784	『*Generic Routing Encapsulation (GRE)*』
RFC 2890	『*Key Sequence Number Extensions to GRE*』
RFC 4023	『*Encapsulating MPLS in IP or Generic Routing Encapsulation*』
RFC 4364	『*BGP/MPLS IP Virtual Private Networks (VPNs)*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

MPLS VPN over mGRE の機能情報

表 1 に、この機能のリリース履歴を示します。

プラットフォームのサポートおよびソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator を使用すると、Cisco ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 1　MPLS VPN over mGRE の機能情報

機能名	リリース	機能情報
MPLS VPN over mGRE	12.2(33)SRE 15.1(2)T 15.0(1)SY	この機能では、mGRE を介した MPLS レイヤ 3 VPN トラフィックの搬送がサポートされています。この機能では、Cisco 7600 シリーズ ルータ上の SIP-400 および ES-40 もサポートされています。 この機能に関する詳細については、次の各項を参照してください。 • 「L3VPN カプセル化プロファイルの設定」（P.5） • 「BGP およびルート マップの設定」（P.7） この機能では、コマンド **l3vpn encapsulation ip**、**protocol gre**、**show l3vpn encapsulation ip**、**transport ipv4**、**set ip next-hop**、**set ipv6 next-hop** が導入または変更されています。