MPLS VPN over mGRE

MPLS VPN over mGRE 機能は、IP 専用ネットワークで接続されているネットワーク間に Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）接続を提供できるようにすることによって、MPLS をサポートするという通信事業者の要件を克服します。これにより、MPLS の Label Switched Path（LSP; ラベル スイッチド パス）では Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）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）による 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）Provider Edge（PE; プロバイダー エッジ）ベースの Virtual Private Network（VPN; バーチャル プライベート ネットワーク）を展開できます。これにより、オーバーレイ方式を使用しないで VPN サービスを提供することができます。

機能情報の確認

お使いのソフトウェア リリースが、このモジュールで説明されている機能の一部をサポートしていないことがあります。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.16）を参照してください。

Cisco Feature Navigator を使用すると、プラットフォーム サポートおよび Cisco ソフトウェア イメージ サポートに関する情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

目次

- 「MPLS VPN over mGRE の機能情報」（P.16）

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、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

- トンネル タグ トラフィックは、MPLS VPN over mGRE をサポートするライン カード経由で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 間のマルチキャスト トラフィックの転送はサポートされません。
- GRE トンネルの宛先アドレスおよび送信元アドレスが mGRE と同じである場合は、トンネルで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ではルートキャッシュが切り替えられます。
- L3VPN プロファイルが削除され、再び追加された場合は、**clear ip bgp soft** コマンドを使用して Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）をクリアする必要があります。
- mGRE 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 Stateful Switchover（SSO; ステートフル スイッチオーバー）には対応していません。ただし、mGRE と SSO は共存します。
- mGRE と Multicast Distribution Tree（MDT; マルチキャスト分散ツリー）トンネルに同じループバック アドレスを設定しないでください。

MPLS VPN over mGRE 機能の制限事項は、次のとおりです。

  - ハードウェアで、すべての GRE オプションがサポートされるわけではありません（GRE 拡張ヘッダーや GRE キーなど）。
  - トンネルでは、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 アカウンティングなどの機能はサポートされていません。

MPLS VPN over mGRE に関する情報

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の PE ルータが接続されます。

さらに、mGRE による MPLS VPN を設定すると、標準ベースの IP コアを使用して、L3 PE ベースの VPN サービスを展開できます。これにより、オーバーレイ方式を使用しないで VPN サービスを提供することができます。MPLS VPN over mGRE を設定すると、システムは IPv4 ベースの mGRE トンネルを使用して、PE 間で VPN ラベル付きの IPv4 および IPv6 パケットをカプセル化します。

MPLS VPN over mGRE 機能を設定するには、次の概念を理解しておく必要があります。

- 「MPLS VPN over mGRE」（P.3）

MPLS VPN over mGRE

GRE は、2 つのピアがトンネルのエンドポイントを構成するポイントツーポイント トンネリング プロトコルです。GRE はネットワーク レイヤのパケットを IP トンネリング パケットにカプセル化するように設計されています。mGRE は同様のプロトコルですが、トンネルの一方は単一のエンドポイントで、それがトンネルの他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 に接続された支社間に共通のリンクが提供されます。mGRE はポイントツーマルチポイント モデルなので、MPLS VPN の PE デバイスを相互接続するためにフル メッシュ構造の GRE トンネルは必要ありません。

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 ルータが MPLS をサポートしている必要があります。この機能は、サービス プロバイダーがバックボーン事業者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 機能は、IP 専用ネットワークで接続されているネットワーク間に MPLS 接続を提供できるようにすることによって、MPLS をサポートするという通信事業者の要件を克服します。これにより、MPLS の LSP では 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。

mGRE による MPLS VPN を設定すると、標準ベースの IP コアを使用して、L3 PE ベースの VPN サービスを展開できます。これにより、LSP や Label Distribution Protocol（LDP; ラベル配布プロトコル）を使用しないで VPN サービスを提供することができます。システムは IPv4 ベースの mGRE トンネルを使用して、PE 間で VPN ラベル付きの IPv4 および IPv6 パケットをカプセル化します。

また、MPLS VPN over mGRE 機能により、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、特定トラフィックのルーティングに使用されるカプセル化方式をシステムが決定でき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す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転送」（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 トラフィックは LSP を使用して送信されます。MPLS VPN over mGRE 機能では、ユーザ定義のルート マップを使用して、mGRE トンネルで到達可能な VPN プレフィクスと LSP を使用して到達可能な VPN プレフィクスを決定します。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、ネクスト ホップ トンネル テーブルを使用して VPN トラフィックのカプセル化方式を決定します。

mGRE トンネルを使用してトラフィックをルーティングするために、システムは mGRE トンネルでトラフィックをカプセル化することによってすべてのネクスト ホップに到達可能であることを示す代替アドレス空間を作成します。特定のルートが mGRE トンネルを使用するように設定するには、ユーザがそのルート用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、代替アドレス空間へのルートの Network Layer Reachability Information（NLRI; ネットワーク レイヤ到着可能性情報）が再マッピングされます。あるルートの再マッピング エントリがルート マップに存在しない場合、そのルート上のトラフィックは LSP を使用して転送されます。

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; 仮想ルーティング / 転送）インスタンスに保持されます。このアドレス空間経由で到達可能なすべてのトラフィックが mGRE トンネルで確実にカプセル化されるように、システムにはトンネル外への単一のデフォルト ルートが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のトンネルも作成されます。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できます。

トンネル エンドポイントの検出および転送

MPLS VPN over mGRE 機能が正常に機能するためには、システムがシステム内のリモート PE を検出し、これらのリモート PE のトンネル転送情報を作成できる必要があります。また、リモート PE が有効でなくなったときを検出し、その PE のトンネル転送情報を削除できることも必要です。

入力 PE は、BGP による VPN アドバタイズメントを受信すると、ルート ターゲット属性（入力 PE が VRF に挿入）とアドバタイズメントの MPLS VPN ラベルを使用して、プレフィクスを適切なカスタマーに関連付けます。挿入されたルートのネクスト ホップは、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）含まれます。PE はこの情報を使用して、NLRI がアクティブまたは非アクティブになったときにシステムに通知します。システムは、この通知を使用して PE 転送情報をアップデートします。

システムは新しいリモート PE の通知を受信すると、その情報をトンネル エンドポイント データベースに追加します。これによって、システムはトンネル インターフェイスに関連付けられた隣接関係を作成します。この隣接関係の説明には、カプセル化に関する情報と、カプセル化パケットを新しいリモート PE に送信するためにシステムで実行する必要のあるその他の処理に関する情報が含まれます。

この隣接情報は、トンネル カプセル化 VRF に挿入されます。ユーザが（ルート マップを使用して）VPN の NLRI を VRF 内のルートに再マッピングすると、システムはその NLRI を隣接関係にリンクさせます。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

出力 PE は、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パケットを受信すると、そのパケットを非カプセル化して VPN ラベル タグ付きのパケットを作成し、MPLS Forwarding（MFI）コードに送信します。

トンネルの送信元

MPLS VPN over mGRE 機能では、mGRE トンネルとして設定された単一のトンネルを使用して、多数のエンドポイント（リモート PE）を持つシステムを設定します。トンネル カプセル化パケットの送信元を識別するために、システムではトンネル送信元情報が使用されます。

送信側（入力）PE では、VPN パケットがトンネルに送信されるとき、トンネル宛先は NLRI です。受信側（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。したがって、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、システムは ::FFFF:IPv4-PE-address という形式の IPv4 射影アドレスを使用してアドバタイジング PE の IPv6 アドレスを作成します。受信側 PE は、VPN タグの IPv6 プレフィクス用のネクスト ホップを、IPv6 の NLRI に埋め込まれた IPv4 アドレスに設定します。これにより、PE は VPNv4 トラフィックをマッピングするのと同じように、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 が VPNv6 アップデートを受信すると、そのアップデートは IPv6 ルート マップに適用されます。MPLS VPN over mGRE 機能では、IPv6 ルート マップを使用して、Tunnel_Encap VRF にネクスト ホップ情報を設定します。

MPLS VPN over mGRE の設定方法

mGRE トンネルによる MPLS VPN を展開するには、VRF インスタンスを作成し、L3 VPN カプセル化をイネーブルにして設定し、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、BGP VPNv4 と VPNv6 の交換を設定してアップデートがルート マップでフィルタリングされるようにします。

MPLS VPN over mGRE を展開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について説明します。

（注） この設定では、IPv6、MPLS、IP、および Layer 2 Tunneling Protocol version 3（L2TPv3）などのトランスポート 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 モードを開始して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 トランスポートの送信元モードを指定し、トランスポートの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は、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 アップデートのネクスト 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は、**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と基盤となるトンネル 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、BGP VPNv4 と VPNv6 の交換を設定してアップデートがルート マップでフィルタリングされるようにすることもできます。

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 ルータに対してルータを識別する自律システムの番号を指定し、渡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 モードを開始して、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`	Cisco IOS ソフトウェアが IGP を待たずにネットワーク ルートをアドバタイズできるようにします。
ステップ 9	**redistribute connected** **例：** `Router(config-router-af)# redistribute connected`	あるルーティング 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、ターゲット プロトコルが、ソース プロトコルによって認識されたルートおよびソース プロトコルが実行されている各インターフェイス上の接続プレフィクスを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、標準の VPNv4 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（BGP など）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`	指定されたルート 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ルーティング セッション（BGP など）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`	指定されたルート 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、あるルーティング プロトコルから別のルーティング プロトコルにルートを再分配するための条件を定義します。 • **redistribute** ルータ コンフィギュレーション コマンドは、指定されたマップ タグを使用して、このルート マップを参照します。複数のルート マップが同じマップ タグ名を共有する場合があります。 • このルート マップの一致基準が満たされた場合、ルートは設定アクションによる制御に応じて再分配されます。 • 一致基準が満たされない場合、同じマップ タグを持つ次のルート マップがテストされます。あるルートが同じ名前を共有する一連のルート マップの一致基準のいずれも満たさなかった場合、ルートはその設定で再分配されません。 • *position* 引数は、すでに同じ名前で設定されているルート マップのリスト内に新しいルート 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 パケットが、トンネル カプセル化のために VRF に送信されることを示します。
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 パケットが、トンネル カプセル化のために VRF に送信されることを示します。

	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

設定が正しく動作していることを確認するには、次の例を使用します。

シスコ エクスプレス フォワーディング（CEF）スイッチング

CEF スイッチングが予想どおりに動作していることを確認できます。

```
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

作成されたトンネル エンドポイントを確認できます。

```
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
```

隣接関係

対応する隣接関係が作成されていることを確認できます。

```
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、基盤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

この例では、MPLS VPN over mGRE の設定シーケンスを示します。

```
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 XE Multiprotocol Label Switching Configuration Guide*』
シスコ エクスプレス フォワーディング	『*Cisco IOS XE IP Switching Configuration Guide*』
総称ルーティング カプセル化	『*Cisco IOS XE Interface and Hardware Component Configuration Guide*』

規格

規格	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、および機能セットの 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 サポートとソフトウェア 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 を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートするフトウェア イメージを確認できます。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 には、一連のソフトウェア リリースのうち、特定の機能のサポートが初めて導入されたソフトウェア リリースだけを示します。その機能は、特に明記されていない限り、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	Cisco IOS XE リリース 3.1S	この機能では、mGRE による MPLS レイヤ 3 VPN トラフィックの伝送のサポートが提供されます。 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） この機能によって、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。