



ポイントツーポイント レイヤ2サービスの の実装

このモジュールでは、ポイントツーポイントレイヤ2 (L2) 接続の概念および設定情報を提供します。

次のポイントツーポイント サービスがサポートされます。

- ローカルスイッチング：単一の Cisco ASR 9000 シリーズ ルータへのポイントツーポイント内部回線（ローカル接続とも呼ばれます）。
- 疑似回線：Cisco ASR 9000 シリーズルータからの仮想ポイントツーポイント回線。疑似回線は、MPLS 上で実装されます。



(注) ポイントツーポイントレイヤ2 サービスは、MPLS レイヤ2 VPN と呼ばれます。



(注) Cisco ASR 9000 シリーズルータでのポイントツーポイントレイヤ2サービスの詳細、およびこのモジュールに記載されているコマンドの説明については、「関連ドキュメント」セクションを参照してください。設定作業の実行中に必要になることのある他のコマンドのドキュメントを見つけるには、Cisco IOS XR ソフトウェア マスター コマンド インデックスで、オンライン検索してください。

ポイントツーポイントレイヤ2サービスの実装機能の履歴

リリース	変更内容
リリース 3.7.2	この機能が導入されました。
リリース 3.9.0	スケール拡張機能が導入されました。
リリース 4.0.0	Any Transport over MPLS (AToM) 機能のサポートが追加されました。

リリース	変更内容
リリース 4.0.1	次の機能のサポートが追加されました。 <ul style="list-style-type: none"> • 疑似回線のロードバランシング • Any Transport over MPLS (AToM) 機能 <ul style="list-style-type: none"> • HDLC over MPLS (HDLCoverMPLS) • PPP over MPLS (PPPoMPLS)
リリース 4.1.0	Flexible ルータ ID 機能のサポートが追加されました。
リリース 4.2.0	次の機能のサポートが追加されました。 <ul style="list-style-type: none"> • MPLS トランスポートプロファイル • Circuit EMulation (CEM) over Packet
リリース 4.3.0	L2VPN ノンストップルーティング機能のサポートが追加されました。
リリース 4.3.1	次の機能のサポートが追加されました。 <ul style="list-style-type: none"> • L2TPv3 over IPv6 トンネル • ATMoverMPLS セルリレー VP モード • GTP ロードバランシング
リリース 5.1.0	次の機能のサポートが追加されました。 <ul style="list-style-type: none"> • ATM/CEMoverMPLS の双方向疑似回線 (PW) • マルチセグメント PW の PW グループ化 • ATM/CEMoverMPLS のホットスタンバイ PW • MR-APS のホットスタンバイ PW との統合
リリース 5.1.2	次のサポートが追加されました。 <ul style="list-style-type: none"> • 動的単一セグメント疑似回線 • 疑似回線の障害が発生した後のネットワークコンバージェンスの高速化

リリース	変更内容
リリース 6.1.2	次の機能に対するサポートが追加されました。 <ul style="list-style-type: none"> • L2TPv3 over IPv4 • PWHE インターフェイスおよびアクセス疑似回線を設定するための EVPN-VPWS 拡張

- [ポイントツーポイント レイヤ2 サービス実装の前提条件 \(3 ページ\)](#)
- [ポイントツーポイント レイヤ2 サービスの実装に関する情報 \(3 ページ\)](#)
- [ポイントツーポイント レイヤ2 サービスを実装する方法 \(32 ページ\)](#)
- [ポイントツーポイント レイヤ2 サービスの設定例 \(120 ページ\)](#)

ポイントツーポイント レイヤ2 サービス実装の前提条件

適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。このコマンドリファレンスには、各コマンドに必要なタスク ID が含まれます。

ユーザ グループの割り当てが原因でコマンドを使用できないと考えられる場合、AAA 管理者に連絡してください。

ポイントツーポイント レイヤ2 サービスの実装に関する情報

ポイントツーポイントレイヤ2 サービスを実装するには、次の概念を理解する必要があります。

レイヤ2 バーチャル プライベート ネットワークの概要

レイヤ2 バーチャルプライベート ネットワーク (L2VPN) は、IP または MPLS 対応の L2 スイッチド IP ネットワークで LAN の動作をエミュレートすることで、イーサネットデバイス同士が共通の LAN セグメントに接続した場合と同様に通信できるようにします。ポイントツーポイント L2 接続は、L2VPN を作成する場合に重要です。

インターネット サービス プロバイダー (ISP) が、フレーム リレーまたは非同期転送モード (ATM) インフラストラクチャを IP インフラストラクチャに置き換える場合、IP または MPLS 対応の L2 スイッチド IP インフラストラクチャを使用する標準的な方法を提供する必要があります。これらの方法は、カスタマーに実用的な L2 インターフェイスを提供し、具体的には、カスタマー サイトのペア間の仮想回線を提供します。

L2VPN システムを構築するには、ISP とカスタマーの間での調整が必要です。ISP は L2 接続を提供し、カスタマーは ISP から取得したデータ リンク リソースを使用してネットワークを構築します。L2VPN サービスでは、ISP は、カスタマーのネットワーク トポロジ、ポリシー、ルーティング情報、ポイントツーポイントリンクに関する情報や、他の ISP からのネットワーク ポイントツーポイントリンクに関する情報を必要としません。

ISP には、次の機能を備えたプロバイダー エッジ (PE) ルータが必要です。

- レイヤ 3 (L3) パケット内への L2 プロトコル データ ユニット (PDU) のカプセル化。
- any-to-any L2 転送のインターコネクト。
- パケットスイッチネットワーク上での L2 Quality-of-Service (QoS) のエミュレーション。
- L2 サービスの設定の簡素化。
- 各種のトンネリングメカニズム (MPLS、L2TPv3、IPSec、GRE など) のサポート。
- L2VPN プロセスデータベースには、回線および接続に関するすべての情報が含まれます。

レイヤ2 ローカルスイッチングの概要

ローカルスイッチングにより、同じルータ上の同じタイプの2つのインターフェイス間で L2 データを切り替えることができます (たとえば、イーサネットからイーサネット)。インターフェイスは、同じラインカード上にあっても、2つの異なるラインカード上にあってもかまいません。これらのタイプのスイッチング中、レイヤ2アドレスが、レイヤ3アドレスの代わりに使用されます。ローカルスイッチング接続は、一方の接続回線 (AC) から他方の接続回線に L2 トラフィックを切り替えます。ローカルスイッチング接続で設定される2つのポートは、そのローカル接続に関連する AC です。ローカルスイッチング接続の動作は、2つのブリッジポートしかないブリッジドメインの動作と類似しており、トラフィックはローカル接続の一方のポートに入り、他方のポートから出ます。ただし、ローカル接続に関するブリッジングがないため、MAC 学習やフラッドングはありません。また、インターフェイスの状態が DOWN の場合、ローカル接続の AC は UP 状態ではありません (この動作は、ブリッジドメインの動作に準拠したときにも異なります)。

ローカルスイッチング AC は、L2 トランク (メイン) インターフェイス、バンドルインターフェイス、EFP など、多種多様な L2 インターフェイスを使用します。

また、同一ポートのローカルスイッチング機能を使用すると、同じインターフェイス上の2つの回線の間でレイヤ2データをスイッチングできます。

L2VPN での ATMoMPLS の概要

ATMoMPLS は、MPLS コアを介したレイヤ2 ポイントツーポイント接続の一種です。

ATMoMPLS 機能を実装するために、Cisco ASR 9000 シリーズルータはカスタマーエッジ (CE) デバイスが Cisco ASR 9000 シリーズルータに接続されているプロバイダーネットワークのエッジでプロバイダーエッジ (PE) ルータの役割を果たします。

L2VPN での仮想回線接続検証

仮想回線接続性検証 (VCCV) は、L2VPN の運用、管理、およびメンテナンス (OAM) 機能であり、ネットワーク オペレータが、指定した疑似回線上で IP ベースのプロバイダー エッジ間 (PE-to-PE) キープアライブ プロトコルを実行できるようにし、疑似回線データ パス転送で障害が発生しないようにします。ディスポジション PE は、指定した疑似回線に関連付けられる制御チャネルで VCCV パケットを受信します。疑似回線が各方向の PE 間で確立されると、VCCV に使用される制御チャネル タイプと接続検証タイプがネゴシエートされます。

2つのタイプのパケットが判定結果出力に着信します。

- タイプ 1：通常の Ethernet-over-MPLS (EoMPLS) データ パケットを指定します。
- タイプ 2：VCCV パケットを指定します。

Cisco ASR 9000 シリーズルータは、シグナリング中にイネーブルにされた場合にインバンド制御ワードを使用する、ラベルスイッチドパス (LSP) VCCV タイプ 1 をサポートしています。IPv4 では、VCCV エコー応答は、応答モードである IPv4 として送信されます。応答は IP、MPLS、またはその両方の組み合わせとして転送されます。

出力側の MPLS 転送では、VCCV pings カウンタがカウントされます。ただし、入力側では、これらはルート プロセッサから発信され、MPLS 転送カウンタとしてカウントされません。

Ethernet over MPLS

Ethernet-over-MPLS (EoMPLS) は、MPLS 対応 L3 コアを通じてイーサネット トラフィックのトンネリング メカニズムを提供し、(ラベル スタックを使用して) イーサネット プロトコル データ ユニット (PDU) を MPLS パケット内部にカプセル化して、それらを MPLS ネットワーク経由で転送します。

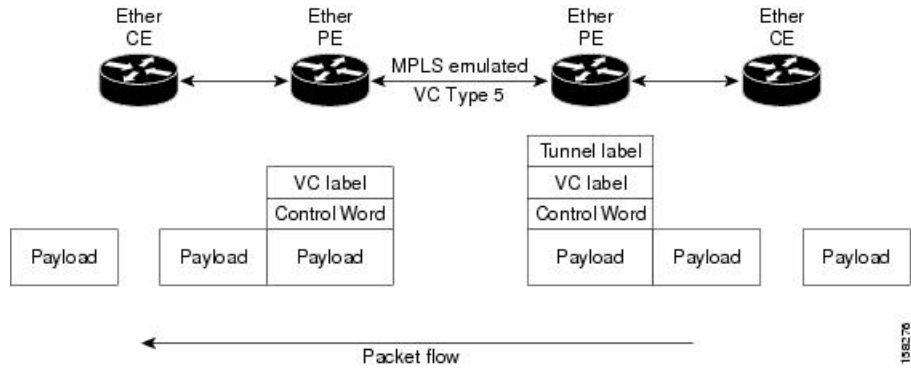
EoMPLS 機能は、次のサブセクションで説明します。

イーサネット ポート モード

イーサネット ポート モードでは、疑似回線の両端がイーサネット ポートに接続されます。このモードでは、ポートが疑似回線を介してトンネル化されるか、またはローカルスイッチング (接続回線から接続回線へのクロスコネクトと呼ばれる) を使用して、1つの接続回線 (AC) から同じ PE ノードに接続されている別の AC にパケットまたはフレームを切り替えます。

次の図に、イーサネットポートモードの例を示します。

図 1:イーサネットポートモードのパケットフロー

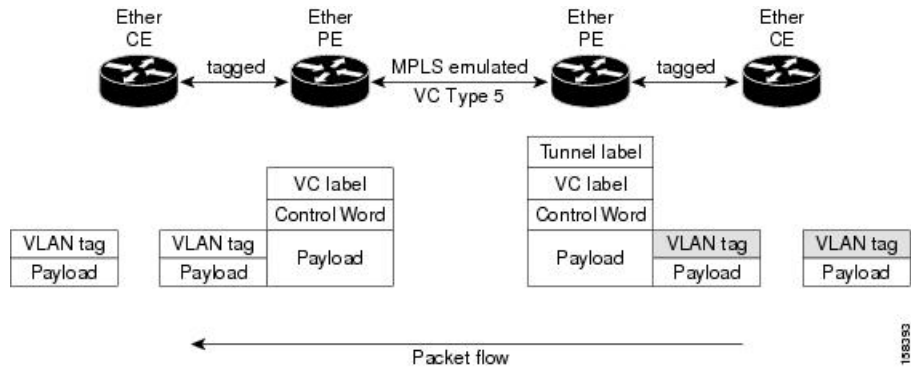


VLAN モード

VLANモードでは、カスタマー側とプロバイダー側のリンクで、各VLANは、仮想接続（VC）タイプ4またはVCタイプ5を使用して個別L2VPN接続として設定できます。VCタイプ5はデフォルトのモードです。

次の図に示されているように、イーサネットPEは、入力ポートから疑似回線にトラフィックを内部的に切り替えるために、イーサネットポートに内部VLANタグを関連付けます。ただし、疑似回線にトラフィックを移動する前に、内部VLANタグを削除します。

図 2: VLANモードのパケットフロー



出力VLAN PEでは、PEは、疑似回線から到着するフレームにVLANタグを関連付け、トラフィックを内部的に切り替えた後、イーサネットトランクポートにトラフィックを送信します。



(注) ポートがトランクモードであるため、VLAN PEはVLANタグを削除せず、追加されたタグを持つポート経由でフレームを転送します。

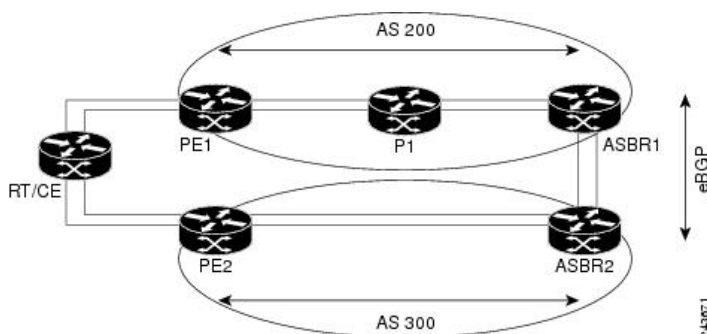
Inter-AS モード

Inter-AS は、複数のプロバイダーまたはマルチドメイン ネットワークを通じて VPN を拡張できるピアツーピア タイプ モデルです。これにより、サービス プロバイダーは相互にピアアップでき、地理的に離れた位置でエンドツーエンドの VPN 接続が実現します。

EoMPLS サポートでは、単一 AS トポロジを想定でき、このトポロジでは、ポイントツーポイント EoMPLS 相互接続の 2 つの終端にある PE ルータを接続する疑似回線が、同一自律システムに存在します。または、複数の AS トポロジを想定でき、このトポロジでは、PE ルータが iBGP および eBGP ピアリングを使用して 2 つの異なる AS に存在できます。

次の図は、各 AS で iBGP/LDP を使用した基本的な二重 AS トポロジを持つ Inter-AS を介した MPLS を示しています。

図 3: Inter-AS を介した EoMPLS : 基本的な二重 AS トポロジ



QinQ モード

QinQ は、複数の 802.1Q タグ (IEEE 802.1Q QinQ VLAN タグ スタッキング) を指定するための 802.1Q の拡張です。レイヤ 3 VPN サービス終了および L2VPN サービス転送は、QinQ サブインターフェイスではイネーブルです。

Cisco ASR 9000 シリーズルータは、プロバイダー エッジルータでのサブインターフェイスの設定に基づき、レイヤ 2 トンネリングまたはレイヤ 3 転送を実装します。この機能は、SPA および固定 PLIM で最大 2 つの QinQ タグのみサポートします。

- L2VPN 接続回線のレイヤ 2 QinQ VLAN : QinQ L2VPN 接続回線は、仮想回線タイプ 4 とタイプ 5 の両方の疑似回線を使用したポイントツーポイント EoMPLS ベースのクロスコネクタ用と、802.1q VLAN およびポートモードでの QinQ の完全なインターワーキングのサポートなど、ポイントツーポイント ローカル スイッチングベースのクロスコネクタ用のレイヤ 2 転送サブインターフェイスで設定されます。
- レイヤ 3 QinQ VLAN : レイヤ 3 の終端ポイントとして使用されます。VLAN はいずれも入力プロバイダーエッジで削除され、フレームが転送されるときリモートプロバイダーエッジで追加され戻されます。

QinQ 上のレイヤ 3 サービスは次のとおりです。

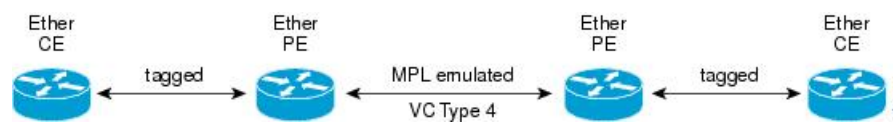
- IPv4 ユニキャストおよびマルチキャスト

- IPv6 ユニキャストおよびマルチキャスト
- MPLS
- Intermediate System-to-Intermediate System (IS-IS) で使用されるコネクションレス型ネットワーク サービス (CLNS)

QinQ モードでは、各 CE VLAN は SP VLAN 内に伝送されます。QinQ モードでは VC タイプ 5 を使用する必要がありますが、VC タイプ 4 もサポートされます。各イーサネット PE では、内部 (CE VLAN) と外部 (SP VLAN) の両方を設定する必要があります。

次の図に、VC タイプ 4 を使用した QinQ を示します。

図 4: QinQ を介した EoMPLS モード



QinAny モード

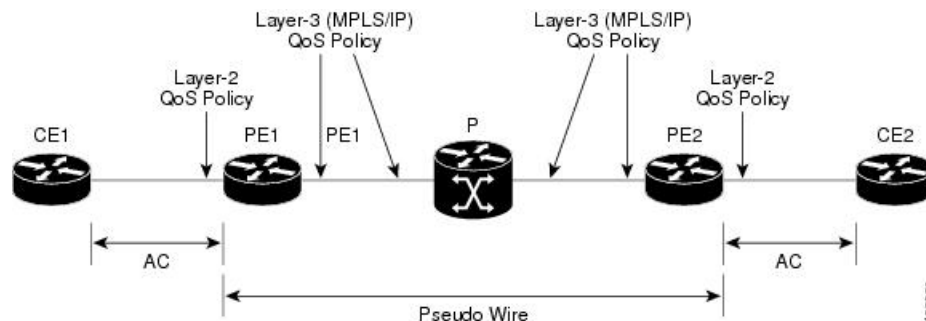
QinAny モードでは、サービス プロバイダー VLAN タグは、プロバイダー エッジ VLAN の入力ノードと出力ノードの両方で設定されます。カスタマー エッジ VLAN タグが不明なため、カスタマー エッジ VLAN タグが疑似回線上のパケットで送信されることを除き、QinAny モードはタイプ 5 VC を使用する Q-in-Q モードに似ています。

QoS

L2VPN テクノロジーを使用して、ポートおよび VLAN の動作モードの両方に Quality of Service (QoS) レベルを割り当てることができます。

L2VPN テクノロジーでは、PE ルータの QoS 機能が、エッジ方向のインターフェイス (別名、接続回線) で L2 ペイロードベースである必要があります。次の図は、一般的な L2VPN ネットワークでの L2 および L3 QoS サービスポリシーを表しています。

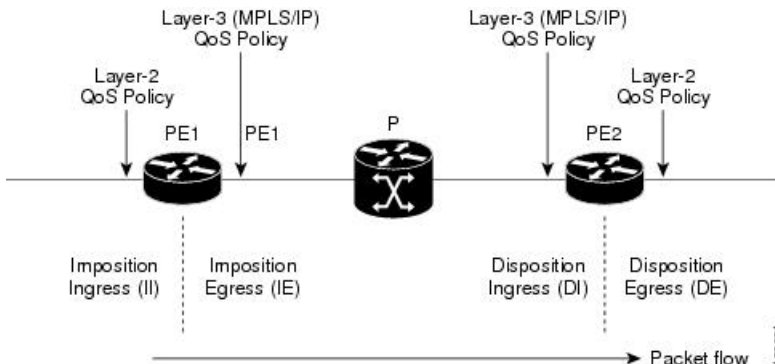
図 5: L2VPN QoS 機能の適用



次の図は、QoS サービスポリシーを設定できるプロバイダーエッジデバイス内の4つのパケット処理パスを表しています。L2VPN ネットワークでは、パケットはエッジ方向のインターフェ

イスでL2パケットとして送受信され、コア方向のインターフェイスでMPLS (EoMPLS) パケットとして転送されます。

図 6: L2VPN QoS リファレンス モデル



ハイアベイラビリティ

L2VPNは、ルートプロセッサとラインカードの両方でコントロールプレーンを使用し、ラインカードでフォワーディングプレーン要素を使用します。

L2VPNの可用性は次の要件を満たします。

- ルートプロセッサまたはラインカードでのコントロールプレーンの障害は、回線の転送パスには影響しません。
- ルータプロセッサのコントロールプレーンは、ラインカードの制御およびフォワーディングプレーンに影響を与えずに、フェールオーバーをサポートします。
- L2VPNは既存のラベル配布プロトコル (LDP) のグレースフルリスタートメカニズムと統合されます。

優先トンネルパス

優先トンネルパスの機能により、特定のトラフィックエンジニアリングトンネルに疑似回線をマッピングできます。接続回線は、リモートPEルータのIPアドレス (IGPまたはLDPを使用して到達可能) ではなく、特定のMPLSトラフィックエンジニアリングトンネルインターフェイスに相互接続されます。優先トンネルパスを使用する場合、L2トラフィックを転送するトラフィックエンジニアリングトンネルが2台のPEルータ間で動作することが常に想定されます (つまり、始端はインポジションPEルータで、終端はディスポジションPEルータです)。



- (注)
- 現在、優先トンネルパス設定はMPLSカプセル化だけに適用されます。

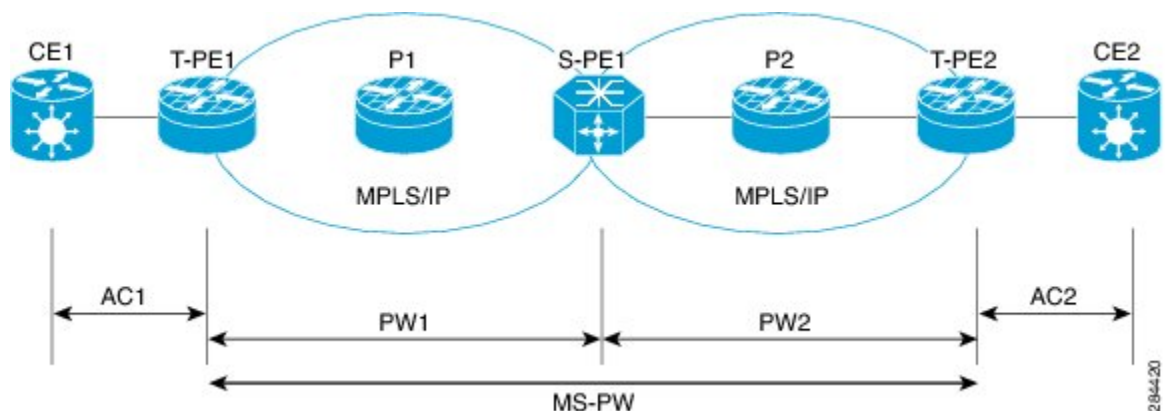
マルチセグメント疑似回線

疑似回線は Public Switched Network (PSN) 上でレイヤ2 プロトコルデータユニット (PDU) を転送します。マルチセグメント疑似回線は、静的または動的に設定された、複数の隣接する疑似回線セグメントのセットです。これらのセグメントは単一の疑似回線として機能し、以下を実行できます。

- 管理ドメインまたはプロビジョニングドメインを隔離することで、エンドツーエンドサービスを管理する。
- 相互自律システム (Inter-AS) の境界を越えて、プロバイダー エッジ (PE) ノードの IP アドレスをプライベートにする。自律システム境界ルータ (ASBR) の IP アドレスを使用し、それらのルータを疑似回線の集約ルータとして扱う。ASBR は、2つのドメインの疑似回線を結合します。

マルチセグメント疑似回線は、Inter-AS 境界または2つのマルチプロトコルラベルスイッチング (MPLS) ネットワークにまたがるすることができます。

図 7: マルチセグメント疑似回線 : 例



疑似回線は、2台の PE ノード間のトンネルです。2種類の PE ノードがあります。

- スイッチング PE (S-PE) ノード
 - マルチセグメント疑似回線の先行する疑似回線セグメントと後続の疑似回線セグメントの PSN トンネルを終端させます。
 - マルチセグメント疑似回線の先行する疑似回線セグメントと後続の疑似回線セグメントのコントロールプレーンとデータプレーンを切り替えます。
- 終端 PE (T-PE) ノード
 - マルチセグメント疑似回線の最初と最後の両方のセグメントに配置されます。
 - このノードで、カスタマー方向の接続回線 (AC) が疑似回線フォワーダにバインドされます。



(注) すべてのマルチセグメント疑似回線は、T-PE で終端する必要があります。

マルチセグメント疑似回線は、次の場合に2つの一般的なケースで使用されます。

- 送信元と宛先の PE ノード間で PW 制御チャネルを確立することができない場合。

PW コントロールチャネルを確立するには、リモート PE ノードがアクセス可能である必要があります。場合によっては、トポロジ、動作、またはセキュリティ上の制約により、ローカル PE ノードがリモートノードにアクセスできない場合があります。

マルチセグメントの疑似回線は、2つの独立した疑似回線セグメントを動的に構築し、疑似回線スイッチングを実行して、送信元と宛先の PE ノード間の PW 制御チャネルを確立します。

- エッジ間の疑似回線エミュレーション (PWE3) のシグナリングとカプセル化プロトコルが異なる場合。

PE ノードの接続先のネットワークでは、異なる PW シグナリングおよびカプセル化プロトコルが使用されています。場合によっては、1つのセグメント PW を使用できません。

マルチセグメント疑似回線は PW スwitching ポイントで適切なインターワーキングが実行されており、ネットワーク内の PE ノード間で PW 接続を有効にします。

疑似回線冗長性

疑似回線冗長性を使用すると、ネットワーク内の障害を検出して、サービスの提供を続行可能な別のエンドポイントにレイヤ2サービスを再ルーティングするようにネットワークを設定できます。この機能により、リモート PE ルータで発生した障害、または PE ルータと CE ルータ間のリンクで発生した障害から回復できます。

L2VPN は、ルーティングプロトコルを通じて疑似回線冗長化機能を提供します。エンドツーエンド PE ルータ間の接続が障害になった場合、指示された LDP セッションとユーザデータの代替パスに引き継ぐことができます。ただし、ネットワークの一部は、この再ルーティングメカニズムでサービスの中断から保護されません。

疑似回線冗長性を使用すると、バックアップ疑似回線を設定できます。ネットワークに冗長疑似回線と冗長ネットワーク エlement を設定することもできます。

プライマリ疑似回線の障害前に、バックアップ疑似回線にトラフィックをスイッチングする機能が使用され、ルータのメンテナンスなどの計画された疑似回線の停止が処理されます。



(注) 疑似回線冗長性は、ポイントツーポイントの Virtual Private Wire Service (VPWS) 疑似回線に対してのみ提供されます。

疑似回線のロードバランシング

冗長性を維持しつつ、ネットワークを最大限利用するには、通常、複数のリンクでのトラフィックのロードバランシングが必要です。精度の高い、より均等な分散を実現するには、プロビジョニングされたパイプの一部であるトラフィックフローのロードバランシングが理想的です。ロードバランシングは、IPアドレス、Macアドレス、またはそれらの組み合わせに従い、フローベースにすることができます。またロードバランシングは、送信元または宛先のIPアドレス、あるいは送信元または宛先のMACアドレスに従い、フローベースにすることができます。IPヘッダーの処理に進むことができない場合、またはIPv6がフローベースの場合、トラフィックはデフォルトのフローベースMACアドレスにフォールバックします。

この機能は、L2VPN下の疑似回線に適用されます。これには、VPWSとVPLSが含まれます。



(注) 疑似回線クラスに対し仮想回線（VC）ラベルベースのロードバランシングをイネーブルにすると、L2VPN下のグローバルフローベースのロードバランシングが上書きされます。

疑似回線のグループ化

疑似回線（PW）が確立されると、各PWに、すべてのPWに共通するグループIDが割り当てられます。このグループIDは、同一の物理ポートで作成されます。物理ポートが機能しなくなった場合や無効になった場合は、自動保護スイッチング（APS）がピアルータに対してアクティブになるように信号を送り、L2VPNが単一のメッセージを送信して、物理ポートに関連付けられたグループIDを持つすべてのPWのステータス変更をアドバタイズします。単一のL2VPN信号であることにより、応答での煩雑な処理や切断を防ぐことができます。

CEMインターフェイスでは、フレーム化または非フレーム化T1およびT3などの親コントローラに対して、さまざまなレベルの設定が許可されます。最適なグループ化を行うために、物理コントローラのハンドルがグループIDとして使用されます。



(注) 疑似回線のグループ化はデフォルトでディセーブルです。

疑似回線のネットワークコンバージェンスには、次のようなイベントでは通常の2秒よりも長くかかる場合があります。

- アクティブな動作ルータの手動リロード
- インターフェイスまたはコントローラのシャットダウン
- 有効な保護ルータでのラインカードのリロード、シャットダウン、または電源遮断
- 有効な保護ルータでのルータプロセッサフェールオーバー（RPFO）
- 2つのコントローラまたは共有ポートアダプタ（SPA）の同時障害
- 2つの自動保護スイッチング（APS）グループスイッチオーバー

イーサネットワイヤサービス

イーサネットワイヤサービスは、ポイントツーポイントのイーサネットセグメントをエミュレートするサービスです。これは、プロバイダーエッジがレイヤ2で動作し、通常レイヤ2ネットワークで実行される以外、イーサネット専用回線（EPL）、レイヤ1ポイントツーポイントサービスに似ています。EWSは特定のUNIで受信されたすべてのフレームをカプセル化し、フレームに含まれる内容を参照せずに、これらのフレームを単一出力UNIに転送します。このサービスの動作はEWSをVLANタグ付きフレームで使用できることを示します。VLANタグは、一部の例外を除いてEWS（ブリッジプロトコルデータユニット（BPDU））に対して透過的です。これらの例外には、IEEE 802.1x、IEEE 802.2ad、およびIEEE 802.3xが含まれます。これは、これらのフレームがローカルで意味を持ち、カスタマーとサービスプロバイダーの両方がそれらのフレームをローカルで終了できるよう支援されるためです。

サービスプロバイダーはインターフェイスでフレームを単純に受け取り、実際のフレームを参照せずにこれらを送信するため（ただし、形式と長さが特定のインターフェイスに適合していることは確認します）、EWSはカスタマーのイーサネットフレーム内にあるVLANタグに関与しません。

EWSはall-to-oneバンドリングの概念に対応しています。つまり、EWSはポイントツーポイント回線の一方のエンドのポートと他方のエンドのポートをマッピングします。EWSはポート間サービスです。したがって、カスタマーが1つのスイッチまたはルータをn個のスイッチまたはルータに接続する必要がある場合は、n個のポートおよびn個の疑似回線または論理回線が必要になります。

考慮すべき1つの重要なポイントは、EWSはイーサネットレイヤ1接続を広範にエミュレートするにもかかわらず、サービスは共有インフラストラクチャで提供され、したがって、すべてのインターフェイス帯域幅を常に使用できる可能性は低く、またそのようにする必要もないということです。EWSは、通常、多くのユーザが伝送パスのどこかで回線を共有する、サブラインレートサービスです。その結果、コストがEPLのコストよりも、ほとんどの場合、小さくなります。SPは、レイヤ1EPLとは異なり、特定契約の特定目的を達成するために、QoSおよびトラフィックエンジニアリングを実装する必要があります。ただし、カスタマーアプリケーションに本当の意味でのワイヤレート透過サービスが必要な場合、DWDM（高密度波長分割多重）、CDWM（低密度波長分割多重）、SONET/SDHなどの光送信デバイスを使用して提供されるEPLサービスを検討する必要があります。

IGMP スヌーピング

IGMP スヌーピングは、レイヤ2でマルチキャストトラフィックを抑制する方法を提供します。IGMPスヌーピングアプリケーションは、ブリッジドメインのホストによって送信されたIGMPメンバーシップレポートをスヌーピングすることで、レイヤ2マルチキャスト転送テーブルを設定して、少なくとも1つの関係メンバーを持つポートだけにトラフィックを送信できます。これにより、マルチキャストトラフィックの量が大幅に削減されます。

IGMPは、レイヤ3で設定され、IPv4マルチキャストネットワーク内のホストが、関与するマルチキャストトラフィックを通知する手段、ルータがレイヤ3のネットワーク内のマルチキャストトラフィックのフローを制御および制限する手段を提供します。

IGMP スヌーピングは、IGMP メンバーシップ レポート メッセージの情報を使用して、対応する情報を転送テーブルに構築し、レイヤ 2 の IP マルチキャスト トラフィックを制限します。転送テーブルのエントリは<ルート, OIF リスト> という形式で、

- ルートは <*, G> ルートまたは <S, G> ルートです。
- OIF リストは、指定されたルートと、ブリッジドメイン内のすべてのマルチキャスト ルータ (mrouter) ポートに関する IGMP メンバーシップ レポートを送信したすべてのブリッジ ポートで構成されます。

IGMP スヌーピング機能により、マルチキャスト ネットワークで次の利点が得られます。

- 基本的な IGMP スヌーピングは、VPLS ブリッジドメイン全体をフラッドするマルチキャスト トラフィックを削減することで、帯域幅の使用量を減らします。
- オプションの設定オプションを使用すると、IGMP スヌーピングは、1つのブリッジ ポートでホストから受信された IGMP レポートをフィルタリングし、他のブリッジポートでホストへの漏出を防止することで、ブリッジドメイン間のセキュリティを確保できます。
- オプションの設定オプションを使用すると、IGMP スヌーピングは、IGMP メンバーシップ レポート (IGMPv2) を抑制することで、またはアップストリーム IP マルチキャスト ルータへの IGMP プロキシレポート (IGMPv3) として動作することで、アップストリーム IP マルチキャスト ルータへのトラフィックの影響を低減できます。

IGMP スヌーピングの設定方法については、『Cisco ASR 9000 Series Aggregation Services Router Multicast Configuration Guide』の「Implementing Layer 2 Multicast with IGMP Snooping」モジュールを参照してください。

適用できる IGMP スヌーピングコマンドは『Cisco ASR 9000 Series Aggregation Services Router Multicast Command Reference』で説明します。

IP インターワーキング

カスタマー環境では、ソリューションによりネットワーク終端で異種転送を使用する AToM をサポートする必要があります。このソリューションには、1つのカスタマー エッジ (CE) デバイスの転送を別の転送に変換する機能 (たとえば、フレームリレーからイーサネットなど) が必要です。Cisco ASR 9000 シリーズ SPA インターフェイスプロセッサ 700 および Cisco ASR 9000 シリーズイーサネット ラインカードにより、Cisco ASR 9000 シリーズ ルータで複数のレガシーサービスをサポートできます。

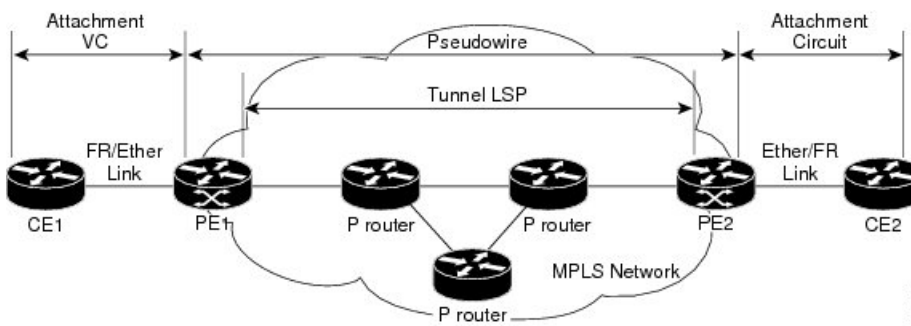
IP インターワーキングは、IP/MPLS バックボーン上でレイヤ 2 トラフィックを転送するためのソリューションです。IP インターワーキングは、AToM トンネルを使用するイーサネット、フレームリレーなど、多くのタイプのレイヤ 2 フレームに対応します。IP インターワーキングは、プロバイダー エッジ (PE) ルータでパケットをカプセル化し、それらをバックボーンを介してクラウドの反対側の PE ルータに転送し、カプセル化を削除し、それらを宛先に転送します。トランスポート層では、一方の側でイーサネットを使用し、もう一方の側でフレームリレーを使用できます。IP インターワーキングは、AToM トンネルの異種エンドポイント間で実行されます。



(注) MPLS とローカル接続のシナリオでは、イーサネットとフレーム リレー ベースのネットワーク間でルーテッド インターワーキングのみサポートされます。

次の図は、イーサネット接続 VC とフレームリレー接続 VC 間の相互運用性を表しています。

図 8: MPLS コア上の IP インターワーキング



接続回線は (AC) は、CE デバイスを PE デバイスに接続する物理的または論理的なポートまたは回線です。疑似回線 (PW) は、2つの AC を接続する双方向仮想接続 (VC) です。MPLS ネットワークでは、PW は LSP トンネル内で伝送されます。PE1 および PE2 のコア方向のラインカードとして、Cisco ASR 9000 シリーズ SPA インターフェイス プロセッサ 700 または Cisco ASR 9000 シリーズ イーサネット ラインカードが使用可能です。

IP インターワーキング モードでは、入力 PE で受信されたパケットからレイヤ 2 (L2) ヘッダーが削除され、IP ペイロードだけが出力 PE に送信されます。出力 PE では、パケットが出力ポートから送信される前に、L2 ヘッダーが付加されます。

上の図では、CE1 および CE2 を、フレームリレー (FR) インターフェイスまたはギガビットイーサネット (GigE) インターフェイスにすることができます。CE1 が FR で、CE2 が GigE または dot1q、あるいは QinQ であるとしします。イーサネット CE (CE2) から着信するパケットの場合、CE 方向の PE (PE2) の入力 LC は、L2 フレーミングを削除し、そのパケットを、疑似回線上で IPoMPLS カプセル化を使用して出力 PE (PE1) に転送します。出力 PE のコア方向のラインカードは、MPLS ラベルを削除しますが、制御ワードを保持し、それを FRCE (CE1) 方向の出力ラインカードに伝送します。FR PE では、ラベルディスポジション後、レイヤ 3 (L3) パケットは FR 上でカプセル化されます。

同様に、FR CE から着信した IP パケットは疑似回線上で IPoMPLS カプセル化に変換されます。コアから着信するパケットは IP ペイロードのみを伝送するため、イーサネット PE 側では、ラベルディスポジション後、PE は、パケットを CE に伝送する前に、そのパケットに L2 イーサネット パケット ヘッダーを追加して戻します。

これらのモードは、AToM で IP インターワーキングをサポートします。

• イーサネットとフレームリレー

イーサネット CE デバイスから着信するパケットには、MAC (ポートモード、タグなし、シングル タグ、ダブル タグ)、IPv4 ヘッダー、およびデータが含まれます。イーサネット ラインカードは L2 フレーミングを削除し、その後、出力ラインカードに L3 パケット

を転送します。出力ラインカードは、出力ポートからパケットを送信する前に、FR L2 ヘッダーを追加します。

- イーサネットとイーサネット

CE デバイスは両方ともイーサネットです。各イーサネットインターフェイスは、ポートモード、タグなし、シングルタグ、またはダブルタグにすることができます。ただし、これは IP インターワーキングの一般的なシナリオではありません。

AToM iMSG

この機能により、アクセス ネットワーク内のインターワーキング レイヤですべての非イーサネット機能を終了し、これらの接続を、レイヤ3 エッジルータで終端可能なイーサネットセントリック サービスに変換することができます。現在は、時分割多重 (TDM) ベースのサービスはレイヤ3 エッジルータ上で直接終端しています。L3 ネットワークの簡素でより低コストなモデルは、TDM の複雑さをアクセス レイヤに移動することによってイネーブルになります。

レイヤ2 カプセル化は、入力ラインカード側の入力 PE の接続回線によって IP パケットから削除されます。MPLS カプセル化された IP パケットのペイロードは、ファブリックで出力ラインカード側のコアに送信されます。出力ラインカードは MPLS コアを介してパケットを送信します。リモート PE では、MPLS ラベルが削除され、出力 AC のレイヤ2 ヘッダーが追加されて、パケットは最終的に接続された CE に送信されます。L2VPN VPWS は、次をサポートするように拡張されました。

- ポイントツーポイントプロトコル (PPP)
- ハイレベル データリンク コントロール (HDLC)
- マルチリンク ポイントツーポイントプロトコル (MLPPP)
- すべてのカプセル化タイプの QoS サポート

QoS の詳細については、『Cisco ASR 9000 Series Aggregation Services Router Modular Quality of Service Configuration』を参照してください。

TDM AC は、次の SPA で設定できます。

- SPA-8XCHT1/E1
- SPA-4XCT3/DS0
- SPA-1XCHSTM1/OC3
- SPA-2XCHOC12/DS0
- SPA-1XCHOC48/DS3
- SPA-4XT3/E3
- SPA-4XOC3-POS-V2
- SPA-8XOC3-POS
- SPA-8XOC12-POS

- SPA-1XOC48POS/RPR
- SPA-2XOC48POS/RPR

Any Transport over MPLS

Any Transport over MPLS (AToM) は、マルチプロトコル ラベル スイッチング (MPLS) バックボーン上でレイヤ2パケットを転送します。これにより、サービスプロバイダーは、単一の統合されたパケット ベース ネットワーク インフラストラクチャを使用することで、既存のレイヤ2 ネットワークとカスタマー サイトを接続できます。この機能を使用すると、サービスプロバイダーは、別々のネットワークを使用する代わりに、MPLS バックボーン上でレイヤ2 接続を提供できます。

AToM は、入力 PE ルータでレイヤ2 フレームをカプセル化し、2つの PE ルータ間を接続する疑似回線の反対側に位置する対応した PE ルータにそれらを送信します。出力 PE はカプセル化を削除し、レイヤ2 フレームを送信します。

PE ルータ間でレイヤ2 フレームを正常に転送するには、PE ルータを設定する必要があります。ルータ間で、疑似回線と呼ばれる接続を設定します。各 PE ルータで次の情報を指定します。

- イーサネットやフレームリレーなどの疑似回線で転送されるレイヤ2 データのタイプ。
- PE ルータが通信できる、ピア PE ルータのループバック インターフェイスの IP アドレス。
- 疑似回線を識別するピア PE の IP アドレスと VC ID の一意の組み合わせ。

コントロールワード処理

フレームリレー接続の場合、コントロールワードには、順方向明示的輻輳通知 (FECN)、逆方向明示的輻輳通知 (BECN)、および DE ビットが含まれます。

コントロールワードは次で必須です。

- フレーム リレー
- ATM AAL5
- Frame Relay to Ethernet ブリッジ型インターワーキング
- cHDLC/PPP IP インターワーキング
- CEM (回線エミュレーション)

システムは、AToM IP インターワーキング接続を介して、転送エンドポイントから別のエンドポイントにビットをマッピングしません。

コントロールワードがサポートされている場合も、疑似回線のために常に使用することをお勧めします。これは、L2VPN パケットの内容とは関係なく、パケットのデシーケンシングなしで適切なロードバランシングを実行できるためです。コントロールワードがない場合、ロード

バランシングを実行するために使用されるヒューリスティックでは、どのケースでも最適な結果を達成できません。

High-Level Data Link Control over MPLS

接続回線（AC）は、HDLCカプセル化が設定されたメインインターフェイスです。ACとの間のパケットは、MPLS コア ネットワーク上の他のプロバイダーエッジ（PE）との間の、VC タイプ 0x6 の疑似回線（PW）を使用して転送されます。

HDLC over MPLS では、HDLC パケット全体が転送されます。入力 PE ルータは、HDLC フラグおよび FCS ビットだけを削除します。

PPP over MPLS

接続回線（AC）は、PPPカプセル化が設定されたメインインターフェイスです。ACとの間で送受信されるパケットは、MPLS コア ネットワーク上の他のプロバイダーエッジ（PE）との間で、VC タイプ 0x7 の AToM PW を介して転送されます。

PPP over MPLS の場合、入力 PE ルータはフラグ、アドレス、制御フィールド、および FCS ビットを削除します。

Frame Relay over MPLS

Frame Relay over MPLS（FRoMPLS）は、2つのフレームリレーアイランド間の専用回線タイプの接続を提供します。フレームリレートラフィックはMPLS ネットワーク上で転送されます。



(注) データリンク接続識別子（DLCI）の DLCI-DLCI モードがサポートされます。追加の制御情報を伝えるために、制御ワード（DLCI-DLCI モードに必要）が使用されます。

プロバイダーエッジ（PE）ルータは、加入者サイトからフレームリレープロトコルパケットを受信すると、フレームリレーヘッダーおよびフレームチェックシーケンス（FCS）を削除し、関連する仮想回線（VC）ラベルを付けます。削除された逆方向明示的輻轉通知（BECN）、順方向明示的輻轉通知（FECN）、廃棄適性（DE）、およびコマンド/応答（C/R）ビットが制御ワードを使用して個別に送信されます（DLCI-DLCI モードの場合）。

MPLS トランスポート プロファイル

MPLS トランスポート プロファイル（MPLS-TP）トンネルは、IP および MPLS トラフィックが通過する転送ネットワーク サービス レイヤを提供します。MPLS-TP 環境内では、疑似回線（PW）は MPLS-TP トンネルを転送メカニズムとして使用します。MPLS-TP トンネルは、SONET/SDH TDM テクノロジーからパケットスイッチングへの移行に役立つとともに、サービスの高帯域幅での使用と低コスト化をサポートします。転送ネットワークは、接続指向型で静的にプロビジョニングされ、寿命の長い接続を持ちます。通常、転送ネットワークは、ラベ

ルなどの ID を変更する制御プロトコルを回避します。MPLS-TP トンネルは、静的にプロビジョニングされた双方向ラベル スイッチドパス (LSP) を介してこの機能を提供します。

MPLS トランспортプロファイルの設定方法の詳細については、『Cisco ASR 9000 Series Aggregation Services Router MPLS Configuration Guide』を参照してください。

MPLS-TP は、次のスタティックおよびダイナミックなマルチセグメント疑似回線の組み合わせをサポートします。

- スタティック - スタティック
- スタティック - ダイナミック
- ダイナミック - スタティック
- ダイナミック - ダイナミック

MPLS-TP は、次のスタティックおよびダイナミック疑似回線の組み合わせで 1 対 1 L2VPN 疑似回線冗長性をサポートします。

- スタティック疑似回線とスタティック バックアップ疑似回線
- スタティック疑似回線とダイナミック バックアップ疑似回線
- ダイナミック疑似回線とスタティック バックアップ疑似回線
- ダイナミック疑似回線とダイナミック バックアップ疑似回線

既存の TE 優先パス機能は、PW を MPLS-TP 転送トンネルにピン ダウンするために使用します。優先トンネルパスの設定の詳細については、「[優先トンネルパス](#)」を参照してください。ダイナミック疑似回線では、PW ステータスは LDP によって交換されますが、スタティック PW では、ステータスは PW OAM メッセージに転送されます。PW ステータス OAM の設定の詳細については、「[PW ステータス OAM の設定](#)」を参照してください。デフォルトでは、PW を伝送する MPLS TP トンネルのステートの変化によって PW のステートが変化する場合、アラームは生成されません。

Circuit Emulation Over Packet Switched Network

Circuit Emulation over Packet (CEoP) は、パケットスイッチドネットワークで TDM 回線を伝送する方法です。CEoP は物理接続に似ています。CEoP の目標は、専用回線およびレガシー TDM ネットワークを置き換えることです。

CEoP は主に次の 2 つのモードで動作します。

- SAToP (Structure Agnostic TDM over Packet) と呼ばれる非構造化モード

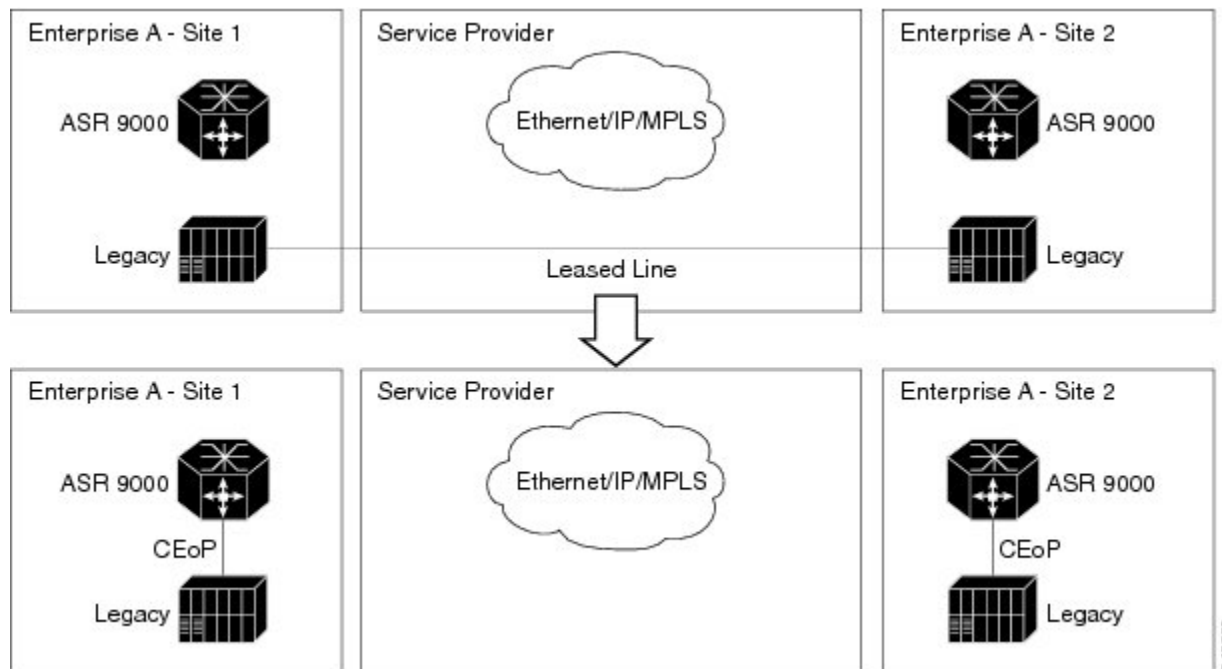
SAToP は、非フレーム化 E1、T1、E3 および T3 などの構造にとらわれない転送だけをアドレス指定します。これにより、すべての TDM サービスはビットストリームに分割され、PW トンネルでの送信用にカプセル化されます。このプロトコルは、TDM トラフィック データおよび同期タイミング情報を透過的に送信できます。SAToP は完全に構造を無視するため、プロバイダー エッジ (PE) ルータは、TDM データを解釈したり TDM シグ

ナリングに参加したりする必要がありません。このプロトコルは PDH ビットストリームを透過的に送信するための簡単な方法です。

- CESoPSN (Circuit Emulation Service over Packet Switched Network) という名前の構造化モード

SAToP と違い、CESoPSN は、エミュレートされた構造化 TDM 信号を送信します。つまり、TDM フレームのフレーム構造を識別して処理し、シグナリングを送信できます。これはアイドルタイムスロットチャンネルを送信しない場合がありますが、E1 トラフィックストリームから CE デバイスの有用なタイムスロットのみを抽出し、伝送用に PW パケットにカプセル化します。CEoP SPA は、ハーフハイト (HH) の共有ポートアダプタ (SPA) です。CEoP SPA ファミリーは、非構造化/構造化 (NxDS0) クォータレート、ハーフハイト SPA である 24xT1/E1、2xT3/E3、および 1xOC3/STM1 で構成されます。

図 9: Circuit Emulation over Packet を使用した企業データのコンバージェンス



CEM機能は、CEoP SPAを持つEngine5ラインカードでのみサポートされています。CEMは、次でサポートされています。

- 1ポートチャネライズド OC3 STM1 ATM CEoP SPA (SPA-1CHOC3-CE-ATM)

CESoPSN および SAToP は、基礎となる転送メカニズムとして MPLS、UDP/IP、および L2TPv3 を使用できます。このリリースでは、MPLS 転送メカニズムだけをサポートしています。

CEoP SPA は次の動作モードをサポートしています。

- 回線エミュレーションモード (CEM)
- ATMモード

- IMA モード



(注) サポートされるのは CEM モードだけです。

Circuit Emulation over Packet Switched Network の利点

CEM はサービスプロバイダーとエンドユーザに次の利点を提供します。

- 機器の設置のコスト削減します。
- ネットワーク運用のコストを削減します。高価な専用回線で、コストを節約するモードだけにアクセスを制限する必要がなくなります。
- メンテナンスが必要なのはコア ネットワークだけのため、メンテナンス コストを抑制できます。
- 投資をアクセス ネットワーク全体にとどめたまま、パケット スイッチド ネットワークでコア ネットワークのリソースをより効率的に利用できます。
- エンドユーザにより安価なサービスを提供できます。

L2VPN ノンストップルーティング

L2VPN ノンストップルーティング (NSR) 機能により、プロセス障害 (クラッシュ) やルートプロセッサフェールオーバー (RPFO) などの、イベントのフラッピングによるラベル配布パス (LDP) セッションを回避できます。NSR プロセス障害スイッチオーバーを使用して NSR をイネーブルにした場合、RPFO を実行することによって、プロセス障害 (クラッシュ) での NSR がサポートされます。

NSR は、障害が発生したルータについて、グレースフルリスタート (GR) なしでコントロールプレーンステートを維持できます。NSR は、定義上、プロトコル拡張の必要がないため、通常はステートフルスイッチオーバー (SSO) を使用してコントロールプレーンステートを維持します。



(注) NSR は、Cisco IOS XR 64 ビット オペレーティング システムの L2VPN ではデフォルトで有効になっています。L2VPN コンフィギュレーション サブモードでは **nsr** コマンドを設定できません。

L2TPv3 over IPv6

L2TPv3 over IPv6 トンネルは、L2TPv3 (レイヤ2 トンネリング プロトコルバージョン3) over IPv6 を使用する静的 L2VPN クロスコネクタであり、クロスコネクタごとに一意の IPv6 送信元アドレスを持ちます。L2TPv3 over IPv6 トンネルは、サブスクリバ VLAN ごとに1つの

L2TPv3 トンネルで構成されます。一意の IPv6 アドレスにより、顧客と配信されるサービスを完全に識別できます。



(注) L2TPv3 over IPv6 トンネルは、ASR 9000 拡張イーサネットラインカードで、ルータおよびラインカードごとに 15000 クロスコネクットの規模でサポートされています。



(注) nV サテライト アクセス インターフェイスは、L2TPv3 over IPv6 をサポートしていません。

概要

L2TPv3 は、レイヤ2バーチャルプライベートネットワーク (VPN) を使用して、IP コアネットワークを介して、レイヤ2ペイロードをトンネリングするための L2TP プロトコルを定義します。2つの顧客のネットワークサイト間のトラフィックが、L2TP データメッセージ (ペイロード) を伝送する IP パケット内にカプセル化され、IP ネットワーク経由で送信されます。IP ネットワークのバックボーンルータは、他の IP トラフィックの処理方法と同じ方法で、このペイロードを処理します。L2TPv3 over IPv6 を実装すると、一意の送信元 IPv6 アドレスを利用してイーサネット接続回線を直接識別することができます。この場合、L2TPv3 セッション ID の処理はバイパスされます。これは、各トンネルに関連付けられるセッションが1つだけであるためです。ただし、このローカル最適化は、同じルータ上の他の L2TPv3 トンネルのセッション ID を通じて回線の多重化を引き続きサポートする能力の妨げにはなりません。

詳細については、次を参照してください。

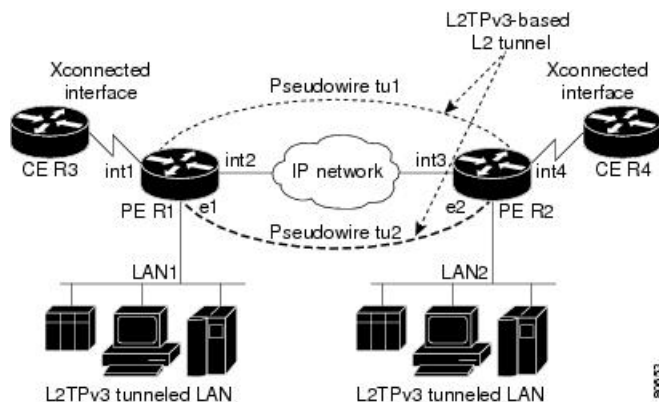
- 設定手順については、「[L2TPv3 over IPv6 トンネルの設定](#)」を参照してください。
- 設定例については、「[L2TPv3 over IPv6 トンネルの設定 : 例](#)」を参照してください。

L2TPv3 over IPv4

L2TPv3 (レイヤ2 トンネリング プロトコルバージョン3) over IPv4 は、L2TPv3 セッション ID を回線識別子として使用して、複数の接続回線が1組の IP アドレスエンドポイントで多重化される、パケット指向のデータネットワークを介してレイヤ2 (L2) 回線をトンネリングする動的メカニズムを提供します。

下の図に、IP ネットワーク上のレイヤ2 トンネリングを使用して VPN をセットアップするための L2TPv3 機能の使用方法を示します。2つのカスタマー ネットワーク サイト間のすべてのトラフィックが、L2TP データメッセージを伝送する IP パケット内にカプセル化され、IP ネットワーク経由で送信されます。IP ネットワークのバックボーンルータは、そのトラフィックを他の IP トラフィックとして処理し、顧客のネットワークのことを何も知る必要がありません。

図 10: L2TPv3 の動作



上の図では、PE ルータ R1 と R2 が L2TPv3 サービスを提供しています。R1 ルータと R2 ルータは、インターフェイスの int1 と int2、IP ネットワーク、およびインターフェイスの int3 と int4 を構成するパスを通る IP バックボーンネットワーク上の疑似回線を使用して相互に通信します。CE ルータの R3 と R4 がクロスコネクされたイーサネットのペアまたは L2TPv3 セッションを使用した 802.1q VLAN インターフェイス経由で通信します。L2TPv3 セッションの tu1 は、R1 上のインターフェイス int1 と R2 上のインターフェイス int4 間に設定された疑似回線です。R1 上のインターフェイス int1 に到着したすべてのパケットが、カプセル化され、疑似回線コントロールチャネル (tu1) 経由で R2 に送信されます。R2 でパケットがカプセル解放され、インターフェイス int4 経由で R4 に送信されます。R4 から R3 にパケットを送信する必要がある場合は、パケットが同じパスを逆にたどります。



(注) L2TPv3 over IPv4 機能は、Cisco ASR 9000 高密度 100GE イーサネットラインカードのみでサポートされています。



(注) nV サテライト アクセス インターフェイスは、L2TPv3 over IPv4 をサポートしていません。

詳細については、次を参照してください。

- 設定手順については、「[L2TPv3 over IPv4 トンネルの設定 \(104 ページ\)](#)」を参照してください。
- 設定例については、「[L2TPv3 over IPv4 トンネルの設定：例 \(136 ページ\)](#)」を参照してください。

動的セグメント疑似回線

単一セグメント疑似回線 (SS-PW) は、2 つの PE ルータ間に PW セグメントが存在するポイントツーポイント疑似回線 (PW) です。

この機能では、FEC 129 情報を動的に使用して、同じ自律システム (AS) の 2 つの PE ルータ間に単一セグメント疑似回線が確立されます。この機能の目的は、シスコ製ルータとサードパーティ製ルータとの相互運用性を確保することです。

アクティブシグナリングとパッシブシグナリング

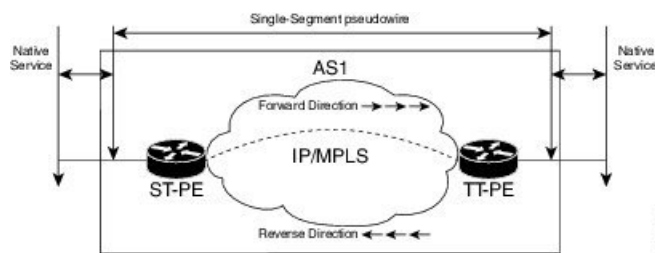
SS-PW が開始され、シグナリングメッセージの送信元となる T-PE は、送信元終端 PE (ST-PE) と呼ばれます。SS-PW シグナリングメッセージを待ち受けて応答する T-PE は、送信先終端 PE (TT-PE) と呼ばれます。

ST-PE から TT-PE へのシグナリングフローは、順方向シグナリングまたはアクティブシグナリングと呼ばれます。TT-PE から ST-PE へのシグナリングフローは、逆方向シグナリングまたはパッシブシグナリングと呼ばれます。

一般的に、プレフィックスアドレスが最も大きい PE がアクティブの役割を果たして ST-PE となり、他の PE はパッシブの TT-PE となります。

次の図は、ST-PE と TT-PE の間の SS-PW シグナリングフローを示しています。

図 11: ST-PE と TT-PE の間の単一セグメント疑似回線



動的単一セグメント疑似回線の機能

ST-PE から TT-PE への疑似回線パスの動的検出は、L2 ルートテーブルを使用して実現されます。ルートテーブルのエントリ (つまり、プレフィックスと、関連付けられた L2VPN へのネクストホップのリスト) は、BGP によって入力されます。

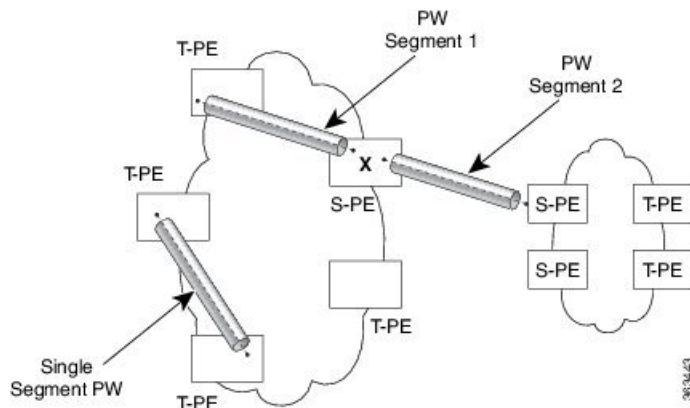


- (注) リリース 5.1.2 では、本シスコ製品は T-PE 上の TAIL に到達するためのルーティング可能なプレフィックスのみをサポートしています。ルーティング可能なプレフィックスは、ターゲット LDP セッションのネイバーアドレスです。送信元から宛先へのパケットの到達可能性は、ユーザ設定によって実現されます (L2VPN 単一セグメント疑似回線の設定 (25 ページ) を参照)。ただし、BGP は、すべての PE 間で L2 ルートを交換するために使用される MS-PW の後続アドレスファミリ識別子 (SAFI) をサポートしています。SS-PW は、BGP MS-PW アドレスファミリを使用して機能します。他のサードパーティルータとの相互運用性を確保するために、本シスコ製品は T-PE ごとに単一の BGP MS-PW ルートをアドバタイズします。ここで、AC-ID (接続回線識別子) の値はワイルドカードエントリです。

サポートされている疑似回線機能は、pw-status、pw-grouping、および tag-impose vlan です。

次の図は、SS-PW を使用した E-line サービスネットワークを示しています。

図 12: SS-PW を使用した E-Line サービスネットワーク



L2VPN 単一セグメント疑似回線の設定に関する前提条件

MPLS LDP、IGP、BGP、L2VPN、およびインターフェイスを、PW の2つのエンドポイントで設定する必要があります。

- MPLS ラベル配布プロトコルを設定します。
- 内部ゲートウェイプロトコル (IGP) を設定します。
- ボーダー ゲートウェイ プロトコル (BGP) を設定します。
- L2VPN のインターフェイスまたは接続を設定します。

L2VPN 単一セグメント疑似回線の設定に関する制限事項

- ルーテッド疑似回線は、Virtual Private Wire Service (VPWS) クロスコネクタでのみ有効にできます。
- クロスコネクタでは、両端を「ネイバルルーテッド」疑似回線として設定することはできません。
- SS-PW はクロスコネクタの両端には設定できません。つまり、T-PE では、クロスコネクタの一方の端が SS-PW の終端となり、もう一方の端は接続回線 (AC) または PW-HE である可能性があります。
- 送信元 AII と AC-ID (接続回線識別子) は、ルータごとに一意です。
- L2TP および MPLS スタティックはサポートされません。

L2VPN 単一セグメント疑似回線の設定

ネットワークで単一セグメント疑似回線を設定するには、次の手順を実行します。

1. (オプション) 関連する L2VPN グローバルパラメータの設定。 [[L2VPN グローバルパラメータの設定](#)] を参照してください

この手順は、デフォルトの BGP ルート識別子 (RD) 自動生成値と、BGP の自律システム番号 (ASN) およびルート識別子 (RID) を上書きするために使用します。

2. L2VPN VPWS SS-PW の設定
3. BGP の L2VPN MS-PW アドレスファミリの設定

アドレスファミリは、ダイナミック擬似回線ルートを交換するために BGP で設定されます。

L2VPN グローバルパラメータの設定

L2VPN グローバルパラメータを設定するには、次の作業を実行します。

手順の概要

1. **configure**
2. **l2vpn**
3. **router-id** *router-id*
4. **pw-routing**
5. **global-id** *global-id*
6. **bgp**
7. **rd** *route-distinguisher*
8. **commit** コマンドまたは **end** コマンドを使用します。

手順の詳細

ステップ 1 **configure**

例 :

```
RP/0/RSP0/cpu 0: router# configure
```

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 **l2vpn**

例 :

```
RP/0/RSP0/cpu 0: router(config)# l2vpn
```

レイヤ 2 VPN 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-id** *router-id*

例 :

```
RP/0/RSP0/cpu 0: router(config)# router 2.2.2.2
```

ルータ ID を指定します。

ステップ4 pw-routing

例：

```
RP/0/RSP0/cpu 0: router(config-l2vpn)# pw-routing
```

疑似回線ルーティング機能を有効にし、疑似回線ルーティング設定サブモードを開始します。

ステップ5 global-id global-id

例：

```
RP/0/RSP0/cpu 0: router(config-l2vpn-pwr)# global-id 1000
```

ルータの L2VPN グローバル ID 値を設定します。

ステップ6 bgp

例：

```
RP/0/RSP0/cpu 0: router(config-l2vpn-pwr)# bgp
```

BGP 疑似回線ルーティング機能を有効にし、BGP 設定サブモードを開始します。

ステップ7 rd route-distinguisher

例：

```
RP/0/RSP0/cpu 0: router(config-l2vpn-pwr-bgp)# rd 192.168.1.3:10
```

BGP ルート識別子を設定します。

ステップ8 commit コマンドまたは end コマンドを使用します。

commit：設定の変更を保存し、コンフィギュレーションセッションに留まります。

end：次のいずれかのアクションを実行することをユーザに要求します。

- [Yes]：設定変更を保存し、コンフィギュレーションセッションを終了します。
- [No]：設定変更をコミットせずにコンフィギュレーションセッションを終了します。
- [Cancel]：設定変更をコミットせずに、コンフィギュレーションモードに留まります。

L2VPN VPWS SS-PW の設定

L2VPN VPWS SS-PW を設定するには、次の作業を実行します。

手順の概要

1. configure

2. **interface type***interface-path-id*
3. **l2vpn**
4. **xconnect group** *group-name*
5. **p2p** *xconnect-name*
6. **interface type** *interface-path-id*
7. **neighbor routed** *global-id: prefix: ac-id source ac-id*
8. (オプション) **pw-class** *class-name*
9. **commit** コマンドまたは **end** コマンドを使用します。

手順の詳細

ステップ1 **configure**

例：

```
RP/0/RSP0/cpu 0: router# configure
```

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 **interface type***interface-path-id*

例：

```
RP/0/RSP0/cpu 0: routerRP/0/RP0RSP0/CPU0:router# interface TenGigE0/1/0/12
```

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、インターフェイスを設定します。

ステップ3 **l2vpn**

例：

```
RP/0/RSP0/cpu 0: router(config)# l2vpn
```

レイヤ2 VPN 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 **xconnect group** *group-name*

例：

```
RP/0/RSP0/cpu 0: router(config-l2vpn)# xconnect group pw-hel
```

自由形式の 32 文字ストリングを使用して、相互接続グループ名を設定します。

ステップ5 **p2p** *xconnect-name*

例：

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc)# p2p pw-ss
```

P2P コンフィギュレーション サブモードを開始します。

ステップ6 **interface type interface-path-id**

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p)# interface gigabitethernet 0/1/0/9
```

インターフェイス タイプとインスタンスを指定します。

ステップ7 **neighbor routed global-id: prefix: ac-id source ac-id**

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p)# neighbor routed 100:2.2.2.2:10 source 10
```

p2p クロスコネクットの疑似回線ルーティング設定サブモードを有効にします。

ステップ8 (オプション) **pw-class class-name**

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p-pwr)# pw-class dynamic_sspw
```

疑似回線クラス サブモードになり、疑似回線クラス テンプレートを定義できます。

ステップ9 **commit** コマンドまたは **end** コマンドを使用します。

commit : 設定の変更を保存し、コンフィギュレーションセッションに留まります。

end : 次のいずれかのアクションを実行することをユーザに要求します。

- [Yes] : 設定変更を保存し、コンフィギュレーションセッションを終了します。
- [No] : 設定変更をコミットせずにコンフィギュレーションセッションを終了します。
- [Cancel] : 設定変更をコミットせずに、コンフィギュレーションモードに留まります。

BGP の L2VPN MS-PW アドレスファミリの設定

BGP に L2VPN MS-PW アドレスファミリを設定するには、次の作業を実行します。

手順の概要

1. **configure**
2. **router bgp autonomous-system-number**
3. **address-family l2vpn mspw**
4. **neighbor ip-address**
5. **address-family l2vpn mspw**
6. **commit** コマンドまたは **end** コマンドを使用します。

手順の詳細

ステップ1 **configure**

例 :

```
RP/0/RSP0/cpu 0: router# configure
```

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 bgp autonomous-system-number**

例 :

```
RP/0/RSP0/cpu 0: router(config)# router bgp 100
```

指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。

ステップ3 **address-family l2vpn mspw**

例 :

```
RP/0/RSP0/cpu 0: router(config-bgp)# address-family l2vpn mspw
```

L2VPN アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。

ステップ4 **neighbor ip-address**

例 :

```
RP/0/RSP0/cpu 0: router(config-bgp)# neighbor 10.10.10.1
```

指定した自律システム内のネイバーの IP アドレスを追加します。

ステップ5 **address-family l2vpn mspw**

例 :

```
RP/0/RSP0/cpu 0: router(config-bgp-nbr-af)# address-family l2vpn mspw
```

ネイバーの L2VPN アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。

ステップ6 **commit** コマンドまたは **end** コマンドを使用します。

commit : 設定の変更を保存し、コンフィギュレーション セッションに留まります。

end : 次のいずれかのアクションを実行することをユーザに要求します。

- [Yes] : 設定変更を保存し、コンフィギュレーション セッションを終了します。
- [No] : 設定変更をコミットせずにコンフィギュレーション セッションを終了します。

- [Cancel] : 設定変更をコミットせずに、コンフィギュレーション モードに留まります。

EVPN 仮想プライベート ワイヤ サービス (VPWS)

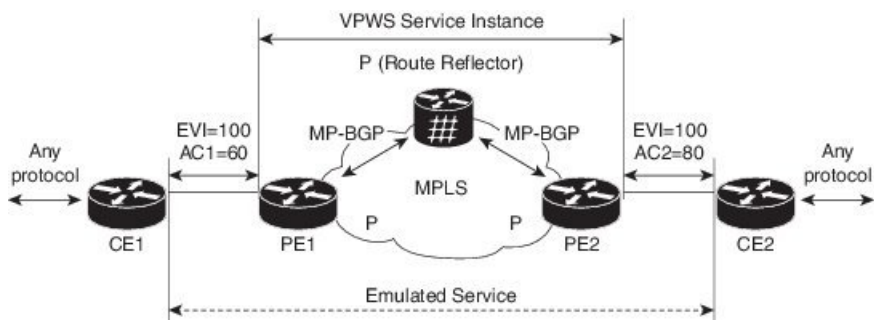
EVPN-VPWS は、ポイントツーポイント サービス用の BGP コントロールプレーン ソリューションです。これにより、PE のペア間で EVPN インスタンスを確立するためのシグナリング およびカプセル化技術が実装されます。EVPN-VPWS には、MAC ルックアップを使用せずに、あるネットワークから別のネットワークにトラフィックを転送する機能があります。VPWS 対応の EVPN により、ポイントツーポイント イーサネット サービスにおいてシングルセグメント およびマルチセグメント PW をシグナリングする必要がなくなります。また、EVPN-VPWS を使用して PWHE インターフェイスとブリッジドメインアクセス疑似回線を設定することもできます。

EVPN-VPWS シングルホームテクノロジーは、IP および MPLS コアで動作します。IP コアでは BGP がサポートされ、MPLS コアではエンドポイント間でのパケットのスイッチングがサポートされます。

EVPN-VPWS シングルホームに関する情報

EVPN-VPWS シングルホーム ソリューションは、EVI イーサネット自動検出ルートごとに必要です。EVPN は、すべての EVPN ルートの伝送に使用する新しい BGP ネットワーク層到達可能性情報 (NLRI) を定義します。BGP 機能アドバタイズメントを使用して、2つのスピーカーが RFC 4760 に従い、EVPN NLRI (AFI 25、SAFI 70) を確実にサポートするようにします。

EVPN VPWS のアーキテクチャでは、PE3 がコントロールプレーンでマルチプロトコル BGP を実行します。次に、EVPN-VPWS 設定を説明する図を示します。



- PE1 上の VPWS サービスには、設定時に指定する次の3つの要素が必要です。
 - VPN ID (EVI)
 - ローカル AC 識別子 (AC1) 。エミュレートされたサービスのローカルエンドを識別します。
 - リモート AC 識別子 (AC2) 。エミュレートされたサービスのリモートエンドを識別します。

PE1 は到達可能性を得るために、MPLS ラベルをローカル AC ごとに割り当てます。

- PE2 上の VPWS サービスは PE1 と同じ方法で設定されます。3 つの同じ要素が必要であり、サービス設定は対称になっている必要があります。

PE2 は到達可能性を得るために、MPLS ラベルをローカル AC ごとに割り当てます。

- PE1 は各ローカルエンドポイント (AC) の EVI イーサネット AD ごとの単一の EVPN を、関連付けられた MPLS ラベルを使用してリモート PE にアドバタイズします。

PE2 は同じタスクを実行します。

- PE2 から EVI EAD ルートごとの EVPN を受け取ると、PE1 はそのローカル L2 RIB にエントリーを追加します。PE1 は AC2 に到達するパスのリスト (たとえば、ネクスト ホップが PE2 の IP アドレスであること) と AC2 の MPLS ラベルを把握しています。

PE2 は同じタスクを実行します。

EVPN-VPWS の利点

EVPN-VPWS の利点は次のとおりです。

- 拡張性が、疑似回線のシグナリングなしで実現されます。
- プロビジョニングの容易さ
- 疑似回線 (PW) は使用されません。
- BGP のベストパス選択 (最適な転送) を活用します。

EVPN-VPWS の前提条件

- BGP が EVPN SAFI 用に設定されていることを確認します。
- EVPN ルートを交換するための「address-family l2vpn evpn」を使用した PE 間の BGP セッション。

EVPN-VPWS に関する制限事項

- VPN ID はルータごとに一意です。
- ルートターゲットのリストを指定する場合は、PE ごとに一意である必要があります (BGP アドレスファミリーごと)。

ポイントツーポイント レイヤ2サービスを実装する方法

このセクションでは、ポイントツーポイントレイヤ2サービスの実装に必要なタスクについて説明します。

ポイントツーポイントレイヤ2サービスのインターフェイスまたは接続の設定

ポイントツーポイントレイヤ2サービスのインターフェイスまたは接続を設定するには、次の作業を実行します。

手順の概要

1. **configure**
2. **interface** *type interface-path-id*
3. **l2transport**
4. **exit**
5. **interface** *type interface-path-id*
6. **commit** コマンドまたは **end** コマンドを使用します。
7. **show interface** *type interface-id*

手順の詳細

ステップ 1 **configure**

例：

```
RP/0/RSP0/cpu 0: router# configure
```

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 **interface** *type interface-path-id*

例：

```
RP/0/RSP0/cpu 0: router(config)# interface TenGigE 0/0/0/0
```

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、インターフェイスを設定します。

ステップ 3 **l2transport**

例：

```
RP/0/RSP0/cpu 0: router(config-if)# l2transport
```

選択したインターフェイスで L2 転送をイネーブルにします。

ステップ 4 **exit**

例：

```
RP/0/RSP0/cpu 0: router(config-if-l2)# exit
```

現在のコンフィギュレーションモードを終了します。

ステップ5 **interface** *type interface-path-id*

例：

```
RP/0/RSP0/cpu 0: router(config)# interface TenGigE 0/0/0/0
```

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、インターフェイスを設定します。

ステップ6 **commit** コマンドまたは **end** コマンドを使用します。

commit：設定の変更を保存し、コンフィギュレーションセッションに留まります。

end：次のいずれかのアクションを実行することをユーザに要求します。

- [Yes]：設定変更を保存し、コンフィギュレーションセッションを終了します。
- [No]：設定変更をコミットせずにコンフィギュレーションセッションを終了します。
- [Cancel]：設定変更をコミットせずに、コンフィギュレーションモードに留まります。

ステップ7 **show interface** *type interface-id*

例：

```
RP/0/RSP0/cpu 0: router show interface TenGigE 0/0/0/0
```

(任意) コミットしたインターフェイスの設定を表示します。

ローカルスイッチングの設定

ローカルスイッチングを設定するには、次の作業を実行します。

手順の概要

1. **configure**
2. **l2vpn**
3. **xconnect group** *group-name*
4. **p2p** *xconnect-name*
5. **interface** *type interface-path-id*
6. **interface** *type interface-path-id*
7. **commit** コマンドまたは **end** コマンドを使用します。

手順の詳細

ステップ1 **configure**

例：

```
RP/0/RSP0/cpu 0: router# configure
```

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 l2vpn

例 :

```
RP/0/RSP0/cpu 0: router(config-subif)# l2vpn
```

L2VPN 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 xconnect group *group-name*

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn)# xconnect group grp_1
```

クロスコネクト グループの名前を入力します。

ステップ4 p2p *xconnect-name*

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc)# p2p vlan1
```

ポイントツーポイント クロスコネクトの名前を入力します。

ステップ5 interface *type interface-path-id*

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p)# interface TenGigE 0/7/0/6.5
```

インターフェイス タイプ ID を指定します。選択できる基準は、次のとおりです。

- GigabitEthernet : ギガビット イーサネット/IEEE 802.3 インターフェイス
- TenGigE : TenGigabit イーサネット/IEEE 802.3 インターフェイス
- CEM : 回線エミュレーション インターフェイス

ステップ6 interface *type interface-path-id*

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p)# interface GigabitEthernet0/4/0/30
```

インターフェイス タイプ ID を指定します。選択できる基準は、次のとおりです。

- GigabitEthernet : ギガビット イーサネット/IEEE 802.3 インターフェイス
- TenGigE : TenGigabit イーサネット/IEEE 802.3 インターフェイス

ステップ7 **commit** コマンドまたは **end** コマンドを使用します。

commit : 設定の変更を保存し、コンフィギュレーションセッションに留まります。

end : 次のいずれかのアクションを実行することをユーザに要求します。

- [Yes] : 設定変更を保存し、コンフィギュレーションセッションを終了します。
- [No] : 設定変更をコミットせずにコンフィギュレーションセッションを終了します。
- [Cancel] : 設定変更をコミットせずに、コンフィギュレーションモードに留まります。

ローカル接続の冗長性の設定

ローカル接続の冗長性を設定するには、次の作業を実行します。

手順の概要

1. **configure**
2. **l2vpn**
3. **xconnect group** *group-name*
4. **p2p** *xconnect-name*
5. **backup interface** *type interface-path-id*
6. **interface** *type interface-path-id*
7. **interface** *type interface-path-id*
8. **commit** コマンドまたは **end** コマンドを使用します。

手順の詳細

ステップ1 **configure**

例 :

```
RP/0/RSP0/cpu 0: router# configure
```

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 **l2vpn**

例 :

```
RP/0/RSP0/cpu 0: router(config-subif)# l2vpn
```

L2VPN 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 **xconnect group** *group-name*

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn)# xconnect group grp_1
```

クロスコネクト グループの名前を入力します。

ステップ4 `p2p xconnect-name`

例：

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc) # p2p vlan1
```

ポイントツーポイント クロスコネクトの名前を入力します。

ステップ5 `backup interface type interface-path-id`

例：

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p) # backup interface Bundle-Ether 0/7/0/6.5
```

ローカル接続の冗長性を設定します。

(注) 接続回線 (AC) は、MCLAGに属するバンドルインターフェイスである必要があります。バックアップインターフェイスは、バンドルまたはイーサネットポートのいずれかです。

ステップ6 `interface type interface-path-id`

例：

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p) # interface Bundle-Ether 0/7/0/6.2
```

インターフェイス タイプ ID を指定します。選択できる基準は、次のとおりです。

- GigabitEthernet：ギガビットイーサネット/IEEE 802.3 インターフェイス
- TenGigE：TenGigabitイーサネット/IEEE 802.3 インターフェイス
- CEM：回線エミュレーションインターフェイス

ステップ7 `interface type interface-path-id`

例：

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p) # interface Bundle-Ether 0/7/0/6.1
```

インターフェイス タイプ ID を指定します。選択できる基準は、次のとおりです。

- GigabitEthernet：ギガビットイーサネット/IEEE 802.3 インターフェイス
- TenGigE：TenGigabitイーサネット/IEEE 802.3 インターフェイス

ステップ8 `commit` コマンドまたは `end` コマンドを使用します。

`commit`：設定の変更を保存し、コンフィギュレーションセッションに留まります。

`end`：次のいずれかのアクションを実行することをユーザに要求します。

- [Yes] : 設定変更を保存し、コンフィギュレーションセッションを終了します。
- [No] : 設定変更をコミットせずにコンフィギュレーションセッションを終了します。
- [Cancel] : 設定変更をコミットせずに、コンフィギュレーションモードに留まります。

スタティック ポイントツーポイント相互接続の設定



- (注) スタティック ポイントツーポイント クロスコネクトを設定する場合、クロスコネクトに関する次の情報を考慮します。
- 相互接続はペアにより一意に識別されます。相互接続名は、グループ内で一意である必要があります。
 - セグメント（接続回線または疑似回線）は一意で、1つの相互接続だけに属することができます。
 - スタティック VC のローカル ラベルはグローバルに一意で、1つの疑似回線だけで使用できます。
 - 1台のルータにつき 16,000 以下の相互接続を設定できます。



- (注) スタティック疑似回線接続はシグナリングに LDP を使用しません。

スタティック ポイントツーポイント相互接続を設定するには、次の作業を実行します。

手順の概要

1. **configure**
2. **l2vpn**
3. **xconnect group group-name**
4. **p2p xconnect-name**
5. **interface type interface-path-id**
6. **neighbor A.B.C.D pw-id pseudowire-id**
7. **mpls static label local { value } remote { value }**
8. **commit** コマンドまたは **end** コマンドを使用します。

手順の詳細

ステップ1 configure

例 :

```
RP/0/RSP0/cpu 0: router# configure
```

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 **l2vpn**

例 :

```
RP/0/RSP0/cpu 0: router(config)# l2vpn
```

L2VPN 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 **xconnect group group-name**

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn)# xconnect group grp_1
```

クロスコネクト グループの名前を入力します。

ステップ 4 **p2p xconnect-name**

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc)# p2p vlan1
```

ポイントツーポイント クロスコネクトの名前を入力します。

ステップ 5 **interface type interface-path-id**

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p)# interface gigabitethernet 0/1/0/9
```

インターフェイス タイプとインスタンスを指定します。

ステップ 6 **neighbor A.B.C.D pw-id pseudowire-id**

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p)# neighbor 10.2.2.2 pw-id 2000
```

クロスコネクトの疑似回線セグメントを設定します。

相互接続ピアの IP アドレスを指定するには、A.B.C.D 引数を使用します。

(注) A.B.C.D は再帰的または非再帰的プレフィックスです。

オプションで、コントロールワードをディセーブルにするか、イーサネットまたは VLAN に transport-type を設定できます。

ステップ7 `mpls static label local { value } remote { value }`

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p-pw)# mpls static label local 699 remote 890
```

ローカルおよびリモート ラベル ID 値を設定します。

ステップ8 `commit` コマンドまたは `end` コマンドを使用します。**commit** : 設定の変更を保存し、コンフィギュレーションセッションに留まります。**end** : 次のいずれかのアクションを実行することをユーザに要求します。

- [Yes] : 設定変更を保存し、コンフィギュレーションセッションを終了します。
- [No] : 設定変更をコミットせずにコンフィギュレーションセッションを終了します。
- [Cancel] : 設定変更をコミットせずに、コンフィギュレーションモードに留まります。

ダイナミック ポイントツーポイント相互接続の設定

ダイナミック ポイントツーポイント相互接続を設定するには、次の作業を実行します。



(注) ダイナミック相互接続では、LDP が稼働中である必要があります。

手順の概要

1. `configure`
2. `l2vpn`
3. `xconnect group group-name`
4. `p2p xconnect-name`
5. `interface type interface-path-id`
6. `neighbor A.B.C.D pw-id pseudowire-id`
7. `commit` コマンドまたは `end` コマンドを使用します。

手順の詳細

ステップ1 `configure`

例 :

```
RP/0/RSP0/cpu 0: router# configure
```

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 l2vpn

例：

```
RP/0/RSP0/cpu 0: router(config)# l2vpn
```

L2VPN 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 xconnect group group-name

例：

```
RP/0/RSP0/cpu 0: router(config-l2vpn)# xconnect group grp_1
```

クロスコネクト グループの名前を入力します。

ステップ4 p2p xconnect-name

例：

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc)# p2p vlan1
```

ポイントツーポイント クロスコネクトの名前を入力します。

ステップ5 interface type interface-path-id

例：

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p)# interface GigabitEthernet0/0/0/0.1
```

インターフェイス タイプ ID を指定します。選択できる基準は、次のとおりです。

- GigabitEthernet : GigabitEthernet/IEEE 802.3 インターフェイス。
- TenGigE : TenGigabitEthernet/IEEE 802.3 インターフェイス。
- CEM : 回線エミュレーション インターフェイス

ステップ6 neighbor A.B.C.D pw-id pseudowire-id

例：

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p)# neighbor 2.2.2.2 pw-id 2000
```

クロスコネクトの疑似回線セグメントを設定します。

オプションで、コントロールワードをディセーブルにするか、イーサネットまたは VLAN に transport-type を設定できます。

ステップ7 commit コマンドまたは end コマンドを使用します。

commit : 設定の変更を保存し、コンフィギュレーションセッションに留まります。

end : 次のいずれかのアクションを実行することをユーザに要求します。

- [Yes] : 設定変更を保存し、コンフィギュレーションセッションを終了します。
- [No] : 設定変更をコミットせずにコンフィギュレーションセッションを終了します。
- [Cancel] : 設定変更をコミットせずに、コンフィギュレーションモードに留まります。

Inter-AS の設定

Inter-AS の設定手順は、L2VPN 相互接続の設定作業と同じです（「[スタティックポイントツーポイント相互接続の設定](#)」セクションおよび「[ダイナミックポイントツーポイント相互接続の設定](#)」セクションを参照）。ただし、相互接続設定で使用されるリモート PE の IP アドレスは iBGP ピアリングを通じて到達可能です。



- (注) この設定を完了するには、IBGP、EBGP、および ASBR の用語および設定に関する知識が必要です。

L2VPN Quality of Service の設定

このセクションでは、ポートモード、VLAN モード、フレームリレーおよび ATM サブインターフェイスで L2VPN Quality of Service (QoS) を設定する方法について説明します。

機能制限

l2transport コマンドはすべての IP アドレス、L3、または CDP の設定で使用できません。

ポートモードでの L2VPN Quality of Service ポリシーの設定

この手順では、ポートモードでの L2VPN QoS ポリシーの設定方法について説明します。



- (注) ポートモードでは、インターフェイス名の形式に、サブインターフェイス番号が含まれません（たとえば、GigabitEthernet0/1/0/1）。

手順の概要

1. **configure**
2. **interface type interface-path-id**
3. **l2transport**
4. **service-policy [input | output] [policy-map-name]**
5. **commit** コマンドまたは **end** コマンドを使用します。
6. **show qos interface type interface-id service-policy [input | output] [policy-map-name]**

手順の詳細

ステップ1 **configure**

例：

```
RP/0/RSP0/cpu 0: router# configure
```

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 **interface type interface-path-id**

例：

```
RP/0/RSP0/cpu 0: router(config)# interface GigabitEthernet 0/0/0/0
```

インターフェイス接続回線を指定します。

ステップ3 **l2transport**

例：

```
RP/0/RSP0/cpu 0: router(config-if)# l2transport
```

L2 スイッチングのインターフェイスまたは接続を設定します。

ステップ4 **service-policy [input | output] [policy-map-name]**

例：

```
RP/0/RSP0/cpu 0: router(config-if)# service-policy input servpoll
```

入力インターフェイスまたは出力インターフェイスに、そのインターフェイスのサービスポリシーとして使用する QoS ポリシーを付加します。

ステップ5 **commit** コマンドまたは **end** コマンドを使用します。

commit : 設定の変更を保存し、コンフィギュレーションセッションに留まります。

end : 次のいずれかのアクションを実行することをユーザに要求します。

- [Yes] : 設定変更を保存し、コンフィギュレーションセッションを終了します。
- [No] : 設定変更をコミットせずにコンフィギュレーションセッションを終了します。
- [Cancel] : 設定変更をコミットせずに、コンフィギュレーションモードに留まります。

ステップ6 **show qos interface type interface-id service-policy [input | output] [policy-map-name]**

例：

```
RP/0/RSP0/cpu 0: router# show qos interface gigabitethernet 0/0/0/0 input servpoll
```

(任意) 定義した QoS サービス ポリシーを表示します。

VLAN モードでの L2VPN Quality of Service ポリシーの設定

この手順では、VLAN モードでの L2VPN QoS ポリシーの設定方法について説明します。



- (注) VLAN モードでは、インターフェイス名にサブインターフェイスを含める必要があります。
例：GigabitEthernet0/1/0/1.1。l2transport コマンドは、同じ CLI 行のインターフェイス タイプに従う必要があります。例：interface GigabitEthernet 0/0/0/0.1 l2transport。

手順の概要

1. **configure**
2. **interface type interface-path-id.subinterface l2transport**
3. **service-policy [input | output] [policy-map-name]**
4. **commit** コマンドまたは **end** コマンドを使用します。

手順の詳細

ステップ 1 **configure**

例：

```
RP/0/RSP0/cpu 0: router# configure
```

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 **interface type interface-path-id.subinterface l2transport**

例：

```
RP/0/RSP0/cpu 0: router(config)# interface GigabitEthernet0/0/0/0.1 l2transport
```

L2 スイッチングのインターフェイスまたは接続を設定します。

(注) VLAN モードでは、**interface** と同じ行に **l2transport** キーワードを入力する必要があります。

ステップ 3 **service-policy [input | output] [policy-map-name]**

例：

```
RP/0/RSP0/cpu 0: router(config-if)# service-policy input servpoll
```

入力インターフェイスまたは出力インターフェイスに、そのインターフェイスのサービスポリシーとして使用する QoS ポリシーを付加します。

ステップ4 **commit** コマンドまたは **end** コマンドを使用します。

commit : 設定の変更を保存し、コンフィギュレーションセッションに留まります。

end : 次のいずれかのアクションを実行することをユーザに要求します。

- [Yes] : 設定変更を保存し、コンフィギュレーションセッションを終了します。
- [No] : 設定変更をコミットせずにコンフィギュレーションセッションを終了します。
- [Cancel] : 設定変更をコミットせずに、コンフィギュレーションモードに留まります。

マルチセグメント疑似回線の設定

ここで説明する作業は、次のとおりです。

マルチセグメント疑似回線設定のプロビジョニング

ポイントツーポイント (p2p) 相互接続としてマルチセグメント疑似回線を設定します。P2P クロスコネクタの詳細については、「[スタティックポイントツーポイント相互接続の設定](#)」を参照してください。

手順の概要

1. **configure**
2. **l2vpn**
3. **xconnect group group-name**
4. **p2p xconnect-name**
5. **neighbor A.B.C.D pw-id value**
6. **pw-class class-name**
7. **exit**
8. **neighbor A.B.C.D pw-id value**
9. **pw-class class-name**
10. **commit**

手順の詳細

ステップ1 **configure**

例 :

```
RP/0/RSP0/cpu 0: router# configure
```

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 **l2vpn**

例 :

```
RP/0/RSP0/cpu 0: router# configure
```

L2VPN 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 **xconnect group** *group-name*

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn)# xconnect group MS-PW1
```

自由形式の 32 文字ストリングを使用して、相互接続グループ名を設定します。

ステップ 4 **p2p** *xconnect-name*

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc)# p2p ms-pw1
```

P2P コンフィギュレーション サブモードを開始します。

ステップ 5 **neighbor** *A.B.C.D* **pw-id** *value*

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p)# neighbor 10.165.200.25 pw-id 100
```

相互接続の疑似回線を設定します。

IP アドレスは、該当する PE ノードの IP アドレスです。

pw-id は PE ノードの **pw-id** と一致する必要があります。

(注) MSPW の場合、クロスコネクタ設定は、ローカル PE、S-PE、およびリモート PE で実行されません。

ステップ 6 **pw-class** *class-name*

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p-pw)# pw-class dynamic_mpls
```

疑似回線クラス サブモードになり、疑似回線クラス テンプレートを定義できます。

ステップ 7 **exit**

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p-pw)# exit
```

疑似回線クラス サブモードを終了し、ルータを親コンフィギュレーション モードに戻します。

ステップ 8 **neighbor** *A.B.C.D* **pw-id** *value*

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p)# neighbor 10.165.202.158 pw-id 300
```

相互接続の疑似回線を設定します。

IP アドレスは、該当する PE ノードの IP アドレスです。

pw-id は PE ノードの **pw-id** と一致する必要があります。

ステップ 9 **pw-class class-name**

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p-pw)# pw-class dynamic_mpls
```

疑似回線クラス サブモードになり、疑似回線クラス テンプレートを定義できます。

ステップ 10 **commit**

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p-pw)# commit
```

実行コンフィギュレーションファイルに設定変更を保存し、コンフィギュレーションセッションを続行します。

グローバル マルチセグメント疑似回線のディスクリプションのプロビジョニング

S-PE ノードには、疑似回線切り替えポイントの Type-Length-Value (TLV) でディスクリプションが必要です。TLV は疑似回線が通過するすべてのスイッチング ポイントを記録し、トラブルシューティングのために便利な履歴を作成します。

各マルチセグメント疑似回線に独自のディスクリプションを設定できます。手順については、「[相互接続のディスクリプションのプロビジョニング](#)」を参照してください。独自のディスクリプションがない場合、このグローバルなディスクリプションが使用されます。

手順の概要

1. **configure**
2. **l2vpn**
3. **description value**
4. **commit**

手順の詳細

ステップ 1 **configure**

例 :

```
RP/0/RSP0/cpu 0: router# configure
```

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 l2vpn

例 :

```
RP/0/RSP0/cpu 0: router(config)# l2vpn
```

L2VPN 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 description value

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn)# description S-PE1
```

疑似回線切り替えポイント TLV を設定します。この TLV は、疑似回線が通過するすべてのスイッチングポイントを記録します。

各マルチセグメント疑似回線に独自のディスクリプションを設定できます。独自のディスクリプションがない場合、このグローバルなディスクリプションが使用されます。

ステップ4 commit

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn)# commit
```

実行コンフィギュレーションファイルに設定変更を保存し、コンフィギュレーションセッションを続行します。

相互接続のディスクリプションのプロビジョニング

S-PE ノードには、疑似回線切り替えポイントの TLV でディスクリプションが必要です。TLV は疑似回線が通過するすべてのスイッチングポイントを記録し、トラブルシューティングのために便利な履歴を作成します。

手順の概要

1. **configure**
2. **l2vpn**
3. **xconnect group group-name**
4. **p2p xconnect-name**
5. **description value**
6. **commit**

手順の詳細

ステップ 1 **configure**

例 :

```
RP/0/RSP0/cpu 0: router# configure
```

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 **l2vpn**

例 :

```
RP/0/RSP0/cpu 0: router(config)# l2vpn
```

L2VPN 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 **xconnect group group-name**

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn)# xconnect group MS-PW1
```

自由形式の 32 文字ストリングを使用して、相互接続グループ名を設定します。

ステップ 4 **p2p xconnect-name**

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc)# p2p ms-pw1
```

P2P コンフィギュレーション サブモードを開始します。

ステップ 5 **description value**

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p)# description MS-PW from T-PE1 to T-PE2
```

疑似回線切り替えポイント TLV を設定します。この TLV は、疑似回線が通過するすべてのスイッチングポイントを記録します。

各マルチセグメント疑似回線に独自のディスクリプションを設定できます。独自のディスクリプションがない場合、グローバルなディスクリプションが使用されます。詳細については、「[マルチセグメント疑似回線設定のプロビジョニング](#)」を参照してください。

ステップ 6 **commit**

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p)# commit
```

実行コンフィギュレーションファイルに設定変更を保存し、コンフィギュレーションセッションを続行します。

スイッチングポイント TLV セキュリティのプロビジョニング

セキュリティ上の理由から、TLV を非表示にでき、それにより、疑似回線が通過するすべてのスイッチングポイントを誰かが表示することを防ぐことができます。

仮想回線接続性検証 (VCCV) は、**switching-tlv** パラメータが「hide」に設定されたマルチセグメント疑似回線では機能しない場合があります。VCCV の詳細については、「[L2VPN での仮想回線接続検証](#)」を参照してください。

手順の概要

1. **configure**
2. **l2vpn**
3. **pw-class class-name**
4. **encapsulation mpls**
5. **protocol ldp**
6. **switching-tlv hide**
7. **commit**

手順の詳細

ステップ 1 configure

例：

```
RP/0/RSP0/cpu 0: router# configure
```

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 l2vpn

例：

```
RP/0/RSP0/cpu 0: router(config)# l2vpn
```

L2VPN 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 pw-class class-name

例：

```
RP/0/RSP0/cpu 0: router(config-l2vpn)# pw-class dynamic_mpls
```

疑似回線クラス サブモードになり、疑似回線クラス テンプレートを定義できます。

ステップ4 encapsulation mpls

例：

```
RP/0/RSP0/cpu 0: router (config-l2vpn-pwc)# encapsulation mpls
```

MPLS に疑似配線カプセル化を設定します。

ステップ5 protocol ldp

例：

```
RP/0/RSP0/cpu 0: router (config-l2vpn-pwc-encap-mpls)# protocol ldp
```

LDP に疑似回線シグナリング プロトコルを設定します。

ステップ6 switching-tlv hide

例：

```
RP/0/RSP0/cpu 0: router (config-l2vpn-pwc-encap-mpls)# switching-tlv hide
```

疑似回線 TLV を非表示に設定します。

ステップ7 commit

例：

```
RP/0/RSP0/cpu 0: router (config-l2vpn-pwc-encap-mpls)#commit
```

実行コンフィギュレーションファイルに設定変更を保存し、コンフィギュレーションセッションを続行します。

マルチセグメント疑似回線のイネーブル化

pw-status コマンドを有効にした後、**pw-status** コマンドを使用します。**pw-status** コマンドはデフォルトでは無効になっています。**pw-status** コマンドを変更すると、L2VPN で設定されたすべての疑似回線が再プロビジョニングされます。

手順の概要

1. **configure**
2. **l2vpn**
3. **pw-status**

4. commit

手順の詳細

ステップ1 configure

例：

```
RP/0/RSP0/cpu 0: router# configure
```

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 l2vpn

例：

```
RP/0/RSP0/cpu 0: router(config)# l2vpn
```

レイヤ2 VPN 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 pw-status

例：

```
RP/0/RSP0/cpu 0: router(config-l2vpn)# pw-status
```

このレイヤ2 VPN で設定されるすべての疑似回線をイネーブルにします。

(注) 疑似回線ステータスを無効にするには、**pw-status disable** コマンドを使用します。

ステップ4 commit

例：

```
RP/0/RSP0/cpu 0: router(config-l2vpn)# commit
```

実行コンフィギュレーションファイルに設定変更を保存し、コンフィギュレーションセッションを続行します。

疑似回線冗長性の設定

疑似回線の冗長性により、プライマリ疑似回線で障害が発生した場合のバックアップ疑似回線を設定できます。プライマリ疑似回線が障害になった場合、PE ルータをバックアップ疑似回線に切り替えることができます。復旧後にプライマリ疑似回線の運用が再開するように選択できます。

次のトピックでは、疑似回線の冗長性を設定する方法について説明します。

ポイントツーポイント疑似回線の冗長性の設定

バックアップ遅延のためにポイントツーポイント疑似回線の冗長性を設定するには、次の作業を実行します。

手順の概要

1. **configure**
2. **l2vpn**
3. **pw-class class-name**
4. **backup disable {delay value | never}**
5. **exit**
6. **xconnect group group-name**
7. **p2p {xconnect-name}**
8. **neighbor A.B.C.D pw-id value**
9. **pw-class class-name**
10. **backup {neighbor A.B.C.D} {pw-id value}**
11. **end** または **commit**

手順の詳細

ステップ1 **configure**

例：

```
RP/0/RSP0/CPU0:router# configure
```

コンフィギュレーションモードに入ります。

ステップ2 **l2vpn**

例：

```
RP/0/RSP0/CPU0:router(config)# l2vpn  
RP/0/RSP0/CPU0:router(config-l2vpn)#
```

L2VPN 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 **pw-class class-name**

例：

```
RP/0/RSP0/CPU0:router(config-l2vpn)# pw-class path1  
RP/0/RSP0/CPU0:router(config-l2vpn-pwc)#
```

疑似回線クラス名を設定します。

ステップ4 **backup disable {delay value | never}**

例：

```
RP/0/RSP0/CPU0:router(config-l2vpn-pwc)# backup disable delay 20
```

このコマンドは、プライマリ疑似回線がアクティブになった後、バックアップ疑似回線から引き継ぐまでの待ち時間を指定します。

- **delay** キーワードを使用して、プライマリ疑似回線がアップ状態になってから、セカンダリ疑似回線が非アクティブになるまでの経過秒数を指定します。範囲は 0 ~ 180 です。
- プライマリ疑似回線が再び使用できるようになった場合に、セカンダリ疑似回線で障害が発生しない限り、セカンダリ疑似回線からプライマリ疑似回線にフォールバックしないように指定するには、**never** キーワードを使用します。

ステップ 5 **exit**

例 :

```
RP/0/RSP0/CPU0:router(config-l2vpn-pwc) # exit
RP/0/RSP0/CPU0:router(config-l2vpn) #
```

現在のコンフィギュレーション モードを終了します。

ステップ 6 **xconnect group group-name**

例 :

```
RP/0/RSP0/CPU0:router(config-l2vpn) # xconnect group A
RP/0/RSP0/CPU0:router(config-l2vpn-xc) #
```

クロスコネクトグループの名前を入力します。

ステップ 7 **p2p {xconnect-name}**

例 :

```
RP/0/RSP0/CPU0:router(config-l2vpn-xc) # p2p xc1
```

ポイントツーポイント クロスコネクトの名前を入力します。

ステップ 8 **neighbor A.B.C.D pw-id value**

例 :

```
RP/0/RSP0/CPU0:router(config-l2vpn-xc-p2p) # neighbor 10.1.1.2 pw-id 2
RP/0/RSP0/CPU0:router(config-l2vpn-xc-p2p-pw) #
```

クロスコネクトの疑似回線セグメントを設定します。

ステップ 9 **pw-class class-name**

例 :

```
RP/0/RSP0/CPU0:router(config-l2vpn-xc-p2p-pw) #pw-class path1
```

疑似回線クラス名を設定します。

ステップ 10 **backup {neighbor A.B.C.D} {pw-id value}**

例 :

```
RP/0/RSP0/CPU0:router(config-l2vpn-xc-p2p-pw)# backup neighbor 10.2.2.2 pw-id 5
RP/0/RSP0/CPU0:router(config-l2vpn-xc-p2p-pw-backup)#
```

相互接続のバックアップ疑似回線を設定します。

- **neighbor** キーワードを使用して、相互接続するピアを指定します。A.B.C.D 引数はピアの IPv4 アドレスです。
- **pw-id** キーワードを使用して、疑似回線 ID を設定します。範囲は 1 ~ 4294967295 です。

ステップ 11 end または commit

例 :

```
RP/0/RSP0/CPU0:router(config-l2vpn-xc-p2p-pw-backup)#end
```

または

```
RP/0/RSP0/CPU0:router(config-l2vpn-xc-p2p-pw-backup)#commit
```

設定変更を保存します。

- **end** コマンドを実行すると、変更をコミットするように要求されます。

```
Uncommitted changes found, commit them before exiting(yes/no/cancel)?
[cancel]:
```

- **yes** と入力すると、実行設定ファイルへの変更が保存され、設定セッションが終了して、ルータが EXEC モードに戻ります。
- **no** と入力すると、設定セッションが終了して、ルータが EXEC モードに戻ります。設定の変更はコミットされません。
- **cancel** と入力すると、現在のコンフィギュレーションセッションが継続します。コンフィギュレーションセッションは終了せず、設定変更もコミットされません。
- 実行コンフィギュレーションファイルに変更を保存し、コンフィギュレーションセッションを継続するには、**commit** コマンドを使用します。

バックアップ疑似回線への強制的な手動切り替え

ルータを強制的にバックアップに切り替える、またはプライマリ疑似回線に戻すには、EXEC モードで **l2vpn switchover** コマンドを使用します。EXEC モード

手動切り替えは、コマンドが入力されたとき、コマンドで指定されたピアが実際に使用可能であり、相互接続が完全なアクティブ状態に移行する場合に限り実行されます。

バックアップ疑似回線の設定

ポイントツーポイント ネイバーのバックアップ疑似回線を設定するには、次の作業を実行します。

手順の概要

1. **configure**
2. **l2vpn**
3. **xconnect group** *group-name*
4. **p2p** *xconnect-name*
5. **neighbor** *ip-address* **pw-id** *value*
6. **neighbor** { *A.B.C.D* } { **pw-id** *value* }
7. **commit** コマンドまたは **end** コマンドを使用します。

手順の詳細

ステップ1 **configure**

例：

```
RP/0/RSP0/cpu 0: router# configure
```

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 **l2vpn**

例：

```
RP/0/RSP0/cpu 0: router(config)# l2vpn
RP/0/RSP0/cpu 0: router(config-l2vpn)#
```

L2VPN 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 **xconnect group** *group-name*

例：

```
RP/0/RSP0/cpu 0: router(config-l2vpn)# xconnect group A
RP/0/RSP0/cpu 0: router(config-l2vpn-xc)#
```

クロスコネク トグループの名前を入力します。

ステップ4 **p2p** *xconnect-name*

例：

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc)# p2p rtrX_to_rtrY
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p)#
```

ポイントツーポイント クロスコネク トの名前を入力します。

ステップ5 neighbor ip-address pw-id value

例：

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p)# neighbor 1.1.1.1 pw-id 2
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p-pw)#
```

クロスコネク트의疑似回線セグメントを設定します。

ステップ6 neighbor { A.B.C.D } { pw-id value }

例：

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p)# neighbor 10.1.1.2 pw-id 11
```

相互接続のバックアップ疑似回線を設定します。

ステップ7 commit コマンドまたは end コマンドを使用します。

commit：設定の変更を保存し、コンフィギュレーションセッションに留まります。

end：次のいずれかのアクションを実行することをユーザに要求します。

- [Yes]：設定変更を保存し、コンフィギュレーションセッションを終了します。
- [No]：設定変更をコミットせずにコンフィギュレーションセッションを終了します。
- [Cancel]：設定変更をコミットせずに、コンフィギュレーションモードに留まります。

ポイントツーポイント疑似回線の冗長性の設定

バックアップ遅延のためにポイントツーポイント疑似回線の冗長性を設定するには、次の作業を実行します。

手順の概要

1. **configure**
2. **l2vpn**
3. **pw-class { class-name }**
4. **backup disable { delayvalue | never }**
5. **exit**
6. **xconnect group group-name**
7. **p2p { xconnect-name }**
8. **neighbor { A.B.C.D } { pw-id value }**
9. **pw-class { class-name }**
10. **backup { neighbor A.B.C.D } { pw-id value }**
11. **commit** コマンドまたは **end** コマンドを使用します。

手順の詳細

ステップ1 configure

例 :

```
RP/0/RSP0/cpu 0: router# configure
```

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 l2vpn

例 :

```
RP/0/RSP0/cpu 0: router(config)# l2vpn
RP/0/RSP0/cpu 0: router(config-l2vpn)#
```

L2VPN 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 pw-class { class-name }

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn)# pw-class path1
RP/0/RSP0/cpu 0: router(config-l2vpn-pwc)#
```

疑似回線クラス名を設定します。

ステップ4 backup disable { delayvalue | never }

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn-pwc)# backup disable delay 20
```

このコマンドは、プライマリ疑似回線がアクティブになってから、バックアップ疑似回線を引き継ぐまでの待ち時間を指定します。

- **delay** キーワードを使用して、プライマリ疑似回線がアップ状態になってから、セカンダリ疑似回線が非アクティブになるまでの経過秒数を指定します。範囲は0～180秒です。
- プライマリ疑似回線が再び使用できるようになった場合に、セカンダリ疑似回線で障害が発生しない限り、セカンダリ疑似回線からプライマリ疑似回線にフォールバックしないように指定するには、**never** キーワードを使用します。

ステップ5 exit

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn-pwc)# exit
RP/0/RSP0/cpu 0: router(config-l2vpn)#
```

現在のコンフィギュレーション モードを終了します。

ステップ 6 `xconnect group group-name`

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn)# xconnect group A
RP/0/RSP0/cpu 0: router(config-l2vpn-xc)#
```

クロスコネクト グループの名前を入力します。

ステップ 7 `p2p {xconnect-name}`

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc)# p2p xc1
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p)#
```

ポイントツーポイント クロスコネクトの名前を入力します。

ステップ 8 `neighbor {A.B.C.D} {pw-id value}`

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p)# neighbor 10.1.1.2 pw-id 2
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p-pw)#
```

クロスコネクトの疑似回線セグメントを設定します。

ステップ 9 `pw-class {class-name}`

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p-pw)# pw-class path1
```

疑似回線クラス名を設定します。

ステップ 10 `backup {neighbor A.B.C.D} {pw-id value}`

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p-pw)# backup neighbor 10.2.2.2 pw-id 5
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p-pw-backup)#
```

相互接続のバックアップ疑似回線を設定します。

- **neighbor** キーワードを使用して、相互接続するピアを指定します。A.B.C.D 引数はピアの IPv4 アドレスです。
- **pw-id** キーワードを使用して、疑似回線 ID を設定します。範囲は 1 ~ 4294967295 です。

ステップ 11 `commit` コマンドまたは `end` コマンドを使用します。

commit : 設定の変更を保存し、コンフィギュレーションセッションに留まります。

end : 次のいずれかのアクションを実行することをユーザに要求します。

- [Yes] : 設定変更を保存し、コンフィギュレーションセッションを終了します。
- [No] : 設定変更をコミットせずにコンフィギュレーションセッションを終了します。
- [Cancel] : 設定変更をコミットせずに、コンフィギュレーションモードに留まります。

バックアップ疑似回線への強制的な手動切り替え

ルータをバックアップまたはプライマリ疑似回線に強制的に切り替えるには、EXECモードで **l2vpn switchover** コマンドを使用します。

手動切り替えは、コマンドが入力されたとき、コマンドで指定されたピアが実際に使用可能であり、相互接続が完全なアクティブ状態に移行する場合に限り実行されます。

優先トンネルパスの設定

この手順では、優先トンネルパスを設定する方法について説明します。



- (注) 優先パスの設定に使用されるトンネルは、MPLSトラフィックエンジニアリング (MPLS-TE) トンネルです。

手順の概要

1. **configure**
2. **l2vpn**
3. **pw-class** {name}
4. **encapsulation mpls**
5. **preferred-path** {interface} {tunnel-ip value | tunnel-te value | tunnel-tp value} [fallback disable]
6. **commit** コマンドまたは **end** コマンドを使用します。

手順の詳細

ステップ1 configure

例 :

```
RP/0/RP0/CPU0:router# configure
```

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 l2vpn

例 :

```
RP/0/RP0/CPU0:router(config)# l2vpn
```

L2VPN 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 pw-class {name}

例：

```
RP/0/RP0/CPU0:router(config-l2vpn)# pw-class path1
```

疑似回線クラス名を設定します。

ステップ4 encapsulation mpls

例：

```
RP/0/RP0/CPU0:router(config-l2vpn-pwc)# encapsulation mpls
```

MPLS に疑似回線カプセル化を設定します。

ステップ5 preferred-path {interface} {tunnel-ip value | tunnel-te value | tunnel-tp value} [fallback disable]

例：

```
RP/0/RP0/CPU0:router(config-l2vpn-pwc-encap-mpls)# preferred-path interface tunnel-te 11 fallback disable
```

優先パス トンネルを設定します。フォールバックのディセーブル化の設定が使用されており、優先パスとして設定されている TE/TP トンネルがダウン状態になると、対応する疑似回線もダウン状態になることがあります。

ステップ6 commit コマンドまたは end コマンドを使用します。**commit** : 設定の変更を保存し、コンフィギュレーションセッションに留まります。**end** : 次のいずれかのアクションを実行することをユーザに要求します。

- [Yes] : 設定変更を保存し、コンフィギュレーションセッションを終了します。
- [No] : 設定変更をコミットせずにコンフィギュレーションセッションを終了します。
- [Cancel] : 設定変更をコミットせずに、コンフィギュレーションモードに留まります。

PW ステータス OAM の設定

疑似回線ステータス OAM を設定するには、次の作業を実行します。

手順の概要

1. configure
2. l2vpn
3. pw-oam refresh transmit seconds
4. end または commit

手順の詳細

ステップ1 configure

例：

```
RP/0/RSP0RP0/CPU0:router# configure
```

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 l2vpn

例：

```
RP/0/RSP0RP0/CPU0:router(config)# l2vpn
```

L2VPN 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 pw-oam refresh transmit seconds

例：

```
RP/0/RSP0RP0/CPU0:router(config-l2vpn)# pw-oam refresh transmit 100
```

疑似回線 OAM 機能を有効にします。

(注) リフレッシュの送信間隔範囲は 1 ~ 40 秒です。

ステップ4 end または commit

例：

```
RP/0/RSP0RP0/CPU0:router(config-l2vpn)# end
```

または

```
RP/0/RSP0RP0/CPU0:router(config-l2vpn)# commit
```

設定変更を保存します。

- **end** コマンドを実行すると、変更をコミットするように要求されます。

```
Uncommitted changes found, commit them before exiting(yes/no/cancel)?[cancel]:
```

- **yes** と入力すると、実行設定ファイルに変更が保存され、設定セッションが終了して、ルータが **EXEC** モードに戻ります。
- **no** と入力すると、設定セッションが終了して、ルータが **EXEC** モードに戻ります。設定の変更はコミットされません。
- **cancel** と入力すると、現在のコンフィギュレーションセッションが継続します。コンフィギュレーションセッションは終了せず、設定変更もコミットされません。
- 実行コンフィギュレーションファイルに変更を保存し、コンフィギュレーションセッションを継続するには、**commit** コマンドを使用します。

フローベースのロードバランシングのイネーブル化

フローベースのロードバランシングをイネーブルにするには、次の作業を実行します。

手順の概要

1. `configure`
2. `l2vpn`
3. `load-balancing flow {src-dst-mac | src-dst-ip}`
4. `end` または `commit`

手順の詳細

ステップ1 `configure`

例：

```
RP/0/RSP0RP0/CPU0:router# configure
```

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 `l2vpn`

例：

```
RP/0/RSP0RP0/CPU0:router(config)# l2vpn
```

L2VPN 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 `load-balancing flow {src-dst-mac | src-dst-ip}`

例：

```
RP/0/RSP0RP0/CPU0:router(config-l2vpn)# load-balancing flow src-dst-ip
```

L2VPN 下のすべての疑似回線およびバンドル EFP に対しフローベースのロードバランシングをイネーブルにします。ただし、疑似回線クラスを通じて疑似回線に対して、および EFP-hash を通じてバンドルに対して明示的に指定されている場合は除きます。

ステップ4 `end` または `commit`

例：

```
RP/0/RSP0RP0/CPU0:router(config-l2vpn)# end
```

または

```
RP/0/RSP0RP0/CPU0:router(config-l2vpn)# commit
```

設定変更を保存します。

- `end` コマンドを実行すると、変更をコミットするように要求されます。

```
Uncommitted changes found, commit them before exiting(yes/no/cancel)?[cancel]:
```

- `yes` と入力すると、実行設定ファイルに変更が保存され、設定セッションが終了して、ルータが EXEC モードに戻ります。

- **no** と入力すると、設定セッションが終了して、ルータが **EXEC** モードに戻ります。設定の変更はコミットされません。
- **cancel** と入力すると、現在のコンフィギュレーションセッションが継続します。コンフィギュレーションセッションは終了せず、設定変更もコミットされません。
- 実行コンフィギュレーションファイルに変更を保存し、コンフィギュレーションセッションを継続するには、**commit** コマンドを使用します。

疑似回線クラスのフローベースのロードバランシングのイネーブル化

疑似回線クラスに対しフローベースのロードバランシングをイネーブルにするには、次の作業を実行します。

手順の概要

1. `configure`
2. `l2vpn`
3. `pw-class {name}`
4. `encapsulation mpls`
5. `load-balancing pw-label`
6. `end` または `commit`

手順の詳細

ステップ 1 `configure`

例 :

```
RP/0/RSP0RP0/CPU0:router# configure
```

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 `l2vpn`

例 :

```
RP/0/RSP0RP0/CPU0:router(config)# l2vpn
```

L2VPN 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 `pw-class {name}`

例 :

```
RP/0/RSP0RP0/CPU0:router(config-l2vpn)# pw-class path1
```

疑似回線クラス名を設定します。

ステップ 4 `encapsulation mpls`

例 :


```
RP/0/RSP0RP0/CPU0:router(config-l2vpn-pwc)# encapsulation mpls
```

MPLS に疑似回線カプセル化を設定します。

ステップ 5 load-balancing pw-label

例 :

```
RP/0/RSP0RP0/CPU0:router(config-l2vpn-pwc-encap-mpls)# load-balancing pw-label
```

仮想回線ベースのロードバランシングを使用するために、定義されたクラスを使用してすべての疑似回線をイネーブルにします。

ステップ 6 end または commit

例 :

```
RP/0/RSP0RP0/CPU0:router(config-l2vpn-pwc-encap-mpls)# end
```

または

```
RP/0/RSP0RP0/CPU0:router(config-l2vpn-pwc-encap-mpls)# commit
```

設定変更を保存します。

- **end** コマンドを実行すると、変更をコミットするように要求されます。

```
Uncommitted changes found, commit them before exiting(yes/no/cancel)?[cancel]:
```

- **yes** と入力すると、実行設定ファイルに変更が保存され、設定セッションが終了して、ルータが **EXEC** モードに戻ります。
- **no** と入力すると、設定セッションが終了して、ルータが **EXEC** モードに戻ります。設定の変更はコミットされません。
- **cancel** と入力すると、現在のコンフィギュレーションセッションが継続します。コンフィギュレーションセッションは終了せず、設定変更もコミットされません。
- 実行コンフィギュレーションファイルに変更を保存し、コンフィギュレーションセッションを継続するには、**commit** コマンドを使用します。

疑似回線のグループ化のイネーブル化

疑似回線のグループ化をイネーブルにするには、次の作業を実行します。

手順の概要

1. **configure**
2. **l2vpn**
3. **pw-grouping**
4. **commit** コマンドまたは **end** コマンドを使用します。

手順の詳細

ステップ1 configure

例：

```
RP/0/RSP0/cpu 0: router# configure
```

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 l2vpn

例：

```
RP/0/RSP0/cpu 0: router(config)# l2vpn  
RP/0/RSP0/cpu 0: router(config-l2vpn)#
```

L2VPN 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 pw-grouping

例：

```
RP/0/RSP0/cpu 0: router(config-l2vpn)# pw-grouping
```

疑似回線のグループ化をイネーブルにします。

ステップ4 commit コマンドまたは end コマンドを使用します。

commit：設定の変更を保存し、コンフィギュレーションセッションに留まります。

end：次のいずれかのアクションを実行することをユーザに要求します。

- [Yes]：設定変更を保存し、コンフィギュレーションセッションを終了します。
- [No]：設定変更をコミットせずにコンフィギュレーションセッションを終了します。
- [Cancel]：設定変更をコミットせずに、コンフィギュレーションモードに留まります。

マルチキャスト接続の設定

『Cisco ASR 9000 Series Aggregation Services Router Multicast Configuration Guide』の「Implementing Multicast Routing on Cisco ASR 9000 Series Aggregation Services Routers」モジュールおよび『Cisco ASR 9000 Series Aggregation Services Router Multicast Command Reference』の「Multicast Routing and Forwarding Commands on Cisco ASR 9000 Series Aggregation Services Routers」モジュールを参照してください。

手順の概要

1. configure
2. multicast-routing [address-family ipv4]
3. interface all enable
4. exit

5. router igmp
6. version {1 | 2 | 3}
7. end または **commit**
8. show pim [ipv4] group-map [**ip-address-name**] [**info-source**]
9. show pim [vrf **vrf-name**] [ipv4] topology [**source-ip-address** [**group-ip-address**]
| entry-flag **flag** | interface-flag | summary] [route-count]

手順の詳細

ステップ1 configure

例：

```
RP/0/RSP0/CPU0:router# configure
```

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 multicast-routing [address-family ipv4]

例：

```
RP/0/RSP0/CPU0:router(config)# multicast-routing
```

マルチキャストルーティング コンフィギュレーション モードを開始します。

- マルチキャストプロセス (**MRIB**、**MFWD**、**PIM**、および **IGMP**) が起動します。
- **IPv4** では、**IGMP** バージョン 3 はデフォルトで有効になっています。
- **IPv4** の場合は、次を使用します。

```
address-family ipv4
```

キーワード

ステップ3 interface all enable

例：

```
RP/0/RSP0/CPU0:router(config-mcast-ipv4)# interface all enable
```

新規および既存のすべてのインターフェイスでマルチキャストルーティングおよび転送をイネーブルにします。

ステップ4 exit

例：

```
RP/0/RSP0/CPU0:router(config-mcast-ipv4)# exit
```

マルチキャストルーティング コンフィギュレーション モードを終了し、ルータを親コンフィギュレーション モードに戻します。

(注) リーフ PE の場合、ブリッジドメインで **IGMPSN** を有効にするには、**IGMPSN** プロファイル内で内部クエリ元を設定していることを確認します。

ステップ5 router igmp

例：

```
RP/0/RSP0/CPU0:router(config)# router igmp
```

(任意) ルータ IGMP コンフィギュレーション モードを開始します。

ステップ6 version {1|2|3}

例 :

```
RP/0/RSP0/CPU0:router(config-igmp)# version 3
```

(任意) ルータ インターフェイスで使用する IGMP バージョンを選択します。

- IGMP のデフォルトはバージョン 3 です。
- ホスト レシーバは、PIM-SSM 動作の IGMPv3 をサポートする必要があります。
- このコマンドがルータ IGMP コンフィギュレーション モードで設定されている場合、パラメータはすべての新規および既存インターフェイスによって継承されます。これらのパラメータは、インターフェイス コンフィギュレーション モードでインターフェイスごとに上書きできます。

ステップ7 end または commit

例 :

```
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# end
```

または

```
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)#commit
```

設定変更を保存します。

- **end** コマンドを実行すると、変更をコミットするように要求されます。

```
Uncommitted changes found, commit them before exiting(yes/no/cancel)?[cancel]:
```

- **yes** と入力すると、実行設定ファイルに変更が保存され、設定セッションが終了して、ルータが **EXEC** モードに戻ります。
- **no** と入力すると、設定セッションが終了して、ルータが **EXEC** モードに戻ります。設定の変更はコミットされません。
- **cancel** と入力すると、現在のコンフィギュレーションセッションが継続します。コンフィギュレーションセッションは終了せず、設定変更もコミットされません。
- 実行コンフィギュレーションファイルに変更を保存し、コンフィギュレーションセッションを継続するには、**commit** コマンドを使用します。

ステップ8 show pim [ipv4] group-map [ip-address-name] [info-source]

例 :

```
RP/0//CPU0:router# show pim ipv4 group-map
```

(任意) グループと PIM 間モードのマッピングを表示します。

ステップ9 show pim [vrf vrf-name] [ipv4] topology [source-ip-address [group-ip-address] | entry-flag flag | interface-flag | summary] [route-count]

例 :

```
RP/0/RSP0/CPU0:router# show pim topology
```

(任意) 特定のグループまたはすべてのグループの PIM トポロジテーブル情報を表示します。

AToM IP インターワーキングの設定

AToM IP インターワーキングを設定するには、次の作業を実行します。

手順の概要

1. **configure**
2. **l2vpn**
3. **xconnect group***group-name*
4. **p2pxconnect***name*
5. **interworking ipv4**
6. **commit** コマンドまたは **end** コマンドを使用します。

手順の詳細

ステップ 1 **configure**

例 :

```
RP/0/RSP0/cpu 0: router# configure
```

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 **l2vpn**

例 :

```
RP/0/RSP0/cpu 0: router(config)# l2vpn
```

L2VPN 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 **xconnect group***group-name*

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn)# xconnect group grp_1
```

クロスコネク トグループの名前を入力します。

ステップ 4 **p2pxconnect***name*

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc)# p2p vlan1
```

ポイントツーポイント クロスコネク トの名前を入力します。

ステップ 5 **interworking ipv4**

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p)# interworking ipv4
```

P2P で IPv4 インターワーキングを設定します。

ステップ6 **commit** コマンドまたは **end** コマンドを使用します。

commit : 設定の変更を保存し、コンフィギュレーションセッションに留まります。

end : 次のいずれかのアクションを実行することをユーザに要求します。

- [Yes] : 設定変更を保存し、コンフィギュレーションセッションを終了します。
- [No] : 設定変更をコミットせずにコンフィギュレーションセッションを終了します。
- [Cancel] : 設定変更をコミットせずに、コンフィギュレーションモードに留まります。

PPP IP インターワーキングの設定

PPP IP インターワーキングを設定するには、次の作業を実行します。

手順の概要

1. `configure`
2. `interface type interface-path-id`
3. `encapsulation ppp`
4. `l2transport`
5. `end`
6. `l2vpn`
7. `xconnect group group-name`
8. `p2p xconnect-name`
9. `interface type interface-path-id`
10. `interface type interface-path-id`
11. `interworking ipv4`
12. `interface type interface-path-id`
13. `neighbor A.B.C.Dpw-id`
14. `pw-class interface-path-id`
15. `exit`
16. `interworking ipv4`
17. `end` または `commit`

手順の詳細

ステップ1 `configure`

例 :

```
RP/0/0/CPU0:router# configure
```

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 `interface type interface-path-id`

例 :

```
RP/0/RSP0/CPU0:router(config)# interface Serial0/2/1/0/1/1/1:0
```

インターフェイス タイプとインスタンスを指定します。

ステップ 3 encapsulation ppp

例 :

```
RP/0/RSP0/CPU0:router(config-if)# encapsulation ppp
```

PPP にカプセル化タイプを設定します。

ステップ 4 l2transport

例 :

```
RP/0/RSP0/CPU0:router(config-if)# l2transport
```

選択したインターフェイスでレイヤ 2 トランスポートをイネーブルにします。

ステップ 5 end

例 :

```
RP/0/RSP0/CPU0:router(config-if-l2)# end
```

グローバル コンフィギュレーション モードに戻ります。

ステップ 6 l2vpn

例 :

```
RP/0/RSP0/CPU0:router(config)# l2vpn
```

L2VPN コンフィギュレーション モードを開始します。

ステップ 7 xconnect group **group-name**

例 :

```
RP/0/RSP0/CPU0:router(config-l2vpn)# xconnect group grp_1
```

クロスコネクト グループの名前を入力します。

ステップ 8 p2p **xconnect-name**

例 :

```
RP/0/RSP0/CPU0:router(config-l2vpn-xc)# p2p 1
```

ポイントツーポイント クロスコネクトの名前を入力します。

ステップ 9 interface type **interface-path-id**

例 :

```
RP/0/RSP0/CPU0:router(config)# interface Serial0/2/1/0/1/1/1:0
```

インターフェイス タイプとインスタンスを指定します。

ステップ 10 interface type **interface-path-id**

例 :

```
RP/0/RSP0/CPU0:router(config)# interface GigabitEthernet0/0/0/1.1
```

インターフェイス タイプとインスタンスを指定します。

ステップ 11 interworking ipv4

例 :

```
RP/0/RSP0/CPU0:router(config-l2vpn-xc-p2p)# interworking ipv4
```

P2P で IPv4 インターワーキングを設定します。

ステップ 12 interface type **interface-path-id**

例 :

```
RP/0/RSP0/CPU0:router(config)# interface GigabitEthernet0/0/0/1.1
```

インターフェイス タイプとインスタンスを指定します。

ステップ 13 neighbor**A.B.C.Dpw-id**

例 :

```
RP/0/RSP0/CPU0:router(config-l2vpn-xc-p2p)# interface Serial0/0/0/0/2/1/1:0
```

クロス接続の疑似回線セグメントを設定します。

相互接続ピアの IP アドレスを指定するには、A.B.C.D 引数を使用します。

(注) A.B.C.D は再帰的または非再帰的プレフィックスです

オプションで、コントロールワードを無効にするか、イーサネットまたは VLAN に transport-type を設定できます。

ステップ 14 pw-class **interface-path-id**

例 :

```
RP/0/RSP0/CPU0:router (config-l2vpn-xc-p2p-pw)# pw-class class_c1
```

疑似回線クラス サブモードになり、疑似回線クラス テンプレートを定義できます。

ステップ 15 exit

例 :

```
RP/0/RSP0/CPU0:router (config-l2vpn-xc-p2p-pw)# exit
```

現在のコンフィギュレーション モードを終了します。

ステップ 16 interworking ipv4

例 :

```
RP/0/RSP0/CPU0:router(config-l2vpn-xc-p2p)# interworking ipv4
```

P2P で IPv4 インターワーキングを設定します。

ステップ 17 end または **commit**

例 :

```
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# end
```


または

```
RP/0/RSP0/CPU0:router (config-l2vpn-bg-bd) #commit
```

設定変更を保存します。

- **end** コマンドを実行すると、変更をコミットするように要求されます。

```
Uncommitted changes found, commit them before exiting(yes/no/cancel)?[cancel]:
```

- **yes** と入力すると、実行設定ファイルに変更が保存され、設定セッションが終了して、ルータが **EXEC** モードに戻ります。
 - **no** と入力すると、設定セッションが終了して、ルータが **EXEC** モードに戻ります。設定の変更はコミットされません。
 - **cancel** と入力すると、現在のコンフィギュレーションセッションが継続します。コンフィギュレーションセッションは終了せず、設定変更もコミットされません。
- 実行コンフィギュレーションファイルに変更を保存し、コンフィギュレーションセッションを継続するには、**commit** コマンドを使用します。

PPP とイーサネット間の IP インターワーキングの設定

PPP IP インターワーキングを設定するには、次の作業を実行します。

手順の概要

1. **configure**
2. **interface type***interface-path-id*
3. **l2transport**
4. **end**
5. **l2vpn**
6. **xconnect group***group-name*
7. **p2p***connect-name*
8. **interface type***interface-path-id*
9. **interface type** *interface-path-id*
10. **interworking ipv4**
11. **interface type** *interface-path-id*
12. **neighbor***A.B.C.Dpw-id*
13. **pw-class***class-name*
14. **pw-class***class-name*
15. **exit**
16. **interworking ipv4**
17. **commit** コマンドまたは **end** コマンドを使用します。

手順の詳細

ステップ1 configure

例 :

```
RP/0/RSP0/cpu 0: router# configure
```

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 interface typeinterface-path-id

例 :

```
RP/0/RSP0/cpu 0: router(config)# interface Serial0/2/1/0/1/1/1:0
```

インターフェイス タイプとインスタンスを指定します。

ステップ3 l2transport

例 :

```
RP/0/RSP0/cpu 0: router(config-if)# l2transport
```

選択したインターフェイスでレイヤ2 トランスポートをイネーブルにします。

ステップ4 end

例 :

```
RP/0/RSP0/cpu 0: router(config-if-l2)# end
```

グローバル コンフィギュレーション モードに戻ります。

ステップ5 l2vpn

例 :

```
RP/0/RSP0/cpu 0: router(config)# l2vpn
```

L2VPN コンフィギュレーション モードを開始します。

ステップ6 xconnect groupgroup-name

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn)# xconnect group grp_1
```

クロスコネクト グループの名前を入力します。

ステップ7 p2pxconnect-name

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc)# p2p 1
```

ポイントツーポイント クロスコネクトの名前を入力します。

ステップ8 interface typeinterface-path-id

例 :

```
RP/0/RSP0/cpu 0: router(config)# interface Serial0/2/1/0/1/1/1:0
```

インターフェイス タイプとインスタンスを指定します。

ステップ 9 **interface type interface-path-id**

例 :

```
RP/0/RSP0/cpu 0: router(config)# interface GigabitEthernet0/0/0/1.1
```

インターフェイス タイプとインスタンスを指定します。

ステップ 10 **interworking ipv4**

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p)# interworking ipv4
```

P2P で IPv4 インターワーキングを設定します。

ステップ 11 **interface type interface-path-id**

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p)# interface Serial0/0/0/0/2/1/1:0
```

インターフェイス タイプとインスタンスを指定します。

ステップ 12 **neighbor A.B.C.Dpw-id**

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p)# interface Serial0/0/0/0/2/1/1:0
```

クロスコネクットの疑似回線セグメントを設定します。

相互接続ピアの IP アドレスを指定するには、A.B.C.D 引数を使用します。

(注) A.B.C.D は再帰的または非再帰的プレフィックスです

オプションで、コントロールワードを無効にするか、イーサネットまたは VLAN に transport-type を設定できます。

ステップ 13 **pw-class class-name**

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p)# interface Serial0/0/0/0/2/1/1:0
```

クロスコネクットの疑似回線セグメントを設定します。

相互接続ピアの IP アドレスを指定するには、A.B.C.D 引数を使用します。

(注) A.B.C.D は再帰的または非再帰的プレフィックスです

オプションで、コントロールワードを無効にするか、イーサネットまたは VLAN に transport-type を設定できます。

ステップ 14 **pw-class class-name**

例 :

```
RP/0/RSP0/cpu 0: router (config-l2vpn-xc-p2p-pw)# pw-class class_cem
```

疑似回線クラス サブモードになり、疑似回線クラス テンプレートを定義できます。

ステップ 15 **exit**

例 :

```
RP/0/RSP0/cpu 0: router (config-l2vpn-xc-p2p-pw)# exit
```

現在のコンフィギュレーション モードを終了します。

ステップ 16 **interworking ipv4**

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p)# interworking ipv4
```

P2P で IPv4 インターワーキングを設定します。

ステップ 17 **commit** コマンドまたは **end** コマンドを使用します。

commit : 設定の変更を保存し、コンフィギュレーションセッションに留まります。

end : 次のいずれかのアクションを実行することをユーザに要求します。

- [Yes] : 設定変更を保存し、コンフィギュレーションセッションを終了します。
- [No] : 設定変更をコミットせずにコンフィギュレーションセッションを終了します。
- [Cancel] : 設定変更をコミットせずに、コンフィギュレーションモードに留まります。

MLPPP IP インターワーキングの設定

cHDLC IP インターワーキングを設定するには、次の作業を実行します。

手順の概要

1. **configure**
2. **interface typeinterface-path-id**
3. **multilink [fragment|interleave|ncp]**
4. **l2transport**
5. **end**
6. **l2vpn**
7. **xconnect group group-name**
8. **p2p xconnect-name**
9. **interface typeinterface-path-id**
10. **interface typeinterface-path-id**
11. **interworking ipv4**
12. **interface typeinterface-path-id**
13. **neighbor{A.B.C.D}{pw-idvalue}**
14. **pw-classclass-name**
15. **exit**
16. **interworking ipv4**
17. **commit** コマンドまたは **end** コマンドを使用します。

手順の詳細

ステップ 1 configure

例 :

```
RP/0/RSP0/cpu 0: router# configure
```

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 interface typeinterface-path-id

例 :

```
RP/0/RSP0/cpu 0: router(config)# interface Multilink0/2/1/0/1
```

インターフェイス タイプとインスタンスを指定します。

ステップ 3 multilink [fragment|interleave|ncp]

例 :

```
RP/0/RSP0/cpu 0: router(config-if)# multilink
```

マルチリンク パラメータを変更します。

ステップ 4 l2transport

例 :

```
RP/0/RSP0/cpu 0: router(config-if-multilink)# l2transport
```

選択したインターフェイスでレイヤ 2 トランスポートをイネーブルにします。

ステップ 5 end

例 :

```
RP/0/RSP0/cpu 0: router(config-if-l2)# end
```

グローバル コンフィギュレーション モードに戻ります。

ステップ 6 l2vpn

例 :

```
RP/0/RSP0/cpu 0: router(config)# l2vpn
```

L2VPN コンフィギュレーション モードを開始します。

ステップ 7 xconnect group group-name

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn)# xconnect group grp_1
```

クロスコネク ト グループの名前を入力します。

ステップ 8 p2p xconnect-name

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc)# p2p 1
```

ポイントツーポイント クロスコネクットの名前を入力します。

ステップ 9 **interface type***interface-path-id*

例 :

```
RP/0/RSP0/cpu 0: router(config)# interface Serial0/2/1/0/1/1:0
```

インターフェイス タイプとインスタンスを指定します。

ステップ 10 **interface type***interface-path-id*

例 :

```
RP/0/RSP0/cpu 0: router(config)# interface GigabitEthernet0/0/0/1.1
```

インターフェイス タイプとインスタンスを指定します。

ステップ 11 **interworking ipv4**

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p)# interworking ipv4
```

P2P で IPv4 インターワーキングを設定します。

ステップ 12 **interface type***interface-path-id*

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p)# interface Serial0/0/0/2/1/1:0
```

インターフェイス タイプとインスタンスを指定します。

ステップ 13 **neighbor***{A.B.C.D}{pw-idvalue}*

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p)# neighbor 120.120.120.120 pw-id 3
```

クロスコネクットの疑似回線セグメントを設定します。

相互接続ピアの IP アドレスを指定するには、A.B.C.D 引数を使用します。

(注) A.B.C.D は再帰的または非再帰的プレフィックスです

オプションで、コントロールワードを無効にするか、イーサネットまたは VLAN に **transport-type** を設定できます。

ステップ 14 **pw-class***class-name*

例 :

```
RP/0/RSP0/cpu 0: router (config-l2vpn-xc-p2p-pw)# pw-class class_cem
```

疑似回線クラス サブモードになり、疑似回線クラス テンプレートを定義できます。

ステップ 15 **exit**

例 :

```
RP/0/RSP0/cpu 0: router (config-l2vpn-xc-p2p-pw)# exit
```

現在のコンフィギュレーション モードを終了します。

ステップ 16 interworking ipv4

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p)# interworking ipv4
```

P2P で IPv4 インターワーキングを設定します。

ステップ 17 commit コマンドまたは end コマンドを使用します。

commit : 設定の変更を保存し、コンフィギュレーションセッションに留まります。

end : 次のいずれかのアクションを実行することをユーザに要求します。

- [Yes] : 設定変更を保存し、コンフィギュレーションセッションを終了します。
- [No] : 設定変更をコミットせずにコンフィギュレーションセッションを終了します。
- [Cancel] : 設定変更をコミットせずに、コンフィギュレーションモードに留まります。

Circuit Emulation over Packet Switched Network の設定

CEoP を設定するには、次の作業を実行します。

CEM 接続回線の疑似回線への追加

CEM 接続回線を疑似回線に追加するには、次の作業を実行します。

手順の概要

1. **configure**
2. **l2vpn**
3. **xconnect groupgroup-name**
4. **p2pxconnect-name**
5. **interface type interface-path-id**
6. **neighborA.B.C.D pw-id**
7. **commit** コマンドまたは **end** コマンドを使用します。

手順の詳細

ステップ 1 configure

例 :

```
RP/0/RSP0/cpu 0: router# configure
```

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 l2vpn

例 :

```
RP/0/RSP0/cpu 0: router(config)# l2vpn
```

L2VPN 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 **xconnect group***group-name*

例：

```
RP/0/RSP0/cpu 0: router(config-l2vpn)# xconnect group grp_1
```

クロスコネク ト グループの名前を入力します。

ステップ4 **p2pxconnect-name**

例：

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc)# p2p vlan1
```

ポイントツーポイント クロスコネク トの名前を入力します。

ステップ5 **interface type***interface-path-id*

例：

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p)# interface CEM0/1/0/9:10
```

インターフェイス タイプとインスタンスを指定します。

ステップ6 **neighbor***A.B.C.D* **pw-id**

例：

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p)# neighbor 120.120.120.120 pw-id 3
```

クロスコネク トの疑似回線セグメントを設定します。

相互接続ピアの IP アドレスを指定するには、**A.B.C.D** 引数を使用します。

(注) **A.B.C.D** は再帰的または非再帰的プレフィックスです

オプションで、コントロールワードを無効にするか、イーサネットまたは VLAN に **transport-type** を設定できます。

ステップ7 **commit** コマンドまたは **end** コマンドを使用します。

commit : 設定の変更を保存し、コンフィギュレーションセッションに留まります。

end : 次のいずれかのアクションを実行することをユーザに要求します。

- [Yes] : 設定変更を保存し、コンフィギュレーションセッションを終了します。
- [No] : 設定変更をコミットせずにコンフィギュレーションセッションを終了します。
- [Cancel] : 設定変更をコミットせずに、コンフィギュレーションモードに留まります。

疑似回線クラスの関連付け

接続回線を疑似回線クラスと関連付けるには、次の作業を実行します。

手順の概要

1. **configure**
2. **l2vpn**
3. **pw-class** *class-name*
4. **encapsulation mpls**
5. **protocol ldp**
6. **end**
7. **xconnect group** *group-name*
8. **p2p** *xconnect-name*
9. **interface** *type interface-path-id*
10. **neighbor** *A.B.C.D pw-id pseudowire-id*
11. **pw-class** *class-name*
12. **commit** コマンドまたは **end** コマンドを使用します。

手順の詳細

ステップ 1 **configure**

例：

```
RP/0/RSP0/cpu 0: router# configure
```

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 **l2vpn**

例：

```
RP/0/RSP0/cpu 0: router (config)# l2vpn
```

レイヤ 2 VPN 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 **pw-class** *class-name*

例：

```
RP/0/RSP0/cpu 0: router (config-l2vpn)# pw-class class_cem
```

疑似回線クラス サブモードになり、疑似回線クラス テンプレートを定義できます。

ステップ 4 **encapsulation mpls**

例：

```
RP/0/RSP0/cpu 0: router (config-l2vpn-pwc)# encapsulation mpls
```

MPLS に疑似配線カプセル化を設定します。

ステップ 5 **protocol ldp**

例 :

```
RP/0/RSP0/cpu 0: router (config-l2vpn-pwc-encap-mpls)# protocol ldp
```

LDP に疑似回線シグナリング プロトコルを設定します。

ステップ 6 **end**

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn-pwc-encap-mpls)# end
```

システムから変更をコミットするように求められます。

```
Uncommitted changes found, commit them before exiting(yes/no/cancel)?[cancel]:
```

- **yes** と入力すると、実行設定ファイルへの変更が保存され、設定セッションが終了して、ルータが EXEC モードに戻ります。
- **no** と入力すると、設定セッションが終了して、ルータが EXEC モードに戻ります。変更はコミットされません。
- **cancel** と入力すると、現在のコンフィギュレーションセッションが継続します。コンフィギュレーションセッションは終了せず、設定変更もコミットされません。

ステップ 7 **xconnect group group-name**

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn)# xconnect group grp_1
```

相互接続グループを設定します。

ステップ 8 **p2p xconnect-name**

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc)# p2p vlan1
```

ポイントツーポイント相互接続を設定します。

ステップ 9 **interface type interface-path-id**

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p)# interface CEM0/1/0/9:20
```

インターフェイス タイプとインスタンスを指定します。

ステップ 10 **neighbor A.B.C.D pw-id pseudowire-id**

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p)# neighbor 10.2.2.2 pw-id 11
```

クロスコネクタの疑似回線セグメントを設定します。

相互接続ピアの IP アドレスを指定するには、A.B.C.D 引数を使用します。

(注) A.B.C.D は再帰的または非再帰的プレフィックスです。

オプションで、コントロールワードをディセーブルにするか、イーサネットまたは VLAN に transport-type を設定できます。

(注) 疑似回線ステータス (pw-status) はデフォルトで有効になっています。必要に応じて、**pw-status disable** コマンドを使用して疑似回線ステータスを無効にします。

ステップ 11 **pw-class class-name**

例 :

```
RP/0/RSP0/cpu 0: router (config-l2vpn-xc-p2p)# pw-class class_cem
```

指定した疑似回線クラスを P2P 接続回線と関連付けます。

ステップ 12 **commit** コマンドまたは **end** コマンドを使用します。

commit : 設定の変更を保存し、コンフィギュレーションセッションに留まります。

end : 次のいずれかのアクションを実行することをユーザに要求します。

- [Yes] : 設定変更を保存し、コンフィギュレーションセッションを終了します。
- [No] : 設定変更をコミットせずにコンフィギュレーションセッションを終了します。
- [Cancel] : 設定変更をコミットせずに、コンフィギュレーションモードに留まります。

疑似回線ステータスのイネーブル化

疑似回線ステータスをイネーブルにするには、次の作業を実行します。

手順の概要

1. configure
2. l2vpn
3. pw-status
4. commit

手順の詳細

ステップ1 configure

例：

```
RP/0/RSP0/CPU0:router# configure
```

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 l2vpn

例：

```
RP/0/RSP0/CPU0:router (config)# l2vpn
```

レイヤ2 VPN 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 pw-status

例：

```
RP/0/RSP0/CPU0:router (config-l2vpn)# pw-status
```

このレイヤ2 VPN で設定されるすべての疑似回線をイネーブルにします。

(注) 疑似回線ステータスをディセーブルにするには、`pw-status disable` コマンドを使用します。

ステップ4 commit

例：

```
RP/0/RSP0/CPU0:router (config-l2vpn)# commit
```

実行コンフィギュレーションファイルに設定変更を保存し、コンフィギュレーションセッションを続行します。

バックアップ疑似回線の設定

ポイントツーポイントネイバーのバックアップ疑似回線を設定するには、次の作業を実行します。

手順の概要

1. **configure**
2. **l2vpn**
3. **xconnect group** *group-name*
4. **p2p** *xconnect-name*
5. **neighbor** *ip-address* **pw-id** *value*
6. **neighbor** { *A.B.C.D* } { **pw-id** *value* }
7. **commit** コマンドまたは **end** コマンドを使用します。

手順の詳細

ステップ1 **configure**

例：

```
RP/0/RSP0/cpu 0: router# configure
```

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 **l2vpn**

例：

```
RP/0/RSP0/cpu 0: router(config)# l2vpn  
RP/0/RSP0/cpu 0: router(config-l2vpn)#
```

L2VPN 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 **xconnect group group-name**

例：

```
RP/0/RSP0/cpu 0: router(config-l2vpn)# xconnect group A  
RP/0/RSP0/cpu 0: router(config-l2vpn-xc)#
```

クロスコネクト グループの名前を入力します。

ステップ4 **p2p xconnect-name**

例：

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc)# p2p rtrX_to_rtrY  
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p)#
```

ポイントツーポイント クロスコネクトの名前を入力します。

ステップ5 **neighbor ip-address pw-id value**

例：

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p)# neighbor 1.1.1.1 pw-id 2  
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p-pw)#
```

クロスコネクトの疑似回線セグメントを設定します。

ステップ6 **neighbor {A.B.C.D} {pw-id value}**

例：

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p)# neighbor 10.1.1.2 pw-id 11
```

相互接続のバックアップ疑似回線を設定します。

ステップ7 **commit** コマンドまたは **end** コマンドを使用します。

commit : 設定の変更を保存し、コンフィギュレーションセッションに留まります。

end : 次のいずれかのアクションを実行することをユーザに要求します。

- [Yes] : 設定変更を保存し、コンフィギュレーションセッションを終了します。
- [No] : 設定変更をコミットせずにコンフィギュレーションセッションを終了します。
- [Cancel] : 設定変更をコミットせずに、コンフィギュレーションモードに留まります。

L2VPN ノンストップルーティングの設定

L2VPN ノンストップルーティングを設定するには、次の作業を実行します。

手順の概要

1. **configure**
2. **l2vpn**
3. **nsr**
4. **logging nsr**
5. **commit** コマンドまたは **end** コマンドを使用します。

手順の詳細

ステップ1 **configure**

例 :

```
RP/0/RSP0/cpu 0: router# configure
```

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 **l2vpn**

例 :

```
RP/0/RSP0/cpu 0: router(config)# l2vpn
```

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 **nsr**

例 :

```
RP/0/RSP0/cpu 0: router (config-l2vpn)# nsr
```

L2VPN ノンストップルーティングをイネーブルにします。

ステップ4 logging nsr

例：

```
RP/0/RSP0/cpu 0: router (config-l2vpn)# logging nsr
```

NSR イベントのロギングをイネーブルにします。

ステップ5 commit コマンドまたは end コマンドを使用します。

commit：設定の変更を保存し、コンフィギュレーションセッションに留まります。

end：次のいずれかのアクションを実行することをユーザに要求します。

- [Yes]：設定変更を保存し、コンフィギュレーションセッションを終了します。
- [No]：設定変更をコミットせずにコンフィギュレーションセッションを終了します。
- [Cancel]：設定変更をコミットせずに、コンフィギュレーションモードに留まります。

MPLS LDP ノンストップルーティングの設定

アクティブとスタンバイの Label Distribution Protocol (LDP; ラベル配布プロトコル) 間でラベル情報を同期するために、LDPのノンストップルーティング (NSR) を有効にするには、次の作業を実行します。リリース 6.1.1 以降では、ステートフル LDP 機能の導入により、アクティブとスタンバイの LDP 間でラベル情報を同期するように LDP NSR を明示的に設定する必要があります。

手順の概要

1. **configure**
2. **mpls ldp**
3. **nsr**
4. **commit** コマンドまたは **end** コマンドを使用します。

手順の詳細

ステップ1 configure

例：

```
RP/0/RSP0/cpu 0: router# configure
```

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 mpls ldp

例：

```
RP/0/RSP0/cpu 0: router(config)# mpls ldp
```

MPLS LDP 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 nsr

例：

```
RP/0/RSP0/cpu 0: router(config-ldp)# nsr
```

LDP ノンストップルーティングをイネーブルにします。

ステップ4 **commit** コマンドまたは **end** コマンドを使用します。

commit : 設定の変更を保存し、コンフィギュレーションセッションに留まります。

end : 次のいずれかのアクションを実行することをユーザに要求します。

- [Yes] : 設定変更を保存し、コンフィギュレーションセッションを終了します。
- [No] : 設定変更をコミットせずにコンフィギュレーションセッションを終了します。
- [Cancel] : 設定変更をコミットせずに、コンフィギュレーションモードに留まります。

L2TPv3 over IPv6 トンネルの設定

L2TPv3 over IPv6 トンネルを設定するには、次のタスクを実行します。

疑似回線のネイバー AFI の設定

疑似回線のネイバー AFI を設定するには、次の作業を実行します。



制約事項 L2TPv3 over IPv6 トンネルは、レイヤ2トランスポートサブインターフェイスでのみサポートされ、物理インターフェイスではサポートされません。

手順の概要

1. **configure**
2. **l2vpn**
3. **xconnect groupgroup-name**
4. **p2pxconnect-name**
5. **interfacetype interface-path-id**
6. **neighbor ipv6 X:X::X pw-idpseudowire-id**
7. **commit** コマンドまたは **end** コマンドを使用します。

手順の詳細

ステップ1 **configure**

例 :

```
RP/0/RSP0/cpu 0: router# configure
```

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 **l2vpn**

例 :

```
RP/0/RSP0/cpu 0: router (config)# l2vpn
```

レイヤ 2 VPN 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 **xconnect group group-name**

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn)# xconnect group grp_1
```

クロスコネクグループを設定し、その名前を指定します。

ステップ4 **p2pxconnect-name**

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc)# p2p vlan1
```

ポイントツーポイント相互接続を設定します。

ステップ5 **interfacetype interface-path-id**

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p)# interface GigabitEthernet0/4/0/30
```

インターフェイス タイプ ID を指定します。選択できる基準は、次のとおりです。

- GigabitEthernet : ギガビット イーサネット/IEEE 802.3 インターフェイス
- TenGigE : TenGigabit イーサネット/IEEE 802.3 インターフェイス

ステップ6 **neighbor ipv6 X:X::X pw-id pseudowire-id**

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p)# neighbor ipv6 1111:2222::cdef pw-id 2000
```

相互接続するピアを指定し、クロスコネク트의疑似回線セグメントを設定します。

ステップ7 commit コマンドまたは **end** コマンドを使用します。

commit : 設定の変更を保存し、コンフィギュレーションセッションに留まります。

end : 次のいずれかのアクションを実行することをユーザに要求します。

- [Yes] : 設定変更を保存し、コンフィギュレーションセッションを終了します。
- [No] : 設定変更をコミットせずにコンフィギュレーションセッションを終了します。
- [Cancel] : 設定変更をコミットせずに、コンフィギュレーションモードに留まります。

L2TPv3のカプセル化とプロトコルの設定

L2TPv3のカプセル化とプロトコルを設定するには、次の作業を実行します。

手順の概要

1. **configure**
2. **l2vpn**
3. **pw-class** *class-name*
4. **encapsulation l2tpv3**
5. **protocol l2tpv3**
6. **commit** コマンドまたは **end** コマンドを使用します。

手順の詳細

ステップ1 configure

例 :

```
RP/0/RSP0/cpu 0: router# configure
```

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 l2vpn

例 :

```
RP/0/RSP0/cpu 0: router (config)# l2vpn
```

レイヤ2 VPN 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 pw-class *class-name*

例 :

```
RP/0/RSP0/cpu 0: router (config-l2vpn)# pw-class l2tpv3_class
```

疑似回線クラスサブモードになり、疑似回線クラステンプレートを定義できます。

次のキーワードは、疑似回線クラス (**pw-class**) 設定モードで設定できますが、これらのキーワードは L2TPv3 over IPv6 トンネルを介した では使用できません。

- **cookie**
- **dfbit**
- **ipv4 source**
- **pmtu**
- **sequencing**
- **transport-mode**

ステップ 4 **encapsulation l2tpv3**

例 :

```
RP/0/RSP0/cpu 0: router (config-l2vpn-pwc)# encapsulation l2tpv3
```

疑似回線カプセル化を L2TPv3 に設定します。

ステップ 5 **protocol l2tpv3**

例 :

```
RP/0/RSP0/cpu 0: router (config-l2vpn-pwc-encap-l2tpv3)# protocol l2tpv3
```

疑似回線シグナリングプロトコルを L2TPv3 に設定します。

ステップ 6 **commit** コマンドまたは **end** コマンドを使用します。

commit : 設定の変更を保存し、コンフィギュレーションセッションに留まります。

end : 次のいずれかのアクションを実行することをユーザに要求します。

- [Yes] : 設定変更を保存し、コンフィギュレーションセッションを終了します。
- [No] : 設定変更をコミットせずにコンフィギュレーションセッションを終了します。
- [Cancel] : 設定変更をコミットせずに、コンフィギュレーションモードに留まります。

L2TPv3 over IPv6 トンネルの送信元 IPv6 アドレスの設定

L2TPv3 over IPv6 トンネルの送信元 IPv6 アドレスを設定するには、次の作業を実行します。

手順の概要

1. **configure**
2. **l2vpn**
3. **xconnect group group-name**

4. **p2p** *xconnect-name*
5. **interface type** *interface-path-id*
6. **neighbor ipv6** *peer-address pw-id pseudowire-id*
7. **source** *pw-source-address*
8. **end** または **commit**

手順の詳細

ステップ1 **configure**

例：

```
RP/0/RSP0/CPU0:router# configure
```

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 **l2vpn**

例：

```
RP/0/RSP0/CPU0:router (config)# l2vpn
```

レイヤ 2 VPN 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 **xconnect group** *group-name*

例：

```
RP/0/RSP0/CPU0:router (config-l2vpn)# xconnect group g1
```

クロスコネクグループを設定します。

ステップ4 **p2p** *xconnect-name*

例：

```
RP/0/RSP0/CPU0:router (config-l2vpn-xc)# p2p xc3
```

ポイントツーポイント クロスコネクを設定します。

ステップ5 **interface type** *interface-path-id*

例：

```
RP/0/RSP0/CPU0:router (config-l2vpn-xc-p2p)# interface GigabitEthernet0/0/0/4.2
```

インターフェイス タイプ ID を指定します。

ステップ6 **neighbor ipv6** *peer-address pw-id pseudowire-id*

例：

```
RP/0/RSP0/CPU0:router (config-l2vpn-xc-p2p)# neighbor ipv6 1111:2222::cdef pw-id 1
```

相互接続するピアを指定し、クロスコネクの疑似回線セグメントを設定します。

ステップ7 **source** *pw-source-address*

例：

```
RP/0/RSP0/CPU0:router (config-l2vpn-xc-p2p-pw)# source 1111:2222::abcd
```

疑似回線の送信元 IPv6 アドレスを設定します。

(注) 送信元 IPv6 アドレスは一意であり、任意に選択する必要があります。このアドレスはルータ内のどのタイプのインターフェイスにも設定できません。

ステップ 8 end または commit

例 :

```
RP/0/RSP0/CPU0:router(config-l2vpn-xc-p2p-pw)# end
```

または

```
RP/0/RSP0/CPU0:router(config-l2vpn-xc-p2p-pw)# commit
```

設定変更を保存します。

- **end** コマンドを実行すると、変更をコミットするように要求されます。

```
Uncommitted changes found, commit them before exiting(yes/no/cancel)?[cancel]:
```

- **yes** と入力すると、実行設定ファイルに変更が保存され、設定セッションが終了して、ルータが **EXEC** モードに戻ります。
- **no** と入力すると、設定セッションが終了して、ルータが **EXEC** モードに戻ります。設定の変更はコミットされません。
- **cancel** と入力すると、現在のコンフィギュレーションセッションが継続します。コンフィギュレーションセッションは終了せず、設定変更もコミットされません。
- 実行コンフィギュレーションファイルに変更を保存し、コンフィギュレーションセッションを継続するには、**commit** コマンドを使用します。

ローカルおよびリモートセッションの設定

ローカルセッションとリモートセッションを設定するには、次の作業を実行します。

手順の概要

1. **configure**
2. **l2vpn**
3. **xconnect group** *group-name*
4. **p2p** *xconnect-name*
5. **interface type** *interface-path-id*
6. **neighbor ipv6** *peer-address* **pw-id** *pseudowire-id*
7. **l2tp static local session** *session-id*
8. **l2tp static remote session** *session-id*
9. **commit** コマンドまたは **end** コマンドを使用します。

手順の詳細

ステップ 1 configure

例 :

```
RP/0/RSP0/cpu 0: router# configure
```

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 **l2vpn**

例 :

```
RP/0/RSP0/CPU0:router (config)# l2vpn
```

レイヤ 2 VPN 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 **xconnect group group-name**

例 :

```
RP/0/RSP0/CPU0:router (config-l2vpn)# xconnect group g1
```

クロスコネクグループを設定します。

ステップ 4 **p2p xconnect-name**

例 :

```
RP/0/RSP0/CPU0:router (config-l2vpn-xc)# p2p xc3
```

ポイントツーポイントクロスコネクを設定します。

ステップ 5 **interface type interface-path-id**

例 :

```
RP/0/RSP0/CPU0:router (config-l2vpn-xc-p2p)# interface GigabitEthernet0/0/0/4.2
```

インターフェイス タイプ ID を指定します。

ステップ 6 **neighbor ipv6 peer-address pw-id pseudowire-id**

例 :

```
RP/0/RSP0/CPU0:router (config-l2vpn-xc-p2p)# neighbor ipv6 1111:2222::cdef pw-id 1
```

相互接続するピアを指定し、クロスコネクの疑似回線セグメントを設定します。

ステップ 7 **l2tp static local session session-id**

例 :

```
RP/0/RSP0/CPU0:router (config-l2vpn-xc-p2p-pw)# l2tp static local session 1
```

(オプション) L2TP 擬似回線のスタティック ローカルセッションを設定します。

(注) ローカルセッション ID を設定すると、カプセル化解除側の処理の場合、ASR9000 シリーズ ルータはこの ID を無視します。

ステップ 8 `l2tp static remote session session-id`

例 :

```
RP/0/RSP0/CPU0:router (config-l2vpn-xc-p2p-pw)# l2tp static remote session 1
```

(オプション) L2TP 擬似回線のスタティック リモートセッションを設定します。

(注) 設定されている場合は、リモートセッション値 (カプセル化解除側の値) は、カプセル化側の処理に使用され、L2TPv3 ヘッダーのセッション値フィールドの値がプログラムされます。

ステップ 9 `commit` コマンドまたは `end` コマンドを使用します。

commit : 設定の変更を保存し、コンフィギュレーションセッションに留まります。

end : 次のいずれかのアクションを実行することをユーザに要求します。

- [Yes] : 設定変更を保存し、コンフィギュレーションセッションを終了します。
- [No] : 設定変更をコミットせずにコンフィギュレーションセッションを終了します。
- [Cancel] : 設定変更をコミットせずに、コンフィギュレーションモードに留まります。

ローカルおよびリモート Cookie の設定

ローカルおよびリモート Cookie を設定するには、次の作業を実行します。

手順の概要

1. `configure`
2. `l2vpn`
3. `xconnect group group-name`
4. `p2p xconnect-name`
5. `interface type interface-path-id`
6. `neighbor ipv6 peer-address pw-id pseudowire-id`
7. `l2tp static local cookie size bytes`
8. `l2tp static local cookie size bytes`
9. `commit` コマンドまたは `end` コマンドを使用します。

手順の詳細

ステップ 1 `configure`

例 :

```
RP/0/RSP0/cpu 0: router# configure
```

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 **l2vpn**

例 :

```
RP/0/RSP0/cpu 0: router (config)# l2vpn
```

レイヤ 2 VPN 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 **xconnect group group-name**

例 :

```
RP/0/RSP0/cpu 0: router (config-l2vpn)# xconnect group g1
```

クロスコネクグループを設定します。

ステップ 4 **p2p xconnect-name**

例 :

```
RP/0/RSP0/cpu 0: router (config-l2vpn-xc) # p2p xc3
```

ポイントツーポイント クロスコネクを設定します。

ステップ 5 **interface type interface-path-id**

例 :

```
RP/0/RSP0/cpu 0: router (config-l2vpn-xc-p2p) # interface GigabitEthernet0/0/0/4.2
```

インターフェイス タイプ ID を指定します。

ステップ 6 **neighbor ipv6 peer-address pw-id pseudowire-id**

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p) # neighbor ipv6 1111:2222::cdef pw-id 1
```

相互接続するピアを指定し、クロスコネクの疑似回線セグメントを設定します。

ステップ 7 **l2tp static local cookie size bytes**

例 :

```
RP/0/RSP0/cpu 0: router (config-l2vpn-xc-p2p-pw) # l2tp static local cookie size 0
```

L2TP 疑似回線のスタティックローカル Cookie サイズ設定を行います。

(注) ゼロ以外の Cookie サイズの場合、Cookie の値は必須の引数です。

ステップ 8 `l2tp static local cookie size bytes`

例 :

```
RP/0/RSP0/cpu 0: router (config-l2vpn-xc-p2p-pw)# l2tp static remote cookie size 0
```

L2TP 疑似回線のスタティックリモート Cookie サイズ設定を行います。

(注) ゼロ以外の Cookie サイズの場合、Cookie の値は必須の引数です。

ステップ 9 `commit` コマンドまたは `end` コマンドを使用します。

commit : 設定の変更を保存し、コンフィギュレーションセッションに留まります。

end : 次のいずれかのアクションを実行することをユーザに要求します。

- [Yes] : 設定変更を保存し、コンフィギュレーションセッションを終了します。
- [No] : 設定変更をコミットせずにコンフィギュレーションセッションを終了します。
- [Cancel] : 設定変更をコミットせずに、コンフィギュレーションモードに留まります。

L2TP スタティックサブモードの有効化

L2TP スタティックサブモードを有効にするには、次の作業を実行します。

手順の概要

1. **configure**
2. **l2vpn**
3. **xconnect group** *group-name*
4. **p2pxconnect** *name*
5. **interface type** *interface-path-id*
6. **neighbor ipv6** *peer-address pw-id pseudowire-id*
7. **l2tp static**
8. **commit** コマンドまたは **end** コマンドを使用します。

手順の詳細

ステップ 1 **configure**

例 :

```
RP/0/RSP0/cpu 0: router # configure
```

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 **l2vpn**

例 :

L2TPv3 ヘッダーの TOS リフレクションの有効化

```
RP/0/RSP0/cpu 0: router (config)# l2vpn
```

レイヤ 2 VPN 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 `xconnect group group-name`

例 :

```
RP/0/RSP0/cpu 0: router (config-l2vpn)# xconnect group g1
```

クロスコネクトグループを設定します。

ステップ 4 `p2pxconnect-name`

例 :

```
RP/0/RSP0/cpu 0: router (config-l2vpn-xc)# p2p xc3
```

ポイントツーポイント クロスコネクトを設定します。

ステップ 5 `interface type interface-path-id`

例 :

```
RP/0/RSP0/cpu 0: router (config-l2vpn-xc-p2p)# interface GigabitEthernet0/0/0/4.2
```

インターフェイス タイプ ID を指定します。

ステップ 6 `neighbor ipv6 peer-address pw-id pseudowire-id`

例 :

```
RP/0/RSP0/cpu 0: router (config-l2vpn-xc-p2p)# neighbor ipv6 1111:2222::cdef pw-id
```

相互接続するピアを指定し、クロスコネクトの疑似回線セグメントを設定します。

ステップ 7 `l2tp static`

例 :

```
RP/0/RSP0/cpu 0: router (config-l2vpn)#
```

L2TP スタティック設定サブモードを開始します。

ステップ 8 `commit` コマンドまたは `end` コマンドを使用します。

commit : 設定の変更を保存し、コンフィギュレーションセッションに留まります。

end : 次のいずれかのアクションを実行することをユーザに要求します。

- [Yes] : 設定変更を保存し、コンフィギュレーションセッションを終了します。
- [No] : 設定変更をコミットせずにコンフィギュレーションセッションを終了します。
- [Cancel] : 設定変更をコミットせずに、コンフィギュレーションモードに留まります。

L2TPv3 ヘッダーの TOS リフレクションの有効化

L2TPv3 ヘッダーでタイプオブサービス (TOS) リフレクションを有効にするには、次の作業を実行します。

手順の概要

1. `configure`
2. `l2vpn`
3. `pw-class class-name`
4. `encapsulation l2tpv3`
5. `protocol l2tpv3`
6. `neighbor ipv6 peer-address pw-id pseudowire-id`
7. `tos {反映 | 値}`
8. `end` または `commit`

手順の詳細

ステップ 1 `configure`

例 :

```
RP/0/RSP0/CPU0:router# configure
```

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 `l2vpn`

例 :

```
RP/0/RSP0/CPU0:router (config)# l2vpn
```

レイヤ 2 VPN 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 `pw-class class-name`

例 :

```
RP/0/RSP0/CPU0:router (config-l2vpn)# pw-class l2tpv3_class
```

疑似回線クラスサブモードになり、疑似回線クラステンプレートを定義できます。

ステップ 4 `encapsulation l2tpv3`

例 :

```
RP/0/RSP0/CPU0:router (config-l2vpn-pwc)# encapsulation l2tpv3
```

疑似回線カプセル化を L2TPv3 に設定します。

ステップ 5 `protocol l2tpv3`

例 :

```
RP/0/RSP0/CPU0:router (config-l2vpn-pwc-encap-l2tpv3)# protocol l2tpv3
```

疑似回線シグナリングプロトコルを L2TPv3 に設定します。

ステップ 6 `neighbor ipv6 peer-address pw-id pseudowire-id`

例 :

```
RP/0/RSP0/CPU0:router (config-l2vpn-xc-p2p)# neighbor ipv6 1111:2222::cdef pw-id
```

相互接続するピアを指定し、クロスコネクットの疑似回線セグメントを設定します。

ステップ7 tos {反映 | 値}

例：

```
RP/0/RSP0/CPU0:router (config-l2vpn-pwc-encap-l2tpv3)# tos reflect
```

または

```
RP/0/RSP0/CPU0:router (config-l2vpn-pwc-encap-l2tpv3)# tos value 50
```

タイプオブサービス (TOS) リフレクションを有効にします。これにより、内部 IP ヘッダーから L2TPv3 ヘッダーに TOS がコピーされます。

また、L2TPv3 疑似回線クラスの TOS の値を設定する場合は、このコマンドを使用します。有効な範囲は 0 ~ 255 です。

ステップ8 end または commit

例：

```
RP/0/RSP0/CPU0:router (config-l2vpn-pwc-encap-l2tpv3)# end
```

または

```
RP/0/RSP0/CPU0:router (config-l2vpn-pwc-encap-l2tpv3)# commit
```

設定変更を保存します。

- **end** コマンドを実行すると、変更をコミットするように要求されます。

```
Uncommitted changes found, commit them before exiting(yes/no/cancel)?[cancel]:
```

- **yes** と入力すると、実行設定ファイルに変更が保存され、設定セッションが終了して、ルータが **EXEC** モードに戻ります。
- **no** と入力すると、設定セッションが終了して、ルータが **EXEC** モードに戻ります。設定の変更はコミットされません。
- **cancel** と入力すると、現在のコンフィギュレーションセッションが継続します。コンフィギュレーションセッションは終了せず、設定変更もコミットされません。
- 実行コンフィギュレーションファイルに変更を保存し、コンフィギュレーションセッションを継続するには、**commit** コマンドを使用します。

L2TPv3 over IPv6 トンネルの TTL の設定

L2TPv3 over IPv6 トンネルの存続可能時間 (TTL) を設定するには、次の作業を実行します。

手順の概要

1. **configure**
2. **l2vpn**
3. **pw-class class-name**
4. **encapsulation l2tpv3**
5. **protocol l2tpv3**

6. ttl value**7. commit** コマンドまたは **end** コマンドを使用します。

手順の詳細

ステップ 1 configure

例 :

```
RP/0/RSP0/cpu 0: router # configure
```

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 l2vpn

例 :

```
RP/0/RSP0/cpu 0: router (config)# l2vpn
```

レイヤ 2 VPN 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 pw-class class-name

例 :

```
RP/0/RSP0/cpu 0: router (config-l2vpn)# pw-class l2tpv3_class
```

疑似回線クラスサブモードになり、疑似回線クラステンプレートを定義できます。

ステップ 4 encapsulation l2tpv3

例 :

```
RP/0/RSP0/cpu 0: router (config-l2vpn-pwc)# encapsulation l2tpv3
```

疑似回線カプセル化を L2TPv3 に設定します。

ステップ 5 protocol l2tpv3

例 :

```
RP/0/RSP0/cpu 0: router (config-l2vpn-pwc-encap-l2tpv3)# protocol l2tpv3
```

疑似回線シグナリングプロトコルを L2TPv3 に設定します。

ステップ 6 ttl value

例 :

```
RP/0/RSP0/cpu 0: router (config-l2vpn-pwc-encap-l2tpv3)# ttl 50
```

ノードホップ内の存続可能時間 (TTL) を指定された値に設定します。範囲は 1 ~ 255 です。

ステップ 7 commit コマンドまたは **end** コマンドを使用します。**commit** : 設定の変更を保存し、コンフィギュレーションセッションに留まります。**end** : 次のいずれかのアクションを実行することをユーザに要求します。

- [Yes] : 設定変更を保存し、コンフィギュレーションセッションを終了します。
- [No] : 設定変更をコミットせずにコンフィギュレーションセッションを終了します。

- [Cancel] : 設定変更をコミットせずに、コンフィギュレーションモードに留まります。

L2TPv3 over IPv6 トンネルのトラフィックミラーリングの設定

L2TPv3 over IPv6 トンネルのトラフィックミラーリングを設定するには、次の作業を実行します。

手順の概要

1. **configure**
2. **l2vpn**
3. **xconnect group***group-name*
4. **p2p** *xconnect-name*
5. **monitor-session** *session-name*
6. **neighbor ipv6** *peer-address* **pw-id** *pseudowire-id*
7. **pw-class** *class-name*
8. **sourcepw** *source-address*
9. **l2tp static local cookie size***sizevaluebytes*
10. **l2tp static remote cookie size***sizevaluebytes*
11. **commit** コマンドまたは **end** コマンドを使用します。

- L2TPv3 over IPv6 の概念については、「[L2TPv3 over IPv6](#)」を参照してください。
- 設定例については、「[L2TPv3 over IPv6 トンネルの設定 : 例](#)」を参照してください。

手順の詳細

ステップ 1 **configure**

例 :

```
RP/0/RSP0/cpu 0: router # configure
```

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 **l2vpn**

例 :

```
RP/0/RSP0/cpu 0: router (config)# l2vpn
```

レイヤ 2 VPN 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 **xconnect group***group-name*

例 :

```
RP/0/RSP0/cpu 0: router (config-l2vpn)# xconnect group span
```

クロスコネクトグループを設定します。

ステップ4 **p2p** *xconnect-name*

例：

```
RP/0/RSP0/cpu 0: router (config-l2vpn-xc)# p2p span-foo
```

ポイントツーポイント クロスコネクトを設定します。

ステップ5 **monitor-session** *session-name*

例：

```
RP/0/RSP0/cpu 0: router (config-l2vpn-xc-p2p)# monitor-session customer-foo
```

モニタセッションを指定します。

ステップ6 **neighbor ipv6** *peer-address pw-id pseudowire-id*

例：

```
RP/0/RSP0/cpu 0: router (config-l2vpn-xc-p2p)# neighbor ipv6 1111:3333::cdef pw-id 1001
```

相互接続するピアを指定し、クロスコネクトの疑似回線セグメントを設定します。

ステップ7 **pw-class** *class-name*

例：

```
RP/0/RSP0/cpu 0: router (config-l2vpn-xc-p2p-pw)# pw-class ts
```

疑似回線クラスサブモードになり、疑似回線クラステンプレートを定義できます。

ステップ8 **sourcepw** *source-address*

例：

```
RP/0/RSP0/cpu 0: router (config-l2vpn-xc-p2p-pw)# source 1111:3333::abcd
```

疑似回線の送信元 IPv6 アドレスを設定します。

ステップ9 **l2tp static local cookie size** *sizevaluebytes*

例：

```
RP/0/RSP0/cpu 0: router (config-l2vpn-xc-p2p-pw)# l2tp static local cookie size 8 value 0xabcd  
0x1234
```

L2TP 疑似回線のスタティックローカル Cookie サイズ設定を行います。

ステップ 10 `l2tp static remote cookie size size value bytes`

例：

```
RP/0/RSP0/cpu 0: router (config-l2vpn-xc-p2p-pw)# l2tp static remote cookie size 8 value 0xcdef0x5678
```

L2TP 疑似回線のスタティックリモート Cookie サイズ設定を行います。

ステップ 11 `commit` コマンドまたは `end` コマンドを使用します。

`commit`：設定の変更を保存し、コンフィギュレーションセッションに留まります。

`end`：次のいずれかのアクションを実行することをユーザに要求します。

- [Yes]：設定変更を保存し、コンフィギュレーションセッションを終了します。
- [No]：設定変更をコミットせずにコンフィギュレーションセッションを終了します。
- [Cancel]：設定変更をコミットせずに、コンフィギュレーションモードに留まります。

詳細については、次を参照してください。

- L2TPv3 over IPv6 の概念については、「[L2TPv3 over IPv6](#)」を参照してください。
- 設定例については、「[L2TPv3 over IPv6 トンネルの設定：例](#)」を参照してください。

L2TPv3 over IPv4 トンネルの設定



制約事項 L2TPv3 over Ipv4 トンネルは、レイヤ 2 転送サブインターフェイスでのみサポートされ、物理インターフェイスではサポートされません。タグなしのトラフィックを L2TPv3 over IPv4 経由で送信する必要がある場合は、タグなしとしてカプセル化されたサブインターフェイスを作成します。

次に、タグなしとしてカプセル化されたサブインターフェイスを作成する例を示します。

```
interface TenGigE0/3/0/1.123 l2transport
 encapsulation untagged
```

L2TPv3 over IPv4 トンネルを設定するには、次のタスクを実行します。

ダイナミック L2TPv3 疑似回線の設定

リモート IPv4 ピアに接続するダイナミック L2TPv3 疑似回線を設定するには、次の作業を実行します。

手順の概要

1. **configure**
2. **l2vpn**
3. **xconnect group name**
4. **p2p name**
5. **interfacetype interface-path-id**
6. **neighbor ipv4 ip-address pw-id number**
7. **pw-class pw-class-name**
8. **commit** コマンドまたは **end** コマンドを使用します。

手順の詳細

ステップ 1 **configure**

例 :

```
RP/0/RSP0/cpu 0: router# configure
```

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 **l2vpn**

例 :

```
RP/0/RSP0/cpu 0: router(config)# l2vpn
```

L2VPN 設定サブモードを開始します。

ステップ 3 **xconnect group name**

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn)# xconnect group L2TPV3_V4_XC_GRP
```

クロスコネクグループの名前を入力します。

ステップ 4 **p2p name**

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc)# p2p L2TPV3_P2P_1
```

p2p コンフィギュレーション サブモードを開始して、ポイントツーポイントの相互接続を設定します。

ステップ 5 **interfacetype interface-path-id**

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p)# interface GigabitEthernet 0/2/0/0.1
```

インターフェイス タイプ ID を指定します。選択できる基準は、次のとおりです。

- GigabitEthernet
- TenGigE

ステップ6 neighbor ipv4 ip-address pw-id number

例：

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p)# neighbor ipv4 26.26.26.26 pw-id 100
```

相互接続の疑似回線を設定します。

ステップ7 pw-class pw-class-name

例：

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p-pw)# pw-class L2TPV3_V4_CLASS
```

疑似回線クラスサブモードを開始して、クロスコネクトの名前を定義します。

ステップ8 commit コマンドまたは end コマンドを使用します。

commit：設定の変更を保存し、コンフィギュレーションセッションに留まります。

end：次のいずれかのアクションを実行することをユーザに要求します。

- [Yes]：設定変更を保存し、コンフィギュレーションセッションを終了します。
- [No]：設定変更をコミットせずにコンフィギュレーションセッションを終了します。
- [Cancel]：設定変更をコミットせずに、コンフィギュレーションモードに留まります。

L2TPv3のカプセル化とプロトコルの設定

L2TPv3のカプセル化とプロトコルを設定するには、次の作業を実行します。

手順の概要

1. **configure**
2. **l2vpn**
3. **pw-class class-name**
4. **encapsulation l2tpv3**
5. **protocol l2tpv3**
6. **commit** コマンドまたは **end** コマンドを使用します。

手順の詳細

ステップ1 configure

例：

```
RP/0/RSP0/cpu 0: router# configure
```

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 l2vpn

例 :

```
RP/0/RSP0/cpu 0: router (config)# l2vpn
```

レイヤ 2 VPN 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 pw-class class-name

例 :

```
RP/0/RSP0/cpu 0: router (config-l2vpn)# pw-class l2tpv3_class
```

疑似回線クラスサブモードになり、疑似回線クラステンプレートを定義できます。

疑似回線クラス (pw-class) 設定モードでは、次のキーワードを設定できます。

- **cookie**
- **dfbit**
- **ipv4 source**

ステップ4 encapsulation l2tpv3

例 :

```
RP/0/RSP0/cpu 0: router (config-l2vpn-pwc)# encapsulation l2tpv3
```

疑似回線カプセル化を L2TPv3 に設定します。

ステップ5 protocol l2tpv3

例 :

```
RP/0/RSP0/cpu 0: router (config-l2vpn-pwc-encap-l2tpv3)# protocol l2tpv3
```

疑似回線シグナリングプロトコルを L2TPv3 に設定します。

ステップ6 commit コマンドまたは end コマンドを使用します。

commit : 設定の変更を保存し、コンフィギュレーションセッションに留まります。

end : 次のいずれかのアクションを実行することをユーザに要求します。

- [Yes] : 設定変更を保存し、コンフィギュレーションセッションを終了します。
- [No] : 設定変更をコミットせずにコンフィギュレーションセッションを終了します。
- [Cancel] : 設定変更をコミットせずに、コンフィギュレーションモードに留まります。

L2TP 制御チャンネルパラメータの設定

L2TP 制御チャンネルパラメータは、制御チャンネル認証、キープアライブメッセージ、および制御チャンネルネゴシエーションで使用されます。L2tpv3 セッションでは、両方の PE ルータで同じ L2TP クラスを設定する必要があります。

次の L2TP 制御チャンネルパラメータは、L2TP クラス設定モードで設定できます。

- L2TP 制御チャンネルの認証
- L2TP 制御チャンネル認証に使用されるパスワード
- 制御メッセージに使用される再送信パラメータ
- 制御チャンネルに使用されるタイムアウトパラメータ
- メンテナンスパラメータ
- L2TPv3 コントロール メッセージ ハッシング

他の疑似回線クラスに継承可能な L2TP 制御チャンネルパラメータのテンプレートを作成するには、次の作業を実行します。

手順の概要

1. **configure**
2. **l2tp-class** *l2tp-class-name*
3. **authentication**
4. **password** { **0** | **7** } *password*
5. **retransmit** { **initial retries** *initial-retries* | **retries** *retries* | **timeout** { **max** | **min** } *timeout* }
6. **hello-interval** *interval*
7. **digest** { **check disable** | **hash** { **MD5** | **SHA1** }] | **secret** { **0** | **7** } *password*]
8. **hidden**

手順の詳細

ステップ 1 configure

例：

```
RP/0/RSP0/cpu 0: router# configure
```

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 l2tp-class l2tp-class-name

例：

```
RP/0/RSP0/cpu 0: router(config)# l2tp-class L2TP-CLASS
```

L2TP クラス名を指定して、L2TP クラス 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 authentication

例：

```
RP/0/RSP0/cpu 0: router(config-l2tp-class)# authentication
```

PE ルータ間の制御チャンネルの認証を有効にします。

ステップ4 password {0 | 7} password

例：

```
RP/0/RSP0/cpu 0: router(config-l2tp-class)# password 7 pwd_1
```

制御チャンネル認証に使用されるパスワードを設定します。

- **[0 | 7]**：共有秘密の入力フォーマットを指定します。デフォルト値は **0** です。
 - **0**：暗号化されたパスワードが後に続くことを指定します。
 - **7**：暗号化されていないパスワードが後に続くことを指定します。
- **password**：ピアルータ間の共通パスワードを定義します。

ステップ5 retransmit { initial retries initial-retries | retries retries | timeout { max | min } timeout }

例：

```
RP/0/RSP0/cpu 0: router(config-l2tp-class)# retransmit retries 10
```

制御パケットの再送信に影響するパラメータを設定します。

- **initial retries**：セッションが中断される前に再送信する SCCRQ の数を指定します。範囲は 1 ~ 1000 です。デフォルトは 2 です。
- **retries**：ピア PE ルータが無応答であると判断する前に実行する再送信の回数を指定します。範囲は 1 ~ 1000 です。デフォルトは 15 です。
- **timeout { max | min }**：制御パケット再送信の最大および最小再送信間隔（秒単位）を指定します。値の範囲は 1 ~ 8 です。デフォルトの最大インターバルは 8 です。デフォルトの最小インターバルは 1 です。

ステップ6 hello-interval interval

例：

```
RP/0/RSP0/cpu 0: router(config-l2tp-class)# hello-interval 10
```

L2TP hello パケット間で使用される交換インターバルを秒単位で指定します。

- **interval** 引数の有効な値の範囲は 0 ~ 1000 です。デフォルト値は 60 です。

ステップ7 `digest { check disable | hash { MD5 | SHA1 } } | secret { 0 | 7 } password]`

例 :

```
RP/0/RSP0/cpu 0: router(config-l2tp-class)# digest hash MD5
```

L2TPv3 制御チャネル認証または整合性チェックを有効にします。

- **secret** : L2TPv3 制御チャネル認証を有効にします。

(注) **digest** コマンドを **secret** キーワードオプションを指定せずに実行した場合は、L2TPv3 整合性チェックが有効になります。

- **{0 | 7}** : 共有秘密の入力フォーマットを指定します。デフォルト値は **0** です。
 - **0** : プレーンテキスト秘密が入力されたことを示します。
 - **7** : 暗号化された秘密が入力されたことを示します。
- **password** : ピアルータ間の共有秘密を定義します。 **password** 引数に入力する値は、**{0 | 7}** キーワードオプションで指定された入力フォーマットに合わせる必要があります。
- **hash { MD5 | SHA1 }** : メッセージ単位ダイジェスト計算に使用されるハッシュ関数を指定します。
 - **MD5** : HMAC-MD5 ハッシュ (デフォルト値) を指定します。
 - **SHA1** : HMAC-SHA-1 ハッシュを指定します。

ステップ8 `hidden`

例 :

```
RP/0/RSP0/cpu 0: router(config-l2tp-class)# hidden
```

L2TPv3 ピアへの制御メッセージの送信時に AVP 隠蔽を有効にします。

L2VPN 単一セグメント疑似回線の設定

ネットワークで単一セグメント疑似回線を設定するには、次の手順を実行します。

1. (オプション) 関連する L2VPN グローバルパラメータの設定。「[L2VPN グローバルパラメータの設定](#)」を参照してください

この手順は、デフォルトの BGP ルート識別子 (RD) 自動生成値と、BGP の自律システム番号 (ASN) およびルート識別子 (RID) を上書きするために使用します。

2. [L2VPN VPWS SS-PW の設定](#)
3. [BGP の L2VPN MS-PW アドレスファミリの設定](#)

アドレスファミリーは、ダイナミック擬似回線ルートを交換するために BGP で設定されま
す。

L2VPN グローバルパラメータの設定

L2VPN グローバルパラメータを設定するには、次の作業を実行します。

手順の概要

1. **configure**
2. **l2vpn**
3. **router-id** *router-id*
4. **pw-routing**
5. **global-id** *global-id*
6. **bgp**
7. **rd** *route-distinguisher*
8. **commit** コマンドまたは **end** コマンドを使用します。

手順の詳細

ステップ 1 **configure**

例 :

```
RP/0/RSP0/cpu 0: router# configure
```

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 **l2vpn**

例 :

```
RP/0/RSP0/cpu 0: router(config)# l2vpn
```

レイヤ 2 VPN 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-id** *router-id*

例 :

```
RP/0/RSP0/cpu 0: router(config)# router 2.2.2.2
```

ルータ ID を指定します。

ステップ 4 **pw-routing**

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn)# pw-routing
```

疑似回線ルーティング機能を有効にし、疑似回線ルーティング設定サブモードを開始します。

ステップ 5 **global-id** *global-id*

例：

```
RP/0/RSP0/cpu 0: router(config-l2vpn-pwr)# global-id 1000
```

ルータの L2VPN グローバル ID 値を設定します。

ステップ 6 **bgp**

例：

```
RP/0/RSP0/cpu 0: router(config-l2vpn-pwr)# bgp
```

BGP 疑似回線ルーティング機能を有効にし、BGP 設定サブモードを開始します。

ステップ 7 **rd** *route-distinguisher*

例：

```
RP/0/RSP0/cpu 0: router(config-l2vpn-pwr-bgp)# rd 192.168.1.3:10
```

BGP ルート識別子を設定します。

ステップ 8 **commit** コマンドまたは **end** コマンドを使用します。

commit：設定の変更を保存し、コンフィギュレーションセッションに留まります。

end：次のいずれかのアクションを実行することをユーザに要求します。

- [Yes]：設定変更を保存し、コンフィギュレーションセッションを終了します。
- [No]：設定変更をコミットせずにコンフィギュレーションセッションを終了します。
- [Cancel]：設定変更をコミットせずに、コンフィギュレーションモードに留まります。

L2VPN VPWS SS-PW の設定

L2VPN VPWS SS-PW を設定するには、次の作業を実行します。

手順の概要

1. **configure**
2. **interface type***interface-path-id*
3. **l2vpn**
4. **xconnect group** *group-name*
5. **p2p** *xconnect-name*

6. **interface type interface-path-id**
7. **neighbor routed global-id: prefix: ac-id source ac-id**
8. (オプション) **pw-class class-name**
9. **commit** コマンドまたは **end** コマンドを使用します。

手順の詳細

ステップ1 **configure**

例 :

```
RP/0/RSP0/cpu 0: router# configure
```

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 **interface type interface-path-id**

例 :

```
RP/0/RSP0/cpu 0: routerRP/0/RP0RSP0/CPU0:router# interface TenGigE0/1/0/12
```

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、インターフェイスを設定します。

ステップ3 **l2vpn**

例 :

```
RP/0/RSP0/cpu 0: router(config)# l2vpn
```

レイヤ2 VPN 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 **xconnect group group-name**

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn)# xconnect group pw-hel
```

自由形式の 32 文字ストリングを使用して、相互接続グループ名を設定します。

ステップ5 **p2p xconnect-name**

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc)# p2p pw-ss
```

P2P コンフィギュレーション サブモードを開始します。

ステップ6 **interface type interface-path-id**

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p)# interface gigabitethernet 0/1/0/9
```

インターフェイス タイプとインスタンスを指定します。

ステップ7 neighbor routed global-id: prefix: ac-id source ac-id

例:

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p)# neighbor routed 100:2.2.2.2:10 source 10
```

p2p クロスコネクットの疑似回線ルーティング設定サブモードを有効にします。

ステップ8 (オプション) pw-class class-name

例:

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p-pwr)# pw-class dynamic_sspw
```

疑似回線クラス サブモードになり、疑似回線クラス テンプレートを定義できます。

ステップ9 commit コマンドまたは end コマンドを使用します。

commit : 設定の変更を保存し、コンフィギュレーションセッションに留まります。

end : 次のいずれかのアクションを実行することをユーザに要求します。

- [Yes] : 設定変更を保存し、コンフィギュレーションセッションを終了します。
- [No] : 設定変更をコミットせずにコンフィギュレーションセッションを終了します。
- [Cancel] : 設定変更をコミットせずに、コンフィギュレーションモードに留まります。

BGP の L2VPN MS-PW アドレスファミリの設定

BGP に L2VPN MS-PW アドレスファミリを設定するには、次の作業を実行します。

手順の概要

1. **configure**
2. **router bgp autonomous-system-number**
3. **address-family l2vpn mspw**
4. **neighbor ip-address**
5. **address-family l2vpn mspw**
6. **commit** コマンドまたは **end** コマンドを使用します。

手順の詳細

ステップ1 configure

例 :

```
RP/0/RSP0/cpu 0: router# configure
```

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 bgp** *autonomous-system-number*

例 :

```
RP/0/RSP0/cpu 0: router(config)# router bgp 100
```

指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。

ステップ 3 **address-family l2vpn mspw**

例 :

```
RP/0/RSP0/cpu 0: router(config-bgp)# address-family l2vpn mspw
```

L2VPN アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。

ステップ 4 **neighbor ip-address**

例 :

```
RP/0/RSP0/cpu 0: router(config-bgp)# neighbor 10.10.10.1
```

指定した自律システム内のネイバーの IP アドレスを追加します。

ステップ 5 **address-family l2vpn mspw**

例 :

```
RP/0/RSP0/cpu 0: router(config-bgp-nbr-af)# address-family l2vpn mspw
```

ネイバーの L2VPN アドレスファミリを指定し、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ます。

ステップ 6 **commit** コマンドまたは **end** コマンドを使用します。

commit : 設定の変更を保存し、コンフィギュレーションセッションに留まります。

end : 次のいずれかのアクションを実行することをユーザに要求します。

- [Yes] : 設定変更を保存し、コンフィギュレーションセッションを終了します。
- [No] : 設定変更をコミットせずにコンフィギュレーションセッションを終了します。
- [Cancel] : 設定変更をコミットせずに、コンフィギュレーションモードに留まります。

単一セグメント疑似回線の確認

SS-PW の接続を確認するには、`ping mpls pseudowire` コマンドを使用します。

L2VPN 単一セグメント疑似回線の情報の表示

`show` コマンドは、L2VPN 単一セグメント疑似回線の情報を表示するために使用されます

- `show bgp l2vpn mspw`
- `show l2vpn pwr summary`
- `show l2vpn xc`

EPVN-VPWS の設定方法

EPVN-VPWS を設定するには、次の手順を実行します。

BGP の L2VPN EVPN アドレス ファミリの設定

BGP に L2VPN EVPN アドレス ファミリを設定するには、このタスクを実行します。

手順の概要

1. `configure`
2. `router bgp autonomous-system-number`
3. `address-family l2vpn evpn`
4. `neighbor ip-address`
5. `address-family l2vpn evpn`
6. `commit` コマンドまたは `end` コマンドを使用します。

手順の詳細

ステップ 1 `configure`

例 :

```
RP/0/RSP0/cpu 0: router# configure
```

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 bgp autonomous-system-number`

例 :

```
RP/0/RSP0/cpu 0: router(config)# router bgp 100
```

指定したルーティング プロセスのルータ コンフィギュレーション モードを開始します。

ステップ 3 `address-family l2vpn evpn`

例 :

```
RP/0/RSP0/cpu 0: router(config-bgp)# address-family l2vpn evpn
```

L2VPN アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。

ステップ 4 neighbor ip-address

例 :

```
RP/0/RSP0/cpu 0: router(config-bgp)# neighbor 10.10.10.1
```

指定した自律システム内のネイバーの IP アドレスを追加します。

ステップ 5 address-family l2vpn evpn

例 :

```
RP/0/RSP0/cpu 0: router(config-bgp-nbr-af)# address-family l2vpn evpn
```

ネイバーの L2VPN アドレス ファミリを指定し、アドレス ファミリ コンフィギュレーション モードを開始します。

ステップ 6 commit コマンドまたは end コマンドを使用します。

commit : 設定の変更を保存し、コンフィギュレーション セッションに留まります。

end : 次のいずれかのアクションを実行することをユーザに要求します。

- [Yes] : 設定変更を保存し、コンフィギュレーション セッションを終了します。
- [No] : 設定変更をコミットせずにコンフィギュレーション セッションを終了します。
- [Cancel] : 設定変更をコミットせずに、コンフィギュレーション モードに留まります。

EVPN-VPWS の設定

EVPN-VPWS を設定するには、次のタスクを実行します。



- (注) PWHE インターフェイスは、EVPN-VPWS を使用しても設定できます。詳細については、[疑似回線ヘッドエンドの設定](#) モジュールを参照してください。

手順の概要

1. **configure**
2. **interface type interface-path-id**
3. **l2vpn**
4. **xconnect group group-name**

5. **p2p** *xconnect-name*
6. **interface type** *interface-path-id*
7. **neighbor evpn evi** *vpn-id target ac-id*
8. **commit** コマンドまたは **end** コマンドを使用します。

手順の詳細

ステップ1 **configure**

例 :

```
RP/0/RSP0/cpu 0: router# configure
```

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 **interface type** *interface-path-id*

例 :

```
RP/0/RSP0/cpu 0: router(config)# interface TenGigE0/1/0/12
```

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、インターフェイスを設定します。

ステップ3 **l2vpn**

例 :

```
RP/0/RSP0/cpu 0: router(config)# l2vpn
```

レイヤ2 VPN 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 **xconnect group** *group-name*

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn)# xconnect group xc1
```

自由形式の 32 文字ストリングを使用して、相互接続グループ名を設定します。

ステップ5 **p2p** *xconnect-name*

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc)# p2p pw-ss
```

P2P コンフィギュレーション サブモードを開始します。

ステップ6 **interface type** *interface-path-id*

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p)# interface gigabitethernet 0/1/0/9
```

インターフェイス タイプとインスタンスを指定します。

ステップ 7 neighbor evpn evi vpn-id target ac-id

例 :

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p)# neighbor evpn evi 100 target 12
```

P2P クロス接続上で EVPN-VPWS エンドポイントを有効にします。

ステップ 8 commit コマンドまたは **end** コマンドを使用します。

commit : 設定の変更を保存し、コンフィギュレーションセッションに留まります。

end : 次のいずれかのアクションを実行することをユーザに要求します。

- [Yes] : 設定変更を保存し、コンフィギュレーションセッションを終了します。
- [No] : 設定変更をコミットせずにコンフィギュレーションセッションを終了します。
- [Cancel] : 設定変更をコミットせずに、コンフィギュレーションモードに留まります。

EVPN-VPWS を使用したアクセス疑似回線の設定

ブリッジドメインは、EVPN VPWS を使用してアクセス疑似回線を設定できます。

手順の概要

1. **configure**
2. **interface type interface-path-id**
3. **l2vpn**
4. **bridge group bridge-group-name**
5. **bridge-domain bridge-domain-name**
6. **neighbor evpn evi vpn-id target ac-id**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure 例 : RP/0/RSP0/cpu 0: router# configure	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	interface type interface-path-id 例 :	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、インターフェイスを設定します。

	コマンドまたはアクション	目的
	RP/0/RSP0/cpu 0: routerRP/0/RP0RSP0/CPU0:router# interface TenGigE0/1/0/12	
ステップ 3	l2vpn 例 : RP/0/RSP0/cpu 0: router(config)# l2vpn	レイヤ2 VPN 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	bridge group <i>bridge-group-name</i> 例 : RP/0/RSP0/cpu 0: router(config-l2vpn)# bridge group access-pw	ブリッジドメインを含めることができるブリッジグループを作成し、ブリッジドメインにネットワークインターフェイスを割り当てます。
ステップ 5	bridge-domain <i>bridge-domain-name</i> 例 : RP/0/RSP0/cpu 0: router(config-l2vpn-bg)# bridge-domain bd1	ブリッジドメインを確立し、L2VPNブリッジグループブリッジドメイン コンフィギュレーションモードを開始します。
ステップ 6	neighbor evpn evi <i>vpn-id</i> target <i>ac-id</i> 例 : RP/0/RSP0/cpu 0: router(config-l2vpn-bg-bd)# neighbor evpn evi 100 target 12	P2P クロス接続上でEVPN-VPWS エンドポイントを有効にします。

例

ポイントツーポイントレイヤ2サービスの設定例

ここで示す設定例は、次のとおりです。

L2VPN インターフェイスの設定：例

次に、L2VPN インターフェイスを設定する例を示します。

```
configure
interface GigabitEthernet0/0/0/0.1 l2transport
encapsulation dot1q 1
rewrite ingress tag pop 1 symmetric
end
```


ローカル スイッチングの設定 : 例

次に、レイヤ2 ローカル スイッチングを設定する例を示します。

```
configure
l2vpn
  xconnect group examples
  p2p example1
  interface TenGigE0/7/0/6.5
  interface GigabitEthernet0/4/0/30
commit
end

show l2vpn xconnect group examples
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
        SB = Standby, SR = Standby Ready
```

XConnect	Group	Name	ST	Segment 1 Description	ST	Segment 2 Description	ST
examples	example1	UP	Te0/7/0/6.5	UP	Gi0/4/0/30	UP	

ローカル接続冗長性設定 : 例

次に、PoA1 に LCR を設定する例を示します。

```
! LCR - CE1
group 107
  mlacp node 1
  mlacp system mac 0001.0001.0107
  mlacp system priority 107
  member
    neighbor 200.0.2.1
  !
! LCR - CE2
group 207
  mlacp node 1
  mlacp system mac 0001.0001.0207
  mlacp system priority 207
  member
    neighbor 200.0.2.1
  !

interface Bundle-Ether107
  description CE5 - LCR
  mlacp iccp-group 107
  mlacp port-priority 10
  no shut

interface Bundle-Ether207
  description CE6 - LCR
  mlacp iccp-group 207
  mlacp port-priority 10
  no shut

interface bundle-e107.1 l2t
  description CE5 - LCR
  encap dot1q 107 second 1
  rewrite ingress tag pop 2 symmetric

interface bundle-e207.1 l2t
  description CE2 - LCR
```

```

encap dot1q 207 second 1
rewrite ingress tag pop 2 symmetric

interface bundle-e307.1 l2t
description PE2 - LCR
encap dot1q 1
rewrite ingress tag pop 1 symmetric

l2vpn
xconnect group lcr-scale
p2p lcr-1
interface bundle-e107.1
interface bundle-e207.1
backup interface bundle-e307.1

```

ポイントツーポイント相互接続の設定 : 例

ここでは、スタティックおよびダイナミック p2p 相互接続の設定例を示します。

スタティック設定

次に、スタティック ポイントツーポイント相互接続の設定例を示します。

```

configure
l2vpn
xconnect group vlan_grp_1
p2p vlan1
interface GigabitEthernet0/0/0/0.1
neighbor 102.2.12.1 2 pw-id 1
mpls static label local 699 remote 890
commit2000

```

ダイナミック設定

次に、ダイナミック ポイントツーポイント相互接続の設定例を示します。

```

configure
l2vpn
xconnect group vlan_grp_1
p2p vlan1
interface TenGigE 0/0/0/0.1
neighbor 2.2.1.1 pw-id 1
commit

```

Inter-AS : 例

次に、AC1 から AC2 への AC 間相互接続の設定例を示します。

```

router-id Loopback0

interface Loopback0
ipv4 address 10.0.0.5 255.255.255.255
!
interface GigabitEthernet0/1/0/0.1 l2transport
encapsulation dot1q 1
!
!
interface GigabitEthernet0/0/0/3
ipv4 address 10.45.0.5 255.255.255.0

```

```
keepalive disable
!
interface GigabitEthernet0/0/0/4
ipv4 address 10.5.0.5 255.255.255.0
keepalive disable
!
router ospf 100
log adjacency changes detail
area 0
interface Loopback0
!
interface GigabitEthernet0/0/0/3
!
interface GigabitEthernet0/0/0/4
!
!
!
router bgp 100
address-family ipv4 unicast
allocate-label all
!
neighbor 10.2.0.5
remote-as 100
update-source Loopback0
address-family ipv4 unicast
!
address-family ipv4 labeled-unicast
!
!
!
l2vpn
xconnect group cisco
p2p cisco1
interface GigabitEthernet0/1/0/0.1
neighbor 10.0.1.5 pw-id 101
!
p2p cisco2
interface GigabitEthernet0/1/0/0.2
neighbor 10.0.1.5 pw-id 102
!
p2p cisco3
interface GigabitEthernet0/1/0/0.3
neighbor 10.0.1.5 pw-id 103
!
p2p cisco4
interface GigabitEthernet0/1/0/0.4
neighbor 10.0.1.5 pw-id 104
!
p2p cisco5
interface GigabitEthernet0/1/0/0.5
neighbor 10.0.1.5 pw-id 105
!
p2p cisco6
interface GigabitEthernet0/1/0/0.6
neighbor 10.0.1.5 pw-id 106
!
p2p cisco7
interface GigabitEthernet0/1/0/0.7
neighbor 10.0.1.5 pw-id 107
!
p2p cisco8
interface GigabitEthernet0/1/0/0.8
neighbor 10.0.1.5 pw-id 108
!
```

```

p2p cisco9
interface GigabitEthernet0/1/0/0.9
neighbor 10.0.1.5 pw-id 109
!
p2p cisco10
interface GigabitEthernet0/1/0/0.10
neighbor 10.0.1.5 pw-id 110
!
!
!
mpls ldp
router-id Loopback0
log
neighbor
!
interface GigabitEthernet0/0/0/3
!
interface GigabitEthernet0/0/0/4
!
!
end

```

L2VPN Quality of Service : 例

次に、ポートモードの L2 インターフェイスにサービス ポリシーをアタッチする例を示します。

```

configure
interface GigabitEthernet 0/0/0/0
l2transport
service-policy input pmap_1
commit

```

疑似回線 : 例

例には、次のデバイスおよび接続が含まれます。

- T-PE1 ノードには次の項目があります。
 - AC インターフェイスとの相互接続 (CE1 方向)
 - S-PE1 ノードへの疑似回線
 - IP アドレス : 209.165.200.225
- T-PE2 ノード
 - AC インターフェイスとの相互接続 (CE2 方向)
 - S-PE1 ノードへの疑似回線
 - IP アドレス : 209.165.200.254
- S-PE1 ノード
 - T-PE1 ノードへの疑似回線セグメントによるマルチセグメント疑似回線相互接続
 - T-PE2 ノードへの疑似回線セグメント
 - IP アドレス : 209.165.202.158

T-PE1 ノードのダイナミック疑似回線の設定 : 例

```
RP/0/RSP0/CPU0:T-PE1# configure
RP/0/RSP0/CPU0:T-PE1 (config)# l2vpn
RP/0/RSP0/CPU0:T-PE1 (config-l2vpn)# pw-class dynamic_mpls
RP/0/RSP0/CPU0:T-PE1 (config-l2vpn-pwc)# encapsulation mpls
RP/0/RSP0/CPU0:T-PE1 (config-l2vpn-pwc-encap-mpls)# protocol ldp
RP/0/RSP0/CPU0:T-PE1 (config-l2vpn-pwc-encap-mpls)# control-word disable
RP/0/RSP0/CPU0:T-PE1 (config-l2vpn-pwc-encap-mpls)# exit
RP/0/RSP0/CPU0:T-PE1 (config-l2vpn-pwc)# exit
RP/0/RSP0/CPU0:T-PE1 (config-l2vpn)# xconnect group XCON1
RP/0/RSP0/CPU0:T-PE1 (config-l2vpn-xc)# p2p xc1
RP/0/RSP0/CPU0:T-PE1 (config-l2vpn-xc-p2p)# description T-PE1 MS-PW to 10.165.202.158
via 10.165.200.254
RP/0/RSP0/CPU0:T-PE1 (config-l2vpn-xc-p2p)# interface gigabitethernet 0/1/0/0.1
RP/0/RSP0/CPU0:T-PE1 (config-l2vpn-xc-p2p)# neighbor 10.165.200.254 pw-id 100
RP/0/RSP0/CPU0:T-PE1 (config-l2vpn-xc-p2p-pw)# pw-class dynamic_mpls
RP/0/RSP0/CPU0:T-PE1 (config-l2vpn-xc-p2p-pw)# commit
```

S-PE1 ノードのダイナミック疑似回線の設定 : 例

```
RP/0/RSP0/CPU0:S-PE1# configure
RP/0/RSP0/CPU0:S-PE1 (config)# l2vpn
RP/0/RSP0/CPU0:S-PE1 (config-l2vpn)# pw-class dynamic_mpls
RP/0/RSP0/CPU0:S-PE1 (config-l2vpn-pwc)# encapsulation mpls
RP/0/RSP0/CPU0:S-PE1 (config-l2vpn-pwc-encap-mpls)# protocol ldp
RP/0/RSP0/CPU0:S-PE1 (config-l2vpn-pwc-encap-mpls)# control-word disable
RP/0/RSP0/CPU0:S-PE1 (config-l2vpn-pwc-encap-mpls)# exit
RP/0/RSP0/CPU0:S-PE1 (config-l2vpn-pwc)# exit
RP/0/RSP0/CPU0:S-PE1 (config-l2vpn)# xconnect group MS-PW1
RP/0/RSP0/CPU0:S-PE1 (config-l2vpn-xc)# p2p ms-pw1
RP/0/RSP0/CPU0:S-PE1 (config-l2vpn-xc-p2p)# description S-PE1 MS-PW between 10.165.200.225
and 10.165.202.158
RP/0/RSP0/CPU0:S-PE1 (config-l2vpn-xc-p2p)# neighbor 10.165.200.225 pw-id 100
RP/0/RSP0/CPU0:S-PE1 (config-l2vpn-xc-p2p-pw)# pw-class dynamic_mpls
RP/0/RSP0/CPU0:S-PE1 (config-l2vpn-xc-p2p-pw)# exit
RP/0/RSP0/CPU0:S-PE1 (config-l2vpn-xc-p2p)# neighbor 10.165.202.158 pw-id 300
RP/0/RSP0/CPU0:S-PE1 (config-l2vpn-xc-p2p-pw)# pw-class dynamic_mpls
RP/0/RSP0/CPU0:S-PE1 (config-l2vpn-xc-p2p-pw)# commit
```

T-PE2 ノードのダイナミック疑似回線の設定 : 例

```
RP/0/RSP0/CPU0:T-PE2# configure
RP/0/RSP0/CPU0:T-PE2 (config)# l2vpn
RP/0/RSP0/CPU0:T-PE2 (config-l2vpn)# pw-class dynamic_mpls
RP/0/RSP0/CPU0:T-PE2 (config-l2vpn-pwc)# encapsulation mpls
RP/0/RSP0/CPU0:T-PE2 (config-l2vpn-pwc-encap-mpls)# protocol ldp
RP/0/RSP0/CPU0:T-PE2 (config-l2vpn-pwc-encap-mpls)# control-word disable
RP/0/RSP0/CPU0:T-PE2 (config-l2vpn-pwc-encap-mpls)# exit
RP/0/RSP0/CPU0:T-PE2 (config-l2vpn-pwc)# exit
RP/0/RSP0/CPU0:T-PE2 (config-l2vpn)# xconnect group XCON1
RP/0/RSP0/CPU0:T-PE2 (config-l2vpn-xc)# p2p xc1
RP/0/RSP0/CPU0:T-PE2 (config-l2vpn-xc-p2p)# description T-PE2 MS-PW to 10.165.200.225 via
10.165.200.254
RP/0/RSP0/CPU0:T-PE2 (config-l2vpn-xc-p2p)# interface gigabitethernet 0/2/0/0.4
RP/0/RSP0/CPU0:T-PE2 (config-l2vpn-xc-p2p)# neighbor 10.165.200.254 pw-id 300
RP/0/RSP0/CPU0:T-PE2 (config-l2vpn-xc-p2p-pw)# pw-class dynamic_mpls
RP/0/RSP0/CPU0:T-PE2 (config-l2vpn-xc-p2p-pw)# commit
```

T-PE1 ノードのダイナミック疑似回線と優先パスの設定 : 例

```

RP/0/RSP0/CPU0:T-PE1# configure
RP/0/RSP0/CPU0:T-PE1 (config)# l2vpn
RP/0/RSP0/CPU0:T-PE1 (config-l2vpn)# pw-class dynamic_mpls
RP/0/RSP0/CPU0:T-PE1 (config-l2vpn-pwc)# encapsulation mpls
RP/0/RSP0/CPU0:T-PE1 (config-l2vpn-pwc-encap-mpls)# protocol ldp
RP/0/RSP0/CPU0:T-PE1 (config-l2vpn-pwc-encap-mpls)# control-word disable
RP/0/RSP0/CPU0:T-PE1 (config-l2vpn-pwc-encap-mpls)# preferred-path interface tunnel-te
1000
RP/0/RSP0/CPU0:T-PE1 (config-l2vpn-pwc-encap-mpls)# exit
RP/0/RSP0/CPU0:T-PE1 (config-l2vpn-pwc)# exit
RP/0/RSP0/CPU0:T-PE1 (config-l2vpn)# xconnect group XCON1
RP/0/RSP0/CPU0:T-PE1 (config-l2vpn-xc)# p2p xc1
RP/0/RSP0/CPU0:T-PE1 (config-l2vpn-xc-p2p)# description T-PE1 MS-PW to 10.165.202.158
via 10.165.200.254
RP/0/RSP0/CPU0:T-PE1 (config-l2vpn-xc-p2p)# interface gigabitethernet 0/1/0/0.1
RP/0/RSP0/CPU0:T-PE1 (config-l2vpn-xc-p2p)# neighbor 10.165.200.254 pw-id 100
RP/0/RSP0/CPU0:T-PE1 (config-l2vpn-xc-p2p-pw)# pw-class dynamic_mpls
RP/0/RSP0/CPU0:T-PE1 (config-l2vpn-xc-p2p-pw)# commit

```

S-PE1 ノードのダイナミック疑似回線と優先パスの設定 : 例

```

RP/0/RSP0/CPU0:S-PE1# configure
RP/0/RSP0/CPU0:S-PE1 (config)# l2vpn
RP/0/RSP0/CPU0:S-PE1 (config-l2vpn)# pw-class dynamic_mpls1
RP/0/RSP0/CPU0:S-PE1 (config-l2vpn-pwc)# encapsulation mpls
RP/0/RSP0/CPU0:S-PE1 (config-l2vpn-pwc-encap-mpls)# protocol ldp
RP/0/RSP0/CPU0:S-PE1 (config-l2vpn-pwc-encap-mpls)# control-word disable
RP/0/RSP0/CPU0:S-PE1 (config-l2vpn-pwc-encap-mpls)# preferred-path interface tunnel-te
1000
RP/0/RSP0/CPU0:S-PE1 (config-l2vpn-pwc-encap-mpls)# exit
RP/0/RSP0/CPU0:S-PE1 (config-l2vpn-pwc)# exit
RP/0/RSP0/CPU0:S-PE1 (config-l2vpn)# pw-class dynamic_mpls2
RP/0/RSP0/CPU0:S-PE1 (config-l2vpn-pwc)# encapsulation mpls
RP/0/RSP0/CPU0:S-PE1 (config-l2vpn-pwc-encap-mpls)# protocol ldp
RP/0/RSP0/CPU0:S-PE1 (config-l2vpn-pwc-encap-mpls)# control-word disable
RP/0/RSP0/CPU0:S-PE1 (config-l2vpn-pwc-encap-mpls)# preferred-path interface tunnel-te
2000
RP/0/RSP0/CPU0:S-PE1 (config-l2vpn-pwc-encap-mpls)# exit
RP/0/RSP0/CPU0:S-PE1 (config-l2vpn-pwc)# exit
RP/0/RSP0/CPU0:S-PE1 (config-l2vpn)# xconnect group MS-PW1
RP/0/RSP0/CPU0:S-PE1 (config-l2vpn-xc)# p2p ms-pw1
RP/0/RSP0/CPU0:S-PE1 (config-l2vpn-xc-p2p)# description S-PE1 MS-PW between 10.165.200.225
and 10.165.202.158
RP/0/RSP0/CPU0:S-PE1 (config-l2vpn-xc-p2p)# neighbor 10.165.200.225 pw-id 100
RP/0/RSP0/CPU0:S-PE1 (config-l2vpn-xc-p2p-pw)# pw-class dynamic_mpls1
RP/0/RSP0/CPU0:S-PE1 (config-l2vpn-xc-p2p-pw)# exit
RP/0/RSP0/CPU0:S-PE1 (config-l2vpn-xc-p2p)# neighbor 10.165.202.158 pw-id 300
RP/0/RSP0/CPU0:S-PE1 (config-l2vpn-xc-p2p-pw)# pw-class dynamic_mpls2
RP/0/RSP0/CPU0:S-PE1 (config-l2vpn-xc-p2p-pw)# commit

```

T-PE2 ノードのダイナミック疑似回線と優先パスの設定 : 例

```

RP/0/RSP0/CPU0:T-PE2# configure
RP/0/RSP0/CPU0:T-PE2 (config)# l2vpn
RP/0/RSP0/CPU0:T-PE2 (config-l2vpn)# pw-class dynamic_mpls
RP/0/RSP0/CPU0:T-PE2 (config-l2vpn-pwc)# encapsulation mpls
RP/0/RSP0/CPU0:T-PE2 (config-l2vpn-pwc-encap-mpls)# protocol ldp
RP/0/RSP0/CPU0:T-PE2 (config-l2vpn-pwc-encap-mpls)# control-word disable

```

```

RP/0/RSP0/CPU0:S-PE1 (config-l2vpn-pwc-encap-mpls) # preferred-path interface tunnel-te
2000
RP/0/RSP0/CPU0:T-PE2 (config-l2vpn-pwc-encap-mpls) # exit
RP/0/RSP0/CPU0:T-PE2 (config-l2vpn-pwc) # exit
RP/0/RSP0/CPU0:T-PE2 (config-l2vpn) # xconnect group XCON1
RP/0/RSP0/CPU0:T-PE2 (config-l2vpn-xc) # p2p xc1
RP/0/RSP0/CPU0:T-PE2 (config-l2vpn-xc-p2p) # description T-PE2 MS-PW to 10.165.200.225 via
10.165.200.254
RP/0/RSP0/CPU0:T-PE2 (config-l2vpn-xc-p2p) # interface gigabitethernet 0/2/0/0.4
RP/0/RSP0/CPU0:T-PE2 (config-l2vpn-xc-p2p) # neighbor 10.165.200.254 pw-id 300
RP/0/RSP0/CPU0:T-PE2 (config-l2vpn-xc-p2p-pw) # pw-class dynamic_mpls
RP/0/RSP0/CPU0:T-PE2 (config-l2vpn-xc-p2p-pw) # commit

```

T-PE1 ノードのスタティック疑似回線の設定 : 例

```

RP/0/RSP0/CPU0:T-PE1# configure
RP/0/RSP0/CPU0:T-PE1 (config) # l2vpn
RP/0/RSP0/CPU0:T-PE1 (config-l2vpn) # xconnect group XCON1
RP/0/RSP0/CPU0:T-PE1 (config-l2vpn-xc) # p2p xc1
RP/0/RSP0/CPU0:T-PE1 (config-l2vpn-xc-p2p) # interface gigabitethernet 0/1/0/0.1
RP/0/RSP0/CPU0:T-PE1 (config-l2vpn-xc-p2p) # neighbor 10.165.200.254 pw-id 100
RP/0/RSP0/CPU0:T-PE1 (config-l2vpn-xc-p2p-pw) # mpls static label local 50 remote 400
RP/0/RSP0/CPU0:T-PE1 (config-l2vpn-xc-p2p-pw) # commit

```

S-PE1 ノードのスタティック疑似回線の設定 : 例

```

RP/0/RSP0/CPU0:S-PE1# configure
RP/0/RSP0/CPU0:S-PE1 (config) # l2vpn
RP/0/RSP0/CPU0:S-PE1 (config-l2vpn) # xconnect group MS-PW1
RP/0/RSP0/CPU0:S-PE1 (config-l2vpn-xc) # p2p ms-pw1
RP/0/RSP0/CPU0:S-PE1 (config-l2vpn-xc-p2p) # neighbor 10.165.200.225 pw-id 100
RP/0/RSP0/CPU0:S-PE1 (config-l2vpn-xc-p2p-pw) # mpls static label local 400 remote 50
RP/0/RSP0/CPU0:S-PE1 (config-l2vpn-xc-p2p-pw) # exit
RP/0/RSP0/CPU0:S-PE1 (config-l2vpn-xc-p2p) # neighbor 10.165.202.158 pw-id 300
RP/0/RSP0/CPU0:S-PE1 (config-l2vpn-xc-p2p-pw) # mpls static label local 40 remote 500
RP/0/RSP0/CPU0:S-PE1 (config-l2vpn-xc-p2p-pw) # commit

```

T-PE2 ノードのスタティック疑似回線の設定 : 例

```

RP/0/RSP0/CPU0:T-PE2# configure
RP/0/RSP0/CPU0:T-PE2 (config) # l2vpn
RP/0/RSP0/CPU0:T-PE2 (config-l2vpn) # xconnect group XCON1
RP/0/RSP0/CPU0:T-PE2 (config-l2vpn-xc) # p2p xc1
RP/0/RSP0/CPU0:T-PE2 (config-l2vpn-xc-p2p) # interface gigabitethernet 0/2/0/0.4
RP/0/RSP0/CPU0:T-PE2 (config-l2vpn-xc-p2p) # neighbor 10.165.200.254 pw-id 300
RP/0/RSP0/CPU0:T-PE2 (config-l2vpn-xc-p2p-pw) # mpls static label local 500 remote 40
RP/0/RSP0/CPU0:T-PE2 (config-l2vpn-xc-p2p-pw) # commit

```

優先パス : 例

次に、優先トンネルパスを設定する例を示します。

```

configure
l2vpn
pw-class path1
encapsulation mpls
preferred-path interface tunnel tp 50 fallback disable

```

MPLS トランスポート プロファイル : 例

ここでは、次の例を示します。

- 優先トンネルパスの設定 : 例
- PW ステータス OAM の設定 : 例

優先トンネルパスの設定 : 例

この設定例では、優先トンネルパスを設定する方法を示します。

```
l2vpn
pw-class foo
  encapsulation mpls
  preferred-path interface tunnel-tp 100 fallback disable
commit
```

PW ステータス OAM の設定 : 例

この設定例では、PW ステータス OAM 機能を設定する方法を示します。

```
l2vpn
pw-oam refresh transmit 100
commit
```

疑似回線ステータスの表示 : 例

show l2vpn xconnect

```
RP/0/RSP0/CPU0:router# show l2vpn xconnect
Legend: ST = State, UP = Up, DN = Down, AD = Admin Down, UR = Unresolved,
        LU = Local Up, RU = Remote Up, CO = Connected

XConnect
Group      Name      ST      Segment 1      Segment 2
-----
Description      ST      Description      ST
-----
MS-PW1      ms-pw1    UP      70.70.70.70    100    UP      90.90.90.90    300    UP
-----
```

show l2vpn xconnect detail

```
RP/0/RSP0/CPU0:router# show l2vpn xconnect detail
Group MS-PW1, XC ms-pw1, state is up; Interworking none
PW: neighbor 70.70.70.70, PW ID 100, state is up ( established )
PW class not set
Encapsulation MPLS, protocol LDP
PW type Ethernet VLAN, control word enabled, interworking none
PW backup disable delay 0 sec
Sequencing not set
PW Status TLV in use
      MPLS          Local                      Remote
-----
Label          16004                      16006
Group ID       0x2000400                  0x2000700
Interface      GigabitEthernet0/1/0/2.2    GigabitEthernet0/1/0/0.3
MTU            1500                      1500
```



```

Control word enabled                enabled
PW type      Ethernet VLAN          Ethernet VLAN
VCCV CV type 0x2                    0x2
              (LSP ping verification) (LSP ping verification)
VCCV CC type 0x5                    0x7
              (control word)          (control word)
              (router alert label)
              (TTL expiry)           (TTL expiry)
-----

Incoming Status (PW Status TLV):
  Status code: 0x0 (Up) in Notification message
Outgoing PW Switching TLVs (Label Mapping message):
  Local IP Address: 80.80.80.80, Remote IP address: 90.90.90.90, PW ID: 300
  Description: S-PE1 MS-PW between 70.70.70.70 and 90.90.90.90
Outgoing Status (PW Status TLV):
  Status code: 0x0 (Up) in Notification message
Statistics:
  packet totals: receive 0
  byte totals: receive 0
Create time: 04/04/2008 23:18:24 (00:01:24 ago)
Last time status changed: 04/04/2008 23:19:30 (00:00:18 ago)
PW: neighbor 90.90.90.90, PW ID 300, state is up ( established )
PW class not set
Encapsulation MPLS, protocol LDP
PW type Ethernet VLAN, control word enabled, interworking none
PW backup disable delay 0 sec
Sequencing not set
PW Status TLV in use
  MPLS      Local      Remote
-----
Label      16004      16006
Group ID   0x2000800  0x2000200
Interface  GigabitEthernet0/1/0/0.3 GigabitEthernet0/1/0/2.2
MTU        1500
Control word enabled                enabled
PW type      Ethernet VLAN          Ethernet VLAN
VCCV CV type 0x2                    0x2
              (LSP ping verification) (LSP ping verification)
VCCV CC type 0x5                    0x7
              (control word)          (control word)
              (router alert label)
              (TTL expiry)           (TTL expiry)
-----

Incoming Status (PW Status TLV):
  Status code: 0x0 (Up) in Notification message
Outgoing PW Switching TLVs (Label Mapping message):
  Local IP Address: 80.80.80.80, Remote IP address: 70.70.70.70, PW ID: 100
  Description: S-PE1 MS-PW between 70.70.70.70 and 90.90.90.90
Outgoing Status (PW Status TLV):
  Status code: 0x0 (Up) in Notification message
Statistics:
  packet totals: receive 0
  byte totals: receive 0
Create time: 04/04/2008 23:18:24 (00:01:24 ago)
Last time status changed: 04/04/2008 23:19:30 (00:00:18 ago)

```

Any Transport over MPLS (AToM) の設定 : 例

次に、Any Transport over MPLS (AToM) を設定する例を示します。

```

config
l2vpn
  xconnect group test
  p2p test
  interface POS 0/1/0/0.1
    neighbor 10.1.1.1 pw-id 100

```

AToM IP インターワーキングの設定：例

次に、IP インターワーキングを設定する例を示します。

```

config
l2vpn
  xconnect group test
  p2p test
  interworking ipv4

```

PPP IP インターワーキングの設定：例

次に、PPP IP インターワーキングを設定する例を示します。

```

interface Serial0/2/1/0/1/1/1:0
  encapsulation ppp
  l2transport
  !
  !
interface Serial0/0/0/0/2/1/1:0
  encapsulation ppp
  l2transport
  !
  !

!! Local Switching Configuration
l2vpn
xconnect group ppp_ip_ls
  p2p 1
  interface Serial0/2/1/0/1/1/1:0
  interface GigabitEthernet0/0/0/1.1
  interworking ipv4
  !

!! PW Configuration
l2vpn
xconnect group ppp_ip_iw
  p2p 1
  interface Serial0/0/0/0/2/1/1:0
  neighbor 120.120.120.120 pw-id 3
  pw-class class1
  !
  interworking ipv4

```

cHDLC IP インターワーキングの設定：例

次に、cHDLC IP インターワーキングを設定する例を示します。

```

interface Serial0/2/1/0/1/1/2:0
  l2transport

interface Serial0/0/0/0/2/1/2:0

```

```
l2transport

!! Local Switching Configuration
l2vpn
xconnect group ppp_ip_ls
  p2p 1
  interface Serial0/2/1/0/1/1/2:0
  interface GigabitEthernet0/0/0/2.1
  interworking ipv4
!

!! PW Configuration
l2vpn
xconnect group ppp_ip_iw
  p2p 1
  interface Serial0/0/0/0/2/1/2:0
  neighbor 120.120.120.120 pw-id 3
  pw-class class1
!
  interworking ipv4
```

MLPPP IP インターワーキングの設定 : 例

次に、MLPPP IP インターワーキングを設定する例を示します。

```
interface Multilink0/2/1/0/1
  multilink
l2transport
!

interface Multilink0/2/1/0/51
Multilink
l2transport

!! Local Switching Configuration
l2vpn
xconnect group mlppp_ip_ls
  p2p 1
  interface Multilink0/2/1/0/1
  interface GigabitEthernet0/0/0/1.151
  interworking ipv4
!

!! PW Configuration
l2vpn
xconnect group mlppp_ip_iw
  p2p 151
  interface Multilink0/2/1/0/51
  neighbor 140.140.140.140 pw-id 151
  pw-class test
!
  interworking ipv4
!
```

Circuit Emulation over Packet Switched Network の設定 : 例

次に、Circuit Emulation Over Packet Switched Network を設定する例を示します。

CEM 接続回線の PW への追加

```

l2vpn
xconnect group gr1
  p2p p1
    interface CEM 0/0/0/0:10
    neighbor 3.3.3.3 pw-id 11
  !
!
```

疑似回線クラスの関連付け

```

l2vpn
pw-class class-cem
  encapsulation mpls
  protocol ldp
!
!
xconnect group gr1
  p2p p1
    interface CEM0/0/0/0:20
    neighbor 1.2.3.4 pw-id 11
    pw-class class-cem
  !
!
```

疑似回線ステータスのイネーブル化

```

l2vpn
pw-status
commit
```

疑似回線ステータスのディセーブル化

```

l2vpn
pw-status disable
commit
```

バックアップ疑似回線の設定

```

l2vpn
pw-status
pw-class class-cem
  encapsulation mpls
  protocol ldp
!
!
xconnect group gr1
  p2p p1
    interface CEM0/0/0/0:20
    neighbor 1.2.3.4 pw-id 11
    pw-class class-cem
    backup neighbor 9.9.9.9 pw-id 1221
    pw-class class-cem
  !
!
```

L2VPN ノンストップルーティングの設定 : 例

次に、L2VPN ノンストップルーティングを設定する例を示します。

```
config
l2vpn
nsr
logging nsr
```

疑似回線のグループ化のイネーブル化：例

次に、疑似回線のグループ化をイネーブルにする例を示します。

```
config
l2vpn
pw-grouping
```

L2TPv3 over IPv6 トンネルの設定：例

ここでは、次の例を示します。

疑似回線のネイバー AFI の設定：例

IPv6 疑似回線ネイバーをサポートするには、AFI を次のように設定する必要があります。

```
l2vpn
xconnect group g1
p2p xc3
interface GigabitEthernet0/0/0/4.2
neighbor ipv6 1111:2222::cdef pw-id 1
```

L2TPv3 のカプセル化とプロトコルの設定：例

L2TPv3 トンネルの場合、カプセル化とプロトコルを L2TPv3 に設定する必要があります。



(注) デフォルトのカプセル化とプロトコルは MPLS です。

```
l2vpn
pw-class ts
encapsulation l2tpv3
protocol l2tpv3
```

L2TPv3 over IPv6 トンネルの送信元 IPv6 アドレスの設定：例

次に、L2TPv3 over IPv6 トンネルの送信元 IPv6 アドレスを設定する例を示します。

```
l2vpn
xconnect group g1
p2p xc3
interface GigabitEthernet0/0/0/4.2
neighbor ipv6 1111:2222::cdef pw-id 1
source 1111:2222::abcd
```

ローカルおよびリモートセッションの設定：例

L2TPv3 over IPv6 トンネルの場合、ローカルおよびリモートセッション ID は疑似回線で設定されます。ただし、この設定はオプションです。

```

l2vpn
xconnect group g1
p2p xc3
interface GigabitEthernet0/0/0/4.2
neighbor ipv6 1111:2222::cdef pw-id 1
l2tp static local session 1
l2tp static remote session 1

```

ローカルおよびリモート Cookie の設定 : 例

L2TPv3 over IPv6 トンネルの場合、ローカルおよびリモート Cookie は疑似回線で設定されま
す。Cookie ロールオーバーのサポートが拡張され、セカンダリローカル Cookie を設定できる
ようになりました。次に、サイズ 0 の Cookie を設定する例を示します。

```

l2vpn
xconnect group g1
p2p xc3
interface GigabitEthernet0/0/0/4.2
neighbor ipv6 1111:2222::cdef pw-id 1
l2tp static local cookie size 0
l2tp static remote cookie size 0

```

次に、サイズ 4 の Cookie を設定する例を示します。

```

l2vpn
xconnect group g1
p2p xc3
interface GigabitEthernet0/0/0/4.2
neighbor ipv6 1111:2222::cdef pw-id 1
l2tp static local cookie size 4 value <0x0-0xffffffff>
l2tp static remote cookie size 4 value <0x0-0xffffffff>

```

次に、サイズ 8 の Cookie を設定する例を示します（下位 4 バイトが最初に入力され、その後
に上位 4 バイトが続きます）。

```

l2vpn
xconnect group g1
p2p xc3
interface GigabitEthernet0/0/0/4.2
neighbor ipv6 1111:2222::cdef pw-id 1
l2tp static local cookie size 8 value <0x0-0xffffffff> <0x0-0xffffffff>
l2tp static remote cookie size 8 value <0x0-0xffffffff> <0x0-0xffffffff>

```

L2TPv3 over IPv6 トンネルで Cookie ロールオーバーをサポートするには、セカンダリローカル
Cookie を設定します。local cookie secondary コマンドは、ローカルルータのセカンダリ Cookie
値を指定します。



- (注) プライマリおよびセカンダリ Cookie は同じサイズに設定する必要があります。プライマリま
たはセカンダリローカル Cookie は、リモートエンドから受信する Cookie 値と一致する必要が
あります。そうでない場合、パケットはドロップされます。

```

l2vpn
xconnect group g1
p2p xc3
interface GigabitEthernet0/0/0/4.2
neighbor ipv6 1111:2222::cdef pw-id 1
l2tp static local cookie secondary size 8 value <0x0-0xffffffff> <0x0-0xffffffff>

```

L2TP スタティックサブモードの有効化：例

次に、L2TP スタティックサブモードを有効にする例を示します。

```
l2vpn
xconnect group g1
p2p xc3
interface GigabitEthernet0/0/0/4.2
neighbor ipv6 1111:2222::cdef pw-id 1
l2tp static
local cookie <>
```

L2TPv3 ヘッダーの TOS リフレクションの有効化：例

L2TPv3 over IPv6 トンネルの場合、タイプオブサービス (TOS) リフレクションの有効化や、L2TPv3 ヘッダーへの特定の TOS 値の設定が各疑似回線クラスに対してサポートされます。



- (注) デフォルトでは、TOS は VLAN ヘッダーのサービスクラス (COS) フィールドからコピーされます。基本となるパケットが IPv4 または IPv6 パケットでない場合、TOS リフレクションが設定されている場合でも、COS フィールドは VLAN ヘッダーからコピーされます。

次に、L2TPv3 ヘッダーに TOS リフレクションを設定する例を示します。

```
l2vpn
pw-class ts
encapsulation l2tpv3
protocol l2tpv3
tos reflect
```

This example shows how to set a TOS value in the L2TPv3 header:

```
l2vpn
pw-class ts
encapsulation l2tpv3
protocol l2tpv3
tos value 64
```

L2TPv3 over IPv6 トンネルの TTL の設定：例

L2TPv3 over IPv6 トンネルの場合、疑似回線クラスで TTL 設定がサポートされます。

```
l2vpn
pw-class ts
encapsulation l2tpv3
protocol l2tpv3
ttl <1-255>
```

L2TPv3 over IPv6 トンネルのトラフィックミラーリングの設定：例

次に、EFP をモニタセッションに関連付ける例を示します。

```
interface GigabitEthernet0/0/0/4.2 l2transport
monitor-session customer-foo
```

レイヤ 2 SPAN は L3 インターフェイスでサポートされています。ただし、レイヤ 2 フレームはミラーリングされません。

L2TPv3 over IPv4 トンネルの設定 : 例

```
interface GigabitEthernet0/0/0/4.2
ipv6 address <>
monitor-session customer-foo
```

SPAN はメインインターフェイスでもサポートされています。

```
interface GigabitEthernet0/4/0/3
l2transport
monitor-session customer-foo
```

次に、モニタセッションをグローバルに作成する例を示します。

```
monitor-session customer-foo
destination pseudowire
```

次に、モニタセッションと L2TPv3 over IPv6 トンネルとの間にクロスコネクトを作成する例を示します。

```
l2vpn
xconnect group span
p2p span-foo
monitor-session customer-foo
neighbor ipv6 1111:3333::cdef pw-id 1001
pw-class ts
source 1111:3333::abcd
l2tp static local cookie size 8 value 0xabcd 0x1234
l2tp static remote cookie size 8 value 0xcdef 0x5678
```

詳細については、次を参照してください。

- L2TPv3 over IPv6 トンネルの概念については、「[L2TPv3 over IPv6](#)」を参照してください
- 設定手順については、「[L2TPv3 over IPv6 トンネルの設定](#)」を参照してください

L2TPv3 over IPv4 トンネルの設定 : 例

ここでは、次の例を示します。

ダイナミック L2TPv3 疑似回線の設定

リモート IPv4 ピアに接続するダイナミック L2TPv3 疑似回線を設定するには、次の作業を実行します。

手順の概要

1. **configure**
2. **l2vpn**
3. **xconnect group name**
4. **p2p name**
5. **interfacetype interface-path-id**
6. **neighbor ipv4 ip-address pw-id number**
7. **pw-class pw-class-name**
8. **commit** コマンドまたは **end** コマンドを使用します。

手順の詳細

ステップ1 **configure**

例：

```
RP/0/RSP0/cpu 0: router# configure
```

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 **l2vpn**

例：

```
RP/0/RSP0/cpu 0: router(config)# l2vpn
```

L2VPN 設定サブモードを開始します。

ステップ3 **xconnect group name**

例：

```
RP/0/RSP0/cpu 0: router(config-l2vpn)# xconnect group L2TPV3_V4_XC_GRP
```

クロスコネクグループの名前を入力します。

ステップ4 **p2p name**

例：

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc)# p2p L2TPV3_P2P_1
```

p2p コンフィギュレーション サブモードを開始して、ポイントツーポイントの相互接続を設定します。

ステップ5 **interfacetype interface-path-id**

例：

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p)# interface GigabitEthernet 0/2/0/0/0.1
```

インターフェイス タイプ ID を指定します。選択できる基準は、次のとおりです。

- GigabitEthernet
- TenGigE

ステップ6 **neighbor ipv4 ip-address pw-id number**

例：

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p)# neighbor ipv4 26.26.26.26 pw-id 100
```

相互接続の疑似回線を設定します。

ステップ7 **pw-class pw-class-name**

例：

L2TPv3 のカプセル化とプロトコルの設定 : 例

```
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p-pw)# pw-class L2TPV3_V4_CLASS
```

疑似回線クラスサブモードを開始して、クロスコネクトの名前を定義します。

ステップ 8 **commit** コマンドまたは **end** コマンドを使用します。

commit : 設定の変更を保存し、コンフィギュレーションセッションに留まります。

end : 次のいずれかのアクションを実行することをユーザに要求します。

- [Yes] : 設定変更を保存し、コンフィギュレーションセッションを終了します。
- [No] : 設定変更をコミットせずにコンフィギュレーションセッションを終了します。
- [Cancel] : 設定変更をコミットせずに、コンフィギュレーションモードに留まります。

L2TPv3 のカプセル化とプロトコルの設定 : 例

次に、L2TPv3 トンネルのカプセル化とプロトコルを設定する例を示します。

```
configure
l2vpn
  pw-class L2TPV3_V4_CLASS
    encapsulation l2tpv3
    protocol l2tpv3 class L2TP-CLASS
    dfbit set
    ipv4 source 25.25.25.25
    cookie size 4
  !
!
```

L2TP 制御チャネルパラメータの設定 : 例

次の例は、一般的な L2TPv3 制御チャネル設定を示しています。

```
configure
l2tp-class L2TP-CLASS
  authentication
  retransmit retries 5
  retransmit initial retries 10
  retransmit initial timeout max 5
  retransmit timeout max 6
  hidden
  password 7 1511021F07257A767B
  hello-interval 10
  digest hash MD5
!
```

EVPN-VPWS の設定例

EVPN-VPWS の設定 : 例

次に、EVPN-VPWS サービスを設定する例を示します。

```
RP/0/RSP0/cpu 0: router# configure
```

```
RP/0/RSP0/cpu 0: router(config)# l2vpn
RP/0/RSP0/cpu 0: router(config-l2vpn)# xconnect group pw-hel
RP/0/RSP0/cpu 0: router(config-l2vpn-xc)# p2p pw-ss
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p)# interface gigabitethernet 0/1/0/9
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p)# neighbor evpn evi 100 target 12 source 10
```

次に、PWHE インターフェイスへの EVPN-VPWS を設定する例を示します。

```
RP/0/RSP0/cpu 0: router# configure
RP/0/RSP0/cpu 0: router(config)# l2vpn
RP/0/RSP0/cpu 0: router(config-l2vpn)# xconnect group xg1
RP/0/RSP0/cpu 0: router(config-l2vpn-xc)# p2p pwhe1
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p)# interface PW-Ether 1
RP/0/RSP0/cpu 0: router(config-l2vpn-xc-p2p)# neighbor evpn evi 2 target 20 source 20
```

EVPN-VPWS を使用したアクセス PW の設定 : 例

次の例は、ブリッジドメインが EVPN-VPWS を使用してアクセス擬似回線を設定する方法を示しています。

```
RP/0/RSP0/cpu 0: router# configure
RP/0/RSP0/cpu 0: router(config)# l2vpn
RP/0/RSP0/cpu 0: router(config-l2vpn)# bridge group bg1
RP/0/RSP0/cpu 0: router(config-l2vpn-bg)# bridge-domain bd1
RP/0/RSP0/cpu 0: router(config-l2vpn-bg-bd)# neighbor evpn evi 1 target 100
```

