ワイドエリアネットワークコンフィギュレーションガイド：レイヤ2サービス

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次

第 1 章

最初にお読みください

Cisco IOS XE 16 に関する重要な情報

Cisco IOS XE リリース 3.7.0E（Catalyst スイッチング用）および Cisco IOS XE リリース 3.17S（アクセスおよびエッジルーティング用）の 2 つのリリースは、コンバージドリリースの 1 つのバージョン - Cisco IOS XE 16 - に統合されました。この 1 つのリリースでスイッチングおよびルーティング ポートフォリオのアクセスおよびエッジ製品を幅広くカバーしています。

（注） 技術構成ガイドの機能情報の表に、機能の導入時期を記載しています。他のプラットフォームがその機能をサポートした時期については、記載があるものも、ないものもあります。特定の機能が、使用しているプラットフォームでサポートされているかどうかを判断するには、製品のランディング ページに掲載された技術構成ガイドを参照してください。技術構成ガイドが製品のランディング ページに表示されると、その機能が該当のプラットフォームでサポートされているかどうかが示されます。

第 2 章

ワイドエリア ネットワーキングの概要

Cisco IOS ソフトウェアは、ほぼすべてのネットワーク環境のニーズに適合するさまざまなワイドエリア ネットワーキング機能を提供します。シスコは、Switched Multimegabit Data Service（SMDS）を介したセル リレー、ISDN を介した回線交換、フレーム リレーを介したパケット交換、および非同期転送モード（ATM）を介した回線交換とパケット交換の両方の利点を提供します。LAN エミュレーション（LANE）は、ATM とその他のタイプの LAN とを接続します。『*Cisco IOS Wide-Area Networking Configuration Guide*』は、次のソフトウェア コンポーネントの設定に関する一連の一般的なガイドラインを示します。

このモジュールは、それぞれの技術の概要を示します。特定の設定については、該当するモジュールを参照してください。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

フレーム リレー

Cisco フレーム リレー実装では、現在 IP、DECnet、AppleTalk、XNS、Novell IPX、CLNS、Banyan VINES、トランスペアレント ブリッジングのルーティングをサポートします。

当初、フレーム リレー アクセスは専用回線に限定されていましたが、ダイヤルアップ アクセスがサポートされるようになりました。ダイヤラ プロファイルまたは従来のダイヤルオンデマンド ルーティング（DDR）の詳細については、モジュール「Dial-on-Demand Routing Configuration」を参照してください。

フレーム リレーをサポートするインターフェイスで中央のサーバからソフトウェアをダウンロードして、新しいルータまたはアクセス サーバにソフトウェアをインストールするには、モジュール「Loading and Maintaining System Images」を参照してください。

フレーム リレー ネットワーク上のシステム ネットワーク アーキテクチャ（SNA）デバイス間のアクセスを設定するには、モジュール「Configuring SNA Frame Relay Access Support」を参照してください。

フレーム リレー ソフトウェアは、次の機能を提供します。

- フレーム リレー ローカル管理インターフェイス（LMI）の通常実装される次の 3 つの仕様をサポートしています。
  - Northern Telecom、Digital Equipment Corporation、StrataCom、およびシスコが共同開発したフレーム リレー インターフェイス仕様
  - ANSI 導入フレーム リレー信号仕様 T1.617 Annex D
  - ITU-T 導入フレーム リレー信号仕様 Q.933 Annex A
- 次の ITU-T I シリーズ（ISDN）推奨事項 I122「Framework for Additional Packet Mode Bearer Services」に準拠しています。
  - ANSI 導入フレーム リレー カプセル化仕様 T1.618
  - ITU-T 導入フレーム リレー カプセル化仕様 Q.922 Annex A
- ブリッジングを除き、RFC 2427 に沿ったインターネット技術特別調査委員会（IETF）カプセル化に準拠しています。
- 次のようにキープアライブ メカニズム、マルチキャスト グループ、およびステータス メッセージをサポートしています。
  - キープアライブ メカニズムでは、ネットワーク サーバとスイッチの間で情報を交換することで、データが流れていることをスイッチが確認します。
  - マルチキャスト メカニズムは、ローカル データリンク接続識別子（DLCI）およびマルチキャスト DLCI をネットワーク サーバに提供します。この機能は、共同のフレーム リレー仕様の実装に固有のものです。

- ステータス メカニズムは、スイッチによって認識されている DLCI に関する現在のステータス レポートを提供します。

- 同じサイトおよびルータで PVC と SVC の両方をサポートしています。

SVC を使用すると、必要な場合にだけ宛先エンドポイントへのパスを設定し、不要になった場合はパスを破棄することで、フレーム リレー ネットワークを介してアクセスできます。

- Cisco IOS Release 11.2 以降、フレーム リレー トラフィック シェーピングをサポートしています。トラフィック シェーピングは、以下を提供します。
  - 個々の回線に対するレート適用。アウトバウンド トラフィックのピーク レートを、認定情報レート（CIR）またはユーザ設定可能なその他のレートに設定できます。
  - 仮想回線ごとの動的トラフィック スロットリング。逆方向明示的輻輳通知（BECN）パケット□ネットワーク上の輻輳を示すと、アウトバウンド トラフィック レートは自動的に逓減します。輻輳が緩和されると、アウトバウンド トラフィック レートは再び逓増します。
  - 仮想回線ごとに高度なキューイングをサポート。個別の仮想回線にカスタム キューイング、プライオリティ キューイング、および均等化キューイングを設定できます。

- フレーム リレーから DECnet Phase IV および CLNS への輻輳情報の伝送。このメカニズムは、着信 DLCI 上の順方向明示的輻輳通知（FECN）ビットを確認した後、フレーム リレー層から上位層プロトコルに FECN ビットをプロモートします。このフレーム リレー輻輳情報を使用して、エンドホストの送信レートを調整します。デフォルトで FECN ビット プロモーションは、フレーム リレー カプセル化を使用したすべてのインターフェイス上でイネーブルになっています。設定は必要ありません。

- AppleTalk、Banyan VINES、DECnet、IP、IPX の各プロトコル、および DECnet、CLNP、Banyan VINES 用のネイティブ hello パケットに対する、フレーム リレー Inverse ARP のサポート（RFC 1293 で規定）。これにより、フレーム リレーを実行中のルータは、仮想回線に関連付けられたデバイスのプロトコル アドレスを検出できるようになります。

- フレーム リレー スイッチングのサポート。これにより、パケットは DLCI（フレーム リレーで Media Access Control（MAC）レベル アドレスに相当するもの）に基づいて切り替えられます。ルータは、フレーム リレー ネットワーク内にハイブリッド DTE スイッチまたはピュア フレーム リレー DCE アクセス ノードとして設定されます。

フレーム リレー スイッチングは、1 つの DLCI に着信するすべてのトラフィックを、別の DLCI 上で同じネクストホップ アドレスに送信できる場合に使用されます。このような場合、Cisco IOS ソフトウェアは、宛先アドレスを検出するためにフレームを個別に検査する必要がないので、ルータに対する処理負荷が軽減されます。

シスコが採用しているフレーム リレー スイッチングでは、次の機能が提供されています。

-
  - IP トンネルでのスイッチング
  - ネットワーク間インターフェイス（NNI）でのほかのフレーム リレー スイッチへのスイッチング

- ローカル シリアル間のスイッチング
- ISDN B チャネルでのスイッチング
- スイッチド PVC でのトラフィック シェーピング
- スイッチド PVC での輻輳管理
- ユーザネットワーク インターフェイス（UNI）DCE でのトラフィック ポリシング
- スイッチド PVC での FRF.12 フラグメンテーション

- 物理インターフェイスに関連付けられたサブインターフェイスのサポート。ソフトウェアでは、1 つ以上の PVC が個別のサブインターフェイス下にグループ化され、これらは 1 つの物理インターフェイス下に配置されます。「Configuring Frame Relay」モジュールを参照してください。
- すべてのプラットフォーム上のフレーム リレー カプセル化シリアルおよび High-Speed Serial Interface（HSSI）に対する、高速パス トランスペアレント ブリッジングのサポート（RFC 1490 で規定）。
- フレーム リレー DTE MIB のサポート（RFC 1315 で規定）。ただし、エラー テーブルは実装されていません。フレーム リレー MIB を使用するには、MIB パブリケーションを参照してください。
- フレーム リレー フラグメンテーションのサポート。シスコは、次の 3 つのタイプのフレーム リレー フラグメンテーションを開発してきました。
  - エンドツーエンド FRF.12 フラグメンテーション

FRF.12 フラグメンテーションは、FRF.12 実装合意によって定義されています。この標準規格は、長いデータ フレームを小さい部分（フラグメント）にフラグメント化し、リアルタイム フレームと交互に送信するために開発されました。エンドツーエンド FRF.12 フラグメンテーションが推奨されるのは、音声を伝送するほかの PVC とリンクを共有する PVC と、Voice over IP（VoIP）を送信する PVC に使用する場合です。

- FRF.11 Annex C を使用したフレーム リレー フラグメンテーション

VoFR（FRF.11）とフラグメンテーションがいずれも PVC で設定される場合、フレームリレー フラグメントは FRF.11 Annex C 形式で送信されます。このフラグメンテーションが使用されるのは、FRF.11 音声トラフィックが PVC で送信され、データに FRF.11 Annex C 形式が使用される場合です。

FRF.11 Annex C を使用するフレーム リレー フラグメンテーションの設定作業と設定例については、『*Cisco IOS Voice, Video, and Fax Configuration Guide*』のモジュール「Configuring Voice over Frame Relay」を参照してください。

- シスコ独自のフラグメンテーション

シスコ独自のフラグメンテーションは、音声トラフィックにも使用されるPVC上のデータ パケットに使用されます。

シスコ独自のフラグメンテーションの設定作業と設定例については、『*Cisco IOS Voice, Video, and Fax Configuration Guide*』のモジュール「Configuring Voice over Frame Relay」を参照してください。

フレーム リレー ATM インターネットワーキング

Cisco IOS ソフトウェアは、フレーム リレー ATM インターワーキングに対するフレーム リレー フォーラムの実装合意をサポートしています。フレーム リレー ATM インターワーキングを使用すると、フレーム リレーと ATM ネットワークの間で、異なるネットワーク プロトコルでもデータを交換できます。フレーム リレー ATM インターワーキングには 2 つのタイプがあります。

FRF.5 フレーム リレー ATM ネットワーク インターワーキング

FRF.5 はフレーム リレー エンド ユーザに対して、FRF.5 をサポートする中間 ATM ネットワーク経由で通信するためのネットワーク インターワーキング機能を提供します。マルチプロトコル カプセル化およびその他の高層手順は、専用回線経由の場合と同様に透過的に転送されます。

FRF.5 で、Frame Relay Bearer Service と Broadband ISDN（BISDN）相手先固定接続（PVC）サービス間のインターワーキング要件を記述します。

FRF.5 標準は、フレーム リレー フォーラム ドキュメント番号 FRF.5『*Frame Relay/ATM PVC Network Interworking Implementation Agreement*』で定義されています。この実装合意のどのセクションが Cisco IOS ソフトウェアでサポートされているかについては、『Frame Relay-ATM Interworking Supported Standards』を参照してください。

FRF.8 フレーム リレー ATM サービス インターワーキング

FRF.8 はフレーム リレー エンド ユーザに対して、ATM エンド ユーザと通信するためのサービス インターワーキング機能を提供します。トラフィックは、さまざまなフレーム リレーおよびATM 機器間での通信を提供するプロトコル コンバータによって変換されます。

FRF.8 は、フレーム リレー PVC と ATM PVC の 1 対 1 のマッピングを表します。

FRF.8 標準は、フレーム リレー フォーラム ドキュメント番号 FRF.8『*Frame Relay/ATM PVC Network Service Interworking Implementation Agreement.*』で定義されています。この実装合意のどのセクションが Cisco IOS ソフトウェアでサポートされているかについては、『Frame Relay-ATM Interworking Supported Standards』を参照してください。

レイヤ 2 バーチャル プライベート ネットワーク

L2VPN サービスはポイントツーポイントです。これらは、MPLS またはピュア IP（L2TPv3）コアを介したレイヤ 2 ポイントツーポイント接続を提供します。

レイヤ 2 トンネリング プロトコル バージョン 3

レイヤ 2 トンネリング プロトコル バージョン 3 機能が、シスコのレイヤ 2 VPN サポートを拡張します。レイヤ 2 トンネリング プロトコル バージョン 3（L2TPv3）は、IETF l2tpext ワーキング グループ ドラフトであり、L2TP 上でレイヤ 2 ペイロードをトンネリングするよう L2TP が強化されています。具体的には、レイヤ 2 VPN を使用して IP コア ネットワーク上でレイヤ 2 ペイロードをトンネリングするための L2TP プロトコルが定義されています。

L2VPN 疑似回線冗長化

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。L2VPN 疑似回線冗長性機能は、すべての障害が発生した場合でも、CE2 ルータが常にネットワークの接続性を維持するための機能を提供します。L2VPN 疑似回線冗長性機能を使用すると、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（PW）と冗長ネットワーク エレメントを設定することもできます。

レイヤ 2 バーチャル プライベート ネットワーク インターワーキング

MPLS および IP を介したレイヤ 2 トランスポートは、Ethernet-to-Ethernet や PPP-to-PPP などの like-to-like 接続回線に対してすでに存在します。L2VPN インターワーキングはこの機能に基づいて構築されており、異なる接続回線どうしが接続できる機能を備えています。インターワーキング機能によって、異なるレイヤ 2 カプセル化間の変換が容易になります。L2VPN インターワーキング機能では、MPLS および L2TPv3 を介したイーサネット、802.1Q（VLAN）、フレームリレー、ATM AAL5、および PPP 接続回線がサポートされます。

レイヤ 2 ローカル スイッチング

ローカル スイッチングを使用すると、同じルータ上の種類が同じ 2 つのインターフェイスの間（たとえば、ATM と ATM の間、フレームリレーとフレームリレーの間）か、種類の異なるインターフェイスの間（たとえば、フレームリレーと ATM の間）で、レイヤ 2 データをスイッチングできます。インターフェイスは、同じラインカード上にあっても 2 つの異なるカード上にあってもかまいません。スイッチングの際には、レイヤ 3 アドレスではなくレイヤ 2 アドレスが使用されます。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。

第 3 章

レイヤ2 トンネリング プロトコル バージョン 3

レイヤ 2 トンネリング プロトコル バージョン 3 機能が、シスコのレイヤ 2 VPN サポートを拡張します。レイヤ 2 トンネリング プロトコル バージョン 3（L2TPv3）は、IETF l2tpext ワーキング グループ ドラフトであり、L2TP 上でレイヤ 2 ペイロードをトンネリングするよう L2TP が強化されています。具体的には、レイヤ 2 VPN を使用して IP コア ネットワーク上でレイヤ 2 ペイロードをトンネリングするための L2TP プロトコルが定義されています。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

レイヤ 2 トンネリング プロトコル バージョン 3 の前提条件

- プロバイダー エッジ（PE）デバイスの xconnect 接続回線を設定（「xconnect 接続回線の設定」を参照）する前に、Cisco Express Forwarding（旧 CEF）機能をイネーブルにする必要があります。インターフェイス上で Cisco Express Forwarding をイネーブルにするには、**ip cef** コマンドまたは **ip cef distributed** コマンドを使用します。
- ルータ上のループバック インターフェイスを L2TPv3 トラフィックの開始および終了用に設定する必要があります。このループバック インターフェイスには、L2TPv3 コントロール チャネルの反対側にあるリモート PE デバイスから到達可能な IP アドレスを設定する必要があります。

レイヤ 2 トンネリング プロトコル バージョン 3 の制約事項

一般的な L2TPv3 の制約事項

- L2TPv3 機能を使用するには、Cisco Express Forwarding をイネーブルにする必要があります。Cisco Express Forwarding がイネーブルになるまで、xconnect コンフィギュレーション モードがブロックされます。Cisco 7500 シリーズなどの分散プラットフォームで、セッションの確立中に Cisco Express Forwarding がディセーブルになった場合は、セッションが解放されます。セッションは、Cisco Express Forwarding が再度イネーブルになるまでダウンしたままになります。Cisco Express Forwarding をイネーブルにするには、**ip cef** コマンドまたは **ip cef distributed** コマンドを使用します。
- PPP、ハイレベル データリンク コントロール（HDLC）、Ethernet、または 802.1q VLAN ポート上のセッション数は、ルータでサポート可能なインターフェイス記述子ブロック（IDB）数で制限されます。PPP、HDLC、イーサネット、および 802.1q VLAN 回線タイプの場合は、回線ごとに IDB が必要です。
- L2TPv3 を使用してフレームリレー D チャネル データリンク接続識別子（DLCI）をトンネリングする場合は、回線ごとの IDB は不要です。その結果、メモリ要件はかなり小さくなります。Engineering Field Test（EFT）プログラムのスケーラビリティ ターゲットは 4000 L2TP セッションです。

- Any Transport over MPLS（AToM）xconnect のインターフェイスを L2TPv3 xconnect に変換するには、インターフェイスから AToM 設定を削除した上で、L2TPv3 を設定します。AToM 設定を削除する前に L2TPv3 を設定した場合は、一部の機能が動作しない可能性があります。
- フレームリレーのサポートには、10 ビット DLCI アドレス指定しか含まれていません。L2TPv3 機能では、フレームリレー拡張アドレス指定がサポートされません。
- インターフェイス キープアライブ機能は、ローカル管理インターフェイス（LMI）に必要なフレームリレー カプセル化を除いて、xconnect が適用されるインターフェイス上で自動的に無効になります。
- 静的 L2TPv3 セッションでは、フレームリレー LMI インターワーキングがサポートされません。
- 静的 L2TPv3 セッションは、キープアライブを使用する Universal Tunnel Interface（UTI）と同時に使用できません。
- IP パケットのレイヤ 2 フラグメンテーションと、静的 L2TPv3 セッション経由の中継システム間（IS-IS）フラグメンテーションがサポートされません。
- レイヤ 3 フラグメンテーションは、パフォーマンスが低下するため推奨できません。
- カスタマー エッジ（CE）ルータでレイヤ 2 シーケンス処理、圧縮、暗号化などの特殊なレイヤ 2 オプションが実行中は、L2TPv3 レイヤ 2（IP パケット）フラグメンテーション機能（「L2TPv3 疑似回線の設定」作業を参照）がサポートされません。このようなオプションの例として、フレームリレー圧縮およびフラグメンテーションや PPP 圧縮があります。このようなシナリオでは、IP ペイロードのフォーマットが IP フラグメンテーションのフォーマットと互換性がありません。
- HA 機能の Stateful Switchover（SSO）、Route Processor Redundancy（RPR）、および RPR+ コンポーネントは、共存レベルでのみサポートされます。SSO、RPR、または RPR+ を使用してスイッチオーバーしようとすると、トンネリングに失敗しますが、そのうち回復します。これには、IPv4 トラフィックと IPv6 トラフィックの両方が含まれます。
- シーケンス処理がイネーブルの場合は、インターワーキングは使用できません。
- dot1q サブインターフェイス上で設定された xconnect のタグなしパケット（ネイティブ VLAN）転送はサポートされていません。
- L2TPv3 xconnect は、EtherSwitch モジュールではサポートされていません。この制限は、EtherSwitch モジュール インターフェイス上で物理的に終端処理されたスイッチ仮想インターフェイス（SVI）にも適用されます。

VLAN 固有の制約事項

- PE デバイスは、デバイス上で手動で設定された静的 VLAN メンバーシップ エントリに対してのみ責任があります。動的 VLAN メンバーシップ エントリ、エントリ エージング、およびメンバーシップ検出はサポートされません。

- その他のレイヤ（レイヤ 2 の MAC アドレスまたはプロトコル タイプ別のメンバーシップ、レイヤ 3 の IP サブネット別のメンバーシップなど）で動作する VLAN メンバーシップの暗黙的タギングはサポートされません。
- ポイントツーマルチポイント設定とマルチポイントツーポイント設定がサポートされません。接続回線と L2TPv3 セッションには 1 対 1 の関係性があります。

L2TPv3 の IPv6 プロトコル逆多重化の制約事項

- IPv6 プロトコル逆多重化は、イーサネット トラフィックに対してのみサポートされています。
- IPv6 プロトコル逆多重化は非インターワーキング セッションを介してサポートされます。

L2TPv3 コントロール メッセージ ハッシングの制約事項

- **digest** コマンドを使用して設定した L2TPv3 コントロール チャネル認証には、ピア デバイス上の双方向設定が必要です。通信するノード上で共有秘密を設定する必要があります。
- すべての L2TPv3 認証方式の互換性マトリクスについては、「IPv6 プロトコル逆多重化」セクションの「有効な設定シナリオ」の表を参照してください。

L2TPv3 ダイジェスト シークレット グレースフル スイッチオーバーの制約事項

- この機能は、認証パスワードが L2TPv3 コントロール メッセージ ハッシング機能を使用して設定されている場合にのみ動作します。従来のチャレンジ ハンドシェーク認証プロトコル（CHAP 型）認証システムで設定された L2TPv3 コントロール チャネル認証パスワードは、L2TPv3 のトンネルとセッションを解放しなければ更新できません。
- Cisco IOS Release 12.0(30)S では、**digest secret** コマンドを使用して最大 2 個のパスワードを同時に設定できます。

L2TPv3 コントロール メッセージ ハッシング機能の詳細については、「L2TPv3 コントロール メッセージ ハッシング」を参照してください。

L2TPv3 トンネリングにおける Quality of Service の制約事項

モジュラ QoS CLI（MQC）を使用して設定された Quality of Service（QoS）ポリシーは、次の制限付きで L2TPv3 トンネル セッションでサポートされます。

フレームリレー インターフェイス（非 ISE/E5）

- 分散型 CEF（dCEF）を備えた Cisco 7500 シリーズ上で L2TPv3 用に設定されたフレーム リレー インターフェイスに適用される QoS ポリシー内で、クラス マップ コンフィギュレーション モードの MQC コマンド **match fr-dlci** とポリシー マップ コンフィギュレーション モードの MQC コマンド **bandwidth** のみがサポートされます。（「Cisco 7500 シリーズ上での L2TPv3 に関する QoS の設定：例」作業を参照）。
- Cisco 12000 シリーズ上では、QoS ポリシーが、次の制限付きで、2 ポート チャネライズド OC-3/STM-1（DS1/E1）または 6 ポート チャネライズド T3（T1）ラインカードのフレームリレー インターフェイス上の TSC ベース L2TPv3 トンネル セッションでサポートされます。
  - **police** コマンドは次のようにサポートされます。
    - *action* キーワードの **transmit** オプションのみが **conform-action** コマンドでサポートされます。
    - *action* キーワードの **set-frde-transmit** オプションのみが **exceed-action** コマンドでサポートされます。
    - *action* キーワードの **drop** オプションのみが **violate-action** コマンドでサポートされます。
    - 逆方向明示的輻輳通知（BECN）設定と明示的輻輳通知（FECN）設定はサポートされません。
    - L2TPv3 疑似回線を設定した場合は、タイプ オブ サービス（ToS）バイトをトンネリングされたフレーム リレー パケット内の IP ヘッダーに設定する必要があります（「L2TPv3 疑似回線の設定」作業を参照）。
    - Cisco 12000 シリーズ ラインカード上の QoS 設定に関する標準的な制約事項のすべてが、Cisco 12000 シリーズ 2 ポート チャネライズド OC-3/STM-1（DS1/E1）または 6 ポート チャネライズド T3 ラインカード上の L2TPv3 用の QoS 設定に適用されます。
  - TSC ベース L2TPv3 トンネリング用に設定された Cisco 12000 シリーズ フレームリレー インターフェイスの入力側：
    - 重み付けランダム早期検出（WRED）設定と Modified Deficit Round Robin（MDRR）設定がサポートされません。
  - TSC ベース L2TPv3 トンネリング用に設定された Cisco 12000 シリーズ フレームリレー インターフェイスの出力側：
    - MDRR が唯一サポートされるキューイング戦略です。
    - WRED が唯一サポートされるパケット破棄戦略です。
    - MDRR は次のモードでのみサポートされます。
      - 低遅延（プライオリティ）キューとクラス デフォルト キューが設定されている場合（低遅延キューは、クラス デフォルト キューとの組み合わせでのみサポートされ、通常の分散ラウンドロビン（DRR）と一緒に設定できません）。

- 低遅延キューが設定されていない場合（この場合は、クラスデフォルトキューを含めて、6 つのキューしかサポートされません）。

- 出力キューイングは、DLCI 単位ではなく、**match ip precedence** コマンドを使用して L2TPv3 フレーム リレー トラフィックのクラスに対して設定された IP precedence 値によって異なります。

例として、「TSC ベースの L2TPv3 トンネル セッションにおけるフレーム リレー インターフェイス上での QoS の設定」を参照してください。

エッジ エンジン（ISE/E5）インターフェイス

Cisco 12000 シリーズ上では、QoS ポリシーが、次の制限付きで、ISE/E5 インターフェイス（サポート ラインカードのリストについては、表 2 と表 3 を参照）上のネイティブ L2TPv3 トンネル セッションでサポートされます。

- フレーム リレーまたは ATM ISE/E5 インターフェイス上のトラフィック ポリシーでは、**police** コマンドの *action* 引数に対する次の conform、exceed、および violate の値のみがサポートされます。

conform-action*actions***set-prec-tunnel set-dscp-tunnel transmit**

exceed-action*actions***drop set-clp**（ATM のみ）**set-dscp-tunnel set-dscp-tunnel** および **set-clp**（ATM のみ）**set-dscp-tunnel** および **set-frde**（フレーム リレーのみ）**set-frde**（フレーム リレーのみ）**set-prec-tunnel set-prec-tunnel** および **set-clp**（ATM のみ）**set-prec-tunnel** および **set-frde**（フレーム リレーのみ）**transmit**

violate-action*actions***drop**

- フレームリレー ISE/E5 インターフェイス上：
  - FECN 設定と BECN 設定がサポートされません。
  - MQC **set** コマンドを使用したフレーム リレー廃棄適性（DE）ビットのマーキングはサポートされません。DE ビットをセット（マーク）するには、ポリシー マップ コンフィギュレーション モードで **policeexceed-action***actions* コマンドを使用します。
  - 従来の QoS（非 MQC）コマンドを使用した Tofab MDRR または WRED の設定はサポートされますが、tunnel precedence 値に基づきます。
  - Packet-over-SONET ISE/E5 インターフェイス上の出力キューイングは、MQC を使用して設定された場合、クラス ベースになります。
  - DLCI 単位ベースの出力キューイングはサポートされません。
- ATM ISE/E5 インターフェイス上：
  - トラフィック シェーピングは、次のサービス カテゴリの ATM 出力インターフェイス上でサポートされます。

- 最低のプライオリティ：UBR（未指定ビット レート）、2 番目のプライオリティ：VBR-nrt（非リアルタイム可変ビット レート）、最高のプライオリティ：VBR-rt（リアルタイム VBR）、最高のプライオリティ：CBR（固定ビット レート）。
- VBR-rt と CBR で同じ最優先シェーピングが共有されることに注意してください。ATM トラフィック シェーピングでは、トラフィックが、それぞれのサービス カテゴリの正当なプライオリティを使用して ATM VC または PVP 上で設定された最大レートに制限されます。
- ATM VC または PVP に対してキュー制限を設定できます。キュー制限は、CLP=1 セル用と CLP0+1 セル用の 2 種類のしきい値が設定可能な 2 つの部分からなるしきい値です。CLP1 しきい値をキュー制限しきい値よりも低くして、キューがパケットでいっぱいになり始めたときに、CLP=1 セルの方が CLP=0 セルよりも先に破棄されるようにする必要があります。
  - ATM ISE/E5 インターフェイスでは（フレームリレー ISE/E5 インターフェイスと同様）デュアル レートの 3-Color Marker ポリサーはサポートされませんが、ATM Forum Traffic Management Version 4.1 準拠の汎用セルレート アルゴリズム（GCRA）ポリサーはサポートされます。GCRA ポリサーでは、レート、ピーク レート、遅延許容値、および ATM 最大バースト サイズが使用され、次の処理がサポートされます。

set-dscp-tunnel および **set-clp-transmit**。

プロトコル逆多重化インターフェイス

プロトコル逆多重化は、IP アドレスと **xconnect** コマンドの組み合わせをインターフェイス上で設定する必要があります。その後で、インターフェイスが正規の L3 として扱われます。レイヤ 2 IPv6 トラフィック上で QoS を適用するには、任意の機能を適用する前に、IPv6 トラフィックを別のクラスに分類する必要があります。

プロトコル逆多重化インターフェイス上では、次の一致基準がレイヤ 2 IPv6 トラフィックの分類に使用されます。

```
class-map match-ipv6
     match protocol ipv6
```

レイヤ 2 IPv6 トラフィックを処理するクラスが存在しない場合は、プロトコル逆多重化インターフェイス上でサービス ポリシーは受け入れられません。

QoS 設定作業とコマンド構文の詳細については、次のマニュアルを参照してください。

- 『*Cisco IOS Quality of Service Solutions Configuration Guide*』
- 『*Cisco IOS Quality of Service Solutions Command Reference*』

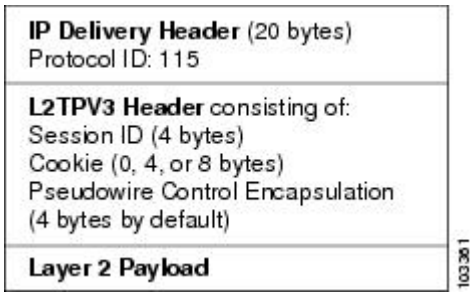
レイヤ 2 トンネリング プロトコル バージョン 3 に関する情報

L2TPv3 は、IPv4（非 UDP）バックボーン ネットワークを介して L2TP サービスを提供する方式です。このプロトコルは、シグナリング プロトコルに加えて、パケット カプセル化仕様に準拠しています。

L2TPv3 ヘッダーの説明

UTI から L2TPv3 に移行するためには、UTI ヘッダーを標準化する必要があります。その結果、L2TPv3 ヘッダーのフォーマットは下の図に示すように新しくなりました。

図 *1*：*L2TPv3* ヘッダーのフォーマット



各 L2TPv3 パケットには、1 つのセッションを表す固有のセッション ID と可変の cookie 長を含む L2TPv3 ヘッダーがあります。L2TPv3 セッション ID とトンネル Cookie フィールド長は CLI 経由で割り当てられます。L2TPv3 用の CLI コマンドの詳細については、「L2TPv3 の設定方法」を参照してください。

Session ID

L2TPv3 セッション ID は、カプセル化を解除するシステム上でセッションの内容を識別するために使用されます。動的セッションの場合は、セッション ID の値が、カプセル解放システムのコンテキスト識別効率を最適化するように選択されます。したがって、カプセル解放実装では、より小さなセッション ID ビット フィールドをサポートすることが選択されます。この L2TPv3 実装では、L2TPv3 セッション ID の上位値が 023 に設定されています。L2TPv3 セッション ID 値の 0 はプロトコルで使用するために予約されています。静的セッションの場合は、セッション ID が手動で設定されます。

（注） ローカル セッション ID は、カプセル解放システム上で一意にする必要があり、下位 10 ビットに制限されています。

セッション cookie

L2TPv3 ヘッダーにコントロール チャネル cookie フィールドが含まれます。コントロール チャネル クッキー フィールドの長さは、パケット カプセル化解除のプラットフォームでサポートされているクッキー長に応じて、0、4、または 8 バイトに変化します。このコントロール チャネル cookie 長は、静的セッションの場合は手動で設定できますが、動的セッションの場合は動的に決定されます。

L2TPv3 コントロール チャネルの両端のプラットフォームが同じ場合は、可変 cookie 長が問題にはなりません。ただし、L2TPv3 コントロール チャネル上で異なるプラットフォームを相互運用させる場合は、両方のプラットフォームで 4 バイトの cookie 長を使用してパケットをカプセル化する必要があります。

疑似回線コントロール カプセル化

L2TPv3 疑似回線コントロール カプセル化は、32 ビット（4 バイト）で構成され、L2TP パケットのシーケンス処理に使用される情報が含まれています（「シーケンス」を参照）。シーケンス処理では、最初のビットとビット 8 ～ 31 が使用されます。ビット 1 は、シーケンス番号フィールド（ビット 8 ～ 31）に有効なシーケンス番号が含まれており、更新すべきかどうかを示します。

L2TPv3 の動作

L2TPv3 には次の機能があります。

- IP ネットワーク上の疑似回線経由のレイヤ 2 トンネリング用 xconnect
- イーサネットおよび VLAN をサポートする xconnect を使用した PE-to-PE デバイス サービス用のレイヤ 2 VPN。静的および動的（新しい L2TPv3 シグナリングを使用）転送セッションを含みます。

初期の Cisco IOS 機能は、次の機能のみをサポートしました。

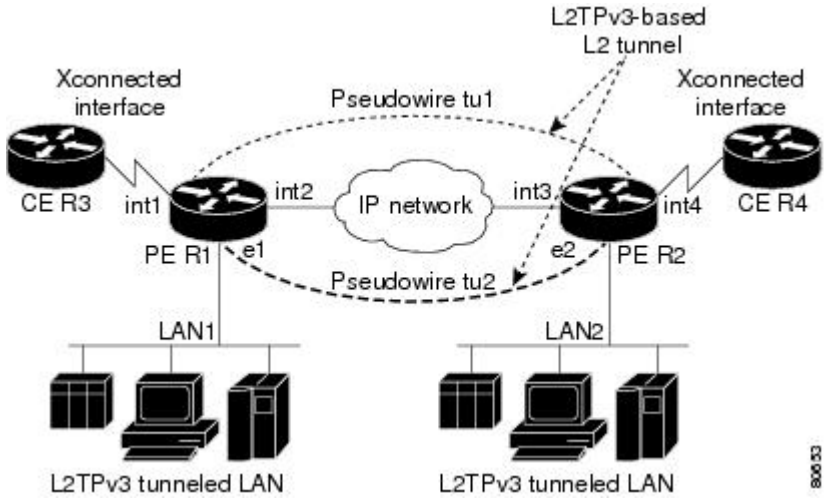
- レイヤ 3 トンネリングではなく、接続回線へのレイヤ 2 トンネリング（L2TP アクセス コンセントレータ（LAC）で使用されているものと同様）
- UDP を使用しない、IP 上での直接的な L2TPv3 データ カプセル化（IP プロトコル番号 115）
- ポイントツーマルチポイント セッションやマルチポイントツーポイント セッションではなく、ポイントツーポイント セッション
- 同一レイヤ2プロトコル間のセッション。イーサネットツーイーサネットやVLAN ツー VLAN など。VLAN ツーイーサネットはサポートされていません。

接続回線は、疑似回線に接続された物理インターフェイスまたはサブインターフェイスです。

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デバイスは、そのトラフィックをほかの IP トラフィックとして処理し、カスタマー ネットワークのことを何も知る必要がありません。

図 *2*：*L2TPv3* の動作



上の図では、PE デバイスの R1 と R2 から L2TPv3 サービスが提供されます。R1 デバイスと R2 デバイスは、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。

この例では、カスタマー エッジ（CE）デバイスの R3 と R4 が xconnect イーサネットのペアまたは L2TPv3 セッションを使用した 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。

L2TPv3 動作に関する次の特徴に注意してください。

- インターフェイス int1 に到着したすべてのパケットが R4 に転送されます。R3 と R4 では介在するネットワークが検出できません。
- イーサネット インターフェイスの場合は、LAN1 からイーサネット インターフェイス e1 上の R1 で受信されたすべてのパケットが、IP で直接カプセル化され、疑似回線セッション tu2 経由で R2 インターフェイス e2 に送信されてから LAN2 に送出されます。
- イーサネット インターフェイス上の VLAN を L2TPv3 セッションにマップすることができます。

L2TPv3 の機能

L2TPv3 では、静的および動的セッションを使用したイーサネットおよび VLAN の xconnect がサポートされています。

静的 L2TPv3 セッション

通常、L2TP コントロール プレーンには、セッションをセットアップするためのセッション パラメータ（セッション ID や cookie など）のネゴシエーションに対して責任があります。ただし、一部の IP ネットワークでは、シグナリングなしでセッションが確立できるようにセッションを設定する必要があります。L2TP データ ヘッダー内のフィールドに固定値を設定することによって、PE デバイス用の静的 L2TPv3 セッションをセットアップできます。静的 L2TPv3 セッションを使用すれば、PE デバイスで、セッションがバインドされた接続回線が検出されたらすぐにレイヤ 2 トラフィックをトンネリングさせることができます。

静的設定により、コントロール接続パラメータを動的にネゴシエーションすることなくセッションを確立することができます。したがって、セッションは **show l2tun session** コマンド出力で表示されますが、**show l2tun tunnel** コマンドの出力にはコントロール チャネル情報の情報が表示されません。

（注） L2TPv3 静的セッションでは、L2TP コントロール チャネルを起動して、ピア認証とデッド ピア検出を実行できます。hello の失敗が原因で L2TP コントロール チャネルが確立できない、または、解放された場合は、静的セッションも解放されます。

静的 L2TPv3 セッションを使用している場合は、コントロール メッセージを交換するためのファシリティがないため、LMI などの回線インターワーキングを実行できません。回線インターワーキングを実行するには、動的セッションを使用する必要があります。

動的 L2TPv3 セッション

動的 L2TP セッションは、属性/値（AV）ペアを含むコントロール メッセージの交換を通して確立されます。各 AV ペアには、転送されるレイヤ 2 リンクの特性（ペイロード タイプや仮想回線（VC）ID など）に関する情報が含まれています。

複数の L2TP セッション（転送先レイヤ 2 回線ごとに 1 つずつ）を PE デバイスのペア間に配置して、単一のコントロール チャネルで保守できます。セッション ID と cookies は動的に生成され、動的セッション セットアップの一部として交換されます。シーケンス処理設定などの情報も交換されます。回線状態の変化（UP/DOWN）は Set Link Info（SLI）メッセージを使用して伝送されます。

コントロール チャネル パラメータ

L2TP クラス設定手順では、別の疑似回線クラスに継承可能な L2TP コントロール チャネル パラメータのテンプレートを作成します。L2TP コントロール チャネル パラメータは、コントロール チャネル認証、キープアライブ メッセージ、およびコントロール チャネル ネゴシエーションで使用されます。L2TPv3 セッションでは、コントロール チャネルの両端にある PE デバイス上で設定された疑似回線で同じ L2TP クラスを指定する必要があります。L2TP コントロール チャネル パラメータの設定はオプションです。ただし、L2TP クラスは、疑似回線クラスに関連付ける前に設定する必要があります（「L2TPv3 疑似回線の設定」作業を参照）。

L2TPv3 コントロール チャネル認証パラメータ

コントロール チャネル メッセージ認証には、L2TPv3 コントロール メッセージ ハッシング機能と CHAP 型 L2TP コントロール チャネルの 2 つの方式があります。L2TPv3 コントロール メッセージ ハッシング機能では、従来の CHAP 型 L2TP コントロール チャネル認証方式よりも堅牢な認証方式が導入されています。両方の認証方式をイネーブルにしてどちらかの認証方式しかサポートしていないピアとの互換性を保証できますが、この設定によってピア PE デバイスに使用する認証方式をコントロールできます。両方の認証方式をイネーブルにする方法は、ソフトウェアのアップグレードに伴う下位互換性の問題を解決する暫定的なソリューションととらえる必要があります。

2 つの認証方式の主な違いは、L2TPv3 コントロール メッセージ ハッシング機能が、受信したコントロール メッセージ内で選択したコンテンツのハッシュを計算するのではなく、ハッシュ内のメッセージ全体を使用する点にあります。加えて、Start Control Channel RePlay（SCCRP）メッセージと Start Control Channel CoNnected（SCCCN）メッセージにしかハッシュ ダイジェストが追加されないのに対して、すべてのメッセージにハッシュ ダイジェストが追加されます。

L2TP コントロール チャネル認証のサポートが下位互換性のために残されています。どちらかまたは両方の認証方式をイネーブルにすることによって、どちらかの認証方式しかサポートしていないピアとの相互運用性を保証できます。

次の表に、さまざまな L2TPv3 認証方式の互換性マトリクスを示します。PE1 で新しい認証が実行されており、考えられる PE1 の認証設定が最初の列に掲載されています。その他の列は、利用可能な認証オプションが異なる PE2 実行ソフトウェアを表します。表内のこれらの列のセルは、PE2 の互換設定オプションを示します。いずれかの PE1/PE2 認証設定でどの認証方式が使用されるかが曖昧な場合は、可能性の高い認証方式が太字で示されています。PE1 と PE2 上で新旧両方の認証方式がイネーブルになっている場合は、両方のタイプの認証が実行されます。

表 *1*：*L2TPv3* 認証方式の互換性マトリクス

PE1 の認証設定	古い認証をサポートしている PE2[1]	新しい認証をサポートしている PE2[2]	新旧両方の認証をサポートしている PE2[3]
なし	なし	なし 新しい整合性チェック	なし 新しい整合性チェック

PE1 の認証設定	古い認証をサポートしている PE2[1]	新しい認証をサポートしている PE2[2]	新旧両方の認証をサポートしている PE2[3]
古い認証	古い認証	—	古い認証 **古い認証**と新しい認証 **古い認証**と新しい整合性チェック
新しい認証	—	新しい認証	新しい認証 古い認証と**新しい認証**
新しい整合性チェック	なし	なし 新しい整合性チェック	なし 新しい整合性チェック
古い認証と新しい認証	古い認証	新しい認証	古い認証 新しい認証 **古い認証と新しい認証** **古い認証**と新しい整合性チェック
古い認証と新しい整合性チェック	古い認証	—	古い認証 **古い認証**と新しい認証 **古い認証**と新しい整合性チェック

1 古い CHAP 型認証システムしかサポートしていない PE ソフトウェア。
2 新しいメッセージ ダイジェスト認証および整合性チェック認証システムしかサポートしていないが、古い CHAP 型認証システムを認識しない PE ソフトウェア。このタイプのソフトウェアは、最新の L2TPv3 ドラフトに基づいて別のベンダーが実装している可能性があります。
3 古い CHAP 型認証システムと、新しいメッセージ ダイジェスト認証および整合性チェック認証システムの両方をサポートする PE ソフトウェア。

Ethernet over L2TPv3

L2TPv3 上のイーサネット機能では、L2TPv3 を使用した IP コア ネットワーク上でのイーサネットベースのレイヤ 2 ペイロード トンネリングがサポートされます。

L2TPv3 上のイーサネット機能は、次の like-to-like スイッチング モードをサポートします。

- イーサネット ポート モード
- イーサネット VLAN モード
- VLAN リライトありのイーサネット VLAN モード
- イーサネット QinQ および QinAny モード

（注） L2TPv3 上の QinQ サポート機能には、L2TPv3 上の QinAny が含まれます。L2TPv3 上の QinAny は、固定の外部 VLAN タグと可変の内部 VLAN タグを持ちます。

L2TPv3 上のイーサネット機能は、次のタイプのインターネットワーキングをサポートします。

- イーサネット ポートから VLAN（ルーテッド）
- イーサネット ポートから VLAN（ブリッジド）
- QinQ からイーサネット VLAN またはポート インターワーキング（ルーテッド）
- QinQ からイーサネット VLAN またはポート インターワーキング（ブリッジド）

（注） QinAny インターワーキングは、内部 VLAN タグが不定であるため、有効な設定ではありません。

L2TPv3 上の GEC

レイヤ 2 トンネリング プロトコル バージョン 3（L2TPv3）上の Gigabit EtherChannel（GEC）では、L2TPv3 を使用した IP コア ネットワーク上での GEC ベースのレイヤ 2 ペイロード トンネリングがサポートされています。GEC（別名ポート チャネル）は、イーサネットおよび dot1q 接続回線（AC）と統合されています。

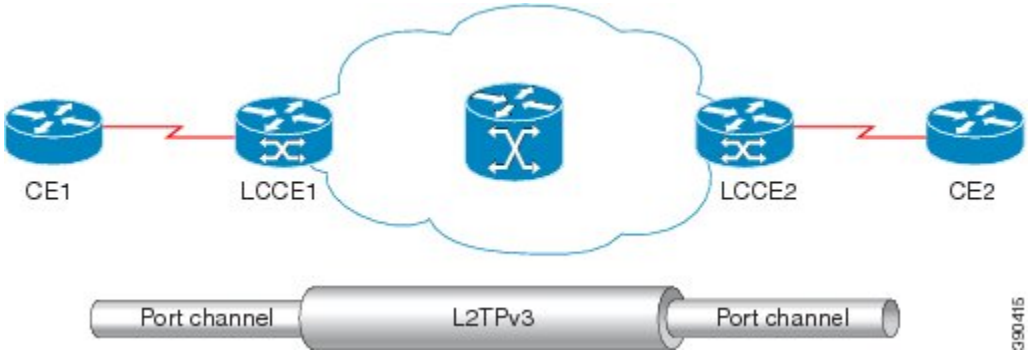
ポート チャネルは、物理リンクをまとめて 1 つのチャネル グループに入れ、最大 8 つの物理リンクの帯域幅を集約した単一の論理リンクを作ります。ポートチャネル内のメンバーポートに障害が発生すると、障害が発生したリンクで伝送されていたトラフィックはポート チャネル内のその他のメンバー ポートに切り替わります。

インターワーキング スイッチングは、次のシナリオでサポートされています。

- ローカル PE 上のカスタマーエッジ-プロバイダーエッジ（CE-PE）接続インターフェイスは、dot1q カプセル化を使用しないポートチャネル インターフェイスです。リモート PE 上の CE-PE 接続インターフェイスは、dot1q カプセル化を使用したポートチャネル インターフェイスです。
- ローカル PE 上の CE-PE 接続インターフェイスは、dot1q カプセル化を使用または使用しないポートチャネル インターフェイスです。リモート PE 上の CE-PE 接続インターフェイスは、dot1q カプセル化を使用または使用しないイーサネット インターフェイスです。

下の図に、L2TPv3 を使用した IP コア ネットワーク上のポート チャネルを示します。CE1 と CE2 は、ポートチャネルを介して L2TP コントロール接続エンドポイント（LCCE）に接続されています。LCCE は、L2TPv3 を使用して IP コア ネットワークに接続されています。

図 *3*：*L2TPv3* 上の *GEC*



シーケンス

受信されるレイヤ 2 フレームの正確なシーケンスは一部のレイヤ 2 技術（シリアル回線などのリンクの特性による）またはプロトコルそのものによって保証されますが、転送されるレイヤ 2 フレームは IP パケットとしてネットワーク上を伝送中に、失われたり、複製されたり、記録されたりします。レイヤ 2 プロトコルで明確なシーケンス処理メカニズムが提供されない場合は、L2TPv3 IETF l2tpext ワーキング グループ ドラフトに記載されているデータ チャネル シーケンス処理メカニズムに従って、データ パケットをシーケンス処理するように L2TP を設定できます。

L2TP データ パケットの受信者は、セッションのネゴシエーション時に、シーケンス処理必須 AV ペアを通してシーケンス処理を実行します。この AV ペアを受信する送信者（または、シーケンス処理するパケットを送信するように手動で設定された送信者）は、L2TPv3 で定義されたレイヤ 2 固有の疑似回線コントロール カプセル化を使用します。

順序が不正なパケットのみを破棄するように L2TP を設定できます。順序が不正なパケットを配信するように L2TP を設定できません。並べ替えメカニズムは使用できません。

シーケンス処理がイネーブルの場合は、インターワーキングは使用できません。

L2TPv3 タイプのサービス マーキング

レイヤ 2 トラフィックが IP ネットワーク上でトンネリングされると、次のいずれかの方法で、タイプ オブ サービス（ToS）ビット内の情報が L2TP カプセル化済み IP パケットに転送される場合があります。

- トンネリングされたレイヤ 2 フレーム自体で IP パケットがカプセル化される場合は、単に、内側 IP パケットの ToS バイトを外側 IP パケット ヘッダーにコピーすることを推奨します。この処理は、「ToS バイト リフレクション」として知られています。
- 疑似回線経由で送信されるすべてのパケットで使用される ToS バイトを指定できます。これは、「静的 ToS バイト設定」として知られています。

ToS の設定方法の詳細については、「例：ローカル HDLC スイッチングのネゴシエーション済み L2TPv3 セッションの設定」を参照してください。

キープアライブ

L2TPv3 キープアライブ メカニズムは、トンネリング プロトコルのエンドポイントのみを対象とします。L2TP には、キープアライブ メカニズムの基礎として機能する、信頼できるコントロール メッセージ配信メカニズムがあります。このキープアライブ メカニズムは、L2TP hello メッセージの交換で構成されます。

キープアライブ メカニズムが必要な場合は、コントロールプレーンが使用されますが、セッションの開始には使用されません。セッションは手動で設定できます。

静的 L2TPv3 セッションの場合は、2 台の L2TP ピア間のコントロール チャネルが Start Control Channel ReQuest（SCCRQ）、SCCRP、および SCCCN コントロール メッセージの交換を通してネゴシエートされます。コントロールチャネルは、hello メッセージの交換を通したキープアライブ メカニズムの維持に対してのみ責任があります。

hello メッセージ間のインターバルはコントロールチャネルごとに設定できます。あるピアでキープアライブ メカニズムを通して別のピアのダウンが検出された場合は、StopCCN コントロール メッセージが送信されてから、そのイベントがそのピアへのすべての疑似回線に通知されます。この通知によって、手動設定されたセッションと動的セッションの両方が解放されます。

MTU の処理

L2TPv3 トンネリングされたリンクごとに適切な最大伝送ユニット（MTU）を設定することが重要です。設定した MTU サイズによって次のことが保証されます。

- トンネリングされたレイヤ 2 フレームの長さは、宛先接続回線の MTU 未満である。
- トンネリングされたパケットは、断片化されず、それを受信した PE で再構築が実施される。

L2TPv3 では MTU が次のように処理されます。

- デフォルトの動作では、パケットがセッション MTU を超えるサイズに断片化されます。
- 疑似回線クラス内で **ip dfbit set** コマンドをイネーブルにした場合は、デフォルトの MTU 動作が、トンネル MTU を超えるすべてのパケットが破棄される動作に変わります。
- 疑似回線クラス内で **ip pmtu** コマンドをイネーブルにした場合は、L2TPv3 コントロール チャネルがパス MTU（PMTU）ディスカバリに追加されます。

この機能をイネーブルにした場合は、次の処理が実行されます。

- L2TPv3 デバイスに送り返された Internet Control Message Protocol（ICMP）到達不能メッセージが解釈され、それに応じて、トンネル MTU が更新されます。フラグメンテーション エラーに関する ICMP 到達不能メッセージを受信するために、CE デバイスから受信された Don't Fragment（DF）ビット値に応じて、または、**ip dfbit set** オプションがイネーブルの場合は静的に、トンネル ヘッダー内の DF ビットがセットされます。トンネル MTU は、周期タイマーに基づいて、定期的にデフォルト値にリセットされます。

- ICMP 到達不能メッセージが CE 側のクライアントに送り返されます。ICMP 到達不能メッセージは、IP パケットが CE-PE インターフェイス上に到着すると必ず CE に送信されます。そのパケット サイズはトンネル MTU を超えています。ICMP 到達不能メッセージが CE に送信される前に、レイヤ 2 ヘッダーの計算が行われます。

L2TPv3 コントロール メッセージ ハッシング

L2TPv3 コントロール メッセージ ハッシング機能では、SCCRQ、SCCRP、および SCCCN メッセージ内でチャレンジ AV とチャレンジ応答 AV のペアが使用される、L2TPv2 から継承された CHAP 型認証システムに代わって、新しいより安全な認証システムが採用されています。L2TPv3 コントロール メッセージ ハッシング機能には、すべてのコントロール メッセージに対するオプションの認証または整合性チェックが組み込まれています。

L2TPv3 コントロール メッセージ ハッシング機能によって導入されるメッセージ単位認証は、次のことを目的として設計されました。

- L2TP ノード間の相互認証を実行します。
- すべてのコントロール メッセージの完全性を確認します。
- 容易にネットワークに仕掛けられる可能性があるコントロール メッセージのなりすまし攻撃やリプレー攻撃から保護します。

新しい認証方式では、次のコマンドが使用されます。

- L2TP コントロール メッセージのヘッダーおよび本文上の計算された一方向ハッシュ
- 通信している L2TP ノードで定義する必要がある事前設定された共有秘密
- ナンス AV ペアを使用して交換されるローカルとリモートの乱数値

受信された制御メッセージは、必要なセキュリティ要素に足りないものがあるとドロップされます。

L2TPv3 コントロール メッセージ整合性チェックは、共有秘密の設定が不要の一方向メカニズムです。ローカル PE デバイス上で整合性チェックがイネーブルになっている場合は、コントロール メッセージが共有秘密またはナンス AV ペアを使用せずに計算されたメッセージ ダイジェスト付きで送信され、リモート PE デバイスで確認されます。確認に失敗した場合は、リモート PE デバイスでそのコントロール メッセージが破棄されます。

L2TPv3 コントロール メッセージ ハッシング機能をイネーブルにすると、コントロール メッセージの送受信ごとにメッセージ全体のダイジェスト計算が必要になるため、コントロール チャネルとセッションの確立中のパフォーマンスに影響する可能性があります。これは、この機能によってもたらされるセキュリティ強化との予想されたトレードオフです。加えて、受信ウィンドウのサイズが小さすぎると、ネットワークが輻輳する可能性があります。L2TPv3 コントロール メッセージハッシング機能がイネーブルになっている場合は、メッセージダイジェスト確認をイネーブルにする必要があります。メッセージダイジェスト確認では、データ パス受信シーケンス番号の更新が非アクティブにされ、最小ローカル受信ウィンドウ サイズが 35 に制限されます。

コントロールチャネル認証を設定することも、コントロールメッセージ整合性チェックを設定することもできます。両方のピアをコントロール チャネル認証に参加させ、両方のデバイス上で共有秘密を設定する必要があります。コントロール メッセージ整合性チェックは一方向のため、どちらか一方のピア上にしか設定できません。

L2TPv3 コントロール メッセージ レート制限

L2TPv3 コントロール メッセージ レート制限機能は、L2TPv3 を実行するデバイス上のサービス拒絶（DoS）攻撃の可能性をなくすために導入されました。L2TPv3 コントロール メッセージ レート制限機能によって、L2TPv3 トンネルを終端する PE に到着した SCCRQ コントロール パケットが処理可能なレートに制限されます。SCCRQ コントロール パケットは、L2TPv3 トンネルの構築プロセスを開始して、PE デバイスの大量のコントロール プレーン リソースを要求します。

L2TPv3 コントロール メッセージ レート制限機能のための設定は不要です。この機能は、サポートされているリリースのバックグラウンドで自動的に動作します。

L2TPv3 ダイジェスト シークレット グレースフル スイッチオーバー

L2TPv3 コントロールチャネル メッセージの認証は、参加しているすべてのピア PE デバイス上で設定されたパスワードを使用して行われます。この機能が追加される以前は、このパスワードを変更するには、新しいパスワードを追加する前に設定から古いパスワードを削除する必要があり、L2TPv3 サービスが中断されていました。認証パスワードは、物理的に離れた場所に配置されることが多い、すべてのピア PE デバイス上で更新する必要があります。すべてのピア PE デバイスを同時に新しいパスワードに更新することによって、L2TPv3 サービスの中断を最小限に抑えるのは困難です。

L2TPv3 ダイジェスト シークレット グレースフル スイッチオーバー機能を使用すれば、L2TPv3 コントロール チャネル メッセージの認証に使用するパスワードを、確立された L2TPv3 トンネルを解放せずに変更できます。この機能は、L2TPv3 制御メッセージ ハッシング機能を使用して認証パスワードが設定されている場合に限り動作します。従来の CHAP 型認証システムで設定された認証パスワードは、L2TPv3 トンネルを解放しなければ更新できません。

L2TPv3 ダイジェスト シークレット グレースフル スイッチオーバー機能を使用すれば、2 つのコントロール チャネル パスワードを同時に設定できるため、先に古いパスワードを削除しなくても、新しいコントロールチャネルパスワードをイネーブルにすることができます。確立済みのトンネルは、新しいパスワードにすぐに更新されますが、古いパスワードも、設定から削除されるまで引き続き使用されます。これによって、まだ新しいパスワードを使用するように更新されていないピア PE デバイスを使用して、これまでどおりの認証を継続できます。すべてのピア PE デバイスが新しいパスワードに設定されたら、古いパスワードを設定から削除できます。

新旧両方のパスワードが設定されている間は、古いパスワードを使用した認証が失敗した場合にのみ、新しいパスワードを使用した認証が実行されます。

L2TPv3 疑似回線

疑似回線クラス設定手順では、疑似回線用の設定テンプレートを作成します。このテンプレートまたはクラスは、疑似回線上で接続回線トラフィックを転送するために使用される L2TPv3 セッションに関するセッション レベル パラメータを設定するために使用します。

疑似回線設定では、データ カプセル化タイプ、コントロールプロトコル、シーケンス処理、レイヤ 3 フラグメンテーション、ペイロード固有のオプション、IP プロパティなどの L2TPv3 シグナリング メカニズムの特性を指定します。疑似回線のセットアップにシグナリングが使用されたかどうかを判断する設定も含まれています。

encapsulation l2tpv3 コマンドを指定すると、**no encapsulation l2tpv3** コマンドでは削除できません。また、**encapsulation mpls** コマンドではその設定を変更できません。このような方式では次のようなエラー メッセージが表示されます。

```
Encapsulation changes are not allowed on an existing pw-class.
```

このコマンドを削除するには、**no pseudowire-class** コマンドを使用して疑似回線を削除する必要があります。カプセル化のタイプを変更するには、**no pseudowire-class** コマンドで疑似回線を削除し、疑似回線を再作成して新しいカプセル化タイプを指定します。

L2TPv3 トンネルの手動クリア

L2TPv3 トンネルを手動でクリアできます。この機能が追加される以前は、特定の L2TPv3 トンネルを手動でクリアするためのプロビジョニングはありませんでした。この機能によって、ユーザは L2TPv3 ネットワークの管理が容易になります。

L2TPv3 トンネルの管理

xconnect 設定の管理と xconnect 設定に伴う問題の診断を促進するために、新しいコマンドと拡張されたコマンドが導入されています。これらのコマンドに特定の設定作業は関連付けられていません。

- **debugvpdn**：このコマンドの出力には、認証失敗メッセージが含まれています。
- **showl2tunsession**--The **hostname** キーワードを使用すれば、ピア ホスト名を出力できます。
- **showl2tuntunnel**：**authentication** キーワードを使用すれば、L2TP コントロール チャネル認証 AV ペアに関するグローバル情報を表示できます。
- **showxconnect**：このコマンドの出力は、xconnect 接続回線および疑似回線に関する情報を表示します。また、すべての xconnect 設定に関する情報を参照するための適切な単一点も提供します。
- **xconnectloggingpseudowirestatus**：このコマンドは、疑似回線ステータス イベントの syslog レポート機能をイネーブルにします。

これらの Cisco IOS コマンドについては、http://tools.cisco.com/Support/CLILookup にある Command Lookup Tool にアクセスするか、『Cisco IOS Master Commands List, All Releases』を参照してください。

L2TPv3 プロトコル逆多重化

L2TPv3 プロトコル逆多重化機能では、IPv4 ネットワークから IPv6 トラフィックをオフロードするための専用の IPv6 ネットワークを利用してネイティブ IPv6 をサポートできるようになりました。IPv6 トラフィックは、CE デバイス上の設定に影響を与えることなく、L2TPv3 疑似回線を使用して IPv6 ネットワークに透過的にトンネリングされます。IPv4 トラフィックは、これまでどおり、IPv4 ネットワーク内部でルーティングされるため、既存の IPv4 ネットワークの性能と信頼性が維持されます。

IPv4 PE デバイスは、IPv4 トラフィックからの着信 IPv6 トラフィックを逆多重化するように設定する必要があります。IPv6 デバイスと相対する PE デバイスは、IPv6 を設定する必要がありません。IPv6 ネットワークの設定はこのマニュアルの範囲を超えています。IPv6 ネットワークの設定方法については、『IPv6 Configuration Guide』を参照してください。

Dot1q および QinQ カプセル化用の L2TPv3 カスタム Ethertype

Dot1q および QinQ カプセル化の L2TPv3 カスタム Ethertype 機能により、QinQ または Dot1Q カプセル化を使用して 0x8100 以外の Ethertype をギガビット イーサネット インターフェイス上で設定できます。カスタム Ethertype 0x9100、0x9200、0x88A8 を設定できます。これにより、マルチベンダー ギガビット イーサネット環境の相互運用性を実現できます。

L2TPv3 上の HDLC

レイヤ 2 データ カプセル化の HDLC は、ポートツーポート レイヤ 2 トラフィックのカプセル化を提供します。IPv4、IPv6、および非 IP パケット（IS-IS など）を含むすべての HDLC トラフィックは、L2TPv3 でトンネリングされます。HDLC は、インターワーキング モードをサポートしていません。

（注） L2TPv3 は、HDLC のみに対して IPv4 トンネルをサポートしています。IPv4 トンネルは、IPv4 パケットと IPv6 パケットをサポートしています。

L2TPv3 の利点

VPN の導入が容易になる

L2TPv3 は、ベンダー間の相互運用によってカスタマー柔軟性の向上およびサービス可用性の向上を保証する業界標準のレイヤ 2 トンネリング プロトコルです。

MPLS が不要になる

サービス プロバイダーは、コア IP バックボーン内にマルチプロトコル ラベル スイッチング（MPLS）を導入して IP バックボーン上の L2TPv3 を使用した VPN をセットアップする必要がないため、運用コストが削減され、収益が増大します。

任意のペイロードに対する IP 上のレイヤ 2 トンネリングがサポートされる

L2TPv3 では、IP コア ネットワーク上のペイロードのレイヤ 2 トンネリングをサポートするように L2TP が機能強化されています。また、基本 L2TP プロトコルが、トンネリングされるレイヤ 2 ペイロードとは別のものとして位置付けられています。

その他の利点

- 認証用のクッキーを提供します。
- セッション ステート アップデートと複数セッションを提供します。
- インターワーキング（Ethernet-VLAN、Ethernet-QinQ、および VLAN-QinQ）をサポートしています。

サポートされている L2TPv3 ペイロード

（注） L2TPv3 トンネリングされた各パケットには、このセクションで説明されているペイロードのレイヤ2フレーム全体が含まれています。シーケンス処理（「シーケンス」を参照）が必要な場合は、レイヤ2固有のサブレイヤ（「疑似回線コントロール カプセル化」を参照）が L2TPv3 ヘッダーに追加され、シーケンス番号フィールドが提供されます。

イーサネット

PE デバイスで受信されたイーサネット フレームは、その全体に L2TP データ ヘッダーが付加された形にカプセル化されます。もう一方の端では、受信された L2TP データ パケットから、L2TP データ ヘッダーが除去されます。その後で、ペイロード、つまり、イーサネット フレームが適切な接続回線に転送されます。

L2TPv3 トンネリング プロトコルは基本的にブリッジとして機能するため、イーサネット フレームのどの部分も検査する必要がありません。インターフェイス上で受信されたすべてのイーサネット フレームがトンネリングされ、すべての L2TP トンネリング済みイーサネット フレームがインターフェイスから転送されます。

（注） L2TPv3 でイーサネット フレームを処理する方法によっては、イーサネット インターフェイスを無差別モードに設定して、デバイスに接続されたイーサネット セグメント上で受信されたすべてのトラフィックを取得する必要があります。すべてのフレームが L2TP 疑似回線経由でトンネリングされます。

VLAN

L2TPv3 では、次の方法で VLAN メンバーシップがサポートされます。

- 日付なしイーサネット フレームが受信されるポート ベース
- タグ付きイーサネット フレームが受信される VLAN ベース

L2TPv3 では、イーサネット xconnect でポート ベースの VLAN メンバーシップとタグ付きイーサネット フレームの受信がサポートされます。タグ付きイーサネット フレームには、2 バイトのタグ プロトコル識別子（TPID）フィールドと 2 バイトのタグ コントロール情報（TCI）フィールドからなる 4 バイト長のタグ ヘッダー（802.1Q で定義された）が含まれています。TPID は TCI が続いていることを示します。TCI はさらに次の 3 つのフィールドに分解されます。

- ユーザ プライオリティ フィールド
- フォーマット形式表示（CFI）
- 12 ビットの VLAN ID（VID）

L2TPv3 では、VLAN スイッチングをサポートするように設定されたイーサネット サブインターフェイスを xconnect サービスにバインドすることによって、サブインターフェイス上で指定された VID を使用してタグ付けされたすべてのイーサネット トラフィックを別の PE にトンネリングすることができます。VLAN イーサネット フレームはその全体が転送されます。受信する PE では、トンネリングされたトラフィックを接続回線に転送する前に、その VID を別の値に書き換えることができます。

VLAN の書き換えを成功させるために、スパニングツリー プロトコル（STP）をディセーブルにしなければならない場合があります。この操作は、**nospanning-treevlan** コマンドを使用して、VLAN ごとに実行できます。

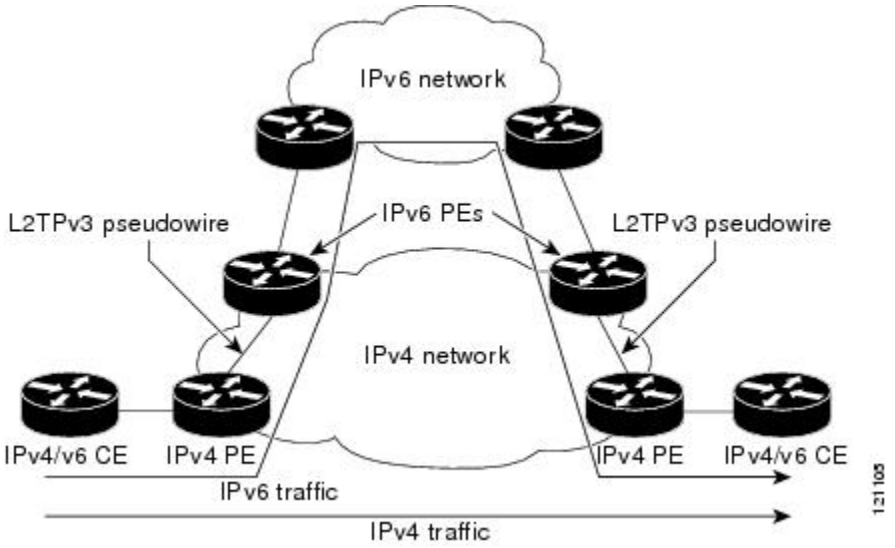
（注） L2TPv3 で VLAN パケットが処理される方法によっては、デバイスに接続されたイーサネット セグメント上で受信されたすべてのトラフィックを取得するように、イーサネット インターフェイスを無差別モードで設定する必要があります。すべてのフレームが L2TP 疑似回線経由でトンネリングされます。

IPv6 プロトコル逆多重化

IPv6 をサポートするためのサービスプロバイダーネットワークのアップグレードは長期に渡るコストのかかるプロセスです。暫定的なソリューションとして、L2TPv3 用のプロトコル逆多重化機能を使用すれば、専用の IPv6 ネットワークをセットアップして、IPv4 ネットワークから IPv6 トラフィックをオフロードすることによって、ネイティブ IPv6 サポートを提供できます。IPv6 トラフィックは、CE デバイス上の設定に影響を与えることなく、L2TPv3 疑似回線を使用して IPv6 ネットワークに透過的にトンネリングされます。IPv4 トラフィックは、これまでどおり、IPv4 ネットワーク内部でルーティングされるため、既存の IPv4 ネットワークの性能と信頼性が維持されます。

下の図に、IPv6 トラフィックを IPv4 ネットワークから専用の IPv6 ネットワークにオフロードするネットワーク展開を示します。PE デバイスで、IPv4 トラフィックから IPv6 トラフィックが逆多重化されます。IPv6 トラフィックは L2TPv3 疑似回線経由で IPv6 ネットワークにルーティングされますが、IPv4 トラフィックは通常どおりにルーティングされます。IPv4 PE デバイスは、IPv4 トラフィックからの着信 IPv6 トラフィックを逆多重化するように設定する必要があります。IPv6 デバイスと相対する PE デバイスは、IPv6 を設定する必要がありません。

図 *4*：*IPv4* トラフィックからの *IPv6* トラフィックのプロトコル逆多重化



IP アドレスが設定されていない場合は、プロトコル逆多重化設定が拒否されます。IP アドレスが設定されている場合は、xconnect コンフィギュレーションモード中にプロトコル逆多重化をイネーブルにしなければ、**xconnect** コマンド設定が拒否されます。**xconnect** コマンド設定とプロトコル逆多重化設定がイネーブルで、IP アドレスが設定されている場合は、IP アドレスを削除できません。設定済みの IP アドレスを変更または削除するには、最初に、**xconnect** コマンド設定をディセーブルにする必要があります。

次の表に、設定の有効な組み合わせを示します。

表 *2*：有効な設定シナリオ

シナリオ	IP アドレス	xconnect 設定	プロトコル逆多重化設定
ルーティング	はい	いいえ	--
L2VPN	いいえ	はい	いいえ
IPv6 プロトコル逆多重化	はい	はい	はい

Cisco ASR 1000 シリーズ ルータ上での L2TPv3 のパフォーマンス効果

L2TPv3 でサポートされる接続回線およびトンネルの最大数は次のとおりです。

- Embedded Services Processor 10（ESP10）を搭載した First-generation Cisco ASR 1000 Series 第 1 世代の Cisco ASR 1000 シリーズ ルート プロセッサ（RP1）
  - イーサネット用の接続回線：一般的なユーザ環境においてシステムあたり 8000。これには、ポートあたり 4000 および SPA あたり 8000 が含まれます。
  - L2TPv3 トンネル：1000（一般的なユーザ環境の場合）および 2000（最大数）。
- Embedded Services Processor 20（ESP20）を搭載した Second-generation Cisco ASR 1000 Series 第 2 世代の Cisco ASR 1000 シリーズ ルート プロセッサ（RP2）
  - イーサネット用の接続回線：一般的なユーザ環境においてシステムあたり 16,000。これには、ポートあたり 4000 および SPA あたり 8000 が含まれます。
  - L2TPv3 トンネル：2000（一般的なユーザ環境の場合）および 4000（最大数）

L2TPv3 では、大きいパケット（MTU よりも大きいパケット サイズ）のフラグメンテーションを引き起こす可能性があるトンネル カプセル化が TCP パケットに追加されます。大きい TCP パケットに小さい TCP パケット（セッション MTU よりも小さいパケット サイズ）が続くシナリオを考えてみましょう。L2TPv3 カプセル化の後、カプセル化された大きい TCP パケットはフラグメント化されますが、カプセル化された小さい TCP パケットはフラグメント化されません。Cisco ASR 1000 シリーズ ルータ上では、大きい TCP パケットのフラグメンテーションとリアセンブルには追加のプロセッサ サイクルが必要です。Cisco ASR 1000 シリーズ ルータはマルチスレッド処理の後に従うので、小さいパケットは処理時間がより短くなり、フラグメント化された大きなパケットの前に送られる可能性があります。このプロセスでは、受信者側のパケット シーケンスが変わる可能性があります。

回避策として、**ip pmtu** コマンドをイネーブルにして、トンネリングされたパケットのフラグメンテーションを防ぐことができます（「MTU の処理」を参照）。

レイヤ 2 トンネリング プロトコル バージョン 3 の設定方法

L2TP コントロール チャネル パラメータの設定

L2TP クラス コンフィギュレーション モードを開始したら、L2TP コントロール チャネル パラメータを任意の順序で設定できます。認証要件が複数存在する場合は、複数の L2TP クラス コントロール チャネル パラメータのセットを別々の L2TP クラス名で設定できます。ただし、IP アドレスのペア間の接続に適用できるのは、1 つのパラメータのセットだけです。

L2TP コントロール チャネル タイミング パラメータの設定

次の L2TP コントロール チャネル タイミング パラメータを L2TP クラス コンフィギュレーション モードで設定できます。

- コントロール チャネルに使用される受信ウィンドウのパケット サイズ
- コントロール メッセージに使用される再送信パラメータ
- コントロール チャネルに使用されるタイムアウト パラメータ

この作業では、L2TP クラス内の一連のタイミング コントロール チャネル パラメータを設定します。タイミング コントロール チャネル パラメータ設定のすべてがオプションであり、任意の順序で設定できます。これらのパラメータが設定されなかった場合は、デフォルト値が適用されます。

手順の概要

1. **enable**
2. **configureterminal**
3. **l2tp-class** [*l2tp-class-name*]
4. **retransmit** {**initialretries***initial-retries*| **retries***retries*| **timeout** {**max** | **min**} *timeout*}
5. **timeoutsetup***seconds*
6. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**l2tp-class** [*l2tp-class-name*] 例： `Device(config)# l2tp-class class1`	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。 • *l2tp-class-name* 引数はオプションです。ただし、複数の L2TP クラスを設定するには、それぞれに固有の *l2tp-class-name* を指定する必要があります。
ステップ 4	**retransmit** {**initialretries***initial-retries*| **retries***retries*| **timeout** {**max** | **min**} *timeout*} 例： `Device(config-l2tp-class)# retransmit retries 10`	（任意）コントロール パケットの再送信に影響するパラメータを設定します。 • **initialretries**：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。*initial-retries* 引数の有効な値の範囲は 1 ～ 1000 です。デフォルト値は 2 です。 • **retries**：ピア PE デバイス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。*retries* 引数の有効な値の範囲は 1 ～ 1000 です。デフォルト値は 15 です。 • **timeout** {**max** | **min**}：コントロール パケットを再送信するインターバルの最大値と最小値を秒単位で指定します。*timeout* 引数の有効な値の範囲は 1 ～ 8 です。デフォルトの最大インターバルは 8 です。デフォルトの最小間隔は 1 です。
ステップ 5	**timeoutsetup***seconds* 例： `Device(config-l2tp-class)# timeout setup 400`	（任意）コントロール チャネルのセットアップに許可する時間を秒単位で設定します。 • *seconds* 引数の有効な値の範囲は 60 ～ 6000 です。デフォルト値は 300 です。
ステップ 6	**exit** 例： `Device(config-l2tp-class)# exit`	L2TP クラス コンフィギュレーション モードを終了します。

L2TPv3 コントロール チャネル認証パラメータの設定

L2TP コントロール チャネルの認証設定

L2TP コントロール チャネルの認証方式は、L2TPv2 から継承された古い CHAP 型認証システムです。

次の L2TP コントロール チャネル認証パラメータを L2TP クラス コンフィギュレーション モードで設定できます。

- L2TP コントロール チャネルの認証
- L2TP コントロール チャネルの認証に使用されるパスワード
- コントロール チャネルの認証に使用されるローカル ホスト名

この作業では、L2TP クラス内の一連の認証コントロール チャネル パラメータを設定します。認証コントロールチャネルパラメータ設定のすべてがオプションであり、任意の順序で設定できます。これらのパラメータが設定されなかった場合は、デフォルト値が適用されます。

手順の概要

1. **enable**
2. **configureterminal**
3. **l2tp-class** [*l2tp-class-name*]
4. **authentication**
5. **password** [**0** | **7**] *password*
6. **hostname***name*
7. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**l2tp-class** [*l2tp-class-name*] 例： `Device(config)# l2tp-class class1`	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。 • *l2tp-class-name* 引数はオプションです。ただし、複数の L2TP クラスを設定するには、それぞれに固有の *l2tp-class-name* を指定する必要があります。
ステップ 4	**authentication** 例： `Device(config-l2tp-class)# authentication`	（任意）PE デバイス間のコントロール チャネルに対する認証をイネーブルにします。
ステップ 5	**password** [**0** | **7**] *password* 例： `Device(config-l2tp-class)# password cisco`	（任意）コントロール チャネルの認証に使用されるパスワードを設定します。 • [**0** | **7**]：（任意）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 デバイス間の共通パスワードを定義します。
ステップ 6	**hostname***name* 例： `Device(config-l2tp-class)# hostname yb2`	（任意）L2TP コントロール チャネル認証時にデバイスを識別するために使用されるホスト名を指定します。 • このコマンドを使用しなかった場合は、デフォルトのデバイスのホスト名が使用されます。
ステップ 7	**exit** 例： `Device(config-l2tp-class)# exit`	L2TP クラス コンフィギュレーション モードを終了します。

L2TPv3 コントロール メッセージ ハッシングの設定

この作業では、L2TP クラスの L2TPv3 コントロール メッセージ ハッシング機能を設定します。

手順の概要

1. **enable**
2. **configureterminal**
3. **l2tp-class** [*l2tp-class-name*]
4. **digest** [**secret** [**0** | **7**]*password*] [**hash** {**md5** | **sha**}]
5. **digest** check
6. **hidden**
7. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**l2tp-class** [*l2tp-class-name*] 例： `Device(config)# l2tp-class class1`	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。 • *l2tp-class-name* 引数はオプションです。ただし、複数の L2TP クラスを設定するには、それぞれに固有の *l2tp-class-name* を指定する必要があります。
ステップ 4	**digest** [**secret** [**0**	**7**]*password*] [**hash** {**md5**	**sha**}] 例： `Device(config-l2tp-class)# digest secret cisco hash sha`	（任意）L2TPv3 コントロール チャネル認証または整合性チェックをイネーブルにします。 • **secret**：（任意）L2TPv3 コントロール チャネル認証をイネーブルにします。 （注） **digest** コマンドを **secret** キーワード オプションを指定せずに発行した場合は、L2TPv3 整合性チェックがイネーブルになります。 • [**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。

	コマンドまたはアクション	目的

		• *password*：ピア デバイス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 | sha}**：（任意）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 ハッシングを指定します。
		  • **sha**：HMAC-SHA-1 ハッシングを指定します。
		デフォルトのハッシュ関数は **md5** です。

ステップ 5	**digest** check **例：** `Device(config-l2tp-class)# digest check`	（任意）受信されたコントロール メッセージ内のメッセージ ダイジェストの確認をイネーブルにします。 • メッセージ ダイジェストの確認はデフォルトでイネーブルになっています。 （注） メッセージ ダイジェストの確認は、**digest secret** コマンドを使用して認証をイネーブルにしていなければ、ディセーブルにできません。認証が **digest secret** コマンドを使用して設定されていない場合は、ダイジェスト チェックをディセーブルにして性能を向上させることができます。
ステップ 6	**hidden** **例：** `Device(config-l2tp-class)# hidden`	（任意）L2TPv3 ピアへのコントロール メッセージの送信時に AV ペア隠蔽をイネーブルにします。 • AV ペア隠蔽はデフォルトでディセーブルになっています。 • クッキー AV ペアの隠蔽だけがサポートされています。 • cookie が L2TP クラス コンフィギュレーション モードで設定されている場合（「L2TPv3 セッション パラメータの手動設定」を参照）は、AV ペア隠蔽をイネーブルにすると、**digest secret** コマンドで設定されたパスワードを使用して cookie が隠し AV ペアとしてピアに送信されます。 （注） AV ペア隠蔽は、認証が **digest secret** コマンドを使用してイネーブルにされており、ほかの認証方式が設定されていない場合にのみイネーブルにされます。
ステップ 7	**exit** **例：** `Device(config-l2tp-class)# exit`	L2TP クラス コンフィギュレーション モードを終了します。

L2TPv3 ダイジェスト シークレット グレースフル スイッチオーバーの設定

確立された L2TPv3 トンネルを中断せずに、古い L2TPv3 コントロール チャネル認証パスワードから新しい L2TPv3 コントロール チャネル認証パスワードへの移行を行うには、次の作業を実行します。

はじめる前に

この作業を実行する前に、「L2TPv3 コントロール メッセージ ハッシングの設定」作業に記載されているように、コントロール チャネル認証をイネーブルにする必要があります。

（注） この作業は、古い CHAP 型コントロール チャネル認証システムで設定された認証パスワードとの互換性がありません。

手順の概要

1. **enable**
2. **configureterminal**
3. **l2tp-class***l2tp-class-name*
4. **digest** [**secret** [**0** | **7**] *password*] [**hash** {**md5** | **sha**}]
5. **end**
6. **showl2tuntunnelall**
7. **configureterminal**
8. **l2tp-class** [*l2tp-class-name*]
9. **nodigest** [**secret** [**0** | **7**] *password* [**hash** {**md5** | **sha**}]
10. **end**
11. **showl2tuntunnelall**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**l2tp-class***l2tp-class-name* 例： `Device(config)# l2tp-class class1`	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 4	**digest** [**secret** [**0** | **7**] *password*] [**hash** {**md5** | **sha**}] 例： `Device(config-l2tp-class)# digest secret cisco2 hash sha`	L2TPv3 コントロール チャネル認証で使用される新しいパスワードを設定します。 • いつでも最大 2 個のパスワードを設定できます。 （注） 現在は、新旧両方のパスワードを使用して認証が行われます。
ステップ 5	**end** 例： `Device(config-l2tp-class)# end`	コンフィギュレーション セッションを終了して、特権 EXEC モードに移行します。
ステップ 6	**showl2tuntunnelall** 例： `Device# show l2tun tunnel all`	（任意）レイヤ2 トンネルの現在の状態と、ローカルとリモートの L2TP ホスト名、パケット カウントの合計、コントロール チャネル情報などの、設定されたトンネルに関する情報を表示します。 • トンネルは数秒以内に新しいコントロール チャネル認証パスワードに更新する必要があります。数分が経過しても、トンネルが 2 つの秘密が設定されたことを示すように更新されなかった場合は、そのトンネルを手動でクリアして、障害レポートを Cisco Technical Assistance Center（TAC）に登録する必要があります。L2TPv3 トンネルを手動でクリアするには、「L2TPv3 トンネルの手動クリア」で説明されている作業を実行します。 （注） このコマンドは、トンネルでコントロールチャネル認証用の新しいパスワードが使用されているかどうかを判断するために発行します。指定した L2TP クラス内のトンネルごとに表示される出力に、2 つの秘密が設定されていることが示されるはずです。
ステップ 7	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 8	**l2tp-class** [*l2tp-class-name*] 例： `Device(config)# l2tp-class class1`	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。

	コマンドまたはアクション	目的
		• *l2tp-class-name* 引数はオプションです。ただし、複数の L2TP クラスを設定するには、それぞれに固有の *l2tp-class-name* を指定する必要があります。
ステップ 9	**nodigest** [**secret** [**0** | **7**] *password* [**hash** {**md5** | **sha**}] 例： `Device(config-l2tp-class)# no digest secret cisco hash sha`	L2TPv3 コントロール チャネル認証に使用されていた古いパスワードを削除します。 （注） 古いパスワードは、すべてのピア PE デバイスが新しいパスワードに更新されるまで削除しないでください。
ステップ 10	**end** 例： `Device(config-l2tp-class)# end`	コンフィギュレーション セッションを終了して、特権 EXEC モードに移行します。
ステップ 11	**showl2tuntunnelall** 例： `Device# show l2tun tunnel all`	（任意）レイヤ 2 トンネルの現在の状態と、ローカルとリモートの L2TP ホスト名、パケット カウントの合計、コントロール チャネル情報などの、設定されたトンネルに関する情報を表示します。 • トンネルで、古いコントロール チャネル認証パスワードが使用されなくなっているはずです。数分が経過しても、トンネルが 1 つの秘密しか設定されていないことを示すように更新されなかった場合は、そのトンネルを手動でクリアして、障害レポートを TAC に登録する必要があります。L2TPv3 トンネルを手動でクリアするには、「L2TPv3 トンネルの手動クリア」で説明されている作業を実行します。 （注） このコマンドは、すべてのトンネルでコントロールチャネル認証用の新しいパスワードが使用されることを保証するために発行します。指定した L2TP クラス内のトンネルごとに表示される出力に、1 つの秘密が設定されていることが示されるはずです。

L2TP コントロール チャネル メンテナンス パラメータの設定

L2TP hello パケット キープアライブ インターバル コントロール チャネル メンテナンス パラメータは、L2TP クラス コンフィギュレーション モードで設定できます。

この作業では、hello メッセージに使用されるインターバルを L2TP クラス内に設定します。このコントロールチャネルパラメータ設定はオプションです。このパラメータが設定されなかった場合は、デフォルト値が適用されます。

手順の概要

1. **enable**
2. **configureterminal**
3. **l2tp-class** [*l2tp-class-name*]
4. **hello***interval*
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**l2tp-class** [*l2tp-class-name*] 例： `Device(config)# l2tp-class class1`	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。 • *l2tp-class-name* 引数はオプションです。ただし、複数の L2TP クラスを設定するには、それぞれに固有の *l2tp-class-name* を指定する必要があります。
ステップ 4	**hello***interval* 例： `Device(config-l2tp-class)# hello 100`	（任意）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 5	**exit** 例： `Device(config-l2tp-class)# exit`	L2TP クラス コンフィギュレーション モードを終了します。

L2TPv3 疑似回線の設定

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. **enable**
2. **configureterminal**
3. **pseudowire-class** [*pw-class-name*]
4. **encapsulationl2tpv3**
5. **protocol** {**l2tpv3**| **none**} [*l2tp-class-name*]
6. **iplocalinterface***interface-name*
7. **ippmtu**
8. **iptos** {**value***value* | **reflect**}
9. **ipdfbitset**
10. **ipttl***value*
11. **ipprotocol** {**l2tp** | *protocol-number*}
12. **sequencing** {**transmit** | **receive** |**both**}
13. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**pseudowire-class** [*pw-class-name*] 例： `Device(config)# pseudowire-class etherpw`	疑似回線クラス コンフィギュレーション モードを開始して、オプションで L2TP 疑似回線クラスの名前を指定します。
ステップ 4	**encapsulationl2tpv3** 例： `Device(config-pw)# encapsulation l2tpv3`	トンネル IP トラフィックに対するデータ カプセル化方式として L2TPv3 を使用するように指定します。

	コマンドまたはアクション	目的
ステップ 5	**protocol** {**l2tpv3**| **none**} [*l2tp-class-name*] 例： `Device(config-pw)# protocol l2tpv3 class1`	（任意）指定した L2TP クラス内のコントロール チャネル パラメータを使用して作成された疑似回線を管理するための L2TPv3 シグナリング プロトコルを指定します（「L2TP コントロール チャネル パラメータの設定」を参照）。 • *l2tp-class-name* 引数を指定しなかった場合は、L2TP コントロール チャネル パラメータのデフォルト値が使用されます。デフォルトの **protocol** オプションは **l2tpv3** です。 • この疑似回線クラスを使用して作成された L2TPv3 セッション内でシグナリングを使用しない場合は、**protocol none** を入力します。
ステップ 6	**iplocalinterface***interface-name* 例： `Device(config-pw)# ip local interface e0/0`	トンネリングされたパケットを送信するためのソース IP アドレスとして IP アドレスが使用される PE デバイス インターフェイスを指定します。 • PE デバイスのペア間で設定された疑似回線ごとに同じローカル インターフェイス名を使用することも、別のローカル インターフェイス名を使用することもできます。 （注） このコマンドは、データ カプセル化方式として L2TPv3 を使用する pseudowire-class 設定の場合に設定する必要があります。
ステップ 7	**ippmtu** 例： `Device(config-pw)# ip pmtu`	（任意）トンネリングされたトラフィックの PMTU を検出できるようにして、フラグメンテーションをサポートします。 • このコマンドは、L2TPv3 セッション トラフィックを伝送するバックボーン ネットワーク上のフラグメンテーション エラーを示す ICMP 到達不能メッセージの処理をイネーブルにします。また、このコマンドは、セッションに送信され、DF ビットがセットされた IP パケットに対する MTU チェックをイネーブルにします。MTU を超えたすべての IP パケットが破棄され、ICMP 到達不能メッセージが送信されます。MTU 検出はデフォルトでディセーブルになっています。 （注） 手順 5 で **protocol none** コマンドを使用してシグナリングをディセーブルにした場合は、**ip pmtu** コマンドがサポートされません。 • このコマンドは、データが疑似回線に入る前に、IP パケットのフラグメンテーションをイネーブルにするために疑似回線クラス設定でイネーブルにする必要があります。 （注） データが疑似回線に入る前に IP パケットのフラグメンテーションをイネーブルにするには、疑似回線クラス コンフィギュレーション モードで **ip dfbit set** コマンドも入力することを推奨します。これによって、PMTU がより迅速に検出されます。

	コマンドまたはアクション	目的
		（注） **ip pmtu** コマンドがイネーブルになっている場合は、内側 IP ヘッダーから外側 IP ヘッダーに DF ビットがコピーされます。レイヤ 2 フレーム内で IP ヘッダーが見つからなかった場合は、外側 IP ヘッダー内の DF ビットが 0 に設定されます。
ステップ 8	**iptos** {**value***value* | **reflect**} 例： `Device(config-pw)# ip tos reflect`	（任意）トンネリングされたパケットの IP ヘッダー内の ToS バイト値を設定するか、内側 IP ヘッダーからの ToS バイト値を反映させます。 • *value* 引数の有効な値の範囲は 0 ～ 255 です。デフォルトの ToS バイト値は 0 です。
ステップ 9	**ipdfbitset** 例： `Device(config-pw)# ip dfbit set`	（任意）トンネリングされたパケットの外側ヘッダー内の DF ビット値を設定します。 • このコマンドは、（性能上の理由から）トンネリングされたパケットの再構築をピア PE デバイス上で実行したくない場合に使用します。 • このコマンドは、デフォルトでディセーブルになっています。
ステップ 10	**ipttl***value* 例： `Device(config-pw)# ip ttl 100`	（任意）トンネリングされたパケットの IP ヘッダー内の存続可能時間（TTL）バイト値を設定します。 • *value* 引数の有効な値の範囲は 1 ～ 255 です。デフォルトの TTL バイト値は 255 です。
ステップ 11	**ipprotocol** {**l2tp** | *protocol-number*} 例： `Device(config-pw)# ip protocol l2tp`	（任意）トンネリングパケットに使用される IP プロトコルを設定します。
ステップ 12	**sequencing** {**transmit** | **receive** |**both**} 例： `Device(config-pw)# sequencing both`	（任意）疑似回線上のデータ パケットのシーケンス処理がイネーブルになっている方向を指定します。 • **transmit**：使用されているデータ カプセル化方式に従って、疑似回線上で送信されたデータ パケットのヘッダー内のシーケンス番号フィールドを更新します。 • **receive**：疑似回線上で受信されたデータ パケットのヘッダー内のシーケンス番号フィールドを保存します。順序が不正なパケットは破棄されます。 • **both**：**transmit** オプションと **receive** オプションの両方をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 13	**exit** 例： `Device(config-pw)# exit`	疑似回線 クラス コンフィギュレーション モードを終了します。

xconnect 接続回線の設定

設定する仮想回線識別子によって、PE デバイス上で設定された疑似回線と CE デバイス上の接続回線間のバインディングが構築されます。L2TPv3 コントロール チャネルの一方の端にある PE デバイスに設定された仮想回線識別子をもう一方の端にあるピア PE デバイスにも設定する必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***typeslot/port*
4. **xconnect***peer-ip-addressvcidpseudowire-parameters* [**sequencing** {**transmit** | **receive** | **both**}]
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***typeslot/port* 例： `Device(config)# interface ethernet 0/0`	タイプ別のインターフェイス（イーサネットなど）、スロット番号、およびポート番号を指定して、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**xconnect***peer-ip-address vcid* **pseudowire-parameters** [**sequencing** {**transmit** | **receive** | **both**}] 例： `Device(config-if)# xconnect 10.0.3.201 123 pw-class vlan-xconnect`	ピア PE デバイスの IP アドレスと、コントロール チャネルの両端にある PE 間で共有される 32 ビットの仮想回線識別子を指定します。 • ピア デバイス ID（IP アドレス）と仮想回線 ID はデバイス上で固有の組み合わせにする必要があります。 • 次の疑似回線クラス パラメータのいずれかを *pseudowire-parameters* 引数に設定する必要があります。 • **encapsulation** {**l2tpv3** [**manual**] | **mpls**}：疑似回線上でデータのカプセル化に使用されるトンネリング方式を指定します。 ◦ **l2tpv3**：L2TPv3 がトンネリング方式として使用されます。 ◦ **manual**：（任意）L2TPv3 コントロール チャネルでシグナリングが使用されません。このコマンドは、接続回線の L2TPv3 パラメータを手動で設定するためにデバイスを xconnect コンフィギュレーション モードにします。 ◦ **mpls**：MPLS がトンネリング方式として使用されます。 • **pw-class** {*pw-class-name*}：データ カプセル化タイプ（L2TPv3）が取得される疑似回線クラス設定。 • オプションの **encapsulation** パラメータは、使用される疑似回線トンネリング方式（L2TPv3 または MPLS）を指定します。L2TPv3 コントロール チャネルでシグナリングを使用しない場合は、**manual** を入力します。**encapsulationl2tpv3manual** キーワードの組み合わせによって xconnect 設定サブモードが開始されます。L2TPv3 コントロール チャネルの設定を完了させるために入力する必要のあるその他の L2TPv3 コマンドについては、「L2TPv3 セッション パラメータの手動設定」を参照してください。**encapsulation** 値を入力しなかった場合は、「xconnect 接続回線の設定」作業で **password** コマンドを使用して入力したカプセル化方式が使用されます。 • オプションの **pw-class** パラメータによって、xconnect 文が特定の疑似回線クラスにバインドされます。その後は、疑似回線クラスがそれにバインドされたすべての

	コマンドまたはアクション	目的
		接続回線用のテンプレート設定として機能します。より高度なオプションを設定する必要がある場合は pseudowire-class オプションを指定します。 （注） **encapsulation** オプションと **pw-class** オプションのどちらかまたは両方を指定する必要があります。 （注） データ カプセル化方式として L2TPv3 を選択した場合は、**pw-class** キーワードを指定する必要があります。 • オプションの **sequencing** パラメータは、受信パケット、送信パケット、または送受信パケットのどのパケットに対してシーケンス処理が必要かを指定します。
ステップ 5	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。

L2TPv3 セッション パラメータの手動設定

シグナリングが不要なために、**xconnectl2tpv3manual** コマンドを使用して接続回線を xconnect 用の L2TPv3 疑似回線にバインドする場合（「xconnect 接続回線の設定」を参照）は、L2TP 固有のパラメータを設定して L2TPv3 コントロール チャネル設定を完了する必要があります。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***typeslot/port*
4. **xconnect***peer-ip-addressvc-id***encapsulationl2tpv3manualpw-class***pw-class-name***
5. **l2tpid***local-session-idremote-session-id*
6. **l2tpcookielocal***sizelow-value* [*high-value*]
7. **l2tpcookieremote***sizelow-value* [*high-value*]
8. **l2tphello***l2tp-class-name*
9. **exit**
10. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***typeslot/port* 例： `Device(config)# interface ethernet 0/0`	タイプ別のインターフェイス（イーサネットなど）、スロット番号、およびポート番号を指定して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**xconnect***peer-ip-address vc-id* **encapsulation l2tpv3 manual pw-class** *pw-class-name* 例： `Device(config-if)# xconnect 10.0.3.201 123 encapsulation l2tpv3 manual pw-class vlan-xconnect`	ピア PE デバイスの IP アドレスと、コントロール チャネルの両端にある PE 間で共有される 32 ビットの仮想回線識別子を指定して、xconnect コンフィギュレーション モードを開始します。 • ピア デバイス ID（IP アドレス）と仮想回線 ID はデバイス上で固有の組み合わせにする必要があります。 • **encapsulation l2tpv3 manual** パラメータは、疑似回線トンネリング方式として L2TPv3 を使用するように指定して、xconnect コンフィギュレーション モードを開始します。 • 必須の **pw-class** *pw-class-name* キーワードと引数の組み合わせは、データ カプセル化タイプ（L2TPv3）が取得される疑似回線クラス設定を指定します。

	コマンドまたはアクション	目的
ステップ 5	**l2tpid***local-session-idremote-session-id* 例： `Device(config-if-xconn)# l2tp id 222 111`	ローカル L2TPv3 セッションとピア PE デバイス上のリモート L2TPv3 セッション用の識別子を設定します。 • このコマンドは、接続回線設定を完了するためと、静的 L2TPv3 セッション設定のために必要です。
ステップ 6	**l2tpcookielocal***sizelow-value* [*high-value*] 例： `Device(config-if-xconn)# l2tp cookie local 4 54321`	（任意）ピア PE で着信（受信）L2TP パケットの cookie フィールドに格納する必要のある値を指定します。 • cookie フィールドのサイズは 4 または 8 バイトにすることができます。このコマンドを入力しなかった場合は、L2TP パケットのヘッダー内に cookie 値が格納されません。 • 着信パケット内の cookie 長を 8 バイトに設定した場合は、上位 4 バイトの値と下位 4 バイトの値を指定する必要があります。
ステップ 7	**l2tpcookieremote***sizelow-value* [*high-value*] 例： `Device(config-if-xconn)# l2tp cookie remote 4 12345`	（任意）デバイスで発信（送信）L2TP パケットの cookie フィールドに格納する値を指定します。 • cookie フィールドのサイズは 4 または 8 バイトにすることができます。このコマンドを入力しなかった場合は、L2TP パケットのヘッダー内に cookie 値が格納されません。 • 発信パケット内の cookie 長を 8 バイトに設定した場合は、上位 4 バイトの値と下位 4 バイトの値を指定する必要があります。

	コマンドまたはアクション	目的
ステップ 8	**l2tphello***l2tp-class-name* 例： `Device(config-if-xconn)# l2tp hello l2tp-defaults`	（任意）hello キープアライブ メッセージ間に使用されるインターバルなどのコントロール チャネル設定パラメータに使用される L2TP クラス名を指定します（「L2TP コントロールチャネルパラメータの設定」を参照）。 （注） このコマンドは、コントロールチャネルパラメータをネゴシエートするためのコントロールプレーンが存在せず、コントロール チャネルが L2TP hello メッセージの交換を通してキープアライブをサポートするために使用されることを前提とします。デフォルトで、hello メッセージは送信されません。
ステップ 9	**exit** 例： `Device(config-if-xconn)# exit`	xconnect コンフィギュレーション モードを終了します。
ステップ 10	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。

L2TPv3 のプロトコル逆多重化の設定

イーサネット インターフェイスのプロトコル逆多重化の設定

イーサネット インターフェイス上のプロトコル逆多重化機能を設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***typeslot/port*
4. **ipaddress***ip-addressmask* [**secondary**]
5. **xconnect***peer-ip-addressvcid***pw-class***pw-class-name*
6. **matchprotocolipv6**
7. **exit**
8. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***typeslot/port* 例： `Device(config)# interface ethernet 0/1`	タイプ別のインターフェイス、スロット番号、およびポート番号を指定して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ipaddress***ip-addressmask* [**secondary**] 例： `Device(config-if)# ip address 172.16.128.4`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。
ステップ 5	**xconnect***peer-ip-addressvcid***pw-class***pw-class-name** 例： `Device(config-if)# xconnect 10.0.3.201 888 pw-class demux`	ピア PE デバイスの IP アドレスと、コントロール チャネルの両端にある PE 間で共有される 32 ビットの VCI を指定して、xconnect コンフィギュレーション モードを開始します。 • ピア デバイス ID（IP アドレス）と仮想回線 ID はデバイス上で固有の組み合わせにする必要があります。 • **pw-class***pw-class-name*：データ カプセル化タイプ（L2TPv3）が取得される疑似回線クラス設定。**pw-class** パラメータによって、xconnect 文が特定の疑似回線クラスにバインドされます。その後

	コマンドまたはアクション	目的
		は、疑似回線クラスがそれにバインドされたすべての接続回線用のテンプレート設定として機能します。 （注） L2TPv3 セッションは手動でプロビジョニングすることもできます。L2TPv3 セッション パラメータの手動による設定方法については、「L2TPv3 セッション パラメータの手動設定」を参照してください。
ステップ 6	**matchprotocolipv6** 例： `Device(config-if-xconn)# match protocol ipv6`	IPv6 トラフィックのプロトコル逆多重化をイネーブルにします。
ステップ 7	**exit** 例： `Device(config-if-xconn)# exit`	xconnect コンフィギュレーション モードを終了します。
ステップ 8	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。

Dot1q および QinQ カプセル化の L2TPv3 カスタム Ethertype の設定

dot1q および QinQ カプセル化の L2TPv3 カスタム Ethertype 機能により、QinQ または dot1Q カプセル化を使用して 0x8100 以外の Ethertype をギガビット イーサネット インターフェイス上で設定できます。カスタム Ethertype 0x9100、0x9200、0x88A8 を設定できます。Ethertype フィールド タイプを定義するには、**dot1q tunneling ethertype** コマンドを使用します。

カスタム Ethertype を設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **interface***typenumber*
4. **dot1qtunnelingethertype** {**0x88A8**|**0x9100**|**0x9200**}
5. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface***typenumber* 例： `Device(config)# interface gigabitethernet 1/0/0`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**dot1qtunnelingethertype** {**0x88A8**|**0x9100**|**0x9200**} 例： `Device(config-if)# dot1q tunneling ethertype 0x9100`	Q-in-Q VLAN タギングを実装するときにピア装置で使用される Ethertype フィールド タイプを定義します。
ステップ 5	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。

L2TPv3 上の GEC の設定

レイヤ 2 トンネリング プロトコル バージョン 3（L2TPv3）上の Gigabit EtherChannel（GEC）を設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **interfaceLoopback0**
4. **ip address***ip-address*
5. **exit**
6. **pseudowire-class**[*pw-class-name*]
7. **encapsulationl2tpv3**
8. **ip local interface** *interface-name*
9. **exit**
10. **interface port-channel***channel-number*
11. **xconnect** *peer-ip-address* **encapsulationl2tpv3pw-class** *pw-class-name*
12. **exit**
13. **interface gigabitethernet***interface-type-number*
14. **channel-group***channel-group-number*
15. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interfaceLoopback0** 例： `Device(config)# interface Loopback0`	ループバック インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip address***ip-address* 例： `Device(config-if)# ip address 10.1.0.1 255.255.255.255`	インターフェイスに IP アドレスを割り当てます。
ステップ 5	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 6	**pseudowire-class**[*pw-class-name*] 例： `Device(config)# pseudowire-class l2tpv3`	疑似回線クラス コンフィギュレーション モードを開始して、オプションでレイヤ 2 トンネリング プロトコル（L2TP）疑似回線クラスの名前を指定します。
ステップ 7	**encapsulationl2tpv3** 例： `Device(config-pw)# encapsulation l2tpv3`	トンネル IP トラフィックに対するデータ カプセル化方式として L2TPv3 を使用するように指定します。
ステップ 8	**ip local interface** *interface-name* 例： `Device(config-pw)# ip local interface loopback0`	トンネリングされたパケットを送信するためのソース IP アドレスとして IP アドレスが使用されるプロバイダー エッジ（PE）インターフェイスを指定します。 • PE デバイス間に設定するすべての疑似回線クラスに、同じローカル インターフェイス名を使用します。 （注） このコマンドは、データ カプセル化方式として L2TPv3 を使用する pseudowire-class 設定の場合に設定する必要があります。
ステップ 9	**exit** 例： `Device(config-pw)# exit`	疑似回線クラス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 10	**interface port-channel***channel-number* 例： `Device# interface port-channel 1`	ポート チャネルを定義し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 11	**xconnect** *peer-ip-address* **encapsulationl2tpv3pw-class** *pw-class-name* 例： `Device(config-subif)# xconnect 10.0.3.201 1234 encapsulation l2tpv3 pw-class l2tpv3`	ピア PE デバイスの IP アドレスと、コントロール チャネルの両端にある PE 間で共有される 32 ビットの仮想回線識別子（VCI）を指定します。 • ピア デバイス ID と VCI の組み合わせは、一意である必要があります。 • **pw-class***pw-class-name*：データ カプセル化タイプ（L2TPv3）が取得される疑似回線クラス設定。**pw-class** パラメータによって、**xconnect** 文が特定の疑似回線クラスにバインドされます。その後は、疑似回線クラスがそれにバインドされたすべての接続回線用のテンプレートとして機能します。

	コマンドまたはアクション	目的
ステップ 12	**exit** 例： `Device(config-subif)# exit`	サブインターフェイス コンフィギュレーション モードを終了して、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 13	**interface gigabitethernet***interface-type-number* 例： `Device(config)# interface gigabitEthernet 0/0/0`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 14	**channel-group***channel-group-number* 例： `Device(config-if)# channel-group 1`	EtherChannel グループにインターフェイスを追加します。
ステップ 15	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

Dot1Q を使用した GEC の設定

レイヤ 2 トンネリング プロトコル バージョン 3（L2TPv3）上の VLAN を使用した Gigabit EtherChannel（GEC）を設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **interfaceport-channel***interface-number*
4. **encapsulationdot1q** *vlan-id*
5. **xconnect** *peer-ip-address* **encapsulationl2tpv3pw-class** *pw-class-name*
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interfaceport-channel***interface-number* 例： `Device(config)# interface port-channel 1.1`	ポート チャネルを定義し、サブインターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**encapsulationdot1q** *vlan-id* 例： `Device(config-subif)# encapsulation dot1q 100`	トンネル IP トラフィックに対するデータ カプセル化方式として dot1q を使用するように指定します。
ステップ 5	**xconnect** *peer-ip-address* **encapsulationl2tpv3pw-class** *pw-class-name* 例： `Device(config-subif)# xconnect 10.0.3.201 1234 encapsulation l2tpv3 pw-class l2tpv3`	ピア プロバイダー エッジ（PE）デバイスの IP アドレスと、コントロール チャネルの両端にある PE デバイス間で共有される 32 ビットの仮想回線識別子（VCI）を指定します。 • ピア デバイス ID と VCI の組み合わせは、一意である必要があります。 • **pw-class***pw-class-name*：データ カプセル化タイプ（L2TPv3）が取得される疑似回線クラス設定。**pw-class** パラメータによって、**xconnect** 文が特定の疑似回線クラスにバインドされます。その後は、疑似回線クラスがそれにバインドされたすべての接続回線用のテンプレートとして機能します。
ステップ 6	**end** 例： `Device# end`	サブインターフェイス コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

QinQ を使用した GEC の設定

レイヤ 2 トンネリング プロトコル バージョン 3（L2TPv3）上の queue-in-queue（QinQ）を使用した Gigabit EtherChannel（GEC）を設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configureterminal**
3. **interfaceport-channel***interface-number*
4. **encapsulationdot1q** *vlan-id* **second-dot1q** *second-vlan-id*
5. **xconnect** *peer-ip-address* **encapsulationl2tpv3pw-class** *pw-class-name*
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interfaceport-channel***interface-number* 例： `Device(config)# interface port-channel 1.1`	ポート チャネルとしてサブインターフェイスを定義し、サブインターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**encapsulationdot1q** *vlan-id* **second-dot1q** *second-vlan-id* 例： `Device(config-subif)# encapsulation dot1q 100 second-dot1q 200`	トンネル IP トラフィックに対するデータ カプセル化方式として QinQ を使用するように指定します。
ステップ 5	**xconnect** *peer-ip-address* **encapsulationl2tpv3pw-class** *pw-class-name* 例： `Device(config-subif)# xconnect 10.0.3.202 1234 encapsulation l2tpv3 pw-class l2tpv3`	ピア プロバイダー エッジ（PE）デバイスの IP アドレスと、コントロールチャネルの両端にある PE デバイス間で共有される 32 ビットの仮想回線識別子（VCI）を指定します。 • ピア デバイス ID と VCI の組み合わせは、一意である必要があります。

	コマンドまたはアクション	目的
		• **pw-class***pw-class-name*：データ カプセル化タイプ（L2TPv3）が取得される疑似回線クラス設定。**pw-class** パラメータによって、**xconnect** 文が特定の疑似回線クラスにバインドされます。その後は、疑似回線クラスがそれにバインドされたすべての接続回線用のテンプレートとして機能します。
ステップ 6	**end** 例： `Device# end`	サブインターフェイス コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

L2TPv3 トンネルの手動クリア

特定の L2TPv3 トンネルとそのトンネル内のすべてのセッションを手動でクリアするには、次の作業を実行します。

手順の概要

1. **enable**
2. **clearl2tun** {**l2tp-class***l2tp-class-name* | **tunnelid***tunnel-id* | **localip***ip-address* | **remoteip***ip-address* | **all**}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**clearl2tun** {**l2tp-class***l2tp-class-name*	**tunnelid***tunnel-id*	**localip***ip-address*	**remoteip***ip-address*	**all**} 例： `Device# clear l2tun tunnel id 56789`	指定された L2TPv3 トンネルをクリアします（L2TPv3 トンネル セッションが設定されていない場合は、このコマンドを使用できません）。 • **l2tp-class***l2tp-class-name*：指定された L2TP クラス名を持つすべての L2TPv3 トンネルが解放されます。 • **tunnelid***tunnel-id*：指定されたトンネル ID を持つ L2TPv3 トンネルが解放されます。 • **localip***ip-address*：指定されたローカル IP アドレスを持つすべての L2TPv3 トンネルが解放されます。

	コマンドまたはアクション	目的
		• **remoteip***ip-address*：指定されたリモート IP アドレスを持つすべての L2TPv3 トンネルが解放されます。 • **all**：すべての L2TPv3 トンネルが解放されます。

レイヤ2 トンネリング プロトコル バージョン3の設定例

（注） このマニュアルで使用している IP アドレスは、実際のアドレスを示すものではありません。マニュアル内の例、コマンド出力、および図は、説明のみを目的として使用されています。説明の中に実際のアドレスが使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

例：xconnect イーサネット インターフェイスの静的 L2TPv3 セッションの設定

L2TPv3 は、セッションを手動でプロビジョニング可能な唯一のカプセル化方式です。この例では、事前にすべてのコントロールチャネルパラメータがセットアップされている静的セッションの設定方法を示します。使用されるコントロール プレーンと、コントロール チャネルをセットアップするためのネゴシエーション フェーズはありません。イーサネットインターフェイス（int e0/0）が確立されるとすぐに、PE デバイスでトンネリングされたトラフィックの送信が開始されます。仮想回線識別子の 123 は使用されません。PE からセッション ID 111 および cookie 12345 を含む L2TP データが送信されます。その後、PE では、セッション ID 222 および cookie 54321 を含む L2TP データ パケットの受信が待機されます。

```
l2tp-class l2tp-defaults
 retransmit initial retries 30
 cookie-size 8
pseudowire-class ether-pw
 encapsulation l2tpv3
 protocol none
 ip local interface Loopback0
interface Ethernet 0/0
 xconnect 10.0.3.201 123 encapsulation l2tpv3 manual pw-class ether-pw
 l2tp id 222 111
 l2tp cookie local 4 54321
 l2tp cookie remote 4 12345
 l2tp hello l2tp-defaults
```

例：xconnect VLAN サブインターフェイスのネゴシエーション済み L2TPv3 セッションの設定

次に、VLAN xconnect インターフェイスの動的 L2TPv3 セッションの設定例を示します。この例では、VLAN ID が 5 の VLAN トラフィックだけがトンネリングされます。反対方向では、123 の仮想回線識別子で識別された L2TPv3 セッションを通して、VLAN ID フィールドが 5 に書き換えられたフレームが受信されます。L2TPv3 は、コントロール プレーン プロトコルとデータ カプセル化の両方に使用されます。

```
l2tp-class class1
 authentication
 password secret
pseudowire-class vlan-xconnect
 encapsulation l2tpv3
 protocol l2tpv3 class1
 ip local interface Loopback0
interface Ethernet0/0.1
 encapsulation dot1q 5
 xconnect 10.0.3.201 123 pw-class vlan-xconnect
```

例：ローカル HDLC スイッチングのネゴシエーション済み L2TPv3 セッションの設定

次に、ローカル HDLC スイッチングの動的 L2TPv3 セッションの設定例を示します。この例では、仮想回線識別子を IP アドレスごとに一意にする必要があるため、L2TPv3 疑似回線のエンドポイントで 2 種類の IP アドレスを設定する必要があることに注意してください。

```
interface loopback 1
 ip address 10.0.0.1 255.255.255.255
interface loopback 2
 ip address 10.0.0.2 255.255.255.255
pseudowire-class loopback1
 encapsulation l2tpv3
 ip local interface loopback1
pseudowire-class loopback2
 encapsulation l2tpv3
 ip local interface loopback2
interface s0/0
 encapsulation hdlc
 xconnect 10.0.0.1 100 pw-class loopback2
interface s0/1
 encapsulation hdlc
 xconnect 10.0.0.2 100 pw-class loopback1
```

例：L2TPv3 セッションの確認

デバイス上の現在の L2TPv3 セッションに関する情報を表示するには、**show l2tun session brief** コマンドを使用します。

```
Device# show l2tun session brief
L2TP Session Information Total tunnels 1 sessions 1
LocID      TunID      Peer-address    State     Username, Intf/
                                      sess/cir  Vcid, Circuit
2391726297 2382731778 6.6.6.6         est,UP    100, Gi0/2/0
```

デバイス上の現在の L2TPv3 セッションに関する詳細情報を表示するには、**show l2tun session all** コマンドを使用します。

```
Device# show l2tun session all
L2TP Session Information Total tunnels 1 sessions 1
Session id 2391726297 is up, logical session id 36272, tunnel id 2382731778
  Remote session id is 193836624, remote tunnel id 2280318174
  Locally initiated session
  Unique ID is 12
Session Layer 2 circuit, type is Ethernet, name is GigabitEthernet0/2/0
  Session vcid is 100
  Circuit state is UP
    Local circuit state is UP
    Remote circuit state is UP
Call serial number is 98300002
Remote tunnel name is l2tp-asr-2
  Internet address is 6.6.6.6
Local tunnel name is l2tp-asr-1
  Internet address is 3.3.3.3
IP protocol 115
  Session is L2TP signaled
  Session state is established, time since change 00:05:25
    94 Packets sent, 58 received
    9690 Bytes sent, 5642 received
  Last clearing of counters never
  Counters, ignoring last clear:
    94 Packets sent, 58 received
    9690 Bytes sent, 5642 received
    Receive packets dropped:
      out-of-order:             0
      other:                    0
      total:                    0
Send packets dropped:
      exceeded session MTU:     0
      other:                    0
      total:                    0
  DF bit off, ToS reflect disabled, ToS value 0, TTL value 255
  Sending UDP checksums are disabled
  Received UDP checksums are verified
  No session cookie information available
  FS cached header information:
    encap size = 24 bytes
    45000014 00000000 ff73a965 03030303
    06060606 0b8db650
  Sequencing is off
  Conditional debugging is disabled
  SSM switch id is 4101, SSM segment id is 12294
```

例：L2TP コントロール チャネル

L2TP コントロール チャネルは、機能をネゴシエートしたり、ピア PE デバイスの状態をモニタしたり、L2TPv3 セッションの各種コンポーネントを設定したりするために使用されます。

デバイス上のすべての L2TP セッションを処理するその他の L2TP 対応デバイスへの L2TP コントロール チャネルに関する情報を表示するには、**show l2tun tunnel** コマンドを使用します。

```
Device# show l2tun tunnel
L2TP Tunnel Information Total tunnels 1 sessions 1
LocTunID   RemTunID   Remote Name   State  Remote Address  Sessn L2TP Class/
                                                          Count VPDN Group
2382731778 2280318174 l2tp-asr-2    est    6.6.6.6         1     l2tp_default_cl
```

デバイス上のすべての L2TP セッションを処理するその他の L2TP 対応デバイスへの L2TP コントロール チャネルに関する詳細情報を表示するには、**show l2tun tunnel all** コマンドを使用します。

```
Device# show l2tun tunnel all
L2TP Tunnel Information Total tunnels 1 sessions 1
Tunnel id 2382731778 is up, remote id is 2280318174, 1 active sessions
  Locally initiated tunnel
```

```
  Tunnel state is established, time since change 00:02:59
  Tunnel transport is IP  (115)
  Remote tunnel name is l2tp-asr-2
    Internet Address 6.6.6.6, port 0
  Local tunnel name is l2tp-asr-1
    Internet Address 3.3.3.3, port 0
  L2TP class for tunnel is l2tp_default_class
  Counters, taking last clear into account:
    54 packets sent, 35 received
    5676 bytes sent, 3442 received
  Last clearing of counters never
  Counters, ignoring last clear:
    54 packets sent, 35 received
    5676 bytes sent, 3442 received
Control Ns 5, Nr 4
  Local RWS 1024 (default), Remote RWS 1024
  Control channel Congestion Control is disabled
  Tunnel PMTU checking disabled
  Retransmission time 1, max 1 seconds
  Unsent queuesize 0, max 0
  Resend queuesize 0, max 2
  Total resends 0, ZLB ACKs sent 2
  Total out-of-order dropped pkts 0
  Total out-of-order reorder pkts 0
  Total peer authentication failures 0
  Current no session pak queue check 0 of 5
  Retransmit time distribution: 0 0 0 0 0 0 0 0 0 0
  Control message authentication is disabled
```

例：L2TPv3 コントロール チャネル認証の設定

次に、L2TPv3 コントロール チャネルの CHAP 型認証を設定する例を示します。

```
l2tp-class class0
 authentication
 password cisco
```

次に、L2TPv3 コントロール メッセージ ハッシング機能を使用してコントロール チャネル認証を設定する例を示します。

```
l2tp-class class1
 digest secret cisco hash sha
 hidden
```

次に、L2TPv3 コントロール メッセージ ハッシング機能を使用して、コントロール チャネル整合性チェックを設定する例、およびメッセージ ダイジェストの確認をディセーブルにする例を示します。

```
l2tp-class class2
 digest hash sha
 no digest check
```

次に、L2TPv3 コントロール メッセージ ハッシング機能を使用して、メッセージ ダイジェストの確認をディセーブルにする例を示します。

```
l2tp-class class3
 no digest check
```

例：L2TPv3ダイジェストシークレットグレースフルスイッチオーバーの設定

次に、L2TPv3ダイジェストシークレットグレースフルスイッチオーバー機能を使用して、class1という名前の L2TP クラスの L2TP コントロール チャネル認証パスワードを変更する例を示しま

す。この例では、class1 という名前の L2TP クラスにすでに古いパスワードが設定されているものとします。

```
Device(config)# l2tp-class class1
Device(config-l2tp-class)# digest secret cisco2 hash sha
!
! Verify that all peer PE devices have been updated to use the new password before
! removing the old password.
!
Device(config-l2tp-class)# no digest secret cisco hash sha
```

例：L2TPv3ダイジェストシークレットグレースフルスイッチオーバーの確認

次の **showl2tuntunnelall** コマンドの出力は、L2TPv3 ダイジェスト シークレット グレースフル スイッチオーバー機能に関する情報を示しています。

```
Device# show l2tun tunnel all
! The output below displays control channel password information for a tunnel which has
! been updated with the new control channel authentication password.
!
Tunnel id 12345 is up, remote id is 54321, 1 active sessions
Control message authentication is on, 2 secrets configured
Last message authenticated with first digest secret
!
! The output below displays control channel password information for a tunnel which has
! only a single control channel authentication password configured.
!
Tunnel id 23456 is up, remote id is 65432, 1 active sessions
!
Control message authentication is on, 1 secrets configured
Last message authenticated with first digest secret
!
! The output below displays control channel password information for a tunnel which is
! communicating with a peer that has only the new control channel authentication password
! configured.
!
Tunnel id 56789 is up, remote id is 98765, 1 active sessions
!
Control message authentication is on, 2 secrets configured
Last message authenticated with second digest secret
```

例：IP パケットのフラグメンテーション用疑似回線クラスの設定

次に、CE デバイスで生成された IP トラフィックを疑似回線の手前で断片化可能な疑似回線クラスのサンプル設定を示します。

```
pseudowire class class1
 encapsulation l2tpv3
 ip local interface Loopback0
 ip pmtu
 ip dfbit set
```

例：L2TPv3 のプロトコル逆多重化の設定

次に、IPv4 PE デバイス上で L2TPv3 プロトコル逆多重化機能を設定する例を示します。IPv6 デバイスと相対する PE デバイスは、IPv6 を設定する必要がありません。

```
interface ethernet 0/1
 ip address 172.16.128.4
 xconnect 10.0.3.201 888 pw-class demux
  match protocol ipv6
```

例：L2TPv3 トンネルの手動クリア

次の例は、トンネル ID を使用して特定の L2TPv3 トンネルを手動でクリアする方法を示しています。

```
clear l2tun tunnel 65432
```

例：Dot1q および QinQ カプセル化の L2TPv3 カスタム Ethertype の設定

次に、ギガビット イーサネット インターフェイス上に QinQ または dot1Q カプセル化を使用して、0x8100 以外の Ethertype を設定する例を示します。この例では、ギガビット イーサネット インターフェイス 1/0/0 の Ethertype フィールドが 0x9100 に設定されます。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/0/0
Device(config-if)# dot1q tunneling ethertype 0x9100
```

例：L2TPv3 HDLC like-to-like レイヤ 2 転送の設定

例：動的モードでの L2TPv3 HDLC like-to-like レイヤ 2 転送の設定

次に、動的モードで HDLC カプセル化を使用してシリアル インターフェイス上で xconnect を設定する例を示します。動的モードでは、コントロール チャネルで L2TPv3 シグナリングを使用して L2TPv3 トンネルがセットアップされます。

```
pseudowire-class 774
 encapsulation l2tpv3
 protocol l2tpv3
 ip local interface GigabitEthernet0/0/1.774
!
interface Serial0/2/0:0
 no ip address
 xconnect 4.4.4.4 200 pw-class 774
```

例：静的モードでの L2TPv3 HDLC like-to-like レイヤ 2 転送の設定

次に、静的モードで HDLC カプセル化を使用してシリアル インターフェイス上で xconnect を設定する例を示します。静的モードは、L2TPv3 コントロール チャネルでシグナリングをディセーブ

ルにするために使用されます。シグナリングがディセーブルになっているので、xconnect で手動オプションを指定し、L2TPv3 コントロール チャネル設定を実行するように L2TP 固有のパラメータを設定する必要があります。

```
pseudowire-class pe1-ether-pw
 encapsulation l2tpv3
 protocol none
 ip local interface Loopback1
!
interface Serial0/2/0:0
 no ip address
 xconnect 2.2.2.2 50 encapsulation l2tpv3 manual pw-class pe1-ether-pw
  l2tp id 111 111
  l2tp cookie local 4 54321
  l2tp cookie remote 4 12345
```

例：L2TPv3 上の GEC の設定

次に、レイヤ 2 トンネリング プロトコル バージョン 3（L2TPv3）上の Gigabit EtherChannel（GEC）の設定例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface Loopback0
Device(config-if)# ip address 10.1.0.1 255.255.255.255
Device(config-if)# exit
Device(config)# pseudowire-class l2tpv3
Device(config-pw)# encapsulation l2tpv3
Device(config-pw)# ip local interface loopback0
Device(config-if)# exit
Device(config)# interface port-channel 1
Device(config-if)# xconnect 1.1.1.1 1234 encapsulation l2tpv3 pw-class l2tpv3
Device(config-if)# exit
Device(config)# interface g0/0/0
Device(config-if)# channel-group 1
Device(config-if)# end
```

例：L2TPv3 上の Dot1q を使用した GEC の設定

次に、レイヤ 2 トンネリング プロトコル バージョン 3（L2TPv3）上の dot1q を使用した Gigabit EtherChannel（GEC）の設定例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface port-channel 1
Device(config-if)# interface port-channel 1.1
Device(config-subif)# encapsulation dot1q 100
Device(config-subif)# xconnect 10.0.0.2 1234 encapsulation l2tpv3 pw-class l2tpv3
Device(config-subif)# end
```

例：L2TPv3 上の QinQ を使用した GEC の設定

次に、レイヤ 2 トンネリング プロトコル バージョン 3（L2TPv3）上の queue-in-queue（QinQ）を使用した Gigabit EtherChannel（GEC）の設定例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface port-channel 1
```

```
Device(config-if)# interface port-channel 1.1
Device(config-subif)# encapsulation dot1q 100 second-dot1q 200
Device(config-subif)# xconnect 10.0.0.3 1234 encapsulation l2tpv3 pw-class l2tpv3
Device(config-subif)# end
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Master Commands List, All Releases』
WAN コマンド：完全なコマンド構文、コマンドモード、デフォルト、使用上の注意事項、および例	『Wide-Area Networking Command Reference』
レイヤ 2 トンネル プロトコル バージョン 3	『*Layer 2 Tunneling Protocol Version 3*』
Any Transport over MPLS	『*Any Transport over MPLS*』
Cisco 12000 シリーズ ルータ ハードウェア サポート	『*Cross-Platform Release Notes for Cisco IOS Release 12.0S*』
Cisco 7600 シリーズ ルータ ハードウェア サポート	『*Cross-Platform Release Notes for Cisco IOS Release 12.2SR*』
Cisco 3270 シリーズ ルータ ハードウェア サポート	『*Release Notes for Cisco IOS Software Release 12.2SE*』

標準および RFC

標準/RFC	タイトル
draft-ietf-l2tpext-l2tp-base-03.txt	『*Layer Two Tunneling Protocol (Version 3) 'L2TPv3'*』
draft-martini-l2circuit-trans-mpls-09.txt	『*Transport of Layer 2 Frames Over MPLS*』
draft-ietf-pwe3-frame-relay-03.txt.	『*Encapsulation Methods for Transport of Frame Relay over MPLS Networks*』
draft-martini-l2circuit-encap-mpls-04.txt.	『*Encapsulation Methods for Transport of Layer 2 Frames Over IP and MPLS Networks*』

標準/RFC	タイトル
draft-ietf-pwe3-ethernet-encap-08.txt.	『*Encapsulation Methods for Transport of Ethernet over MPLS Networks*』
draft-ietf-pwe3-hdlc-ppp-encap-mpls-03.txt.	『*Encapsulation Methods for Transport of PPP/HDLC over MPLS Networks*』
draft-ietf-ppvpn-l2vpn-00.txt.	『*An Architecture for L2VPNs*』

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

レイヤ 2 トンネリング プロトコル バージョン 3 に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 3：レイヤ 2 トンネリング プロトコル バージョン 3 に関する機能情報

機能名	リリース	機能情報
レイヤ 2 トンネリング プロトコル バージョン 3	XE 2.6 XE 2.6.2 XE 3.3S XE 3.11S	レイヤ 2 トンネリング プロトコル バージョン 3（L2TPv3）機能が、シスコのレイヤ 2 VPN サポートを拡張します。 Cisco IOS XE Release 2.6 で、次の機能が追加されました。 • Ethernet over L2TPv3 • レイヤ 2 VPN（L2VPN）：AToM と L2TPv3 のための Syslog、SNMP Trap、および show コマンドの機能強化 • L2TPv3 コントロール メッセージ ハッシング • L2TPv3 コントロール メッセージ レート制限 • L2TPv3 ダイジェスト シークレット グレースフル スイッチオーバー • L2TPv3 プロトコル逆多重化 • Dot1q および QinQ カプセル化用の L2TPv3 カスタム Ethertype Cisco IOS XE Release 2.6.2 で、**ip pmtu** コマンドのサポートが追加されました。 Cisco IOS XE Release 3.3S で、L2TPv3 上の HDLC のサポートが追加されました。 **clear l2tun**、**debug vpdn**、**ip pmtu**、**l2tp cookie local**、**l2tp cookie remotel2tp hello**、**l2tp id**、and **xconnect** の各コマンドが追加または変更されました。

用語集

AV ペア：Attribute-Value（属性/値）ペア。

CEF：Cisco Express Forwarding。大規模で動的なトラフィック パターンを使用してネットワークのパフォーマンスと拡張性を最適化する、レイヤ 3 IP スイッチング テクノロジー。

データリンク コントロール レイヤ：SNA アーキテクチャ モデル内のレイヤ 2。特定の物理リンク上のデータ転送に責任があります。ほぼ OSI モデルのデータリンク層に対応します。

DCE：Data Circuit-terminating Equipment（データ回線終端装置）（ITU-T 拡張）。ユーザとネットワークを結ぶインターフェイスのネットワーク側を構成する通信ネットワークのデバイスおよび接続。

DFbit：Don't Fragment ビット。パケットをフラグメンテーションしないことを示す IP ヘッダーのビット。

DTE：Data Terminal Equipment（データ端末装置）。データのソース、宛先、またはその両方として機能する、ユーザネットワーク インターフェイスのユーザ側にあるデバイス。

HDLC：High-Level Data Link Control（ハイレベル データリンク コントロール）。ISO で開発された汎用のリンクレベル通信プロトコル。HDLC は、リンク接続上の同期したコード透過型のシリアル情報転送を管理します。

ICMP：Internet Control Message Protocol。ネットワーク エラーとエラー メッセージを処理するネットワーク プロトコル。

IDB：Interface Descriptor Block（インターフェイス記述子ブロック）。

IS-IS：Intermediate System-to-Intermediate System。DECnet Phase V ルーティングに基づく OSI リンク状態階層型ルーティング プロトコル。これによって、IS（デバイス）では、ネットワーク トポロジを決定するための単一指標に基づいてルーティング情報が交換されます。

L2TP：2 つのトンネリング プロトコル（シスコからのレイヤ 2 フォワーディング（L2F）と Microsoft からのポイントツーポイント トンネリング プロトコル（PPTP））の PPP 結合機能に対する拡張。L2TP は、シスコとその他の業界リーダーから支持されている IETF 標準です。

L2TPv3：RFC 2661（L2TP）内の機能を強化した L2TP の草案。

LMI：Local Management Interface（ローカル管理インターフェイス）。

MPLS：Multiprotocol Label Switching（マルチプロトコル ラベル スイッチング）。ラベルを使用して IP トラフィックを転送するスイッチング方式です。このラベルによって、事前に確立された IP ルーティング情報に基づくパケットの転送先がネットワーク内のデバイスに指示されます。

MQC：Modular quality of service CLI（モジュラ Quality of Service CLI）。

MTU：Maximum Transmission Unit（最大伝送単位）。特定のインターフェイスが扱える最大パケット サイズ（バイト数）。

PMTU：Path MTU（パス MTU）。

PVC：相手先固定接続。永続的に確立される固定回線です。エンドポイントとサービス クラスがネットワーク管理によって定義されるフレームリレー論理リンク。X.25 相手先固定接続と同様

に、PVCは、発信フレームリレーネットワーク要素アドレス、発信データリンク コントロール識別子、終端フレームリレーネットワーク要素アドレス、および終端データリンク コントロール識別子で構成されます。発信は、PVC が開始するアクセス インターフェイスを意味します。終端は、PVCが停止するアクセスインターフェイスを意味します。データ ネットワーク企業の多くが 2 地点間の PVC を必要としています。PVC を使用すると、特定の仮想回線が常に存在する必要がある状況で、回線の確立と解放に関する帯域幅が節約されます。連続通信が必要なデータ終端装置で PVC が使用されます。

PW：Pseudowire（疑似回線）。

SNMP：Simple Network Management Protocol（簡易ネットワーク管理プロトコル）。TCP/IP ネットワークでほぼ独占的に使用されているネットワーク管理プロトコル。SNMP は、ネットワーク デバイスをモニタし制御する手段、およびコンフィギュレーション、統計情報収集、パフォーマンス、およびセキュリティを管理する手段を提供します。

トンネリング：標準的なポイントツーポイント カプセル化スキームの実装に必要なサービスを提供するように設計されたアーキテクチャ。

UNI：User-Network Interface（ユーザネットワーク インターフェイス）。

VPDN：Virtual Private Dialup Network（バーチャル プライベート ダイヤルアップ ネットワーク）。モデム、アクセス サーバ、ISDN デバイスなどの一般的なアクセス インフラストラクチャを共有するためのそれぞれが独立したプロトコル ドメインを可能にするネットワーク。VPDN を使用すれば、ISP クラウドを通してリモート アクセス トラフィックをトンネリングする ISP を利用した安全なネットワークを設定できます。

第 4 章

L2VPN 疑似回線冗長化

L2VPN 疑似回線冗長化機能を使用すると、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（L2）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。この機能を使用すると、リモート プロバイダー エッジ（PE）ルータまたは PE とカスタマー エッジ（CE）ルータの間のリンクの障害から復旧できます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

L2VPN 疑似回線冗長性の前提条件

- このフィーチャ モジュールを使用するには、基本的な L2 バーチャル プライベート ネットワーク（VPN）を設定する方法を理解していることが必要です。
  - Any Transport over MPLS
  - L2 VPN インターワーキング
  - レイヤ 2 トンネリング プロトコル バージョン 3（L2TPv3）
- L2VPN疑似回線冗長性機能では、ネットワーク内の障害を検出できるように、次のメカニズムが存在することが必要です。
  - ラベル スイッチド パス（LSP）ping/traceroute および Any Transport over MPLS Virtual Circuit Connection Verification（AToM VCCV）
  - ローカル管理インターフェイス（LMI）
  - 運用管理および保守（OAM）

L2VPN 疑似回線冗長性の制限

- ラベル配布プロトコル（LDP）のデフォルトのセッション ホールドダウン タイマーでは、約 180 秒以内に障害を検出できます。ソフトウェアがより早く障害を検出できるように、この時間を設定することができます。詳細については、**mpls ldp holdtime** コマンドを参照してください。
- L2VPN 疑似回線冗長性は、L2TPv3 を使用した疑似回線インターワーキング モードをサポートしていません。疑似クラスでインターワーキング IP が設定されている場合は、CE 間の接続が影響を受ける可能性があります。
- プライマリおよびバックアップ疑似回線では、同じ種類のトランスポート サービスが動作している必要があります。プライマリおよびバックアップ疑似回線では、AToM または L2TPv3 が設定されている必要があります。
- バックアップ ピアは、非静的 L2TPv3 セッションでのみ設定できます。バックアップ L2TPv3 セッションは、静的 L2TPv3 セッションにはできません。プライマリ疑似回線とバックアップ疑似回線のカプセル化タイプは同じである必要があります。
- L2VPN 疑似回線冗長性を L2VPN インターワーキングとともに使用する場合、インターワーキング方法は、プライマリ疑似回線とバックアップ疑似回線で同じであることが必要です。
- L2VPN 疑似回線冗長性は、マルチプロトコル ラベル スイッチング（MPLS）疑似回線における Experimental（EXP）ビットの設定をサポートしています。
- L2VPN 疑似回線冗長性は、MPLS 疑似回線上の異なる疑似回線カプセル化タイプをサポートしていません。

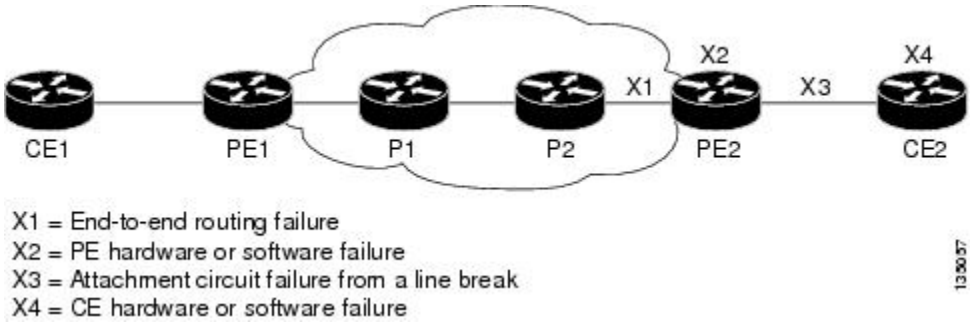
- **mpls l2transport route**コマンドはサポートされていません。代わりに **xconnect** コマンドを使用します。
- プライマリ疑似回線が動作可能な場合、同時にバックアップ疑似回線を完全に動作可能にはできません。バックアップ疑似回線は、プライマリ疑似回線が障害になった後にだけアクティブにできます。
- AToM VCCV 機能は、アクティブな疑似回線でだけサポートされます。
- 複数のバックアップ疑似回線はサポートされていません。

L2VPN 疑似回線冗長性に関する情報

L2VPN 疑似回線冗長性の概要

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。下の図に、サービスの中断に対して脆弱なネットワークの部分を示します。

図 *5* : ***L2VPN*** **ネットワーク内の潜在的な障害ポイント**

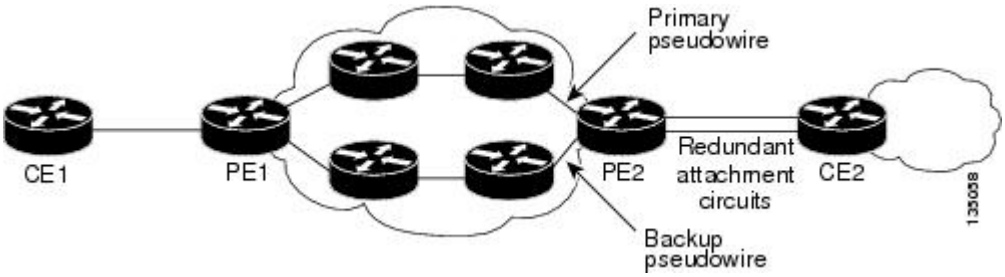


L2VPN 疑似回線冗長性機能は、上の図のすべての障害が発生した場合でも、CE2 ルータが常にネットワークの接続性を維持するための機能を提供します。

L2VPN 疑似回線冗長性機能を使用すると、バックアップ疑似回線を設定できます。下の 3 つの図に示す冗長な疑似回線と冗長なネットワーク要素を使用してネットワークを設定できます。

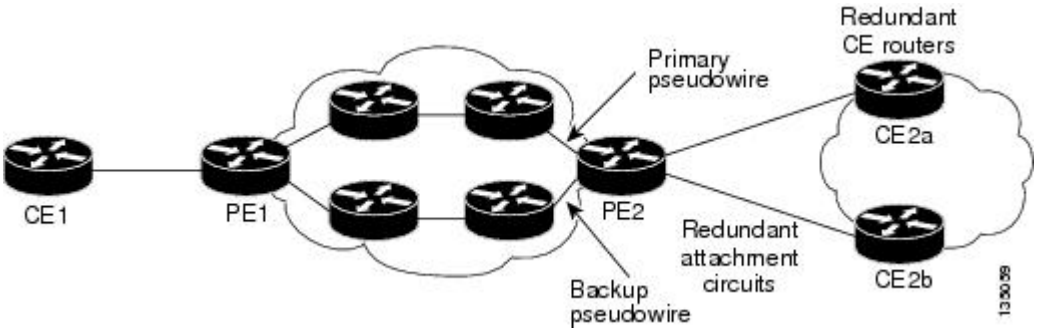
下の図に、冗長な疑似回線と冗長な接続回線を使用したネットワークを示します。

図 *6*：冗長な *PW* と冗長な接続回線を使用した *L2VPN* ネットワーク



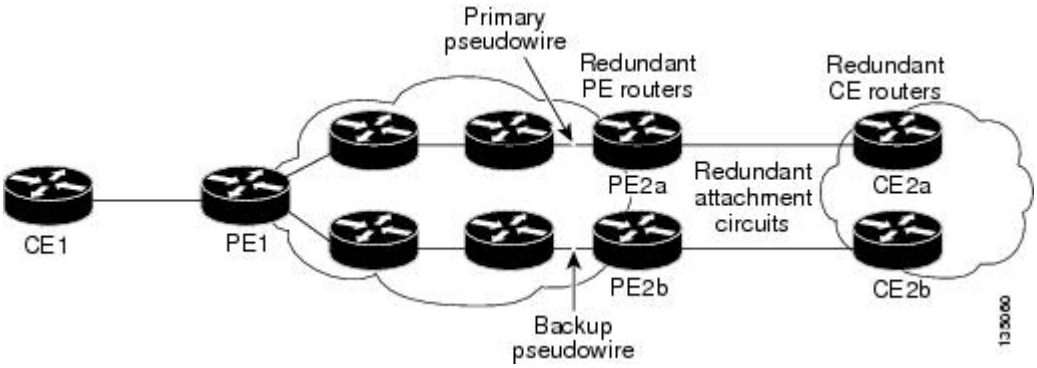
下の図に、冗長な疑似回線、接続回線、CE ルータを使用したネットワークを示します。

図 *7*：冗長な *PW*、接続回線、*CE* ルータを使用した *L2VPN* ネットワーク



下の図に、冗長な疑似回線、接続回線、CE ルータ、および PE ルータを使用したネットワークを示します。

図 *8*：冗長な *PW*、接続回線、*CE* ルータ、*PE* ルータを使用した *L2VPN* ネットワーク



L2VPN 疑似回線冗長性の設定方法

L2VPN疑似回線冗長性機能を使用すると、プライマリ疑似回線が障害になった場合に備えて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。プライマリ疑似回線が再度アップ状態になった後で、その使用を再開できます。

疑似配線の設定

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、疑似回線と呼ぶ接続を設定します。

疑似回線クラス設定グループは、トンネリング メカニズムの次の特性を指定します。

- カプセル化のタイプ
- 制御プロトコル
- ペイロード固有のオプション

AToM VC が正常に動作するためには、疑似回線クラスの一部として **encapsulation mpls** コマンドを指定する必要があります。**xconnect** コマンドの中で **encapsulation mpls** コマンドを省略すると、次のエラーが表示されます。

```
% Incomplete command.
```

疑似回線クラスを設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **pseudowire-class** name
4. **encapsulation mpls**
5. **interworking** {**ethernet** | **ip**}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**pseudowire-class** name 例： `Router(config)# pseudowire-class atom`	指定した名前の疑似回線クラスを確立します。疑似回線クラス コンフィギュレーション モードを開始します。
ステップ 4	**encapsulation mpls** 例： `Router(config-pw-class)# encapsulation mpls`	トンネリング カプセル化を指定します。AToM の場合、カプセル化タイプは **mpls** です。
ステップ 5	**interworking** {**ethernet** | **ip**} 例： `Router(config-pw-class)# interworking ip`	（任意）異なるレイヤ2カプセル化の間の変換をイネーブルにします。

L2VPN プロトコルベース CLI 機能に関連するコマンドを使用した疑似回線の設定

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、疑似回線と呼ぶ接続を設定します。

疑似回線クラス設定グループは、トンネリング メカニズムの次の特性を指定します。

- カプセル化のタイプ
- 制御プロトコル
- ペイロード固有のオプション

AToM VC が正常に動作するためには、疑似回線クラスの一部として **encapsulation mpls** コマンドを指定する必要があります。 **l2vpn xconnectcontext** コマンドの中で **encapsulation mpls** コマンドを省略すると、次のエラーが表示されます。

```
% Incomplete command.
```

疑似回線クラスを設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface pseudowire** *number*
4. **encapsulation mpls**
5. **neighbor** *peer-address vcid-value*
6. **interworking** {**ethernet** | **ip**}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface pseudowire** *number* 例： `Router(config)# interface pseudowire 1`	指定した値を持つインターフェイス疑似回線を確立します。疑似回線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	**encapsulation mpls** 例： `Router(config-pw)# encapsulation mpls`	トンネリング カプセル化を指定します。AToM の場合、カプセル化タイプは **mpls** です。
ステップ 5	**neighbor** *peer-address vcid-value* 例： `Router(config-pw)# neighbor 10.0.0.1 123`	レイヤ 2 VPN（L2VPN）疑似回線のピア IP アドレスと仮想回線（VC）ID を指定します。
ステップ 6	**interworking** {**ethernet**	**ip**} 例： `Router(config-pw)# interworking ip`	（任意）異なるレイヤ2カプセル化の間の変換をイネーブルにします。

L2VPN 疑似回線冗長性の設定

L2VPN 疑似回線冗長性機能を設定するには、次の作業を実行します。

はじめる前に

xconnect コマンドの設定方法は、転送タイプごとに若干異なります。次の設定手順では、サブインターフェイス コンフィギュレーション モードで設定する Ethernet VLAN over MPLS を使用しています。ほかの転送タイプに対して **xconnect** コマンドを設定する方法については、「*Any Transport over MPLS*」を参照してください。

手順の概要

1. **enable**
2. **configureterminal**
3. **interfacegigabitethernet***slot*/*subslot*/*interface*.*subinterface*
4. **encapsulationdot1q***vlan-id*
5. **xconnect***peer-router-idvcid* {**encapsulation mpls**| **pw-class** *pw-class-name}*
6. **backuppeer***peer-router-ip-addrvcid* [**pw-class** *pw-class-name*]
7. **backupdelay***enable-delay*{*disable-delay* | **never**}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interfacegigabitethernet***slot*/*subslot*/*interface*.*subinterface* 例： `Router(config)# interface gigabitethernet0/0/0.1`	ギガビット イーサネット サブインターフェイスを指定し、サブインターフェイス コンフィギュレーション モードを開始します。 （注） 隣接 CE ルータのサブインターフェイスがこの PE ルータと同じ VLAN 上にあることを確認します。

	コマンドまたはアクション	目的
ステップ 4	**encapsulationdot1q***vlan-id* 例： `Router(config-subif)# encapsulation dot1q 100`	サブインターフェイスでの 802.1Q VLAN パケットの受信をイネーブルにします。 （注） Ethernet over MPLS が稼働している CE ルータと PE ルータ間のサブインターフェイスは、同じサブネット内になければなりません。
ステップ 5	**xconnect***peer-router-idvcid* {**encapsulation mpls**| **pw-class** *pw-class-name}* 例： `Router(config-subif)# xconnect 10.0.0.1 123 pw-class atom`	接続回線を疑似回線 VC にバインドし、xconnect コンフィギュレーション モードを開始します。 • このコマンドの構文は、その他のレイヤ 2 トランスポートの場合と同じです。
ステップ 6	**backuppeer***peer-router-ip-addrvcid* [**pw-class** *pw-class-name*] 例： `Router(config-if-xconn)# backup peer 10.0.0.3 125 pw-class atom`	疑似回線 VC の冗長ピアを指定します。 疑似回線クラス名は、疑似回線クラスを作成したときに指定した名前と同じである必要がありますが、プライマリ **xconnect** コマンドで使用した名前とは異なる pw-class を **backup peer** コマンドで使用できます。
ステップ 7	**backupdelay***enable-delay*{*disable-delay* | **never**} 例： `Router(config-if-xconn)# backup delay 5 never`	プライマリ疑似回線の VC がダウンしてから、バックアップ疑似回線の VC に引き継ぐまでの待ち時間（秒単位）を指定します。範囲は 0 ～ 180 です。 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の VC を引き継ぐまでの待ち時間を指定します。指定できる範囲は 0 ～ 180 秒です。**never** キーワードを指定した場合、プライマリ疑似回線の VC はバックアップを引き継ぎません。

L2VPN プロトコルベース CLI 機能に関連するコマンドを使用した L2VPN 疑似回線冗長性の設定

L2VPN 疑似回線冗長性機能を設定するには、次の作業を実行します。

はじめる前に

l2vpn xconnect context コマンドの設定方法は、転送タイプごとに若干異なります。次の設定手順では、サブインターフェイス コンフィギュレーション モードで設定する Ethernet VLAN over MPLS

を使用しています。ほかの転送タイプに対して **l2vpn xconnect context** コマンドを設定する方法については、「*Any Transport over MPLS*」を参照してください。

手順の概要

1. **enable**
2. **configureterminal**
3. **interfacegigabitethernet***slot*/*subslot*/*interface*.*subinterface*
4. **encapsulationdot1q***vlan-id*
5. **end**
6. **interfacepseudowire***number*
7. **sourcetemplate type pseudowire***template-name*
8. **neighbor***peer-address vcid-value*
9. **exit**
10. **l2vpn xconnectcontext***context-name*
11. **member pseudowire***interface-number*
12. **member pseudowire***interface-number*
13. **member gigabitethernet***interface-number*
14. **redundancydelay***enable-delay*{*disable-delay* | **never**}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interfacegigabitethernet***slot*/*subslot*/*interface*.*subinterface* 例： `Device(config)# interface gigabitethernet0/0/0.1`	ギガビット イーサネット サブインターフェイスを指定し、サブインターフェイス コンフィギュレーション モードを開始します。 隣接 CE ルータのサブインターフェイスがこの PE ルータと同じ VLAN 上にあることを確認します。

	コマンドまたはアクション	目的
ステップ 4	**encapsulationdot1q***vlan-id* 例： `Device(config-subif)# encapsulation dot1q 100`	サブインターフェイスでの 802.1Q VLAN パケットの受信をイネーブルにします。 Ethernet over MPLS が稼働している CE ルータと PE ルータ間のサブインターフェイスは、同じサブネット内になければなりません。その他すべてのサブインターフェイスとバックボーン ルータは、同じサブネット上にある必要はありません。
ステップ 5	**end** 例： `Router(config-subif)# end`	特権 EXEC モードに戻ります。
ステップ 6	**interfacepseudowire***number* 例： `Router(config)# interface pseudowire 100`	疑似回線インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	**sourcetemplate type pseudowire***template-name* 例： `Router(config-if)# source template type pseudowire atom`	atom という名前の疑似回線タイプのソース テンプレートを設定します。
ステップ 8	**neighbor***peer-address vcid-value* 例： `Router(config-if)#  neighbor 10.0.0.1 123`	レイヤ 2 VPN（L2VPN）疑似回線のピア IP アドレスと仮想回線（VC）ID を指定します。
ステップ 9	**exit** 例： `Router(config-if)# exit`	特権 EXEC モードに戻ります。
ステップ 10	**l2vpn xconnectcontext***context-name* 例： `Router(config)# l2vpn xconnect context con1`	レイヤ 2 VPN（L2VPN）クロス コネクト コンテキストを作成して、xconnect コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 11	**member pseudowire***interface-number* 例： `Device(config-xconnect)# member pseudowire 100 group GR_1 priority 2`	レイヤ 2 VPN （L2VPN）クロス コネクトを形成するメンバー疑似回線を指定します。
ステップ 12	**member pseudowire***interface-number* 例： `Device(config-xconnect)# member pseudowire 1001 group GR_1 priority 2`	冗長性のために 2 番目のメンバー疑似回線を指定します。
ステップ 13	**member gigabitethernet***interface-number* 例： `Device(config-xconnect)# member GigabitEthernet0/0/0.1 service instance 1`	ギガビット イーサネット メンバー インターフェイスの場所を指定します。
ステップ 14	**redundancydelay***enable-delay*{*disable-delay* | **never**} 例： `Device(config-xconnect)# redundancy delay 0 0 group GR_1`	プライマリ疑似回線の VC がダウンしてから、バックアップ疑似回線の VC に引き継ぐまでの待ち時間（秒単位）を指定します。値の範囲は 0 ～ 180 です。 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の VC を引き継ぐまでの待ち時間を指定します。値の範囲は 0 ～ 180 秒です。**never キーワード**を指定した場合、プライマリ疑似回線の VC はバックアップを引き継ぎません。

バックアップ疑似回線の VC への強制的な手動切り替え

バックアップまたはプライマリ疑似回線にルータを強制的に切り替えるには、特権 EXEC モードで **xconnect backup force switchover** コマンドを入力します。切り替え先のプライマリ接続回線（AC）のインターフェイスか、ピア ルータの IP アドレスと VC ID を指定できます。

手動切り替えができるのは、コマンドで指定するインターフェイスまたはピアが実際に使用できる場合であり、コマンドを実行すると、xconnect は完全にアクティブな状態に移行します。

手順の概要

1. **enable**
2. **xconnectbackupforce-switchover{interface***interface-info*| **peer** *ip-address vcid}*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**xconnectbackupforce-switchover{interface***interface-info*| **peer** *ip-address vcid}* 例： `Router# xconnect backup force-switchover peer 10.10.10.1 123`	ルータをバックアップ疑似回線またはプライマリ疑似回線に切り替えることを指定します。

L2VPN 疑似回線冗長性設定の確認

L2VPN 疑似回線冗長性機能が正しく設定されていることを確認するには、次の作業を実行します。

手順の概要

1. **showmplsl2transportvc**
2. **showxconnectall**
3. **xconnectloggingredundancy**

手順の詳細

ステップ 1 **showmplsl2transportvc**

次に、**show mpls l2transport vc** コマンドの出力例を示します。この例で、プライマリ接続回線はアップです。バックアップ接続回線は使用可能ですが、現在選択されていません。

例：

```
Router# show mpls l2transport vc
Local intf     Local circuit          Dest address    VC ID      Status
```

```
-------------  ----------------------- --------------- ---------- ----------
Et0/0.1        Eth VLAN 101            10.0.0.2        101        UP
Et0/0.1        Eth VLAN 101            10.0.0.3        201        DOWN
Router# show mpls l2transport vc detail
Local interface: Et0/0.1 up, line protocol up, Eth VLAN 101 up
   Destination address 10.0.0.2 VC ID: 101, VC status UP
   .
   .
   .
Local interface: Et0/0.1 down, line protocol down, Eth VLAN 101 down
   Destination address 10.0.0.3 VC ID: 201, VC status down
   .
   .
   .
```

ステップ 2 **showxconnectall**

この例で、トポロジは接続回線 1 から疑似回線 1 であり、疑似回線 2 がバックアップとして使用されています。

例：

```
Router# show xconnect all
Legend: XC ST=Xconnect State, S1=Segment1 State, S2=Segment2 State
UP=Up, DN=Down, AD=Admin Down, IA=Inactive, NH=No Hardware
XC ST  Segment 1                         S1 Segment 2                          S2
------+---------------------------------+--+---------------------------------+--
UP pri ac   Et0/0(Ethernet)              UP mpls 10.55.55.2:1000               UP
IA sec ac   Et0/0(Ethernet)              UP mpls 10.55.55.3:1001               DN
```

この例で、トポロジは接続回線 1 から接続回線 2 であり、疑似回線が接続回線 2 のバックアップとして使用されています。

例：

```
Router# show xconnect all
Legend: XC ST=Xconnect State, S1=Segment1 State, S2=Segment2 State
UP=Up, DN=Down, AD=Admin Down, IA=Inactive, NH=No Hardware
XC ST  Segment 1                         S1 Segment 2                          S2
------+---------------------------------+--+---------------------------------+--
UP pri ac   Se6/0:150(FR DLCI)           UP ac   Se8/0:150(FR DLCI)            UP
IA sec ac   Se6/0:150(FR DLCI)           UP mpls 10.55.55.3:7151               DN
```

ステップ 3 **xconnectloggingredundancy**

show mpls l2transport vc コマンドと **show xconnect** コマンドに加え、**xconnect logging redundancy** コマンドを使用して、xconnect 冗長性グループのステータスを追跡できます。

例：

```
Router(config)# xconnect logging redundancy
```

このコマンドを設定すると、切り替えが発生したときに次のメッセージが表示されます。

プライマリ メンバーをアクティブ化する場合

例：

```
00:01:07: %XCONNECT-5-REDUNDANCY: Activating primary member 10.55.55.2:1000
```

バックアップ メンバーをアクティブ化する場合

例：

```
00:01:05: %XCONNECT-5-REDUNDANCY: Activating secondary member 10.55.55.3:1001
```

L2VPN プロトコルベース CLI 機能に関連するコマンドを使用した L2VPN 疑似回線冗長性設定の確認

L2VPN 疑似回線冗長性機能が正しく設定されていることを確認するには、次のコマンドを使用します。

手順の概要

1. **showl2vpnatomvc**
2. **showl2vpnservice all**
3. **loggingredundancy**
4. **loggingpseudowire status**

手順の詳細

ステップ 1 **showl2vpnatomvc**

この例で、プライマリ接続回線はアップです。バックアップ接続回線は使用可能ですが、現在選択されていません。**show** の出力は次のように表示されます。

例：

```
Device# show l2vpn atom vc
Local intf     Local circuit           Dest address    VC ID      Status
-------------  ----------------------- --------------- ---------- ----------
Et0/0.1        Eth VLAN 101            10.0.0.2        101        UP
Et0/0.1        Eth VLAN 101            10.0.0.3        201        DOWN
Router# show l2vpn atom vc detail
Local interface: Et0/0.1 up, line protocol up, Eth VLAN 101 up
   Destination address 10.0.0.2 VC ID: 101, VC status UP
   .
   .
   .
Local interface: Et0/0.1 down, line protocol down, Eth VLAN 101 down
   Destination address 10.0.0.3 VC ID: 201, VC status down
   .
   .
   .
```

ステップ 2 **showl2vpnservice all**

この例で、トポロジは接続回線 1 から疑似回線 1 であり、疑似回線 2 がバックアップとして使用されています。

例：

```
Device# show l2vpn service all
Legend: St=State    XC St=State in the L2VPN Service      Prio=Priority
        UP=Up       DN=Down             AD=Admin Down     IA=Inactive
        SB=Standby  HS=Hot Standby      RV=Recovering     NH=No Hardware
        m=manually selected

  Interface          Group       Encapsulation                  Prio  St  XC St
  ---------          -----       -------------                  ----  --  -----
VPWS name: foo, State: UP
  Eth1/1.1                       Eth1/1.1:100(Eth VLAN)         0     UP  UP
  pw101              blue        102.1.1.1:100(MPLS)            2     UP  UP
  pw102              blue        103.1.1.1:100(MPLS)            5     SB  IA
  pw103              blue        104.1.1.1:100(MPLS)            8     SB  IA
  pw104              blue        105.1.1.1:100(MPLS)            11    SB  IA
```

この例で、トポロジは接続回線 1 から接続回線 2 であり、疑似回線が接続回線 2 のバックアップとして使用されています。

例：

```
Device# show l2vpn service all
Legend: XC ST=Xconnect State, S1=Segment1 State, S2=Segment2 State
UP=Up, DN=Down, AD=Admin Down, IA=Inactive, NH=No Hardware
XC ST  Segment 1                       S1 Segment 2                       S2
------+--------------------------------+--+--------------------------------+--
UP pri ac   Se6/0:150(FR DLCI)         UP ac   Se8/0:150(FR DLCI)         UP
IA sec ac   Se6/0:150(FR DLCI)         UP mpls 10.55.55.3:7151            DN
```

ステップ 3 **loggingredundancy**

show l2vpn atom vc コマンドと **show l2vpn service** コマンドに加え、**logging redundancy** コマンドを使用して、xconnect 冗長性ステータス イベントのシステム メッセージ ログ（syslog）レポート機能をイネーブルにできます。

例：

```
Device(config)# l2vpn
Device(config-l2vpn)# logging redundancy
```

このコマンドを設定すると、切り替えが発生したときに次のメッセージが生成されます。

プライマリ メンバーをアクティブ化する場合

例：

```
Device(config)# l2vpn
Device(config-l2vpn)# logging pseudowire status
```

このコマンドを設定すると、疑似回線のステータスをモニタできるように設定されます。

プライマリ メンバーをアクティブ化する場合

例：

```
00:01:07: %XCONNECT-5-REDUNDANCY: Activating primary member 10.55.55.2:1000
```

バックアップ メンバーをアクティブ化する場合

例：

```
00:01:05: %XCONNECT-5-REDUNDANCY: Activating secondary member 10.55.55.3:1001
```

ステップ 4 **loggingpseudowire status**
logging pseudowire status コマンドを使用して、疑似回線のステータスをモニタできます。

例：

```
Device(config)# l2vpn
Device(config-l2vpn)# logging pseudowire status
```

L2VPN 疑似回線冗長性の設定例

各設定例は、次の疑似回線クラスのいずれかを参照しています。

- AToM（like-to-like）疑似回線クラス

```
pseudowire-class mpls
 encapsulation mpls
```

- L2VPN IP インターワーキング

```
pseudowire-class mpls-ip
 encapsulation mpls
 interworking ip
```

例：L2VPN 疑似回線冗長性と AToM（like-to-like）

次の例は、バックアップ疑似回線を使用したハイレベル データリンク コントロール（HDLC）接続回線 xconnect を示します。

```
interface Serial4/0
 xconnect 10.55.55.2 4000 pw-class mpls
 backup peer 10.55.55.3 4001 pw-class mpls
```

次の例は、バックアップ疑似回線を使用したフレームリレー接続回線 xconnect を示します。

```
connect fr-fr-pw Serial6/0 225 l2transport
 xconnect 10.55.55.2 5225 pw-class mpls
 backup peer 10.55.55.3 5226 pw-class mpls
```

例：L2VPN 疑似回線冗長性と L2VPN インターワーキング

次の例は、L2VPN IPインターワーキングとバックアップ疑似回線を使用したイーサネット接続回線 xconnect を示します。

```
interface Ethernet0/0
 xconnect 10.55.55.2 1000 pw-class mpls-ip
 backup peer 10.55.55.3 1001 pw-class mpls-ip
```

次の例は、L2VPN IPインターワーキングとバックアップ疑似回線を使用したイーサネットVirtual LAN（VLAN）接続回線 xconnect を示します。

```
interface Ethernet1/0.1
 encapsulation dot1Q 200
 no ip directed-broadcast
 xconnect 10.55.55.2 5200 pw-class mpls-ip
 backup peer 10.55.55.3 5201 pw-class mpls-ip
```

次の例は、L2VPN IPインターワーキングとバックアップ疑似回線を使用したフレームリレー接続回線 xconnect を示します。

```
connect fr-ppp-pw Serial6/0 250 l2transport
 xconnect 10.55.55.2 8250 pw-class mpls-ip
 backup peer 10.55.55.3 8251 pw-class mpls-ip
```

次の例は、L2VPN IPインターワーキングとバックアップ疑似回線を使用したPPP接続回線xconnectを示します。

```
interface Serial7/0
 encapsulation ppp
 xconnect 10.55.55.2 2175 pw-class mpls-ip
 backup peer 10.55.55.3 2176 pw-class mpls-ip
```

例：レイヤ2ローカルスイッチングを使用したL2VPN疑似回線冗長性

次の例は、イーサネットセグメントE2/0.2に対する疑似回線バックアップを使用したイーサネットVLAN-VLANローカルスイッチングxconnectを示します。E2/0.2に関連付けられているサブインターフェイスがダウンすると、バックアップ疑似回線がアクティブ化されます。

```
connect vlan-vlan Ethernet1/0.2 Ethernet2/0.2
 backup peer 10.55.55.3 1101 pw-class mpls
```

次の例は、フレームリレー セグメント S8/0 150 に対する疑似回線バックアップを使用した、フレームリレー相互間ローカル スイッチング接続を示します。S8/0 上のデータリンク接続識別子（DLCI）150 がダウンした場合、バックアップ疑似回線がアクティブ化されます。

```
connect fr-fr-ls Serial6/0 150 Serial8/0 150
 backup peer 10.55.55.3 7151 pw-class mpls
```

例：L2VPN 疑似回線冗長性とレイヤ 2 トンネリング プロトコル バージョン 3

次に、xconnect セッションのバックアップ ピアを設定する例を示します。

```
pseudowire-class 773
 encapsulation l2tpv3
 ip local interface GigabitEthernet0/0/0.773
!
pseudowire-class 774
 encapsulation l2tpv3
 ip local interface GigabitEthernet0/0/1.774
!
interface GigabitEthernet0/0/0.780
 encapsulation dot1Q 780
 xconnect 10.22.73.14 100 pw-class 773
  backup peer 10.22.74.14 101 pw-class 774
  backup delay 0 0
```

次に、L2VPN 疑似回線冗長性および L2TPv3 を使用してギガビット イーサネット ポートを設定する例を示します。

```
interface GigabitEthernet0/0/2
 xconnect 10.22.70.83 50 pw-class pe1-pw-primary
 backup peer 20.22.70.85 51 pw-class pe1-pw-secondary
```

次に、L2VPN 疑似回線冗長性および L2TPv3 を使用してギガビット イーサネット VLAN を設定する例を示します。

```
interface GigabitEthernet0/0/0.100
 encapsulation dot1q 100
 xconnect 10.22.70.83 60 pw-class pe1-pw-primary
 backup peer 10.22.70.85 61 pw-class pe1-pw-secondary
```

次に、L2VPN 疑似回線冗長性および L2TPv3 を使用してギガビット イーサネット Q-in-Q を設定する例を示します。

```
interface GigabitEthernet0/0/0.200
 encapsulation dot1q 200 second-dot1q 400
 xconnect 10.22.70.83 70 pw-class pe1-pw-primary
 backup peer 10.22.70.85 71 pw-class pe1-pw-secondary
```

次に、L2VPN 疑似回線冗長性および L2TPv3 を使用してギガビット イーサネット Q-in-any を設定する例を示します。

```
interface GigabitEthernet0/0/0.300
 encapsulation dot1q 300 second-dot1q any
 xconnect 10.22.70.83 80 pw-class pe1-pw-primary
 backup peer 10.22.70.85 81 pw-class pe1-pw-secondary
```

次に、L2VPN 疑似回線冗長性および L2TPv3 を使用して HDLC を設定する例を示します。

```
interface Serial0/2/0:0
 no ip address
 xconnect 10.22.71.83 40 pw-class pe1-pw-hdlc
 backup peer 10.22.70.85 41 pw-class pe1-pw-hdlc-2
```

L2VPN プロトコルベース CLI 機能に関連するコマンドを使用した L2VPN 疑似回線冗長性の設定例

各設定例は、次のインターフェイス疑似回線のいずれかを参照しています。

- AToM（like-to-like）インターフェイス疑似回線：

```
interface pseudowire 1
 encapsulation mpls
 neighbor 33.33.33.33 1
```

- L2VPN IP インターワーキング

```
interface pseudowire 1
 encapsulation mpls
 neighbor 33.33.33.33 1
 interworking ip
```

例：L2VPN プロトコルベース CLI 機能に関連するコマンドを使用した L2VPN 疑似回線冗長性と AToM（Like to Like）

次の例は、バックアップ疑似回線を使用したハイレベル データリンク コントロール（HDLC）接続回線 xconnect を示します。

```
interface Serial4/0
 interface pseudowire 100
 source template type pseudowire ether-pw
 neighbor 10.55.55.3 4001
!
l2vpn xconnect context con1
 member pseudowire 100 group GR_1 priority 1
 member pseudowire 1001 group GR_1 priority 2
 member GigabitEthernet0/0/2 service-instance 1
 redundancy delay 0 0 group GR_1
```

次の例は、バックアップ疑似回線を使用したフレームリレー接続回線 xconnect を示します。

```
connect fr-fr-pw Serial6/0 225 l2transport
interface pseudowire 100
 source template type pseudowire ether-pw
 neighbor 10.55.55.3 5226
!
l2vpn xconnect context con1
 member pseudowire 100 group GR_1 priority 1
 member pseudowire 1001 group GR_1 priority 2
 member GigabitEthernet0/0/2 service-instance 1
 redundancy delay 0 0 group GR_1
```

例：L2VPN プロトコルベース CLI 機能に関連するコマンドを使用した L2VPN 疑似回線冗長性と L2VPN インターワーキング

次の例は、L2VPN IP インターワーキングとバックアップ疑似回線を使用したイーサネット接続回線 xconnect を示します。

```
interface Ethernet0/0
interface pseudowire 100
 source template type pseudowire ether-pw
!
l2vpn xconnect context con1
 member pseudowrire 100 group GR_1 priority 1
 member pseudowire 1001 group GR_1 priority 2
 member GigabitEthernet0/0/2 service-instance 1
 redundancy delay 0 0 group GR_1
 interworking ip
```

次の例は、L2VPN IP インターワーキングとバックアップ疑似回線を使用したイーサネット Virtual LAN（VLAN）接続回線 xconnect を示します。

```
interface Ethernet1/0.1
 encapsulation dot1Q 200
 no ip directed-broadcast
 interface pseudowire 100
 source template type pseudowire ether-pw
!
l2vpn xconnect context con1
 member pseudowrire 100 group GR_1 priority 1
 member pseudowire 1001 group GR_1 priority 2
 member GigabitEthernet0/0/2 service-instance 1
 redundancy delay 0 0 group GR_1
 interworking ip
```

次の例は、L2VPN IP インターワーキングとバックアップ疑似回線を使用したフレームリレー接続回線 xconnect を示します。

```
connect fr-ppp-pw Serial6/0 250 l2transport
 interface pseudowire 100
 source template type pseudowire ether-pw
!
l2vpn xconnect context con1
 member pseudowrire 100 group GR_1 priority 1
 member pseudowire 1001 group GR_1 priority 2
 member GigabitEthernet0/0/2 service-instance 1
 redundancy delay 0 0 group GR_1
 interworking ip
```

次の例は、L2VPN IP インターワーキングとバックアップ疑似回線を使用した PPP 接続回線 xconnect を示します。

```
interface Serial7/0
 encapsulation ppp
 interface pseudowire 100
 source template type pseudowire ether-pw
!
l2vpn xconnect context con1
 member pseudowire 100 group GR_1 priority 1
 member pseudowire 1001 group GR_1 priority 2
 member GigabitEthernet0/0/2 service-instance 1
 redundancy delay 0 0 group GR_1
 interworking ip
```

例：L2VPN プロトコルベース CLI 機能に関連するコマンドを使用した L2VPN 疑似回線冗長性とレイヤ2 トンネリング プロトコル バージョン 3

次に、xconnect セッションのバックアップ ピアを設定する例を示します。

```
interface pseudowire 773
 encapsulation l2tpv3
 ip local interface GigabitEthernet0/0/0.773
!
interface pseudowire 774
 encapsulation l2tpv3
 ip local interface GigabitEthernet0/0/1.774
!
interface GigabitEthernet0/0/0.780
 encapsulation dot1Q 780
 interface pseudowire 100
 source template type pseudowire ether-pw
 neighbor 10.22.73.14 100
!
l2vpn xconnect context con1
 member pseudowire 100 group GR_1 priority 1
 member pseudowire 1001 group GR_1 priority 2
 member GigabitEthernet0/0/2 service-instance 1
 redundancy delay 0 0 group GR_1
 interworking ip
```

次に、L2VPN 疑似回線冗長性および L2TPv3 を使用してギガビット イーサネット ポートを設定する例を示します。

```
interface GigabitEthernet0/0/2
 interface pseudowire 100
 source template type pseudowire ether-pw
 neighbor 10.22.70.83 50
!
l2vpn xconnect context con1
 member pseudowire 100 group GR_1 priority 1
 member pseudowire 1001 group GR_1 priority 2
 member GigabitEthernet0/0/2 service-instance 1
 redundancy delay 0 0 group GR_1
 interworking ip
```

次に、L2VPN 疑似回線冗長性および L2TPv3 を使用してギガビット イーサネット VLAN を設定する例を示します。

```
interface GigabitEthernet0/0/0.100
 encapsulation dot1q 100
 interface pseudowire 100
 source template type pseudowire ether-pw
 neighbor 10.22.70.83 60
!
l2vpn xconnect context con1
 member pseudowire 100 group GR_1 priority 1
 member pseudowire 1001 group GR_1 priority 2
 member GigabitEthernet0/0/2 service-instance 1
 redundancy delay 0 0 group GR_1
 interworking ip
```

次に、L2VPN 疑似回線冗長性および L2TPv3 を使用してギガビット イーサネット Q-in-Q を設定する例を示します。

```
interface GigabitEthernet0/0/0.200
 encapsulation dot1q 200 second-dot1q 400
```

```
 interface pseudowire 100
 source template type pseudowire ether-pw
 neighbor 10.22.70.83 70
!
l2vpn xconnect context con1
 member pseudowire 100 group GR_1 priority 1
 member pseudowire 1001 group GR_1 priority 2
 member GigabitEthernet0/0/2 service-instance 1
 redundancy delay 0 0 group GR_1
 interworking ip
```

次に、L2VPN 疑似回線冗長性および L2TPv3 を使用してギガビット イーサネット Q-in-any を設定する例を示します。

```
interface GigabitEthernet0/0/0.300
 encapsulation dot1q 300 second-dot1q any
 interface pseudowire 100
 source template type pseudowire ether-pw
 neighbor 10.22.70.83 80
!
l2vpn xconnect context con1
 member pseudowire 100 group GR_1 priority 1
 member pseudowire 1001 group GR_1 priority 2
 member GigabitEthernet0/0/2 service-instance 1
 redundancy delay 0 0 group GR_1
 interworking ip
```

次に、L2VPN 疑似回線冗長性および L2TPv3 を使用して HDLC を設定する例を示します。

```
interface Serial0/2/0:0
 no ip address
 interface pseudowire 100
 source template type pseudowire ether-pw
 neighbor 10.22.71.83 40
!
l2vpn xconnect context con1
 l2vpn xconnect context con1
 member pseudowire 100 group GR_1 priority 1
 member pseudowire 1001 group GR_1 priority 2
 member GigabitEthernet0/0/2 service-instance 1
 redundancy delay 0 0 group GR_1
 interworking ip
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
ワイドエリア ネットワーキング コマンド	『*Cisco IOS Wide-Area Networking Command Reference*』
Cisco IOS XE マルチプロトコル ラベル スイッチングの設定作業	『*Cisco IOS XE Multiprotocol Label Switching Configuration Guide*』
Cisco IOS XE ワイドエリア ネットワーキングの設定作業	『*Cisco IOS XE Wide-Area Networking Configuration Guide*』

標準

標準	タイトル
なし	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
なし	--

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

L2VPN 疑似回線冗長性の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを

示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *4*：*L2VPN* 疑似回線冗長性の機能情報

機能名	リリース	機能情報
L2VPN 疑似回線冗長化	XE 2.3 XE 3.3S	この機能を使用すると、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。 Cisco IOS XE Release 2.3 では、この機能は Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに統合されました。 Cisco IOS XE Release 3.3S では、この機能はレイヤ 2 トンネリング プロトコル バージョン 3（L2TPv3）をサポートしています。 **backupdelay（L2VPN ローカル スイッチング）**、**backuppeer**、**showxconnect**、**xconnectbackupforce-switchover**、**xconnectloggingredundancy** の各コマンドが追加または変更されています。

第 5 章

レイヤ 2 ローカル スイッチング

レイヤ 2 ローカル スイッチング機能を使用すると、次の 2 つの方法でレイヤ 2 データをスイッチングできます。

- 同じルータ上の 2 つのインターフェイス間
- 同じインターフェイス ポート上の 2 つの回線間（同一ポート スイッチングと呼びます）

この機能では、次のインターフェイス間スイッチングの組み合わせがサポートされています。

- ATM と ATM の間
- ATM とイーサネットの間
- イーサネット/イーサネット VLAN とイーサネット/イーサネット VLAN 間
- フレームリレーとフレームリレーの間

次の同一ポート スイッチング機能がサポートされています。

- ATM 相手先固定接続（PVC）および相手先固定パス（PVP）
- イーサネット VLAN
- フレーム リレー

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、Bug Search Tool およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

レイヤ 2 ローカル スイッチングの前提条件

Cisco ASR 1000 シリーズ Aggregation Services Router のシスコ エクスプレス フォワーディングをイネーブルにする必要があります。

レイヤ 2 ローカル スイッチングの制限事項

- イーサネット/イーサネット VLAN 回線では、Cisco ASR 1000 シリーズ Aggregation Services Router にイーサネット アダプタが必要です。
- フレーム リレー ローカル スイッチングの場合、**frame-relay switching** コマンドをグローバルに実行する必要があります。

レイヤ 2 ローカル スイッチングに関する情報

レイヤ 2 ローカル スイッチングの概要

ローカル スイッチングを使用すると、同じルータ上の種類が同じ 2 つのインターフェイスの間（たとえば、イーサネットとイーサネットの間、フレームリレーとフレームリレーの間）か、種類の異なるインターフェイスの間（たとえば、イーサネット VLAN とイーサネット VLAN の間、イーサネットとイーサネット VLAN の間）で、レイヤ 2 データをスイッチングできます。インターフェイスは、同じラインカード上にあっても2つの異なるカード上にあってもかまいません。スイッチングの際には、レイヤ 3 アドレスではなくレイヤ 2 アドレスが使用されます。

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。

NSF SSO：ローカル スイッチングの概要

ノンストップ フォワーディング（NSF）およびステートフル スイッチオーバー（SSO）では、冗長ルート プロセッサとデータのチェックポイントを使用して、プライマリ ルート プロセッサが停止した場合のパケット損失を最小限に抑えることで、ネットワークの可用性が向上します。NSF/SSO のサポートは、次のローカルにスイッチングされる接続回線で使用できます。

- イーサネット/イーサネット VLAN とイーサネット/イーサネット VLAN 間
- フレームリレーとフレームリレーの間

レイヤ 2 ローカル スイッチングの用途

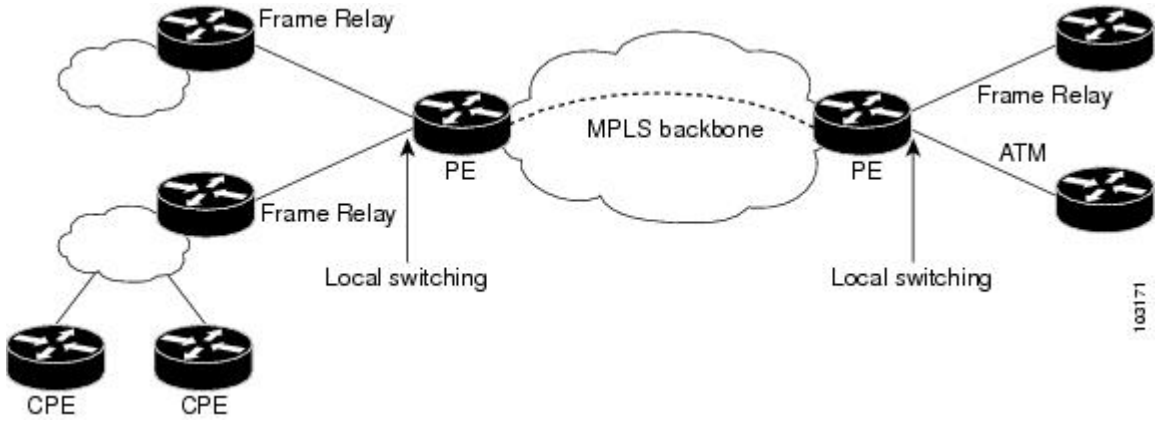
長距離通信事業者（IXC）を利用して 2 つの地域通信事業者間のトラフィックを伝送している既存地域通信事業者（ILEC）は、レイヤ 2 ローカル スイッチング機能を使用できます。電気通信規制では、トラフィックを伝送するための IXC の費用を ILEC が支払うことになっています。場合によって、ILEC は異なるローカル アクセスおよびトランスポート エリア（LATA）にあるカスタマー接続を終端できないことがあります。また、カスタマー接続が、同じルータ上にある同じ LATA で終端する場合もあります。

たとえば、企業 A に、国内全体にわたる 50 を超える LATA があり、各 LATA で 3 台のルータを使用しているとします。企業 A は、地域通信事業者間でトラフィックを伝送するために、企業 B と C を利用しています。この場合、同じルータ上でレイヤ 2 フレームのローカル スイッチングが必要になることがあります。

同様に、ルータがたとえばチャネライズド インターフェイスをしている場合、受信および送信トラフィックを、1 つの物理ポートに存在する 2 つの論理インターフェイス上でスイッチングすることが必要になる場合があります。同一ポート ローカル スイッチング機能は、そのような実装に対応しています。

下の図に、フレーム リレーとフレーム リレーの間、および ATM とフレーム リレーの間のローカル スイッチングを使用するネットワークを示します。

図 *9*：ローカル スイッチングの例



レイヤ 2 ローカル スイッチングの設定方法

イーサネット VLAN の同一ポート スイッチングの設定

イーサネット VLAN の同一ポート 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. **enable**
2. **configureterminal**
3. **interfacefastethernet***slot*/*port*.*subinterface-number*
4. **encapsulationdot1q***vlan-id*
5. **exit**
6. **interfacefastethernet***slot*/*port*.*subinterface-number*
7. **encapsulationdot1q***vlan-id*
8. **exit**
9. **connect***connection-nametypenumbertypenumber*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interfacefastethernet***slot*/*port*.*subinterface-number* 例： `Router(config)# interface fastethernet6/0.1`	1 つ目のファストイーサネットラインカード、サブスロット（使用可能な場合）、ポート、およびサブインターフェイスを指定し、サブインターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**encapsulationdot1q***vlan-id* 例： `Router(config-subif)# encapsulation dot1q 10`	802.1Q VLAN パケットを受信できるようサブインターフェイスをイネーブルにし、最初の VLAN を指定します。
ステップ 5	**exit** 例： `Router(config-subif)# exit`	サブインターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**interfacefastethernet***slot*/*port*.*subinterface-number* 例： `Router(config)# interface fastethernet6/0.2`	2 番目のファストイーサネットラインカード、サブスロット（使用可能な場合）、ポート、およびサブインターフェイスを指定し、サブインターフェイス コンフィギュレーション モードを開始します。
ステップ 7	**encapsulationdot1q***vlan-id* 例： `Router(config-subif)# encapsulation dot1q 20`	802.1Q VLAN パケットを受信できるようサブインターフェイスをイネーブルにし、2 番目の VLAN を指定します。
ステップ 8	**exit** 例： `Router(config-subif)# exit`	サブインターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 9	**connect***connection-nametypenumbertypenumber* 例： `Router(config)# connect conn fastethernet 6/0.1 fastethernet 6/0.2`	同じファスト イーサネット ポート上の 2 つのサブインターフェイス（つまりここでは先に指定したVLAN）間にローカル接続を作成します。

イーサネット ポート モードとイーサネット VLAN の間のローカル スイッチングの設定

イーサネット（ポート モード）とイーサネット VLAN の間のローカル 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. **enable**
2. **configureterminal**
3. **interfacefastethernet***slot*/*subslot*/*port*
4. **interfacefastethernet***slot*/*port*/*subinterface-number*
5. **encapsulationdot1q***vlan-id*
6. **exit**
7. **connect***connection-nametypenumbertypenumber*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**interfacefastethernet***slot*/*subslot*/*port* 例： `Router(config)# interface fastethernet3/0/0`	ファスト イーサネット ラインカード、サブスロット（使用可能な場合）、およびポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 • これは、PEルータの一方の側にある、カスタマーエッジ（CE）ルータとの間でイーサネットパケットをやり取りするインターフェイスです。
ステップ 4	**interfacefastethernet***slot*/*port*/*subinterface-number* 例： `Router(config-if)# interface fastethernet6/0/0.1`	ファスト イーサネット ラインカード、サブスロット（使用可能な場合）、ポート、およびサブインターフェイスを指定し、サブインターフェイス コンフィギュレーション モードを開始します。 • これは、PE ルータの他方の側にある、CE ルータとの間でイーサネットVLANパケットをやり取りするインターフェイスです。
ステップ 5	**encapsulationdot1q***vlan-id* 例： `Router(config-subif)# encapsulation dot1q 100`	802.1QVLANパケットを受け付けるようにインターフェイスをイネーブルにします。
ステップ 6	**exit** 例： `Router(config-subif)# exit`	サブインターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**connect***connection-nametypenumbertypenumber* 例： `Router(config)# connect eth-ethvlan-con fastethernet 3/0/0 fastethernet 6/0/0.1`	2つのインターフェイスの間にローカル接続を作成します。

ATM-to-ATM PVC ローカル スイッチングと同一ポート スイッチングの設定

カプセル化タイプ ATM AAL5 および ATM AAL0 に対してローカル スイッチングを設定できます。

ATM PVC の作成は必須ではありません。PVC を作成しない場合、自動的に作成されます。ATM-to-ATM ローカル スイッチングでは、自動的にプロビジョニングされた PVC にデフォルトのカプセル化タイプ AAL0 のセル リレーが設定されます。

手順の概要

1. **enable**
2. **configureterminal**
3. **interfaceatm***slot*/*port*
4. **pvc***vpi*/*vci***l2transport**
5. **encapsulation***layer-type*
6. **exit**
7. **exit**
8. **connect***connection-nameinterfacepvcinterfacepvc*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interfaceatm***slot*/*port* 例： `Router(config)# interface atm1/0/0`	ATM ラインカード、サブスロット（使用可能な場合）、およびポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**pvc***vpi*/*vci***l2transport** 例： `Router(config-if)# pvc 1/100 l2transport`	VPI と VCI を割り当て、ATM PVC l2transport コンフィギュレーション モードを開始します。 • **l2transport** キーワードは、PVC が終端 PVC ではなくスイッチド PVC であることを示します。
ステップ 5	**encapsulation***layer-type* 例： `Router(cfg-if-atm-l2trans-pvc)# encapsulation aal5`	ATM PVC のカプセル化タイプを指定します。AAL0 と AAL5 がサポートされています。 • 同じルータ上の別の ATM PVC に対して手順 3 ～ 5 を繰り返します。

	コマンドまたはアクション	目的
ステップ 6	**exit** 例： `Router(cfg-if-atm-l2trans-pvc)# exit`	PVC l2transport コンフィギュレーション モードを終了し、インターフェイス コンフィギュレーション モードに戻ります。
ステップ 7	**exit** 例： `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 8	**connect***connection-name interface pvc interface pvc* 例： `Router(config)# connect atm-con atm1/0/0 1/100 atm2/0/0 1/100`	指定した 2 つの相手先固定接続の間にローカル接続を作成します。

ATM-to-ATM PVP ローカル スイッチングの設定

ATM-to-ATM PVP 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。

Cisco IOS Release 12.0(30)S から、ATM PVP 同一ポート スイッチングの設定, （110 ページ）で説明する同一ポート スイッチングが使用できるようになりました。

手順の概要

1. **enable**
2. **configureterminal**
3. **interfaceatm***slot*/*port*
4. **atmpvp***vpi* **l2transport**
5. **exit**
6. **exit**
7. **connect***connection-name interface pvp interface pvp*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interfaceatm***slot*/*port* 例： `Router(config)# interface atm1/0`	ATM ラインカード、サブスロット（使用可能な場合）、およびポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**atmpvp***vpi***l2transport** 例： `Router(config-if)# atm pvp 100 l2transport`	仮想パスを指定し、PVP l2transport コンフィギュレーション モードを開始します。**l2transport** キーワードは、PVP が終端 PVP ではなくスイッチド PVP であることを示します。 • 同じルータ上の別の ATM 相手先固定パスに対して手順 3 と 4 を繰り返します。
ステップ 5	**exit** 例： `Router(config-if-atm-l2trans-pvp)# exit`	PVP l2transport コンフィギュレーション モードを終了し、インターフェイス コンフィギュレーション モードに戻ります。
ステップ 6	**exit** 例： `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**connect***connection-nameinterfacepvpinterfacepvp* 例： `Router(config)# connect atm-con atm1/0 100 atm2/0 200`	指定した 2 つの相手先固定パスの間にローカル接続を作成します。

ATM PVP 同一ポート スイッチングの設定

ATM インターフェイス上で ATM PVP 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. **enable**
2. **configureterminal**
3. **interfaceatm***slot*/*subslot*/*port*
4. **atmpvp***vpi***l2transport**
5. **exit**
6. **exit**
7. **connect***connection-name**interfacepvp**interfacepvp*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interfaceatm***slot*/*subslot*/*port* 例： `Router(config)# interface atm1/0/0`	ATM ラインカード、サブスロット（使用可能な場合）、およびポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**atmpvp***vpi***l2transport** 例： `Router(config-if)# atm pvp 100 l2transport`	1 つの VPI を指定し、PVP l2transport コンフィギュレーション モードを開始します。この同じポート上の他の ATM 相手先固定パスに対し、このステップを繰り返します。 • **l2transport** キーワードは、指定した PVP が終端 PVP ではなくスイッチド PVP であることを示します。
ステップ 5	**exit** 例： `Router(config-if-atm-l2trans-pvp)# exit`	PVP l2transport コンフィギュレーション モードを終了し、インターフェイス コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	**exit** 例： `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**connect***connection-nameinterfacepvpinterfacepvp* 例： `Router(config)# connect atm-con atm1/0/0 100 atm1/0/0 200`	グローバル コンフィギュレーション モードで、指定した 2 つの相手先固定パスの間にローカル接続を作成します。

フレーム リレーとフレーム リレーの間のローカル スイッチングの設定

フレーム リレーとフレーム リレーの間のローカル スイッチングについては、「Distributed Frame Relay Switching」機能モジュールを参照してください。

手順の概要

1. **enable**
2. **configureterminal**
3. **ipcefdistributed**
4. **frame-relayswitching**
5. **interface***typenumber*
6. **encapsulationframe-relay**[**cisco** | **ietf**]
7. **frame-relayinterface-dlci***dlci***switched**
8. **exit**
9. **exit**
10. **connect***connection-nameinterfacedlciinterfacedlci*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipcefdistributed** 例： `Router(config)# ip cef distributed`	シスコ エクスプレス フォワーディングをイネーブルにします。
ステップ 4	**frame-relayswitching** 例： `Router(config)# frame-relay switching`	フレームリレー DCE デバイスまたはネットワーク間インターフェイス（NNI）上で PVC スイッチングをイネーブルにします。
ステップ 5	**interface***typenumber* 例： `Router(config)# interface serial 0`	フレームリレーインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 6	**encapsulationframe-relay**[**cisco** | **ietf**] 例： `Router(config-if)# encapsulation frame-relay`	フレームリレー カプセル化をイネーブルにします。 • デフォルトのカプセル化は **cisco** です。 • カプセル化タイプを指定する必要はありません。
ステップ 7	**frame-relayinterface-dlci***dlci***switched** 例： `Router(config-if)# frame-relay interface-dlci 100 switched`	（任意）スイッチド PVC を作成し、フレームリレー DLCI コンフィギュレーション モードを開始します。 • スイッチド PVC ごとに、ステップ 5 ～ 7 を繰り返します。 • この手順でフレーム リレー PVC を作成しない場合、**connect** コマンドによって自動的に作成されます。
ステップ 8	**exit** 例： `Router(config-fr-dlci)# exit`	フレームリレー DLCI コンフィギュレーション モードを終了し、インターフェイス コンフィギュレーション モードに戻ります。
ステップ 9	**exit** 例： `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 10	**connect***connection-name interface dlci interface dlci* 例： `Router(config)# connect connection1 serial0 100 serial1 101`	フレームリレー PVC 間の接続を定義します。

レイヤ 2 ローカル スイッチングの確認

レイヤ 2 ローカル スイッチングの設定の確認

レイヤ2ローカル スイッチング機能の設定を確認するには、プロバイダーエッジ（PE）ルータで **show connection** コマンドを使用します。

手順の概要

1. **showconnection** [**all** | *element* | **id** *id* | **name** *name* | **port** *port*]

手順の詳細

showconnection [**all** | *element* | **id** *id* | **name** *name* | **port** *port*]
show connection コマンドは、ギガビット イーサネット インターフェイスとその他のローカル ギガビット イーサネット インターフェイス間のローカル接続を表示します。

例：

```
Router# show connection name ethconn1
Connection: 1 - ethconn1
 Current State: UP
 Segment 1: GigabitEthernet0/0/0.1 up
 Segment 2: GigabitEthernet0/0/0.2 up
```

NSF SSO ローカル スイッチングの設定の確認

レイヤ2ローカル スイッチングでは、同じルータ上の次の接続回線のローカル スイッチングに対し、NSF/SSO がサポートされています。

- イーサネット/イーサネット VLAN とイーサネット/イーサネット VLAN 間

ルート プロセッサでの NSF/SSO の設定については、『*Cisco IOS XE High Availability Configuration Guide*』の「Stateful Switchover」モジュールを参照してください。NSF/SSO：レイヤ 2 ローカル スイッチング機能が正しく動作していることを確認するには、次の作業を実行します。

手順の概要

1. **ping**
2. **redundancyforce-switchover**
3. **showconnectionall**
4. **ping**

手順の詳細

ステップ 1 **ping**
ping コマンドを実行するか、2 台の CE ルータ間でトラフィックを発生させます。

ステップ 2 **redundancyforce-switchover**
redundancyforce-switchover コマンドを使用して、アクティブ RP からスタンバイ RP に強制的に切り替えます。この手動の手順により、アクティブな RP の「通常の」制御されたシャットダウンが行われ、スタンバイ RP に切り替えられます。この通常シャットダウンにより、不可欠なクリーンアップが行われます。

ステップ 3 **showconnectionall**
showconnectionall コマンドを発行して、デュアル RP のレイヤ 2 ローカル スイッチング接続が動作していることを確認します。

例：

```
Router# show connection all
D   Name            Segment 1              Segment 2                   State
================================================================================
1    conn            Gi0/0/0.1              Gi0/0/0.2                   UP
```

ステップ 4 **ping**
CE ルータから **ping** コマンドを実行して、切り替えの際の連続的なパケット損失が最小限であることを確認します。

トラブルシューティングのヒント

レイヤ 2 ローカル スイッチングをトラブルシューティングするには、PE ルータで次のコマンドを使用します。

- **debugconn**
- **showconnection**

レイヤ 2 ローカル スイッチングの設定例

例：イーサネット VLAN の同一ポート スイッチングの設定

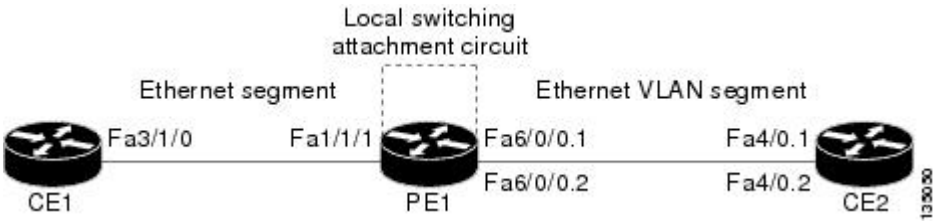
次に、1 つのイーサネット インターフェイス上の 2 つの VLAN 間での同一ポート スイッチングの例を示します。

```
interface fastethernet 0/0.1
 encapsulation dot1q 1
interface fastethernet 0/0.2
 encapsulation dot1q 2
connect conn FastEthernet 0/0.1 FastEthernet 0/0.2
```

例：NSF SSO：イーサネット ポート モードとイーサネット VLAN の間のローカル スイッチングの設定

次の設定は、下の図に示すネットワーク トポロジを使用しています。

図 *10*：*NSF/SSO*：レイヤ *2* ローカル スイッチング：イーサネット間 *VLAN*



次に、PE1 ルータに接続するための CE インターフェイスの設定例を示します。

CE1	CE2
ip routing ! interface fa3/1/0 description: connection to PE fa1/1/1 no shutdown ip address 10.1.1.1 255.255.255.0	ip routing ! interface fa4/0 no shutdown ! interface fa4/0.1 description: connection to PE1 fa6/0/0.1 encapsulation dot1Q 10 ip address 10.1.1.2 255.255.255.0 ! interface fa4/0.2 description - connection to PE1 fa6/0/0.2 encapsulation dot1Q 20 ip address 172.16.1.2 255.255.255.0

次に、CE ルータへの NSF/SSO および PE インターフェイスを持つ PE1 ルータの設定例を示します。

PE1

```
redundancy
 no keepalive-enable
 mode sso
!
!
ip routing
ip cef distributed
!
interface fa1/1/1
 description - connection to CE1 fa3/1/0
 no shutdown
 no ip address
!
!
interface fa6/0/0
 no shutdown
 no ip address
!
interface fa6/0/0.1
 description - connection to CE2 fa4/0.1
 encapsulation dot1Q 10
 no ip address
!
interface fa6/0/0.2
 description - connection to CE2 fa4/0.2
 encapsulation dot1Q 20
 no ip address
```

例：ATM-to-ATM ローカル スイッチングの設定

次に、AAL5 が設定された ATM インターフェイス上のローカル スイッチングの例を示します。

```
interface atm1/0/0
 pvc 0/100 l2transport
 encapsulation aal5
interface atm2/0/0
 pvc 0/100 l2transport
 encapsulation aal5
connect aal5-conn atm1/0/0 0/100 atm2/0/0 0/100
```

例：ATM PVC 同一ポート スイッチングの設定

次に、1 つの ATM インターフェイス上の 2 つの PVC 間での同一ポート スイッチングの例を示します。

```
interface atm1/0/0
 pvc 0/100 l2transport
 encapsulation aal5
 pvc 0/200 l2transport
 encapsulation aal5
connect conn atm1/0/0 0/100 atm1/0/0 0/200
```

例：ATM PVP 同一ポート スイッチングの設定

次に、1 つの ATM インターフェイス上の 2 つの PVP 間での同一ポート スイッチングの例を示します。

```
interface atm1/0/0
 atm pvp 100 l2transport
 atm pvp 200 l2transport
connect conn atm1/0/0 100 atm1/0/0 200
```

例：フレーム リレーとフレーム リレーの間のローカル スイッチングの設定

次に、フレームリレーが設定されたシリアル インターフェイスの例を示します。**connect** コマンドを使用すると、これら 2 つのインターフェイス間でローカル スイッチングが可能になります。

```
frame-relay switching
ip cef distributed
interface serial3/0/0
 encapsulation frame-relay
 frame-relay interface-dlci 100 switched
 frame-relay intf-type dce
interface serial3/1/0
 encapsulation frame-relay ietf
 frame-relay interface-dlci 200 switched
 frame-relay intf-type dce
connect fr-con serial3/0/0 100 serial3/1/0 200
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
WAN コマンド	『*Cisco IOS Wide-Area Networking Command Reference*』

関連項目	マニュアル タイトル
ステートフル スイッチオーバーの設定情報	『*Cisco IOS XE High Availability Configuration Guide*』の「Stateful Switchover」モジュール

標準

規格	タイトル
draft-ietf-l2tpext-l2tp-base-03.txt	『*LayerTwoTunnelingProtocol(Version3)'L2TPv3'*』
draft-martini-l2circuit-trans-mpls-09.txt	『*TransportofLayer2FramesOverMPLS*』
draft-martini-l2circuit-encap-mpls-04.txt	『*EncapsulationMethodsforTransportofLayer2FramesOverIPandMPLSNetworks*』
draft-ietf-ppvpn-l2vpn-00.txt	『*AnArchitectureforL2VPNs*』

MIB

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

RFC

RFC	タイトル
なし	--

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

レイヤ 2 ローカル スイッチングの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 5：レイヤ 2 ローカル スイッチングの機能情報

機能名	リリース	機能情報
レイヤ 2 ローカル スイッチング	Cisco IOS XE Release 2.5	レイヤ 2 ローカル スイッチング機能を使用すると、同じルータ上の 2 つのインターフェイス間でレイヤ 2 データをスイッチングできます。また、場合によっては、同じインターフェイス ポート上の 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。 Cisco IOS XE Release 2.5 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。次のタイプのローカル スイッチングのサポートが追加されました。 • イーサネットとイーサネット VLAN の間 • イーサネット VLAN の同一ポート スイッチング **connect**（L2VPN ローカル スイッチング）および **showconnection** コマンドが追加または変更されました。
レイヤ 2 ローカル スイッチング - ATM と ATM の間	Cisco IOS XE Release 3.3S	この機能は、Cisco IOS XE Release 3.3S で Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに導入されました。 **connect**（L2VPN ローカル スイッチング）および **showconnection** コマンドが追加または変更されました。
レイヤ 2 ローカル スイッチング - フレーム リレーとフレーム リレーの間	Cisco IOS XE Release 3.9S	この機能は、Cisco IOS XE Release 3.9S で、Cisco ISR 4400 シリーズ ルータに導入されました。