レイヤ 2 トンネリング プロトコル バージョン 3

Layer 2 Tunneling Protocol Version 3（L2TPv3; レイヤ 2 トンネリング プロトコル バージョン 3）機能により、シスコのレイヤ 2 Virtual Private Network（VPN; バーチャル プライベート ネットワーク）のサポートが拡大されます。L2TPv3 は、Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）の 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機能が強化されています。具体的には、レイヤ 2 Virtual Private Network（VPN; バーチャル プライベート ネットワーク）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。この機能には、次の利点があります。

- VPN の導入が容易になります。
- Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）が不要です。
- 任意のペイロードに対して IP 上でのレイヤ 2 トンネリングがサポートされます。

機能情報の確認

お使いのソフトウェア リリースが、このモジュールで説明されている機能の一部をサポートしていないことがあります。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、「L2TPv3 の機能情報」（P.45）を参照してください。

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

目次

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

- Provider Edge（PE; プロバイダー エッジ）デバイスの xconnect 接続回線を設定する前に（「xconnect 接続回線の設定」を参照）、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 CEF をイネーブルにするには、**ip cef** コマンドを使用します。
- ルータ上でループバック 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 Provider Edge（PE; プロバイダー エッジ）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

次の各項で、制約事項に関する情報を提供します。

一般的な L2TPv3 の制約事項

- L2TPv3 機能が動作するには、CEF がイネーブルになっている必要があります。xconnect コンフィギュレーション モードは、CEF がイネーブルになるまでブロックされます。CEF をイネーブルにするには、**ip cef** コマンドを使用します。
- IP ローカル インターフェイスは、ループバック インターフェイスにする必要があります。**ip local interface** コマンドで他のインターフェイスを設定しても、その設定は動作しません。
- イーサネット ポート上または VLAN ポート上のセッション数は、ルータでサポート可能な Interface Descriptor Block（IDB; インターフェイス記述子ブロック）の数によって制限されます。イーサネットおよび VLAN 回線タイプの場合、回線ごとに IDB が 1 つ必要です。
- Any Transport over MPLS（AToM）xconnect のインターフェイスを L2TPv3 xconnect に変換する場合は、そのインターフェイスの AToM 設定を削除してから、L2TPv3 を設定します。AToM 設定が正しく削除されていないと、L2TPv3 を設定しても、一部の機能が動作しない場合があります。
- IP パケットのレイヤ 2 フラグメント化および Intermediate System-to-Intermediate System（IS-IS）フラグメント化はサポートされていません。
- パフォーマンスが低下するため、レイヤ 3 フラグメント化は推奨されません。
- イーサネットと VLAN（802.1Q、QinQ、および QinAny）の接続回線のみがサポートされています。
- シーケンス処理がイネーブルの場合、インターワーキングを使用できません。

- L2TPv3 セッションに対して Stateful Switchover（SSO; ステートフル スイッチオーバー）はサポートされていません。代わりに、L2TPv3 は、High Availability（HA; ハイ アベイラビリティ）共存モードで動作します。したがって、すべてのセッションは、Route Processor（RP; ルート プロセッサ）スイッチオーバー時に失われますが、その後に再確立されます。
- 起動時または RP スイッチオーバー時のコンバージェンスには、設定済みのセッション数に応じて多くの時間を要します。

Cisco ASR 1000 シリーズ ルータに対してサポートされている共有ポート アダプタ

次の Shared Port Adapter（SPA; 共有ポート アダプタ）は、Cisco ASR 1000 シリーズ ルータ上で L2TPv3 をサポートします。

- SPA-4X1FE-TX-V2（4 ポート 10BASE-T/100BASE-TX ファスト イーサネット）
- SPA-8X1FE-TX-V2（8 ポート 10BASE-T/100BASE-TX ファスト イーサネット）
- SPA-2X1GE-V2（2 ポート ギガビット イーサネット）
- SPA-5X1GE-V2（5 ポート ギガビット イーサネット）
- SPA-8X1GE-V2（8 ポート ギガビット イーサネット）
- SPA-10XGE-V2（10 ポート ギガビット イーサネット）
- SPA-1X10GE-L-V2（1 ポート ギガビット イーサネット）

VLAN 固有の制約事項

- PE ルータは、手動で設定された静的 VLAN メンバーシップ エントリについてのみ処理します。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ていません。
- 他のレイヤ上で動作している VLAN メンバーシップ（レイヤ 2 での MAC アドレスまたはプロトコル タイプによるメンバーシップ、レイヤ 3 での IP サブネットによるメンバーシップなど）に対する暗黙のタギングはサポートされていません。
- 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はサポートされていません。接続回線と L2TPv3 セッションの間には 1 対 1 の関係があります。

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 セッション上でサポートされています。

L2TPv3 制御メッセージ ハッシングの制約事項

- **digest** コマンドで設定された L2TPv3 コントロール チャネル認証には、ピア ルータ上で双方向設定が必要であり、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ックスについては、表 2 を参照してください。ご使用のプラットフォームとリリースでサポートされる L2TPv3 認証方式の一覧については、「L2TPv3 の機能情報」（P.45）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、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 L2TPv3 コントロール チャネル認証パスワードは、L2TPv3 トンネルとセッションの解放なしで更新することはできません。

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

Modular QoS Command-Line Interface（MQC）で設定される Quality of Service（QoS）ポリシーは、L2TPv3 トンネル セッションでサポートされていますが、次の制約事項があります。

プロトコル逆多重化には、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。それにより、そのインターフェイスは通常の L3 として処理されます。レイヤ 2 IPv6 トラフィックに関する QoS を適用するには、IPv6 トラフィックを別のクラスに分類してから、機能を適用する必要があります。

次の一致基準を使用して、プロトコル逆多重化インターフェイス上のレイヤ 2 IPv6 トラフィックを分類します。

```
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ない場合、サービス ポリシーは、プロトコル逆多重化インターフェイス上で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 ネットワーク上で L2TP サービスを実現するための方法を提供します。これには、パケット カプセル化の仕様だけでなく、シグナリング プロトコルも含まれています。

L2TPv3 機能を設定するには、次の概念を理解しておく必要があります。

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 Route Processor（RP1; 第 1 世代の Cisco ASR 1000 シリーズ ルート プロセッサ）
  - 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 Route Processor（RP2; 第 2 世代の Cisco ASR 1000 シリーズ ルート プロセッサ）
  - 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 の動作

L2TPv3 には次の機能があります。

- IP ネットワーク上での疑似回線を介したレイヤ 2 トンネリングのための 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 ルータ 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。

- 接続回線へのレイヤ 2 トンネリング（L2TP Access Concentrator（LAC; L2TP アクセス コンセントレータ）で使用される）。レイヤ 3 トンネリングはサポートされていません。
- 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）。User Datagram Protocol（UDP; ユーザ データグラム プロトコル）の使用はサポートされていません。
- ポイントツーポイント セッション。ポイントツーマルチポイントやマルチポイントツーポイント セッションはサポートされていません。
- 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、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。

図 1 は、IP ネットワーク上でレイヤ 2 トンネリングを使用して VPN を設定するために、L2TPv3 機能がどのように使用されるかを示しています。2 つのカスタマー ネットワーク サイトの間のすべてのトラフィックは、L2TP データ メッセージを伝送する IP パケットにカプセル化され、IP ネットワークを介して送信されます。IP ネットワークのバックボーン ルータは、これらのトラフィックを他の IP トラフィックと同様に処理し、カスタマー ネットワークに関する情報を必要としません。

図 1　　L2TPv3 の動作：例

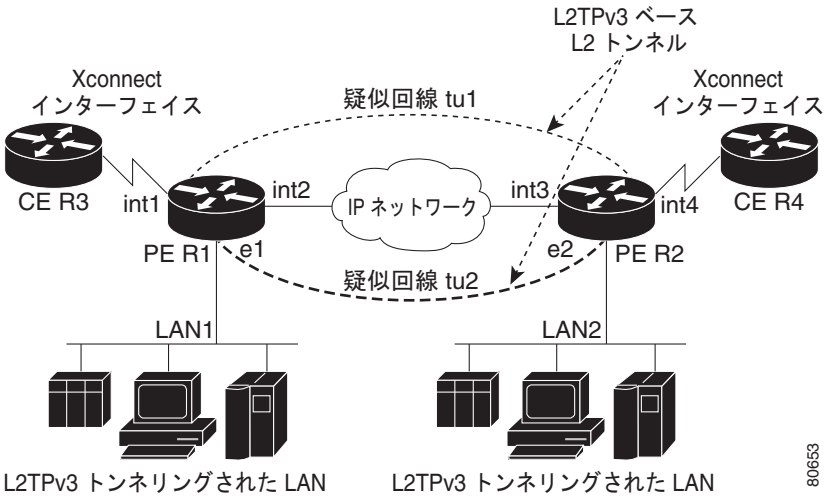


図 1 では、PE ルータ R1 と R2 により、L2TPv3 サービスが提供されます。R1 ルータと R2 ルータは、インターフェイス int1 と int2、IP ネットワーク、およびインターフェイス int3 と int4 からなるパスで、IP バックボーン ネットワーク上の疑似回線を使用して相互に通信します。

この例では、CE ルータ R3 と R4 は、イーサネットまたは VLAN インターフェイスの xconnect ペアで、L2TPv3 セッションを使用して通信します。L2TPv3 セッション 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 の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 に着信したパケットは、カプセル化され、疑似回線コントロール チャネル（tu1）を経由して R2 に送信されます。R2 は、受信したパケットのカプセル化を解除し、そのパケットをインターフェイス int4 から R4 に送信します。R4 が R3 にパケットを送信するときは、同じパスをパケットが逆向きにたどります。

L2TPv3 の動作に関して、次の点にご注意ください。

- インターフェイス int1 で受信されるすべてのパケットが R4 に転送されます。R3 と R4 は、介在するネットワークを検出できません。
- イーサネット インターフェイスの場合、R1 のイーサネット インターフェイス e1 上で受信された LAN1 からのパケットは、IP で直接カプセル化され、疑似回線セッション tu2 を介して R2 のインターフェイス e2 へ送信されます。パケットは、このインターフェイスから LAN2 上へ送信されます。
- イーサネット インターフェイス上の VLAN は、L2TPv3 セッションにマッピングできます。

L2TPv3 を使用する利点

VPN の導入を簡素化

L2TPv3 は、ベンダー間の相互運用性を保証する業界標準のレイヤ 2 トンネリング プロトコルであり、お客様の柔軟性とサービス アベイラビリティを向上します。

MPLS が不要

L2TPv3 サービス プロバイダーは、コア IP バックボーンに MPLS を導入しなくても、IP バックボーン上で L2TPv3 を使用した VPN を設定できます。結果として、運用コストが削減され、収益が増加します。

任意のペイロードに対して IP 上でのレイヤ 2 トンネリングをサポート

L2TPv3 により、IP コア ネットワーク上で任意のペイロードのレイヤ 2 トンネリングをサポートする機能強化が L2TP に対して行われます。L2TPv3 では、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定義されています。

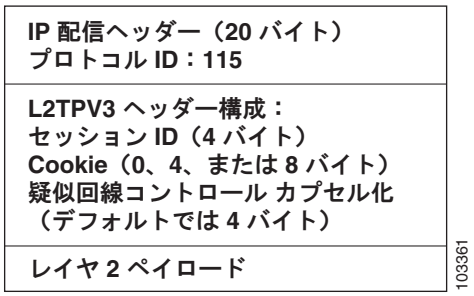
L2TPv3 のその他の利点

- L2TPv3 は、認証用のクッキーを提供します。
- L2TPv3 は、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（イーサネット -VLAN、イーサネット -QinQ、および VLAN-QinQ）がサポートされています。

L2TPv3 ヘッダーの説明

L2TPv3 ヘッダーの形式を図 2 に示します。

図 2　　L2TPv3 ヘッダーの形式



各 L2TPv3 パケットには、L2TPv3 ヘッダーが格納されています。このヘッダーには、1 つのセッションを表す一意のセッション ID と可変のクッキー長が含まれています。L2TPv3 セッション ID とトンネル クッキー フィールド長は、CLI を使用して割り当てられます。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。

セッション 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、セッション ID の値は、カプセル化解除システムにおける内容識別効率を最適化するように選択されます。そのため、カプセル化解除の実装は、より小さいセッション ID ビット フィールドをサポートすることを選択することがあります。この L2TPv3 の実装では、L2TPv3 セッション ID の上位の値が 023 に設定されました。0 の値の L2TPv3 セッション ID 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、セッション ID は手動で設定されます。

（注） ローカル セッション ID は、カプセル化解除システム上で一意でなければなりません。また、下位 10 ビットに制限されています。

セッション クッキー

L2TPv3 ヘッダーには、コントロール チャネル クッキー フィールドが含まれています。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。コントロール チャネル クッキーの長さは、静的セッションの場合は手動で設定できます。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、可変のクッキー長で問題ありません。しかし、異なるプラットフォームが L2TPv3 コントロール チャネルを介して相互運用される場合は、両方のプラットフォームがパケットを 4 バイトのクッキー長で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）。シーケンス処理には、先頭ビットとビット 8 ～ 31 のみが使用されます。

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格納され、それを更新すべきかどうかを示します。

L2TPv3 の機能

L2TPv3 では、次の各項に説明されている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」（ネゴシエートされない、PVC に似た転送されるセッション）
- 「動的 L2TPv3 セッション」（セッション ネゴシエーション用の L2TPv3 コントロール プレーンを使用して、ネゴシエートされ、転送されるセッション）

また、次の項で説明する機能もサポートされています。

- 「L2TPv3 上のイーサネット」
- 「シーケンス」
- 「L2TPv3 タイプ オブ サービス マーキング」
- 「キープアライブ」
- 「MTU の処理」
- 「L2TPv3 制御メッセージ ハッシング」
- 「L2TPv3 制御メッセージ 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 トンネルの手動クリア」
- 「L2TPv3 トンネルの管理」
- 「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」

静的 L2TPv3 セッション

通常、L2TP コントロール プレーンは、セッションを設定するためのセッション パラメータ（セッション ID やクッキーなど）のネゴシエーションを処理します。しかし、IP ネットワークによっては、セッションの確立にシグナリングを要求しないように、セッションを設定しなければならない場合があります。そのため、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り、PE ルータに対して静的 L2TPv3 セッションを設定することができます。静的 L2TPv3 セッションでは、バインド先の接続回線がアップするとすぐに、PE がレイヤ 2 トラフィックをトンネリングできます。

静的設定では、コントロール接続パラメータを動的にネゴシエートせずにセッションが確立されます。したがって、セッションが **show l2tun session** コマンド出力に表示されても、**show l2tun tunnel** コマンド出力にはコントロール チャネル情報が出力されません。

（注） L2TPv3 静的セッションの場合でも、L2TP コントロール チャネルを起動して、ピア認証と停止ピア検出を実行できます。L2TP コントロール チャネルが hello の失敗により確立できない、または解放された場合、静的セッションも解放されます。

静的 L2TPv3 セッションを使用する場合、制御メッセージを交換するための手段がないため、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、Attribute-Value（AV; アトリビュート値）ペアを含む制御メッセージの交換によって確立されます。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、Virtual Circuit（VC; 仮想回線）ID など）に関する情報が含まれています。

一対の PE 間に複数の L2TP セッション（転送されるレイヤ 2 回線ごとに 1 つ）が存在でき、それらを単一のコントロール チャネルで維持できます。セッション ID とクッキーは、動的セッションの設定中に、動的に生成され、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。

L2TPv3 上のイーサネット

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。

シーケンス

受信されるレイヤ 2 フレームの正しいシーケンスは一部のレイヤ 2 テクノロジー（シリアル回線などのリンクの特性）またはプロトコル自体によって保証されていますが、転送されるレイヤ 2 フレームが IP パケットとしてネットワークを移動すると、それらの喪失、複製、または順序の変更が起こる可能性があります。レイヤ 2 プロトコルが明示的なシーケンス処理メカニズムを提供していない場合は、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。

セッションがネゴシエートされるとき、L2TP データ パケットの受信デバイスは、Sequencing Required AV ペアによってシーケンス処理を要求します。送信デバイスは、この AV ペアを受信する（またはシーケンス処理されたパケットを送信するように手動で設定されている）と、L2TPv3 に定義されているレイヤ 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。

順序が正しくないパケットをドロップするようにのみ L2TP を設定できます。正しくない順序でパケットを配信するように L2TP を設定することはできません。並べ替えメカニズムは用意されていません。

シーケンス処理がイネーブルの場合、インターワーキングを使用できません。

L2TPv3 タイプ オブ 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場合、ToS ビットに含まれる情報を、次のいずれかの方法で L2TP カプセル化 IP パケットに移すことができます。

- トンネリングされるレイヤ 2 フレームが IP パケットそのものをカプセル化する場合、内部 IP パケットの ToS バイトを外部 IP パケット ヘッダーに単純にコピーすることが推奨されます。この処理は、「ToS バイト リフレクション」と呼ばれています。
- 静的 ToS バイト設定。疑似回線を介して送信されるすべてのパケットで使用される ToS バイト値を指定します。

キープアライブ

L2TPv3 のキープアライブ 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、信頼できる制御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、セッションの開始にコントロール プレーンが使用されたかどうかに関係なく、コントロール プレーンが使用されます。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、2 つの L2TP ピアの間のコントロール チャネルは、Start Control Channel Request（SCCRQ）、Start Control Channel Replay（SCCRP）、および Start Control Channel Connected（SCCCN）制御メッセージの交換によってネゴシエートされます。コントロール チャネルは、hello メッセージの交換によってキープアライブ メカニズムを維持することのみを担当します。

hello メッセージの間隔は、コントロール チャネルごとに設定できます。キープアライブ メカニズムによって一方のピアがもう一方のピアのダウンを検出すると、そのピアは StopCCN 制御メッセージを送信してから、そのピアに対するすべての疑似回線にそのイベントを通知します。この通知により、手動で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 MTU を設定することが重要です。設定された MTU サイズにより、次のことが保証されます。

- トンネリングされたレイヤ 2 フレームの長さが宛先接続回線の MTU 未満になる。
- トンネリングされたパケットが断片化されず、それにより、受信 PE でそれらが強制的に再構築される。

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、セッション MTU より大きいパケットが断片化されます。
- 疑似回線クラスで **ip dfbit set** コマンドをイネーブルにすると、デフォルトの MTU 動作は、トンネル MTU 内に収まらないパケットをすべてドロップするように変更されます。
- 疑似回線クラスで **ip pmtu** コマンドをイネーブルにすると、L2TPv3 コントロール チャネルはパス MTU 検出に参加します。この機能をイネーブルにすると、次の処理が実行されます。
  - L2TPv3 ルータに返信された ICMP 到達不能メッセージが解読され、それに従ってトンネル 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、トンネル ヘッダー内の Don't Fragment（DF）ビットは、CE から受信した DF ビット値に従って設定されるか、**ip dfbit set** オプションがイネーブルの場合は静的に設定されます。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返信されます。ICMP 到達不能メッセージは、IP パケットが CE-PE インターフェイスに着信し、そのパケット サイズがトンネル MTU よりも大きいときは必ず、CE に送信されます。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 制御メッセージ ハッシング

L2TPv3 制御メッセージ ハッシング機能では、L2TPv2 から継承された Challenge Handshake Authentication Protocol（CHAP; チャレンジ ハンドシェイク認証プロトコル）型認証システム（SCCRQ、SCCRP、および SCCCN メッセージで Challenge AV ペアと Challenge Response AV ペアが使用される）の代わりとなる、新しい、よりセキュアな認証システムを導入します。

L2TPv3 制御メッセージ ハッシング機能で導入されるメッセージ単位の認証は、L2TP ノード間の相互認証を実行し、すべての制御メッセージの完全性をチェックし、制御メッセージのスプーフィング攻撃とリプレイ攻撃から保護するように設計されており、たやすくネットワークへの攻撃を仕掛けることができないようになっています。

L2TPv3 制御メッセージ ハッシング機能では、すべての制御メッセージに対する認証または完全性チェックがオプションとして使用されます。この新しい認証方式では、L2TP 制御メッセージのヘッダーとボディに対して計算された一方向ハッシュ、通信する L2TP ノード上で定義しなければならない事前に設定済みの共有秘密、および Nonce AV ペアを使用して交換されるローカルとリモートのランダムな値が使用されます。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 制御メッセージの完全性チェックは、共有秘密の設定を必要としない一方向メカニズムです。完全性チェックがローカル PE ルータ上でイネーブルになっていると、制御メッセージは、共有秘密や Nonce AV ペアを使用しないで計算されたメッセージ ダイジェストを付けて送信され、リモート PE ルータによって確認されます。確認に失敗すると、リモート PE ルータはその制御メッセージをドロップします。

L2TPv3 制御メッセージ レート制限

L2TPv3 制御メッセージ レート制限機能は、L2TPv3 が稼動しているルータに対するサービス拒絶攻撃の可能性に対処するために導入されました。L2TPv3 制御メッセージ レート制限機能は、L2TPv3 トンネルの終端 PE に着信した SCCRQ 制御パケットの処理に使用できるレートを制限します。SCCRQ 制御パケットを受信すると、L2TPv3 トンネルの構築プロセスが開始され、PE ルータのコントロール プレーン リソースが大量に要求されます。

L2TPv3 制御メッセージ レート制限機能には、必要な設定はありません。この機能は、サポートされているリリースにおいてバックグラウンドで自動的に実行されます。

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 ルータに設定されているパスワードを使用して行われます。この機能の導入前は、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古いパスワードを設定から削除する必要があるため、L2TPv3 サービスが中断します。認証パスワードは、すべてのピア PE 上で更新する必要がありますが、通常、これらの PE は物理的に異なる場所に配置されています。L2TPv3 サービスの中断を最小限に抑えることは、すべての PE ルータを同時に新しいパスワードに更新する必要があるため困難です。

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では、L2TPv3 コントロール チャネル メッセージの認証に使用されるパスワードを、確立済みの 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では、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ます。そのため、古いパスワードを先に削除しなくても、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。これにより、新しいパスワードを使用するための更新がまだ実施されていないピア PE ルータでも、正常に認証が行われます。すべてのピア PE ルータ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。

L2TPv3 トンネルの手動クリア

この機能では、L2TPv3 トンネルを手動でクリアできます。この機能の導入前は、特定の L2TPv3 トンネルを意図的に手動でクリアするためのプロビジョニングが実施されませんでした。この機能では、L2TPv3 ネットワークをより詳細に制御できます。

L2TPv3 トンネルの管理

xconnect 設定の管理と xconnect 設定に関する問題の診断に役立つように、新しいコマンドと機能強化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関連した固有の設定作業はありません。

これらの Cisco IOS コマンドの詳細については、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。

次の新しいコマンドと機能強化されたコマンドが、トンネル管理用に導入されています。

- 「L2TPv3 用の Syslog、SNMP トラップ、および show コマンドの機能強化」

L2TPv3 用の Syslog、SNMP トラップ、および show コマンドの機能強化

この機能では、xconnect 設定における管理と問題診断のための新しいコマンドや機能強化されたコマンドが導入されています。

- **debug vpdn**：このコマンドの出力に、認証失敗メッセージが含まれます。
- **show l2tun session**：**hostname** キーワード オプションにより、ピア ホスト名を出力に表示できます。
- **show l2tun tunnel**：**authentication** キーワード オプションにより、L2TP コントロール チャネル認証の Attribute-Value（AV; アトリビュート値）ペアに関するグローバル情報を表示できます。
- **show xconnect**：xconnect 固有の情報を表示します。すべての xconnect 設定に関する情報について、分類可能な単一の参照ポイントを提供します。
- **xconnect logging pseudowire status**：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。

L2TPv3 プロトコル逆多重化

プロトコル逆多重化機能により、IPv4 ネットワークから IPv6 トラフィックをオフロードする専用の IPv6 ネットワークを利用して、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 ルータ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、IPv4 ネットワーク内で通常どおりにルーティングされ、IPv4 ネットワークの既存のパフォーマンスと信頼性が維持されます。

IPv4 PE ルータは、IPv4 トラフィックから着信 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 ネットワークに接続している PE ルータには、IPv6 設定は必要ありません。IPv6 ネットワークの設定については、このマニュアルの範囲外になります。IPv6 ネットワークの設定に関する詳細については、『*Cisco IOS 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 カプセル化用の L2TPv3 カスタム Ethertype 機能では、QinQ または Dot1Q カプセル化を伴うギガビット イーサネット インターフェイス上で 0x8100 以外の Ethertype を設定できます。このカスタム Ethertype は、0x9100、0x9200、または 0x88A8 に設定できます。これにより、マルチベンダーのギガビット イーサネット環境において相互運用性が実現されます。

サポートされている L2TPv3 ペイロード

L2TPv3 では、疑似回線上でトンネリングされた L2TPv3 パケットに含めることが可能な次のレイヤ 2 ペイロードがサポートされています。

- 「Ethernet」
- 「VLAN」
- 「IPv6 プロトコル逆多重化」

（注） L2TPv3 トンネリングされた各パケットには、ここ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ます。シーケンス処理が必要な場合は（「シーケンス」を参照）、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。

Ethernet

PE ルータに着信したイーサネット フレームは、L2TP データ ヘッダーを付けて全体が単純にカプセル化されます。その反対側の PE ルータでは、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、ペイロードであるイーサネット 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 フレームの内容を調べる必要がありません。インターフェイスで受信されたイーサネット フレームはすべてトンネリングされ、L2TP トンネリングされたすべてのイーサネット フレームがそのインターフェイスから転送されます。

（注） L2TPv3 でのイーサネット フレームの処理方法に対応して、イーサネット インターフェイスは、ルータに接続されたイーサネット セグメント上で受信されるすべてのトラフィックが取得されるように、無差別モードに設定する必要があります。すべてのフレームが L2TP 疑似回線によって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ています。

- ポートベース。日付なしのイーサネット フレームが受信されます。
- VLAN ベース。タグ付きのイーサネット フレームが受信されます。

L2TPv3 では、イーサネット xconnect で、ポートベースの VLAN メンバーシップおよび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、タグ ヘッダー（802.1Q に定義されている）が含まれています。このヘッダーは、4 バイトの長さがあり、2 バイトの Tag Protocol Identifier（TPID）フィールドと 2 バイトの Tag Control Information（TCI）フィールドで構成されます。TPID は、TCI が後に続くことを示します。TCI は、さらに次の 3 つのフィールドに分けられます。

- ユーザ プライオリティ フィールド
- Canonical Format Indicator（CFI）
- 12 ビットの VLAN ID（VID）

L2TPv3 の場合、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は、すべてのイーサネット トラフィックが、そのサブインターフェイスに指定された VID でタグ付けされ、別の PE にトンネリングされるように、xconnect サービスにバインドできます。VLAN イーサネット フレームは、全体がそのまま転送されます。受信 PE は、トンネリングされたトラフィックを接続回線上に転送する前に、そのトラフィックの VID を別の値に書き換えることもできます。

VLAN の書き換えを正常に行うには、Spanning Tree Protocol（STP; スパニング ツリー プロトコル）をディセーブルにしなければならない場合があります。これは、**no spanning-tree vlan** コマンドを使用して、VLAN 単位で行うことができます。

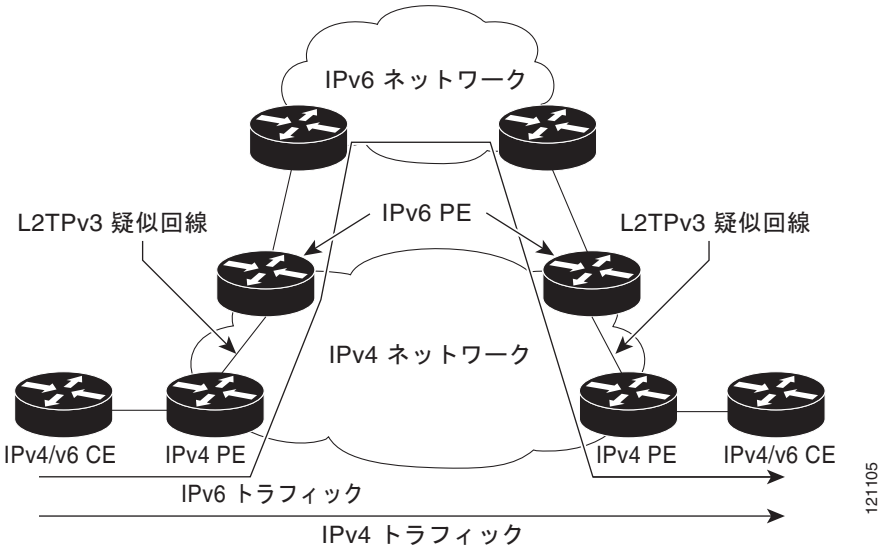
（注） L2TPv3 での VLAN パケットの処理方法に対応して、イーサネット インターフェイスは、ルータに接続されたイーサネット セグメント上で受信されるすべてのトラフィックが取得されるように、無差別モードに設定する必要があります。すべてのフレームが L2TP 疑似回線によってトンネリングされます。

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、長期にわた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 のプロトコル逆多重化機能により、専用の IPv6 ネットワークを構築し、IPv4 ネットワークから IPv6 トラフィックをオフロードして、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 ルータ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、IPv4 ネットワーク内で通常どおりにルーティングされ、IPv4 ネットワークの既存のパフォーマンスと信頼性が維持されます。

図 3 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 ルータは、IPv4 トラフィックから IPv6 トラフィックを逆多重化します。IPv6 トラフィックは、L2TPv3 疑似回線を経由して IPv6 ネットワークにルーティングされます。一方、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 ルータは、IPv4 トラフィックから着信 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 ネットワークに接続している PE ルータには、IPv6 設定は必要ありません。

図 3　　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



プロトコル逆多重化では、IPv4 PE インターフェイス上で IP アドレスと **xconnect** コマンド設定の組み合わせをサポートする必要があります。この設定の組み合わせは、プロトコル逆多重化をイネーブルにしなければ許可されません。IP アドレスが設定されていない場合、プロトコル逆多重化設定は拒否されます。IP アドレスが設定されていても、xconnect コンフィギュレーション モードを終了する前にそのモード中でプロトコル逆多重化をイネーブルにしなければ、**xconnect** コマンド設定は拒否されます。**xconnect** コマンド設定とプロトコル逆多重化がイネーブルの状態で IP アドレスが設定されている場合、その IP アドレスは削除できません。設定済みの IP アドレスを変更または削除するには、先に **xconnect** コマンド設定をディセーブルにする必要があります。

表 1 に、有効な設定の組み合わせを示します。

表 1　　有効な設定シナリオ

シナリオ	IP Address	xconnect 設定	プロトコル逆多重化設定
ルーティング	あり	なし	—

表 1　有効な設定シナリオ （続き）

シナリオ	IP Address	xconnect 設定	プロトコル逆多重化設定
L2VPN	なし	あり	なし
IPv6 プロトコル逆多重化	あり	あり	あり

L2TPv3 の設定方法

ここでは、次の手順について説明します。

- 「L2TP コントロール チャネル パラメータの設定」（P.16）（任意）
- 「L2TPv3 疑似回線の設定」（P.26）（必須）
- 「xconnect 接続回線の設定」（P.30）（必須）
- 「L2TPv3 セッション パラメータの手動設定」（P.31）（必須）
- 「L2TPv3 のプロトコル逆多重化の設定」（P.33）（任意）
- 「Dot1q および QinQ カプセル化用の L2TPv3 カスタム Ethertype の設定」（P.35）（任意）
- 「L2TPv3 トンネルの手動クリア」（P.36）（任意）

L2TP コントロール チャネル パラメータの設定

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 ルータ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任意です。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」を参照）。

L2TP クラスで設定可能な L2TP コントロール チャネル パラメータの主要な 3 つのグループについては、次の項で説明します。

- 「L2TP コントロール チャネル タイミング パラメータの設定」（P.16）
- 「L2TPv3 コントロール チャネル認証パラメータの設定」（P.18）
- 「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」（P.26）

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 L2TP クラス コントロール チャネル 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
- 制御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 パラメータの設定はすべて任意であり、任意の順序で設定できます。これらのパラメータを設定しなければ、デフォルト値が適用されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **l2tp-class** [*l2tp-class-name*]
4. **retransmit** {**initial retries** *initial-retries* | **retries** *retries* | **timeout** {**max** | **min**} *timeout*}
5. **timeout setup** *seconds*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**l2tp-class** [*l2tp-class-name*] **例：** `Router(config)# l2tp-class class1`	L2TP クラス名を指定し、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* 引数の指定は任意です。ただし、複数の L2TP クラスを設定する場合は、それぞれに一意の *l2tp-class-name* を指定する必要があります。
ステップ 4	**retransmit** {**initial retries** *initial-retries* | **retries** *retries* | **timeout** {**max** | **min**} *timeout*} **例：** `Router(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。 • **initial retries**：セッションが中断される前に再送信する SCCRQ の数を指定します。*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 ルータが無応答であると判断する前に実行する再送信の回数を指定します。*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間隔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。デフォルトの最大間隔は 8 です。デフォルトの最小間隔は 1 です。
ステップ 5	**timeout setup** *seconds* **例：** `Router(config-l2tp-class)# timeout setup 400`	（任意）コントロール チャネルの設定に使用可能な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。

L2TPv3 コントロール チャネル認証パラメータの設定

コントロール チャネル メッセージ認証には 2 つの方式を使用できます。L2TPv3 制御メッセージ 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。これらの認証方式の一方しかサポートしていないピアとの相互運用性を保証するために、両方の認証方式をイネーブルにすることも可能です。しかし、この設定では、どの認証方式を使用するかの制御は、ピア PE ルータにまかされることになります。両方の認証方式をイネーブルにすることは、ソフトウェア アップグレード時の下位互換性に関する問題を解決するための暫定的なソリューションであると考えるべきです。

L2TPv3 制御メッセージ ハッシング機能は、受信された制御メッセージ内の選択されたコンテンツに対してハッシュが計算されるのではなく、メッセージ全体がハッシュに使用されるという点が、CHAP 型 L2TP コントロール チャネル認証と大きく異なります。さらに、ハッシュ ダイジェストが、SCCRP メッセージと SCCCN メッセージだけでなく、すべてのメッセージに含められるという点も異なっています。

L2TP コントロール チャネル認証のサポートは、下位互換性のために残されています。一方の認証方式しかサポートしていないピアとの相互運用を可能にするために、一方または両方の認証方式をイネーブルにできます。

表 2 に、さまざまな L2TPv3 認証方式の互換性マトリックスを示します。PE1 が新しい認証を実行する場合に、PE1 に対して考えられるさまざまな認証設定が最初の列に示されています。残りの各列には、使用可能なオプションがそれぞれ異なるソフトウェアを実行している PE2 が示されています。交差部分には、互換性のある PE2 の設定オプションが示されています。PE1 や PE2 の認証設定が、使用される認証方式をあいまいにしている場合は、使用される可能性の高い方の認証方式を太字で示しています。PE1 と PE 2 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 2　　L2TPv3 認証方式の互換性マトリックス

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 新しい完全性チェック	なし 新しい完全性チェック
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**と新しい完全性チェック
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**
新しい完全性チェック	なし	なし 新しい完全性チェック	なし 新しい完全性チェック

表 2　　L2TPv3 認証方式の互換性マトリックス （続き）

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**と新しい完全性チェック
古い認証と新しい完全性チェック	古い認証	—	古い認証 **古い認証**と新しい認証 **古い認証**と新しい完全性チェック

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 ダイジェスト認証と完全性チェック認証システムしかサポートせず、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、他のベンダーにより実装されることがあります。
3. 古い CHAP 型認証システムと、新しいメッセージ ダイジェスト認証と完全性チェック認証システムの両方をサポートしている PE ソフトウェア

L2TPv3 コントロール チャネル メッセージの認証パラメータを設定するには、次の作業のいずれかまたは両方を実行します。

- 「L2TP コントロール チャネルの認証の設定」（P.19）（任意）
- 「L2TPv3 制御メッセージ ハッシングの設定」（P.20）（任意）

L2TPv3 制御メッセージ ハッシング機能を使用して認証を設定する場合は、次の作業を実行することもできます。

- 「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」（P.23）（任意）

L2TP コントロール チャネルの認証の設定

L2TP コントロール チャネルの認証方式は、L2TPv2 から継承された従来の 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 パラメータの設定はすべて任意であり、任意の順序で設定できます。これらのパラメータを設定しなければ、デフォルト値が適用されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **l2tp-class** [*l2tp-class-name*]

4. **authentication**
5. **password** [**0** | **7**] *password*
6. **hostname** *name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**l2tp-class** [*l2tp-class-name*] **例：** `Router(config)# l2tp-class class1`	L2TP クラス名を指定し、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* 引数の指定は任意です。ただし、複数の L2TP クラスを設定する場合は、それぞれに一意の *l2tp-class-name* を指定する必要があります。
ステップ 4	**authentication** **例：** `Router(config-l2tp-class)# authentication`	（任意）PE ルータ間のコントロール チャネルの認証をイネーブルにします。
ステップ 5	**password** [**0**	**7**] *password* **例：** `Router(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）共有秘密の入力形式を指定します。デフォルト値は **0** です。 – **0**：プレーンテキストの秘密が入力されることを指定します。 – **7**：暗号化された秘密が入力されることを指定します。 • *password*：ピア ルータ間の共有パスワードを定義します。
ステップ 6	**hostname** *name* **例：** `Router(config-l2tp-class)# hostname yb2`	（任意）L2TP コントロール チャネル認証時にルータ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い場合、ルータのデフォルトのホスト名が使用されます。

L2TPv3 制御メッセージ ハッシングの設定

L2TPv3 制御メッセージ ハッシング機能は、CHAP 型 L2TP コントロール チャネル認証方式よりもセキュアな新しい認証システムです。L2TPv3 制御メッセージ ハッシングでは、すべての制御メッセージに対する認証または完全性チェックがオプションとして使用されます。このメッセージ単位の認証は、制御メッセージのスプーフィング攻撃とリプレイ攻撃から保護するように設計されており、ネットワークへの攻撃をたやすく仕掛けることができないようになっています。

L2TPv3 制御メッセージ ハッシング機能をイネーブルにすると、送受信される制御メッセージごとにメッセージ内容全体のダイジェスト計算が追加されるため、コントロール チャネルとセッションの確立時にパフォーマンスが低下します。これは、この機能によるセキュリティ強化の実現のために予想されるトレードオフです。さらに、受信ウィンドウ サイズが小さすぎると、ネットワークの輻輳が発生する可能性があります。L2TPv3 制御メッセージ ハッシング機能をイネーブルにする場合は、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 ダイジェスト確認により、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なり、ローカル受信ウィンドウの最小サイズが 35 に制限されます。

コントロール チャネル認証または制御メッセージ完全性チェックを設定することもできます。コントロール チャネル認証には両方のピアによる参加が必要であり、両方のルータ上で共有秘密を設定する必要があります。制御メッセージ完全性チェックは一方向であり、一方のピア上にだけ設定が必要です。

次の作業では、L2TP クラスの L2TPv3 制御メッセージ ハッシング機能を設定します。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**l2tp-class** [*l2tp-class-name*] **例：** `Router(config)# l2tp-class class1`	L2TP クラス名を指定し、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* 引数の指定は任意です。ただし、複数の L2TP クラスを設定する場合は、それぞれに一意の *l2tp-class-name* 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 4	**digest** [**secret** [**0** | **7**] *password*] [**hash** {**md5** | **sha**}] **例：** `Router(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完全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）** **secret** キーワード オプションを指定しないで **digest** コマンドを実行すると、L2TPv3 完全性チェックがイネーブルになります。 • [**0** | **7**]：共有秘密の入力形式を指定します。デフォルト値は **0** です。 – **0**：プレーンテキストの秘密が入力されることを指定します。 – **7**：暗号化された秘密が入力されることを指定します。 • *password*：ピア ルータ間の共有秘密を定義します。*password* 引数には、[**0** | **7**] キーワード オプションで指定した入力形式と一致する形式で値を入力する必要があります。 • **hash** {**md5** | **sha**}：（任意）メッセージ単位の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：** `Router(config-l2tp-class)# digest check`	（任意）受信された制御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ります。 **（注）** **digest secret** コマンドを使用して認証をイネーブルにしている場合は、メッセージ ダイジェストの確認をディセーブルにできません。**digest secret** コマンドによる認証の設定を行っていない場合は、ダイジェスト チェックをディセーブルにして、パフォーマンスを向上できます。

	コマンドまたはアクション	目的
ステップ 6	**hidden** **例：** `Router(config-l2tp-class)# hidden`	（任意）L2TPv3 ピアへの制御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、デフォルトではディセーブルになります。 • クッキー AV ペアの隠蔽だけがサポートされています。 • L2TP クラス コンフィギュレーション モードでクッキーが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）、AV ペア隠蔽をイネーブルにすると、そのクッキーは、**digest secret** コマンドで設定されたパスワードを使用して、隠蔽された 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、他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なります。

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

L2TPv3 コントロール チャネル認証は、参加しているすべてのピア PE ルータに設定されている 1 つのパスワードを使用して行われます。L2TPv3 ダイジェスト シークレット グレースフル スイッチオーバー機能では、確立済みの L2TPv3 トンネルを中断しなくても、古いコントロール チャネル認証パスワードから新しいコントロール チャネル認証パスワードに移行できます。

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に失敗しても、新しいパスワードでのみ認証が行われます。

確立済みの L2TPv3 トンネルを中断しないで古い 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に移行するには、次の作業を実行します。

前提条件

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

制約事項

この作業は、従来の 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はありません。

手順の概要

1. **enable**
2. **configure terminal**
3. **l2tp-class** *l2tp-class-name*
4. **digest** [**secret** [**0** | **7**] *password*] [**hash** {**md5** | **sha**}]
5. **end**
6. **show l2tun tunnel all**
7. **configure terminal**
8. **l2tp-class** [*l2tp-class-name*]
9. **no digest** [**secret** [**0** | **7**] *password* [**hash** {**md5** | **sha**}]]
10. **end**
11. **show l2tun tunnel 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： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**l2tp-class** [*l2tp-class-name*] 例： `Router(config)# l2tp-class class1`	L2TP クラス名を指定し、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： `Router(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。 • パスワードは常に 2 つまで設定できます。 **（注）** この段階では、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： `Router(config-l2tp-class)# end`	特権 EXEC モードを終了することにより、コンフィギュレーション セッションを終了します。

	コマンドまたはアクション	目的
ステップ 6	**show l2tun tunnel all** **例：** `Router# show l2tun tunnel all`	（任意）レイヤ 2 トンネルの現在の状態と設定済みトンネルに関する情報（ローカルおよびリモートの Layer 2 Tunneling Protocol（L2TP; レイヤ 2 トンネリング プロトコル）ホスト名、集約パケット数、コントロール チャネル情報など）を表示します。 • トンネルは数秒で新しいコントロール チャネル認証パスワードに更新されます。数分経過してもトンネルが 2 つの秘密を設定された状態に更新されない場合は、そのトンネルを手動でクリアし、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」の作業を実行します。 **（注）** このコマンドを実行して、コントロール チャネル認証に新しいパスワードを使用していないトンネルが存在していないかどうかを確認します。指定した L2TP クラス内の各トンネルに対し、2 つの秘密が設定済みであることが表示される必要があります。
ステップ 7	**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 8	**l2tp-class** [*l2tp-class-name*] **例：** `Router(config)# l2tp-class class1`	L2TP クラス名を指定し、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* 引数の指定は任意です。ただし、複数の L2TP クラスを設定する場合は、それぞれに一意の *l2tp-class-name* を指定する必要があります。
ステップ 9	**no digest** [**secret** [**0** | **7**] *password* [**hash** {**md5** | **sha**}]] **例：** `Router(config-l2tp-class)# no digest secret cisco hash sha`	L2TPv3 コントロール チャネル認証で使用されている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 ルータ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：** `Router(config-l2tp-class)# end`	特権 EXEC モードを終了することにより、コンフィギュレーション セッションを終了します。
ステップ 11	**show l2tun tunnel all** **例：** `Router# show l2tun tunnel all`	（任意）レイヤ 2 トンネルの現在の状態と設定済みトンネルに関する情報（ローカルおよびリモートの Layer 2 Tunneling Protocol（L2TP; レイヤ 2 トンネリング プロトコル）ホスト名、集約パケット数、コントロール チャネル情報など）を表示します。 • トンネルは、古いコントロール チャネル認証パスワードを使用しなくなっているはずです。数分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状態に更新されない場合は、そのトンネルを手動でクリアし、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」の作業を実行します。 **（注）** このコマンドを実行して、すべてのトンネルがコントロール チャネル認証に新しいパスワードしか使用しないことを確認します。指定した L2TP クラス内の各トンネルに対し、1 つの秘密が設定済みであることが表示される必要があります。

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、L2TP クラス内で hello メッセージに使用される間隔を設定します。このコントロール チャネル パラメータの設定は任意です。このパラメータを設定しなければ、デフォルト値が適用されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **l2tp-class** [*l2tp-class-name*]
4. **hello** *interval*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**l2tp-class** [*l2tp-class-name*] 例： `Router(config)# l2tp-class class1`	L2TP クラス名を指定し、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* 引数の指定は任意です。ただし、複数の L2TP クラスを設定する場合は、それぞれに一意の *l2tp-class-name* を指定する必要があります。
ステップ 4	**hello** *interval* 例： `Router(config-l2tp-class)# hello 100`	（任意）L2TP hello パケットの交換が行われる間隔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。

L2TPv3 疑似回線の設定

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（クラス）を使用して、接続回線トラフィックを疑似回線経由で転送するために使用されるセッションレベルのパラメータを L2TPv3 セッションに設定します。

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 フラグメント化、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。疑似回線の設定にシグナリングが使用されるかどうかを決める設定も含まれます。

単純な L2TPv3 シグナリング設定では、疑似回線クラスの設定は任意です。しかし、送信元 IP アドレスを指定してループバック インターフェイスを設定することを強く推奨します。ループバック インターフェイスを設定しない場合、使用可能で最適なローカル アドレスがルータによって選択されます。これは、コアに接続したインターフェイスに設定されている IP アドレスになる可能性があります。この設定では、コントロール チャネルを確立できなくなる可能性があります。

encapsulation l2tpv3 コマンドを指定した後、そのコマンドを **no encapsulation l2tpv3** コマンドで削除することはできません。また、そのコマンドの設定を、**encapsulation mpls** コマンドで変更することもできません。これらの方法を使用すると、次のエラー メッセージが出力されます。

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

このコマンドを削除するには、疑似回線を **no pseudowire-class** コマンドで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、疑似回線を **no pseudowire-class** コマンドで削除してから、疑似回線を再び確立し、新しいカプセル化タイプを指定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **pseudowire-class** [*pw-class-name*]
4. **encapsulation l2tpv3**
5. **protocol** {**l2tpv3** | **none**} [*l2tp-class-name*]
6. **ip local interface** *interface-name*
7. **ip pmtu**
8. **ip tos** {**value** *value* | **reflect**}
9. **ip dfbit set**
10. **ip ttl** *value*
11. **ip protocol** {**l2tp** | *protocol-number*}
12. **sequencing** {**transmit** | **receive** | **both**}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**pseudowire-class** [*pw-class-name*] **例：** `Router(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、必要に応じて L2TP 疑似回線クラスの名前を指定します。
ステップ 4	**encapsulation l2tpv3** **例：** `Router(config-pw)# encapsulation l2tpv3`	IP トラフィックをトンネリングするデータ カプセル化の方法として L2TPv3 を使用することを指定します。
ステップ 5	**protocol** {**l2tpv3** | **none**}[*l2tp-class-name*] **例：** `Router(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（「L2TP コントロール チャネル パラメータの設定」を参照）で作成された疑似回線を管理するために使用される L2TPv3 シグナリング プロトコルを指定します。 • *l2tp-class-name* 引数を指定しないと、デフォルトの L2TP コントロール チャネル パラメータの値が使用されます。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で作成された L2TPv3 セッション内でシグナリングを使用しない場合、**protocol none** を入力します。
ステップ 6	**ip local interface** *interface-name* **例：** `Router(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送信元 IP アドレスとして使用される IP アドレスを持つ PE ルータ インターフェイスを指定します。 • PE ルータのペアに設定された疑似回線クラスごとに、同じまたは異なるローカル インターフェイス名を使用できます。 **（注）** このコマンドは、データ カプセル化の方法に L2TPv3 を使用する疑似回線クラス設定に対して設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 7	**ip pmtu** **例：** `Router(config-pw)# ip pmtu`	（任意）トンネリングされたトラフィックに対してパス MTU の検出をイネーブルにし、フラグメント化に利用します。 • 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 ネットワーク内で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、セッション内に送信される IP パケットのうち DF ビットが設定されているものに対する MTU チェックをイネーブルにします。MTU より大きい IP パケットはすべてドロップされ、ICMP 到達不能メッセージが送信されます。MTU 検出は、デフォルトではディセーブルになります。 **（注）** ステップ 5において **protocol none** コマンドでシグナリングをディセーブルにした場合、**ip pmtu** コマンドは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ト化が行われる場合の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ト化が行われる場合、疑似回線クラス設定で **ip dfbit set** コマンドも入力することを推奨します。これにより、PMTU の取得が高速化されます。 **（注）** **ip pmtu** コマンドがイネーブルの場合、DF ビットは、内部 IP ヘッダーから外部 IP ヘッダーにコピーされます。レイヤ 2 フレーム内で IP ヘッダーが検出されなければ、外部 IP ヘッダー内の DF ビットは 0 に設定されます。
ステップ 8	**ip tos** {**value** *value* | **reflect**} **例：** `Router(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 バイトの値を設定するか、内部 IP ヘッダーの 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	**ip dfbit set** **例：** `Router(config-pw)# ip dfbit set`	（任意）トンネリングされたパケットの外部ヘッダー内の DF ビットの値を設定します。 • このコマンドは、（パフォーマンス上の理由から）トンネリングされたパケットの再構築をピア PE ルータ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	**ip ttl** *value* **例：** `Router(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 Time To Live（TTL）バイトの値を設定します。 • *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。

	コマンドまたはアクション	目的
ステップ 11	**ip protocol** {**l2tp** | *protocol-number*} **例：** `Router(config-pw)# ip protocol l2tp`	（任意）パケットのトンネリングに使用される IP プロトコルを設定します。
ステップ 12	**sequencing** {**transmit** | **receive** | **both**} **例：** `Router(config-pw)# sequencing both`	（任意）疑似回線内でのデータ パケットのシーケンス処理がイネーブルにされる方向を指定します。 • **transmit**：使用されているデータ　カプセル化の方法に従って、疑似回線上で送信されるデータ 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るデータ 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持します。順序が正しくないパケットはドロップされます。 • **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。

xconnect 接続回線の設定

この設定手順では、イーサネットまたは VLAN 接続回線を xconnect サービス用の L2TPv3 疑似回線にバインドします。設定した仮想回線識別子により、PE ルータ上で設定された疑似回線と CE デバイス内の接続回線の間にバインディングが構築されます。L2TPv3 コントロール チャネルの一端にある PE ルータ上で設定した仮想回線識別子は、反対側にあるピア PE ルータ上でも設定する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type slot/port*
4. **xconnect** *peer-ip-address vcid pseudowire-parameters* [**sequencing** {**transmit** | **receive** | **both**}]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type slot/port* **例：** `Router(config)# interface ethernet 0/0`	タイプ（イーサネットなど）とスロット/ポート番号でインターフェイスを指定して、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：** `Router(config-if)# xconnect 10.0.3.201 123 pw-class vlan-xconnect`	ピア PE ルータの IP アドレス、およびコントロール チャネルの両端にある PE の間で共有される 32 ビットの仮想回線識別子を指定します。 • ピア ルータ ID（IP アドレス）と仮想回線 ID は、ルータ上で一意の組み合わせにならなければなりません。 • 次の仮想回線クラス パラメータの少なくとも 1 つを *pseudowire-parameters* 引数に設定する必要があります。 – **encapsulation** {**l2tpv3** [**manual**] | **mpls**}：疑似回線内でデータをカプセル化するために使用されるトンネリング方法を指定します。 • **l2tpv3**：L2TPv3 がトンネリング方法として使用されます。 • **manual**：（任意）L2TPv3 コントロール チャネル内でシグナリングを使用しません。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ルータを xconnect コンフィギュレーション モードにします。 • **mpls**：MPLS がトンネリング方法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の方法（L2TPv3 または MPLS）を指定します。L2TPv3 コントロール チャネル内でシグナリングを使用しない場合、**manual** を入力します。**encapsulation l2tpv3 manual** キーワードの組み合わせでは、xconnect コンフィギュレーション 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す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** 値を入力しない場合、「xconnect 接続回線の設定」の **password** コマンドで入力したカプセル化方法が使用されます。 • オプションの **pw-class** パラメータは、この xconnect 文を特定の疑似回線クラスにバインドします。それにより、その疑似回線クラスは、自身にバインドされたすべての接続回線に対するテンプレート設定となります。より詳細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** オプションのいずれかを設定する必要があります。両方のオプションを設定することもできます。 **（注）** データ カプセル化方法として L2TPv3 を選択する場合は、**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、送信、またはそれらの両方のパケットに対してシーケンス処理が必要かどうかを指定します。

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、**xconnect l2tpv3 manual** コマンドを使用して接続回線を xconnect サービス用の L2TPv3 疑似回線にバインドした場合は（「xconnect 接続回線の設定」を参照）、その後に 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. **configure terminal**
3. **interface** *type slot/port*
4. **xconnect** *peer-ip-address vc-id* **encapsulation l2tpv3 manual pw-class** *pw-class-name*
5. **l2tp id** *local-session-id remote-session-id*
6. **l2tp cookie local** *size low-value* [*high-value*]
7. **l2tp cookie remote** *size low-value* [*high-value*]
8. **l2tp hello** *l2tp-class-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type slot/port* 例： `Router(config)# interface ethernet 0/0`	タイプ（イーサネットなど）とスロット/ポート番号でインターフェイスを指定して、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： `Router(config-if)# xconnect 10.0.3.201 123 encapsulation l2tpv3 manual pw-class vlan-xconnect`	ピア PE ルータの IP アドレス、およびコントロール チャネルの両端にある PE の間で共有される 32 ビットの仮想回線識別子を指定します。 • ピア ルータ ID（IP アドレス）と仮想回線 ID は、ルータ上で一意の組み合わせにならなければなりません。 • **encapsulation l2tpv3 manual** パラメータは、疑似回線トンネリング方法として L2TPv3 を使用することを指定し、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。
ステップ 5	**l2tp id** *local-session-id remote-session-id* 例： `Router(config-if-xconn)# l2tp id 222 111`	ローカル L2TPv3 セッションとピア PE ルータ上のリモート L2TPv3 セッションに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。

	コマンドまたはアクション	目的
ステップ 6	**l2tp cookie local** *size low-value* [*high-value*] **例：** `Router(config-if-xconn)# l2tp cookie local 4 54321`	（任意）ピア PE が着信（受信）L2TP パケットのクッキー フィールドに格納しなければならない値を指定します。 • クッキー 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い場合、L2TP パケットのヘッダーにクッキー値は格納されません。 • 着信パケット内のクッキー長を 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	**l2tp cookie remote** *size low-value* [*high-value*] **例：** `Router(config-if-xconn)# l2tp cookie remote 4 12345`	（任意）ルータが発信（送信）L2TP パケットのクッキー フィールドに格納しなければならない値を指定します。 • クッキー 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い場合、L2TP パケットのヘッダーにクッキー値は格納されません。 • 発信パケット内のクッキー長を 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 8	**l2tp hello** *l2tp-class-name* **例：** `Router(config-if-xconn)# l2tp hello l2tp-defaults`	（任意）コントロール チャネル設定パラメータ（hello キープアライブ メッセージで使用する間隔など）に使用する 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 プレーンが存在しないこと、および L2TP hello メッセージの交換によるキープアライブ サポートの提供のためにコントロール チャネルが使用されることを前提としています。デフォルトでは、hello メッセージは送信されません。

L2TPv3 のプロトコル逆多重化の設定

プロトコル逆多重化機能により、IPv4 ネットワークから IPv6 トラフィックをオフロードする専用の IPv6 ネットワークを利用して、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 ルータ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、IPv4 ネットワーク内で通常どおりにルーティングされ、IPv4 ネットワークの既存のパフォーマンスと信頼性が維持されます。

IPv4 PE ルータは、IPv4 トラフィックから着信 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 ネットワークに接続している PE ルータには、IPv6 設定は必要ありません。IPv6 ネットワークの設定については、このマニュアルの範囲外になります。IPv6 ネットワークの設定に関する詳細については、『*Cisco IOS IPv6 Configuration Guide*』を参照してください。

IPv6 プロトコル逆多重化をイネーブルにするには、カスタマーに接続している IPv4 PE ルータ上で次の作業を実行します。

- 「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」（P.34）

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で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. **configure terminal**
3. **interface** *type slot*/*port*
4. **ip address** *ip-address mask* [**secondary**]
5. **xconnect** *peer-ip-address vcid* **pw-class** *pw-class-name*
6. **match protocol ipv6**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type slot*/*port* 例： `Router(config)# interface ethernet 0/1`	タイプ、スロット、およびポート番号でインターフェイスを指定して、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	**ip address** *ip-address mask* [**secondary**] 例： `Router(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。

	コマンドまたはアクション	目的
ステップ 5	**xconnect** *peer-ip-address vcid* **pw-class** *pw-class-name* **例：** `Router(config-if)# xconnect 10.0.3.201 888 pw-class demux`	ピア PE ルータの IP アドレス、およびコントロール チャネルの両端にある PE の間で共有される 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 ルータ ID（IP アドレス）と仮想回線 ID は、ルータ上で一意の組み合わせにならなければなりません。 • **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** パラメータは、この xconnect 文を特定の疑似回線クラスにバインドします。それにより、その疑似回線クラスは、自身にバインドされたすべての接続回線に対するテンプレート設定となります。 （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 パラメータを手動で設定する方法については、「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	**match protocol ipv6** **例：** `Router(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。

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

Dot1q および QinQ カプセル化用の L2TPv3 カスタム Ethertype 機能では、QinQ または Dot1Q カプセル化を伴うギガビット イーサネット インターフェイス上で 0x8100 以外の Ethertype を設定できます。このカスタム Ethertype は、0x9100、0x9200、または 0x88A8 に設定できます。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、この項の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **dot1q tunneling ethertype** {**0x88A8** | **0x9100** | **0x9200**}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**interface** *type number* **例：** `Router(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	**dot1q tunneling ethertype** {**0x88A8** | **0x9100** | **0x9200**} **例：** `Router(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。

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. **clear l2tun** {**l2tp-class** *l2tp-class-name* | **tunnel id** *tunnel-id* | **local ip** *ip-address* | **remote ip** *ip-address* | **all**}

手順の詳細

ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**clear l2tun** {**l2tp-class** *l2tp-class-name* | **tunnel id** *tunnel-id* | **local ip** *ip-address* | **remote ip** *ip-address* | **all**} **例：** `Router# clear l2tun tunnel id 56789`	指定した L2TPv3 トンネルをクリアします。（このコマンドは、L2TPv3 トンネル セッションが設定されていない場合は使用できません） • **l2tp-class** *l2tp-class-name*：指定した L2TP クラス名を持つすべての L2TPv3 トンネルが解放されます。 • **tunnel id** *tunnel-id*：指定したトンネル ID を持つ L2TPv3 トンネルが解放されます。 • **local ip** *ip-address*：指定したローカル IP アドレスを持つすべての L2TPv3 トンネルが解放されます。 • **remote ip** *ip-address*：指定したリモート 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。

L2TPv3 の設定例

ここでは、次の設定例について説明します。

（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。

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：例

L2TPv3 は、手動でプロビジョニングされたセッションの設定をサポートする唯一のカプセル化方法です。この例では、すべてのコントロール チャネル パラメータが事前に設定される静的セッション設定の設定方法を示します。使用されるコントロール プレーンはなく、コントロール チャネルを設定するネゴシエーション フェーズも存在しません。PE ルータは、イーサネット インターフェイス（int e0/0）がアップするとすぐに、トンネリングされたトラフィックの送信を開始します。123 の仮想回線識別子は使用されません。この PE は、セッション ID が 111 で、クッキーが 12345 の L2TP データ パケットを送信します。またこの PE は、セッション ID が 222 で、クッキーが 54321 の L2TP データ パケットを待ち受けます。

```
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
```

xconnect VLAN サブインターフェイスのネゴシエートされた L2TPv3 セッションの設定：例

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 トラフィックのみ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る L2TPv3 セッションにより、VLAN ID フィールドの値が 5 に書き換えられた転送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
```

L2TPv3 セッションの確認：例

ルータ上の現在の 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。

```
Router# 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
```

ルータ上の現在の 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。

```
Router# 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
```

L2TP コントロール チャネルの確認：例

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 ルータ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。ルータ上のすべての L2TP セッション用として他の L2TP 対応デバイスに対して設定されている 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。

```
Router# 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
```

ルータ上のすべての L2TP セッション用として他の L2TP 対応デバイスに対して設定されている 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。

```
Router# 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
```

L2TPv3 コントロール チャネル認証の設定：例

次の例では、L2TPv3 コントロール チャネルの CHAP 型認証を設定します。

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

次の例では、L2TPv3 制御メッセージ 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します。

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

次の例では、L2TPv3 制御メッセージ ハッシング機能を使用して、コントロール チャネル完全性チェックを設定し、メッセージ ダイジェストの確認をディセーブルにします。

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

次の例では、L2TPv3 制御メッセージ 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します。

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

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：例

次の例では、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を使用して、L2TP クラス class1 の L2TP コントロール チャネル認証パスワードを変更します。この例では、L2TP クラス class1 に古いパスワードがすでに設定されているものとします。

```
Router(config)# l2tp-class class1
Router(config-l2tp-class)# digest secret cisco2 hash sha
!
! Verify that all peer PE routers have been updated to use the new password before
! removing the old password.
```

```
!
Router(config-l2tp-class)# no digest secret cisco hash sha
```

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：例

次の **show l2tun tunnel all** 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。

```
Router# 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
```

IP パケットのフラグメント化用の疑似回線クラスの設定：例

次に、CE ルータで生成された IP トラフィックを疑似回線に入る前に断片化できる疑似回線クラスの設定例を示します。

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

L2TPv3 のプロトコル逆多重化の設定：例

次の例は、IPv4 PE ルータ上でプロトコル逆多重化機能を設定する方法を示しています。IPv6 ネットワークに接続している PE ルータには、IPv6 設定は必要ありません。

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

L2TPv3 トンネルの手動クリア：例

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
```

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

次の例は、QinQ または Dot1Q カプセル化を伴うギガビット イーサネット インターフェイス上で 0x8100 以外の Ethertype を設定する方法を示しています。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 上で Ethertype フィールドが 0x9100 に設定されます。

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

その他の参考資料

関連資料

関連項目	参照先
L2TPv3	『Layer 2 Tunneling Protocol Version 3 Technical Overview』
L2VPN インターワーキング	『*Cisco IOS Multiprotocol Label Switching Configuration Guide*』の「L2VPN Interworking」
L2VPN 疑似回線スイッチング	『*Cisco IOS Multiprotocol Label Switching Configuration Guide*』の「L2VPN Pseudowire Switching」
L2TP	• 『Layer 2 Tunnel Protocol』 • 『Layer 2 Tunneling Protocol: A Feature in Cisco IOS Software』
CEF の設定	『*Cisco IOS IP Switching Configuration Guide*』の「Part 1: Cisco Express Forwarding」
MTU 検出とパケット フラグメント化	『MTU Tuning for L2TP』
その他の VPN コマンド：完全なコマンドの構文、コマンド モード、デフォルト、使用上の注意事項、例	『*Cisco IOS Dial Technologies Command Reference*』
その他のフレーム リレー コマンド：完全なコマンドの構文、コマンド モード、デフォルト、使用上の注意事項、例	『*Cisco IOS Wide-Area Networking Command Reference*』
IPv6	『*Cisco IOS IPv6 Configuration Guide*』
その他の IPv6 コマンド：完全なコマンドの構文、コマンド モード、デフォルト、使用上の注意事項、例	『*Cisco IOS IPv6 Command Reference*』

規格

規格	タイトル
draft-ietf-l2tpext-l2tp-base-03.txt	『Layer Two Tunneling Protocol (Version 3) "L2TPv3"』

MIB

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

RFC

RFC	タイトル
RFC 1321	『*The MD5 Message Digest Algorithm*』
RFC 2104	『*HMAC-Keyed Hashing for Message Authentication*』
RFC 2661	『*Layer Two Tunneling Protocol "L2TP"*』
RFC 3931	『*Layer Two Tunneling Protocol Version 3 "L2TPv3"*』

シスコのテクニカル サポート

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

L2TPv3 の機能情報

表 3 に、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。

プラットフォーム サポートとソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームをサポートするソフトウェア イメージを判別できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

L2TPv3 機能とその関連機能に対して、**clear l2tun**、**debug vpdn**、**ip pmtu**、**i l2tp cookie local**、**l2tp cookie remote**、**l2tp hello**、**l2tp id**、および **xconnect** の各コマンドが追加または変更されました。

（注） 表 3 に、特定の Cisco IOS XE ソフトウェア リリース群で特定の機能をサポートする Cisco IOS XE ソフトウェア リリースだけを示します。特に明記されていない限り、Cisco IOS XE ソフトウェア リリース群の後続のリリースでもこの機能をサポートします。

表 3　　L2TPv3 の機能情報

リリース	変更内容
Cisco IOS XE リリース 2	
2.6	次の機能が追加されました。 • L2TPv3 上のイーサネット • Layer 2 VPN（L2VPN）：AToM と L2TPv3 用の Syslog、SNMP トラップ、および show コマンドの機能強化 • L2TPv3 制御メッセージ ハッシング • L2TPv3 制御メッセージ 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 のプロトコル逆多重化 • L2TPv3：Dot1q および QinQ カプセル化用のカスタム Ethertype
2.6.2	**ip pmtu** コマンドに対するサポートが追加されました。

用語集

AV ペア：Attribute-Value（AV; アトリビュート値）ペア。

CEF：Cisco Express Forwarding。大規模で動的なトラフィック パターンを持つネットワークに対してネットワーク パフォーマンスとスケーラビリティを最適化するレイヤ 3 IP スイッチング テクノロジー。

DCE：Data Circuit-terminating Equipment（DCE; データ回線終端装置）（ITU-T 拡張）。ユーザネットワーク インターフェイスのネットワーク端を構成する通信ネットワークのデバイスと接続部。

DF ビット：Don't Fragment ビット。パケットを断片化してはならないことを指定するために設定できる IP ヘッダー内のビット。

DTE：Data Terminal Equipment（DTE; データ端末装置）。データの送信元、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。

ICMP：Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）。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（IDB; インターフェイス記述子ブロック）。

L2TP：2 つのトンネリング プロトコル（シスコシステムズの Layer 2 Forwarding（L2F; レイヤ 2 フォワーディング）と Microsoft の Point-to-Point Tunneling Protocol（PPTP; ポイントツーポイント トンネリング プロトコル））の PPP 結合機能に対する拡張。L2TP は、シスコシステムズとその他のネットワーキング業界のリーダーから支持されている Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）標準です。

L2TPv3：RFC 2661（L2TP）内の機能を強化した L2TP の草案バージョン。

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

MPLS：Multiprotocol Label Switching（MPLS; 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。このラベルによって、ネットワーク内のルータおよびスイッチが、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を指示されます。

MQC：Modular Quality Of Service Command-Line Interface（MQC）。

MTU：Maximum Transmission Unit（MTU; 最大伝送ユニット）。特定のインターフェイスで処理可能な最大パケット サイズ（バイト単位）。

PMTU：Path MTU（PMTU; パス MTU）。

PW：Pseudowire（PW; 疑似回線）。

SNMP：Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）。ほぼ例外なく、TCP/IP ネットワークで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 デバイスのモニタおよび制御手段と、設定、統計情報収集、パフォーマンス、およびセキュリティの管理手段を提供します。

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

VPDN：Virtual Private Dialup Network（VPDN）。共通のアクセス インフラストラクチャ（モデム、アクセス サーバ、ISDN ルータなど）を別々の自律したプロトコル ドメインで共有することを可能にするネットワーク。VPDN により、リモート アクセス トラフィックを ISP クラウド経由でトンネリングする ISP を利用したセキュアなネットワークを構成できます。

WAN：Wide-Area Network（WAN; ワイドエリア ネットワーク）。地理的に広大な地域にわたるユーザにサービスを提供するデータ通信ネットワーク。多くの場合、コモン キャリアによって提供される伝送デバイスが使用されます。WAN の例として、SMDS や X.25 があります。

データリンク制御層：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でのデータの伝送を担当します。OSI モデルのデータリンク層にほぼ対応します。

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。
