

レイヤ 2 トンネリング プロトコル バージョン 3 技術概要

はじめに

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) を使用することで、ネイティブ IP コア ネットワークを有するサービス プロバイダーおよび大企業は、高速なレイヤ 2 トンネリングまたはレイヤ 2 Virtual Private Network (VPN; 仮想私設網) サービスを、レイヤ 3 VPN と一緒にエンド ユーザ カスタマーに提供できます。L2TPv3 VPN サービスは、Cisco IOS ソフトウェアをアップグレードするだけで、設備費用をかけることなく提供することができます。

L2TPv3 は、次世代ネットワークのトンネリングおよび VPN テクノロジーにおける主要技術のひとつとなりつつあります。L2TPv3 は、フレーム リレーや Asynchronous Transfer Mode (ATM; 非同期転送モード) のプライバシー性と共に、IP の柔軟性とスケーラビリティを提供します。L2TPv3 の使用により、ネットワーク サービスを、ルーティングされた IP ネットワーク上で配信することができます。サービスの判断は VPN とトンネルのエンドポイントで実行され、中間での前処理なしで切り換えることができるため、高い効率性とスケーラビリティが提供されます。

顧客のネットワーク構築の複雑化やコストを軽減することで、L2TPv3 VPN は、サービス プロバイダーが小規模から中規模の企業まで幅広く、サービスを提供できるようにします。各オフィス間の個々のポイントツーポイントの回線を設定管理することなく、企業はオフィスのルータからサービス プロバイダーの末端ルータへの物理リンクを 1 つ提供するだけで

済みます。サービス プロバイダーは、従来のアプリケーションにあった複雑さを伴わない、管理されたインターネット、イントラネット、およびエクストラネットと共に VPN を顧客に提供することで、サービスを拡大し、新しい収入源を生み出すことができます。

サービス プロバイダーは L2TPv3 を導入することで、次の利点を得ることができます。

- トランスペアレントな LAN と IP 機能を実装したシンプルなトンネリングメカニズムにより、IP VPN サービスを容易に実現します。
- サービス プロバイダーのネットワーク間、およびサービス プロバイダーと顧客のネットワーク間の相互運用を簡略にします。
- パケット コア 拡張 VPN サポートを構築する一方で、従来からの投資を無駄にしません。
- 新しいサービスを容易にします。
- Internetwork Packet Exchange (IPX) や SNA のような非 IP プロトコルの、IP ネットワーク上における伝送を可能にします。

企業顧客は L2TPv3 を導入することで、次の利点を得ることができます。

- サービス プロバイダーおよび顧客のネットワーク間の相互運用を簡略にします。
- 顧客は、VPN を展開する手段として、サービス プロバイダーを活用するか、または企業の設備を活用するかを選択できます。



- IPX や SNA のような非 IP プロトコルの、IP ネットワーク上における伝送を可能にします。
- 設定を容易に行うことができます。
- 拡張 VPN サポートは、セキュリティや Quality of Service (QoS; サービス品質)、管理 VPN などの IOS 機能により、顧客の要件にあわせてカスタマイズできます。

技術概要

IP ネットワーク上の一対のルータ上で L2TPv3 トンネルをセットアップすることにより、この 2 つのルータのインターフェイス間で、高速でトランスパレントなレイヤ 2 接続を提供することができます。この機能は、レイヤ 2 の VPN の構築に使用され、さらには、従来の (フレームリレー、ATM、専用線) ネットワークの移行をサポートするために活用されます。L2TPv3 のトンネル機能は、IOS の基本 IP パッケージで利用できます。

Cisco 7000 および 12000 シリーズ ルータにおける L2TPv3 の動作

ここでは、インターフェイス ベースの L2TPv3 について説明します。2 つの顧客 ネットワーク サイト間に流れているトラフィックは IP パケットにカプセル化され、IP ネットワークに送信されます。IP ネットワークの内部ルータは、他の IP パケットと同じようにこのトラフィックを扱うため、顧客 ネットワーク側について関知する必要はありません。このプロセスは、レイヤ 2 トンネリング (図 1) として知られています。

図 1
L2TPv3 の動作

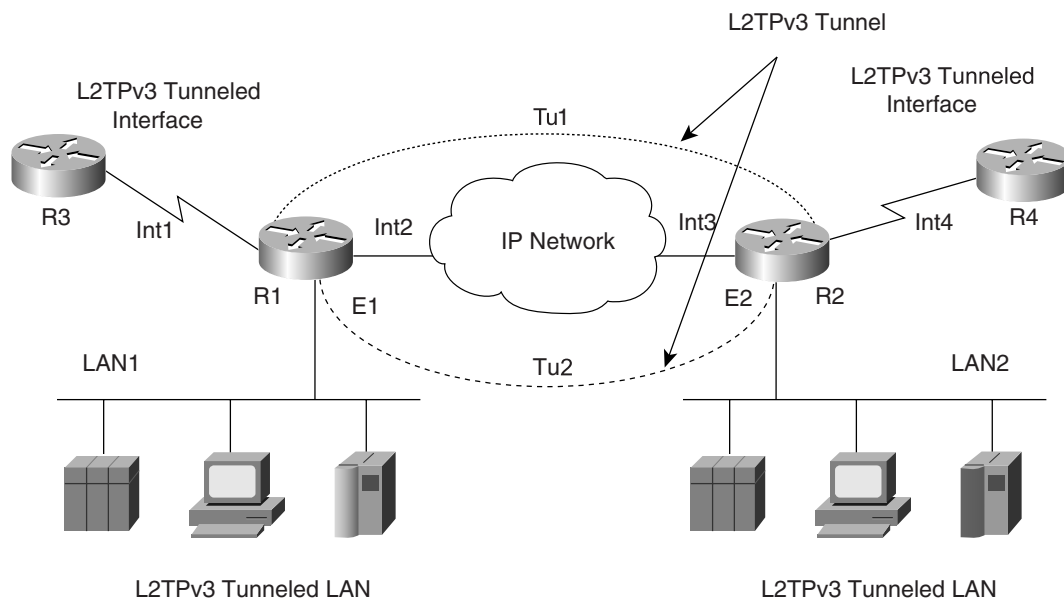


図 1 では、ルータの R1 および R2 が L2TPv3 サービスを提供しています。これらのルータは、インターフェイス Int2、IP ネットワークおよびインターフェイス Int3 から構成されるパスを介して、IP プロトコルを使って互いに通信します。この例では、ルータ R3 および R4 は、L2TPv3 トンネルを使用した Packet Over SONET (POS) インターフェイスで通信します。L2TPv3 トンネル Tu1 は、R1 のインターフェイス Int1 と R2 のインターフェイス Int4 の間で構成されます。R1 のインターフェイス Int1 に着信したパケットはすべて L2TPv3 でカプセル化され、トンネル (Tu1) を経由して R2 に送信されます。R2 はパケットのカプセル化を解除し、それをインターフェイス Int4 から R4 に転送します。R4 がパケットを R3 に送信する必要がある場合、同様のパスを使い、これとは逆の順番でパケットが転送されます。



次の L2TPv3 の動作について注意してください。

- インターフェイス *Int1* で受信されるすべてのパケットは *R4* に転送されます。*R3* および *R4* は、介在するネットワークを見ることはできません。
- Cisco 12000 シリーズ インターネット ルータでは、他の L2TPv3 用ではないカードの LAN ポートには、ルータが接続されている必要があります。CAM（連想メモリ）によって補助された MAC（メディア アクセス制御）フィルタリングは、L2TPv3 を動作させると、すべてのポート上でオフになります。
- これと同様の方式はイーサネット インターフェイスでも使用されています。イーサネット インターフェイス *E1* 上の *R1* で *LAN1* から受信したすべてのパケットは、L2TPv3 でカプセル化され、トンネル *Tu2* を経由して *R2* のインターフェイス *E2* に送信されます。その後、パケットは *LAN2* 上に転送されます。
- これと同様の方式はフレーム リレーのサブインターフェイスでも使用されています。サブインターフェイス上の *R1* で *LAN1* から受信したすべてのパケットは、L2TPv3 でカプセル化され、トンネルを経由して *R2* サブインターフェイスに送信されます。その後、パケットは *LAN2* に転送されます。

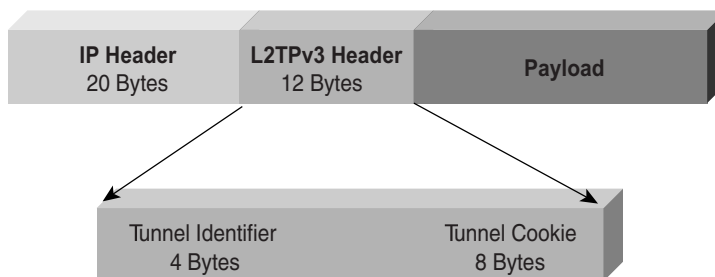
L2TPv3 のヘッダーの解説

データは、L2TPv3 トンネルの入力インターフェイスに入る時、新たに L2TPv3 ヘッダーが加わり、カプセル化されます（図 2）。追加される L2TPv3 のヘッダーの構成は次のとおりです。

- ペイロードから独立したヘッダー（12 バイト）
- IP 配信ヘッダー（20 バイト）

L2TPv3 ヘッダーのフォーマットを図 2 に示します。

図 2
L2TPv3 のパケット カプセル化



L2TPv3 ヘッダーのパラメータは次のとおりです。

- 配信ヘッダー— 配信ネットワーク上で L2TPv3 パケットを運ぶための、IPv4 のヘッダーです。配信ヘッダーは 20 バイトです。
- L2TPv3 ヘッダー— カプセル化を解除する地点で、トンネル内容を一意に識別するために必要な情報を保有します。このペイロードから独立したヘッダーは 12 バイトです。
- ペイロード— L2TPv3 に運ばれます。リンク層のフレーム、またはネットワーク層のパケットです。
- トンネル ID— カプセル化の解除を行うシステム上で、トンネル内容を識別するために使用されます。トンネル ID の値は、カプセル化解除システムにおける内容識別の効率性を最適にするために選択されます。そのために、カプセル化解除の実装は、より小さいトンネル ID のビット フィールドをサポートする場合があります。この実装では、1023 の L2TPv3 トンネル ID でより上位の値を設定することで選択されます。L2TPv3 トンネル ID の値で、0 はプロトコルによって使われるため予約されています。



- トンネル キッキー— L2TPv3 トンネルの 2 つのエンドポイント間で共有される、8 ビットのシグニチャです。このトンネル キッキーは、設定にエラーがあるために発生する、カプセル化解除されたトラフィックの障害を抑制します。このシグニチャは、送信元と宛先ルータの両方で設定され、一致している必要があります。一致していない場合、そのデータは廃棄されます。

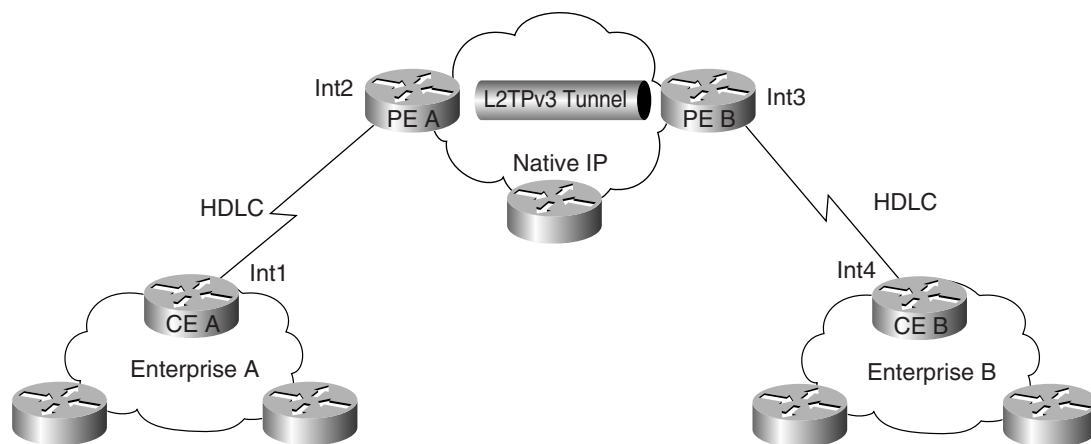
raw モードのサポート

raw モードは、運び込まれる情報のタイプに関わらず、任意の物理インターフェイス上に着信する情報をトンネル化する機能です。raw モードでは、L2TPv3 トンネルの両端に物理インターフェイスが接続されています。このインターフェイスに着信するすべてのパケットおよびフレームがトンネルを通過します。当該トンネルのエンドポイント両端に関連付けられた物理インターフェイスは、同一のタイプである必要があります（ただし、IOS 12.0(xx)S 以降では異なるインターフェイス間でのトンネル設定が可能となっています）。シスコが現在 raw モードでサポートしているインターフェイスは、シリアル、POS、およびイーサネット インターフェイスです。

raw モードは、仮想専用線をサポートするために効果的に使うことができます。仮想専用線は、企業に共通の要望で、混雑していないチャネルサービスを介して、複数のリモート サイトをまとめて接続するものです。

図 3 では、このサービスを提供する L2TPv3 の機能を示しています。

図 3
L2TPv3 の論理トポロジーでの仮想専用線



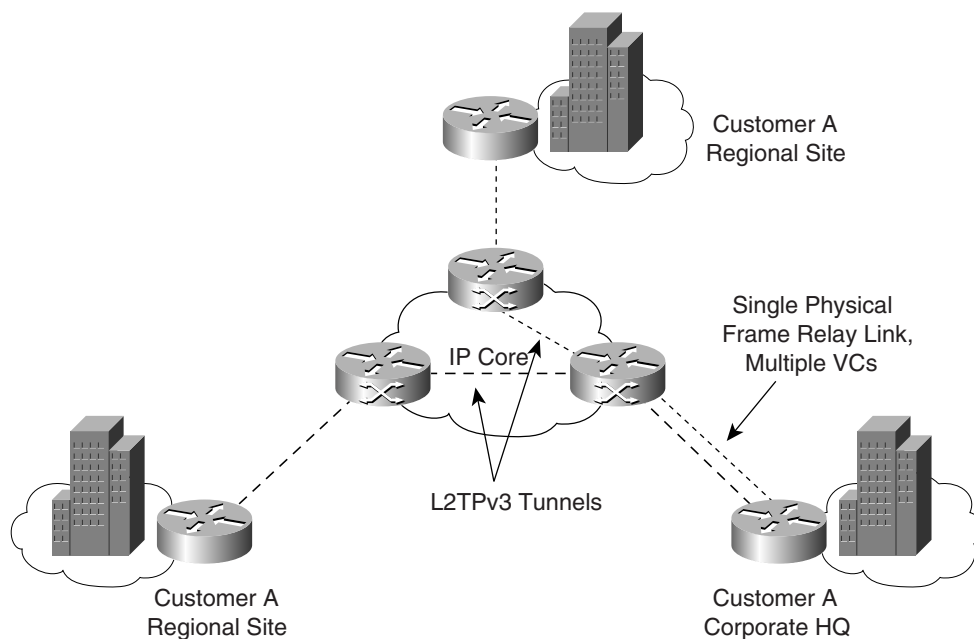
ここでは、2 つの DS-3 シリアル インターフェイスが顧客側のネットワークに接続されています（Enterprise A）。Int2 および Int3 は、L2TPv3 トンネルの入出力ポイントを形成します。サービス プロバイダーは、標準のルーティング プロトコルを使用し、PE A および PE B 間の IP 接続を維持します。これによってレイヤ 2 VPN を確立するための構造が形成されます。顧客側のエッジルータ（CE A）から DS3 上を通過するパケットは、自動的に L2TPv3 ヘッダーでカプセル化され、IP ネットワークから PE B 上の出力インターフェイスに転送、カプセル化が解除されます。そしてオリジナルの High-Level Data Link Control（HDLC; ハイレベル データリンク制御）フレーム全体がシリアル インターフェイス（Int3）から、顧客側のエッジルータ CE B に転送されます。レイヤ 2 回線のエミュレーションは、このように行われています。



フレーム リレー サポート

L2TPv3 におけるフレーム リレー サポートは、単一の物理インターフェイスに割り当てられている個々の Virtual Circuit (VC; 仮想回線) のトンネリングをサポートするよう設計されています。この場合、指定のインターフェイス上に関連した VC は、異なる宛先にトンネリングすることができます。図 4 では、個々の VC をトンネリングする機能を使い、IP コアでハブアンドスポーク形式のネットワーク トポロジーを展開しています。

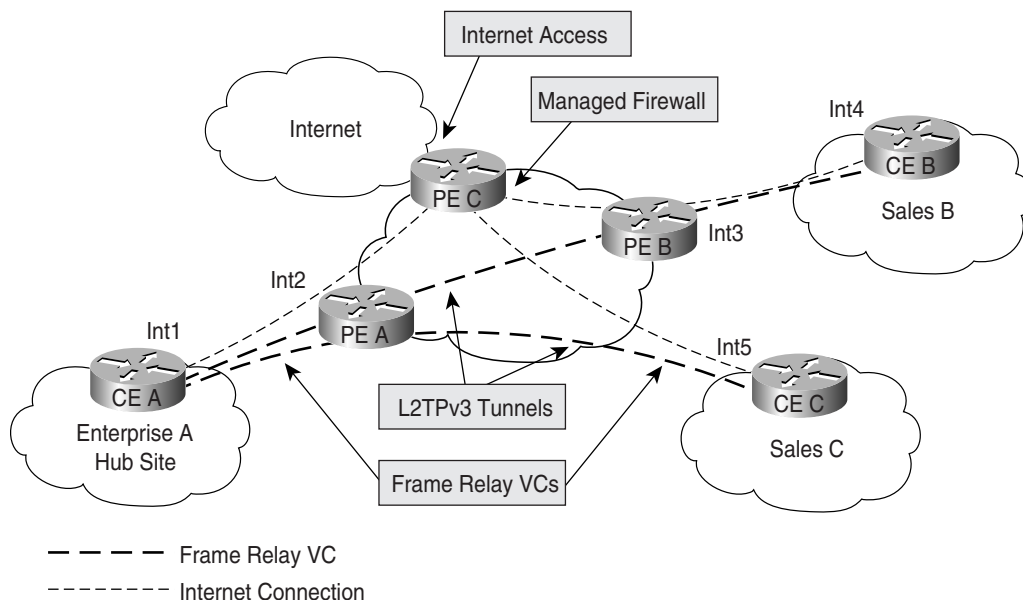
図 4
L2TPv3 のパケット カプセル化



次に、サービスプロバイダーがサポートする可能性があるより高度なサービスの概要を示します。顧客はハブアンドスポーク方式のネットワークのフレーム リレーを使う、従来からの企業です。サービスプロバイダーは、管理されたファイアウォールとマルチメディア サービスを組み込んだインターネット アクセスを提供しようとしています。図 5 では、このサービス アーキテクチャを示しています。



図 5
外部委託されたインターネットおよびファイアウォールのフレーム リレー ハブアンドスポーク アーキテクチャ



企業は、フレーム リレーのカプセル化とポイントツーポイントのサブインターフェイスで構成される従来からのシリアル インターフェイスを使い、サービス プロバイダーと接続しています。このフレーム リレーでは、会社のイントラネットに使用されるサブインターフェイスや、インターネット アクセスを提供するサブインターフェイスが指定されます。この構成は、従来のハブアンドスポーク構成におけるインターネット アクセスの集中化を回避し、ハブ側に必要な帯域幅を軽減します。企業は、固有のルーティング ポリシーを実行したり、高度なセキュリティを実践するため IP Security (IPSec) の暗号化を追加したりすることもできます。

フレーム リレー サブインターフェイスの制限事項

- フレーム リレーのサブインターフェイスがトンネル用に設定されている場合、一意の L2TPv3 トンネルにマッピングされている必要があります (各 L2TPv3 トンネルは、1 対 1 でフレーム リレー サブインターフェイスにマッピングされている必要があります)。
- 入力ルータにある Data-Link Connection Identifier (DLCI) は、出力ルータと同一の DLCI である必要があります。
- L2TPv3 フレーム リレー サブインターフェイスは 10 ビットの DLCI アドレスをサポートします。フレーム リレー拡張アドレス指定はサポートされていません。
- マルチポイント DLCI はサポートされていません。

イーサネット サポート

Cisco 10720 インターネット ルータにおける L2TPv3 の動作

Cisco 10720 インターネット ルータが L2TPv3 機能をサポートすることで、サービス プロバイダーは、イーサネットや VLAN (仮想 LAN) を L2TPv3 トンネルで複数箇所に拡張し、顧客にイーサネット サービスを提供できます。



図 6
Cisco 10720 インターネット ルータ上での L2TPv3 の動作

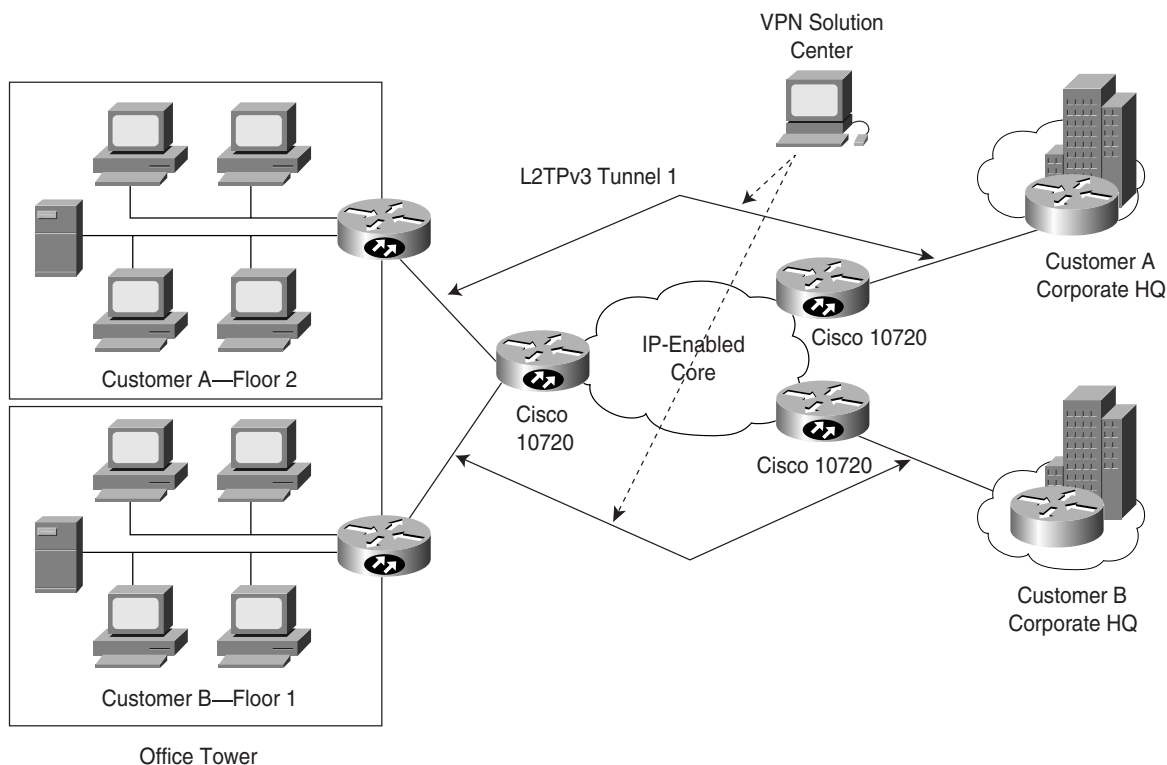


図 6 では、L2TPv3 トンネル末端にある 2 つのルータが、ポイントツーポイントの POS リンクを介して接続されています。サポートされる機能は、L2TPv3 トンネル上のレイヤ 2 間の拡張です。インターフェイス全体、または VLAN のサブインターフェイスを L2TPv3 トンネルにマッピングし、IP ネットワークヘイサネットを拡張できます。このメカニズムにより、サービスプロバイダーはイーサネット サービスを広範囲に提供することができます。

IP バックボーンの顧客を接続するために L2TPv3 を使用した場合、顧客側のネットワークに接続している物理インターフェイスがトンネルの入出力インターフェイスになります。Cisco 10720 インターネット ルータの入出力インターフェイスとして使用可能なインターフェイスは、イーサネット、または 802.1Q カプセル化サブインターフェイスとして使用できます。

通常、インターネット サービスプロバイダーのルータは、IP コア ネットワーク上で設定された IP ルーティング プロトコルを使用して通信します。顧客のルータ (CE ルータ) は、設定された L2TPv3 トンネル上で通信します。Cisco 10720 インターネット ルータで受信されたデータ パケットは、すべて L2TPv3 ヘッダーでカプセル化され、L2TPv3 Tunnel 1 または L2TPv3 Tunnel 2 のいずれかの L2TPv3 トンネルを経由して送信されます。カスタマー サイトから着信したデータ パケットは、メインのイーサネット インターフェイス上を通過できます。ここでは、パケットは L2TPv3 ヘッダーでカプセル化され、他のサイトに送信されています。

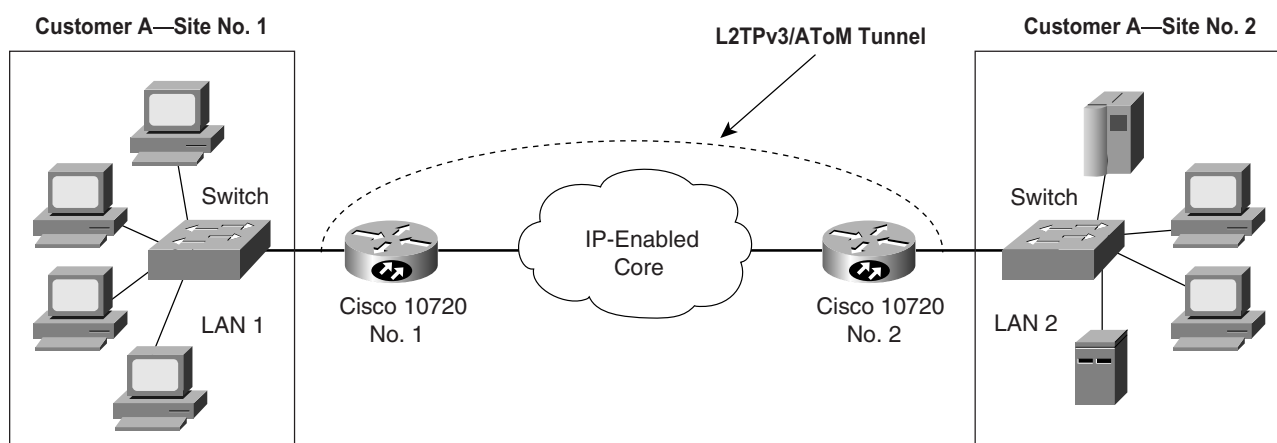
顧客のデータ パケットが、802.1Q カプセル化方式のインターフェイス上から来た場合でも、パケットは L2TPv3 ヘッダーでカプセル化され、他の Cisco 10720 インターネット ルータへ送信されます。受信側の末端で、Cisco 10720 インターネット ルータは L2TPv3 ヘッダーのカプセル化を解除し、他の顧客の CE ルータに向けて、802.1Q カプセル化方式のトラフィックを転送します。



L2TPv3 上のイーサネット

図 7 では、L2TPv3 トンネルを使用した LAN 間接続の動作を示しています。LAN 1 から着信するパケットは、Cisco 10720 インターネット ルータ No.1 のイーサネット インターフェイスに向かいます。顧客からのデータ パケットは、L2TPv3 ヘッダーでカプセル化され、IP コアバックボーン上に送信されます。データ パケットは、ここから Cisco 10720 インターネット ルータ No.2 の出力イーサネット インターフェイスに向けて IP ルーティングされます。

図 7
L2TPv3 上のイーサネット



受信側にある Cisco 10720 インターネット ルータは、データ パケットのカプセル化を解除し、トラフィックを LAN 2 に転送します。トラフィックが LAN 2 から発生した場合、これと同様な方法が使用されます。LAN 1 および LAN 2 が IP バックボーンのネットワーク上で接続され、Cisco 10720 インターネット ルータは、ルーティングや顧客の IP アドレスに関する知識という点で顧客と関わる必要なく、レイヤ 2 のデータ パケットをリレーできます。2 つのカスタマー サイトは、同じ回線に接続しているとみなされます。また、必要であれば、サイトを複数に拡張することも可能です。この事例で大きく異なる点は、カスタマー サイト上にレイヤ 3 のルータが存在しないことです。そのため、L2TPv3 は、サービス プロバイダー上の IP 対応コアヘレイヤ 2 接続を拡張します。

L2TPv3 VLAN トンネル出力時における VLAN ID の上書き

VLAN ID の上書き機能は、Cisco 10720 インターネット ルータ上の 802.1Q VLAN インターフェイスに接続された L2TPv3 のトンネルに適用されます。VLAN にマッピングされた L2TPv3 トンネルの出力側は、出力 802.1Q パケットの VLAN ID をローカル VLAN の ID に上書きします。

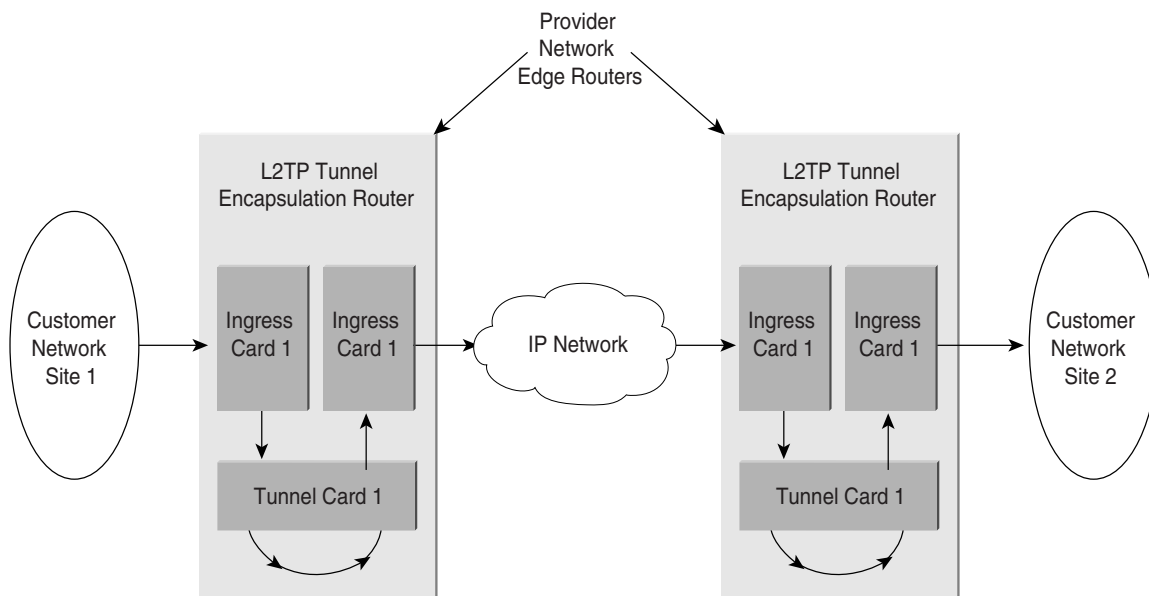
この機能により、L2TPv3 トンネルの両側で異なる VLAN ID を VLAN インターフェイスに使用できます。この VLAN ID の上書き機能を使用する場合、シスコは、Cisco 10720 インターネット ルータのバックボーン インターフェイスとして Spatial Reuse Protocol (SRP) を使用することを推奨します。

Cisco 12000 シリーズ インターネット ルータのトンネル用カード

Cisco 12000 シリーズ インターネット ルータで L2TPv3 を実行する場合、トンネル用のカードが別途必要になります。このトンネル用のカードは Cisco 12000 シリーズ専用であり、Cisco 7200 または 7500 シリーズのルータでは不要です。



図 8
Cisco 12000 シリーズ インターネット ルータで処理される L2TPv3 パケット



注意：図 8 の矢印は、パケットの流れと方向（一方向）を表しています。実際のトンネルのトラフィックは、どちらの方向にも流れます。

カプセル化ルータの動作

図 8 では、Site 1 上の顧客のネットワークからのトラフィックが、プロバイダーのネットワーク エッジ ルータ上の入力インターフェイスに送信されます。インターフェイスが L2TPv3 のトンネリング用に設定されている場合、着信するパケットはすべて、トンネル用カードに転送されます。トンネル用カードは、IP と L2TPv3 ヘッダー情報を含むカプセル化ヘッダーでパケットをカプセル化します。その後、カプセル化されたパケットは適切な出力カードに送信され、通常の IP パケットとして IP ネットワークに送信されます。

トンネルのカプセル化解除ルータの動作

L2TPv3 でカプセル化されたパケットがトンネル用カードに着信すると、パケットのセッション ID および L2TPv3 キーが有効かどうか照合されます。これらのうち一部でも異なる部分がある場合、パケットはそのまま廃棄されます（ユーザに知らされることはありません）。セッション ID と L2TPv3 キーが間違いない場合、トンネル用カードはパケットのカプセル化を解除（IP と L2TPv3 ヘッダーを外す）し、パケットを出力カードに送信します。その後、出力カードは顧客側のネットワークにパケットを送信します。この際、新たにレイヤ 2 のヘッダーが追加されることはありません（レイヤ 2 のヘッダーはトンネルの最初の時点から保持されています）。

注意：トンネル用のカードが非 L2TPv3 のパケット（他の IP、または ping のループバックアドレスのような Internet Control Message Protocol [ICMP]）を受信した場合、そのパケットはライン カードの CPU、およびルート プロセッサに送信されます。



一般的な制限事項

L2TPv3 には次の制限事項があります。

- 設定可能な L2TPv3 トンネルの最大数は、1022 までに制限されています。
- 顧客側のインターフェイスの Maximum Transmission Unit (MTU; 最大伝送ユニット) を設定し、トンネル内で断片化をさせないようにする必要があります。L2TPv3 トンネルは断片化をサポートしていないためです (ソリューションは、現在、開発中)。

IP バックボーンの MTU は、擬似回線上で動作する MTU より x バイト大きな値にする必要があります。x の値は次のとおりです。

- 802.1Q = 50
- イーサネット = 46
- POS = 36
- フレーム リレー = 34
- CHDLC = 36

- 固有のシグナリング、またはキープアライブ メカニズムはありません (現在、開発中)。

可用性

サポートされるプラットフォームおよびリリース

- Cisco 12000 シリーズ インターネット ルータ
- Cisco 10720 メトロ イーサネット ルータ
- Cisco 7200 シリーズ ルータ
- Cisco 7500 シリーズ ルータ

Cisco IOS Software Release 12.0(18)ST

- raw モード — ポート レベルでの L2TPv3 トンネリング (トンネルの各末端のインターフェイスなど)
- プラットフォーム — Cisco 12000、7500、および 7200 シリーズ ルータ

Cisco IOS Software Release 12.0(19)ST

- フレーム リレー — フレーム リレーのポイントツーポイント サブインターフェイス用の L2TPv3 トンネリング (各フレーム リレー Permanent Virtual Circuit [PVC; 相手先固定接続] は一意のトンネルにマッピングされます)
- プラットフォーム — Cisco 12000、7500、および 7200 シリーズ ルータ

Cisco IOS Software Release 12.0(21)ST

- 802.1Q VLAN — 802.1Q のポイントツーポイント サブインターフェイス用の L2TPv3 トンネリング
- プラットフォーム — Cisco 12000、7500、および 7200 シリーズ ルータ

Cisco IOS Software Release 12.0(19)SP

- raw モード — ポート レベルでの L2TPv3 トンネリング (トンネルの各末端のインターフェイスなど)
- 802.1Q VLAN — 802.1Q のポイントツーポイント サブインターフェイス用の L2TPv3 トンネリング
- プラットフォーム — Cisco 10720 インターネット ルータ

注意: L2TPv3 トンネルは基本 IP パッケージでサポートされています。

CISCO SYSTEMS



Corporate Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters

Cisco Systems Europe
11 Rue Camille Desmoulins
92782 Issy-les-Moulineaux
Cedex 9
France
www-europe.cisco.com
Tel: 31 1 58 04 60 00
Fax: 31 1 58 04 61 00

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2002, Cisco Systems, Inc. All rights reserved. CCIP, the Cisco *Powered* Network mark, the Cisco Systems Verified logo, Cisco Unity, Fast Step, Follow Me Browsing, FormShare, Internet Quotient, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ logo, iQ Net Readiness Scorecard, Networking Academy, ScriptShare, SMARTnet, TransPath, and Voice LAN are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That's Possible, The Fastest Way to Increase Your Internet Quotient, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, GigaStack, IOS, IP/TV, LightStream, MGX, MICA, the Networkers logo, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stram, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0201R) 202777/ETMG 03/02