

レイヤ2トンネリング プロトコルバージョン3による IP ネットワークでのレイヤ2 サービス

世界中でインターネットが勢いづいた 1990 年代以降、サービスプロバイダーが競争に勝ち残るための環境は大きく変わりました。目新しさや競争に取り残される不安から、新規に IP ベースのサービスを契約する企業はもう見当たりません。サービスプロバイダーが目下必要に迫られていることは、支出に対してより慎重な環境の中で自分たちの顧客の基盤とサービスによる収益を拡大し、ビジネスを成長させることです。多くの企業はネットワークへの投資に対し、より保守的なアプローチをとっています。新しい IP ベースのサービスは、企業に生産性と競争力を改善する機会を提供し、さらに既存のネットワークにかかる経費も削減します。このようなサービスやコストの削減を提供するサービスプロバイダーが、顧客の基盤とサービスによる収益を拡大させることができます。別々に分かれていた従来のネットワークの維持費を削減するために、既存のネットワークをネイティブ IP ネットワーク コアに統合し、さらに IP ベースのサービスを企業顧客に提供する — この資料は、そういった機会を持つことに焦点を合わせています。

はじめに

世界中の企業や政府の多くは、現在もなお、従来のレイヤ2 接続のサービスを使用しています。ATM やフレームリレー、専用線のようなサービスは、プライベート ネットワークが構築されるポイントツーポイントの接続を提供します。

今日の企業のネットワーク管理者は、企業でイントラネットを実践し運用する場合に、多くの問題や選択肢について考慮しなければなりません。こういったことは内部で扱うべきでしょうか、またはサービスプロバイダーに外部委託すべきでしょうか。アプリケーションに特定したサービス レベルを考慮すべきでしょうか。どのレベルのネットワーク セキュリティが必要でしょうか。少ない予算でサポートできる機能は何でしょうか。

企業顧客の多くは Asynchronous Transfer Mode (ATM; 非同期転送モード)、イーサネット、フレームリレー、および専用線のようなレイヤ2 サービスを使用し、サービスプロバイダーによって会社のイントラネットを相互に接続しています。サービスプロバイダー コアで共通のペケット ベースのインフラストラクチャが使用されれば、現在、末端に存在しているレイヤ2 のフレームを、ペケット スイッチ形式のネットワークでトンネリングさせることができます。

Cisco IOS[®] ソフトウェアは、Internet Engineering Task Force (IETF) 標準トラック プロトコルの 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) を提供することでこれを実現します。また、L2TPv3 により、サービスプロバイダーは IP インフラストラクチャから従来のレイヤ2 サービスを提供することができます。これにより、サービスプロバイダーで次のような点が強化されます。

- コスト効率性に優れたマルチサービスの IP インフラストラクチャを使用することで、従来からのレイヤ2 サービスの供給コストを削減します。
- レガシー ネットワークを増設することなく、既存のレイヤ2 ネットワークを拡張します。
- 顧客へ提供するサービス群を1つにまとめることで、コストを削減します。

フレームリレーなど、従来からのレイヤ2 サービスを、IP ネットワーク インフラストラクチャを使って提供することは、同じサービスを専用のレイヤ2 ネットワークを使用して提供するより、コストを抑えることができます。IP ネットワーク インフラストラクチャは、複数のサービス タイプをサポートします。そのため、マルチサービス ネットワークにより、ネットワークの投資や運営コストをより幅広く、さまざまな顧客基盤

にまで広げることができます。また、L2TPv3 を使用することで、サービス プロバイダーは、レイヤ 2 ネットワークが存在しない地域まで従来のレイヤ 2 サービスを拡大することができます。既存のレイヤ 2 サービスを、IP ネットワークと同じ範囲で提供することができます。

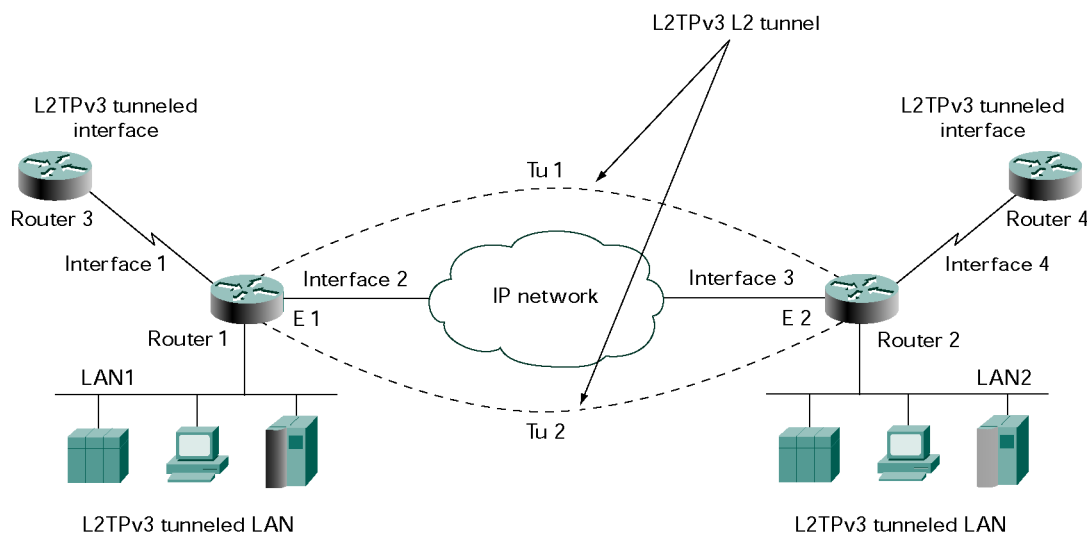
L2TPv3 を使用することで、サービス プロバイダーは、管理されたインターネット、イントラネット、およびエクストラネット サービスを容易に、しかも低コストで 1 つにまとめることができ、製品を向上させることができます。顧客が行ってきた設備投資は、既存のインフラストラクチャを通じてサービス プロバイダーへ接続するので守られます。

シスコシステムズは、インターネットワーキング技術において長い間、革新者としてあり続けてきています。Cisco IOS ソフトウェアが動作する最先端のハードウェア プラットフォームは、効率良く利益を上げるネットワークにとって重要な構成要素です。シスコは顧客と協力して、設備やプロトコル、顧客が必要とするサポートを、顧客が選んだ技術を使って、開発するために尽力します。

L2TPv3 の歴史

L2TPv3 は、L2TPv2 コントロール プレーンの拡張に、最適化された 2 つのフィールド ヘッダーを合わせたものです。L2TPv3 は、ネイティブ IP ベースのインフラストラクチャを使用して、サービス プロバイダーが顧客にトランスペアレントな LAN サービスを提供できるように設計されています (図 1)。L2TPv3 は、802.1Q VLAN (仮想 LAN)、Cisco High-Level Data Link Control (HDLC; ハイレベルデータリンク制御)、イーサネット、フレーム リレー、Packet over SONET (POS)、および PPP (ポイントツーポイント プロトコル) などの複数のレイヤ 2 カプセル化をサポートしています。この機能により、サービスの加入者はフレーム転送で IP ネットワークを使用していることを意識せずに、2 つの同種のインターフェイスをバックツーバックで接続することができます。

図 1
トランスペアレントな LAN サービスの例



L2TPv3 のトンネルは伝送手段を提供し、Router 3 および 4 を POS インターフェイス (Interface 1 および 4) とバックツーバックで接続させます。POS インターフェイスは、IP 伝送ネットワークの存在をまったく意識せずにこの接続を形成します。プロトコルの機能の詳細に関しては、この資料で後述のセクション「レイヤ 2 トンネリング プロトコルバージョン 3 の概要」を参照してください。

機能の互換性

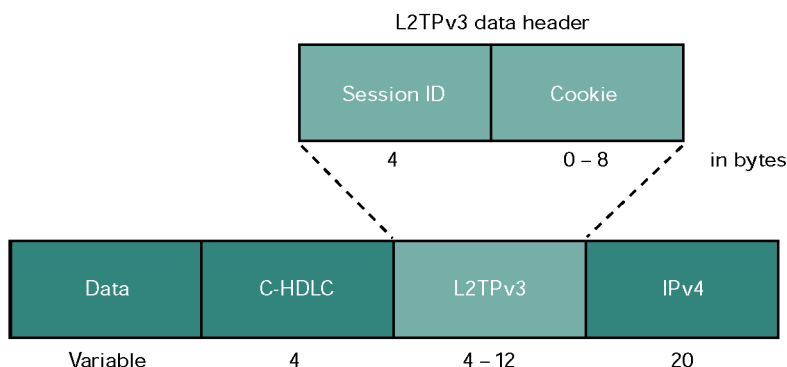
L2TPv3 のトンネル機能は、送信プロトコルとして IP のバージョン 4 を使用しているため、シスコはマルチキャスト、NetFlow、および IP ベースの Quality of Service (QoS; サービス品質) などの一般的な機能を幅広くサポートします。L2TPv3 と IP Security (IPSec) を併用することにより、サービス プロバイダーは、ネットワーク セキュリティのサポートを拡大できますし、企業顧客に自身のセキュリティ管理をまかせることもできます。異なるトラフィック定義とプライオリティ用のマルチキャストと QoS サポートを使用している企業に影響はありません。

L2TPv3 の概要

L2TPv3 には、異なる 2 つのコンポーネント (メッセージ タイプ) が含まれています。1 つはコントロール コネクションといい、エンドポイント間の帯域内で信頼性のあるコネクションとしてセットアップされます。トンネルおよびセッションのセットアップ、解除、管理維持を担当します。これには「制御メッセージ」を使用します。もう 1 つは転送プレーンで、レイヤ 2 データのカプセル化を担当します。レイヤ 2 のデータは「データ メッセージ」により IP ネットワーク上で転送されます。どちらのコンポーネントも単独で実装することができます。

コントロール コネクションがプロバイダーの末端にあるルータのペア間に実装されたものを、L2TP Control Connection Endpoint (LCCE) と呼びます。このコントロール コネクションがセットアップされていれば、セッション ID やその他のレイヤ 2 転送に必要な回線に関わる要求のネゴシエーションが可能です。これらは接続回線 (attachment circuit) と呼ばれます。セッション ID のネゴシエーションが完了すると、送信するレイヤ 2 のデータグラムに追加されます (図 2)。

図 2
IP バージョン 4 ヘッダーにおける L2TPv3 のカプセル化



注: デフォルトのレイヤ 2 特定のサブレイヤは図解していません。

セッション ID は 32 ビットのローカルなフィールドで、宛先または出力トンネル エンドポイントでの呼を識別するために使用されます。セッション ID はコントロール コネクション上でネゴシエートされるか、または L2TPv3 のデータ プレーンのみを使用している場合は静的に定義されます。

クッキーは変数長 (最大 8 バイト) で、ワード配列をとるオプション フィールドです。コントロール コネクションは、通常のセッション ID のルックアップに加え、さらに高い信頼性を得るためにクッキーのネゴシエーションを行い、データ メッセージが正しいセッションに送られているか、または最近再利用されたセッション ID が間違っていて送られていないか確認します。

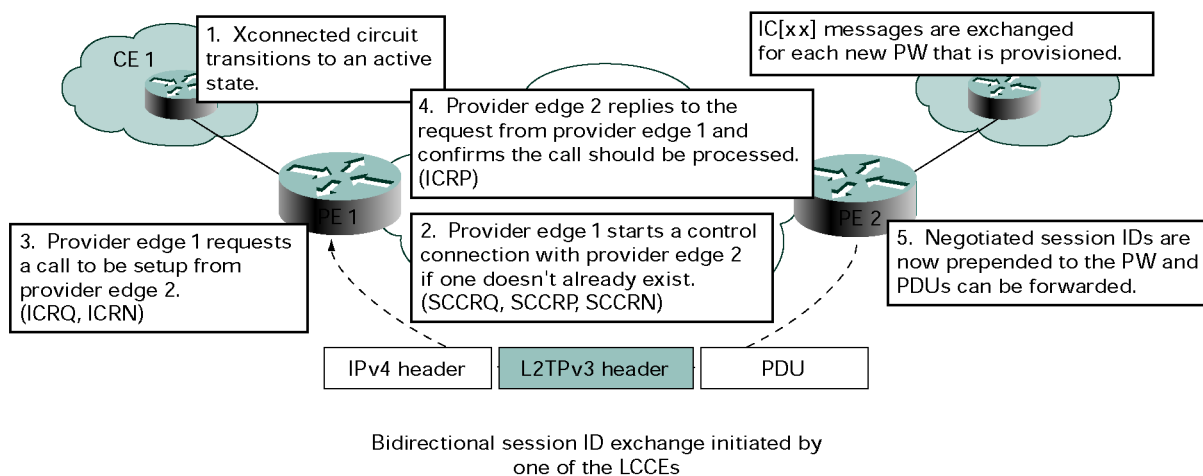
L2TPv3 のコントロール コネクションの運用の詳細は、次の URL で L2TP の IETF ドラフトを参照してください。

<http://www.ietf.org/html.charters/l2tpext-charter.html>

L2TP の仕組み

ここでの説明は、L2TPv3 ベースのサービスの作成に関わるマクロ プロセスに焦点を当てています。図 3 は基本的なプロトコルの動作を表しています。

図 3
プロトコルの動作の概要



1. 最初に、顧客は DS-3 のシリアル インターフェイスを介してサービス プロバイダーのエッジ ルータへ接続し、HDLC のカプセル化を設定します。顧客側のエッジ ルータで特に必要となる設定はありません。

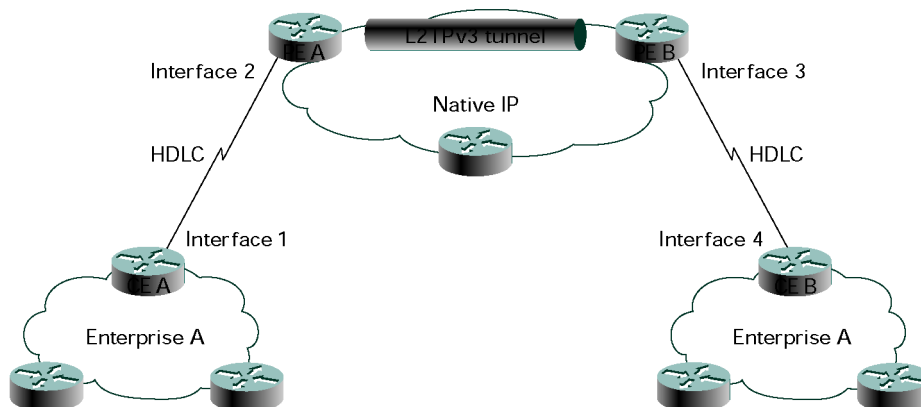
2. プロバイダー エッジルータ（顧客の入力回線が接続されている）のサービスプロバイダー ネットワーク側に、L2TPv3 トンネルおよびこれと対になるプロバイダー エッジルータ（顧客の出力回線が接続されている）の宛先 IP アドレスが設定されます。これには Xconnect CLI（コマンドライン インターフェイス）を使用します。リモートプロバイダー エッジルータで、対応する XConnect を設定する必要があります。
3. この時点で、L2TPv3 は、コントロール コネクションが宛先プロバイダー エッジルータ間に存在しているかどうかを判断します。存在しない場合、プロバイダー エッジルータは接続を開始するために Start-Control-Connection-Request メッセージを送信します。トンネルの確立後は、セッションのネゴシエーションが LCCE 間のレイヤ 2 伝送サービスを要求する接続回線に対して行われます。
4. 次に、セッション ID およびクッキーの値が LCCE 間でネゴシエート可能となり、リモート プロバイダーの末端で適切に逆多重化するための固有の ID を各接続回線に付与します。これは双方向プロセスで、セッション ID は、リモートピアに対してのみ一意となります。L2TPv3 の制御接続がない場合、静的なセッション ID が定義されます。
5. セッション ID が正常にネゴシエートされた後、プロバイダー エッジルータの入力インターフェイスで受信されたデータは、リモートプロバイダー エッジルータのセッション ID を先頭に付加され、外部 IP ヘッダーの宛先 IP アドレスに転送されます。
6. 最後に、パケットは宛先プロバイダー エッジルータで受信されます。L2TPv3 ヘッダーはセッション ID に基づいて逆多重化され、ネゴシエートされたクッキーの値と照合されます。ヘッダーが有効であれば、ストリップされます。オリジナルのレイヤ 2 フレームは、関連する物理ポートを通じて顧客側の宛先エッジルータに転送されます。

L2TPv3 のアプリケーション

仮想専用線

仮想専用線は企業の共通の要求で、混雑していない専用帯域を介してリモートサイトに接続することを目的としています。通常、カプセル化は Cisco HDLC、または PPP が採用されます。図 4 は、このサービスを提供する L2TPv3 の機能を表しています。

図 4
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)。Interface 2 および Interface 3 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、プロバイダー エッジルータ (PE A および PE B) 間の IP 接続を維持します。これには、Intermediate System-to-Intermediate System (IS-IS) プロトコル、または Open Shortest Path First (OSPF) プロトコルなどの標準 Interior Gateway Protocols (IGP; 内部ゲートウェイプロトコル) が使用されています。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 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 HDLC フレーム全体がシリアル インターフェイス (Interface 3) 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。次に、XConnect CLI を使用した一般的なコンフィギュレーションを示します。

XConnect CLI の例

PE_A:

```
interface Loopback0
  ip address 172.18.255.1 255.255.255.255
!
pseudowire-class L2TPv3_Default
  encapsulation l2tpv3
  sequencing both
  ip local interface Loopback0

!
interface Serial4/0
  no ip address
  encapsulation hdlc
  dsu bandwidth 44210
  framing c-bit
  cablelength 10
  xconnect 172.18.255.3 600 pw-class L2TPv3_Default
!
...
```

PE_B:

```
interface Loopback0
  ip address 172.18.255.3 255.255.255.255
!
pseudowire-class L2TPv3_Default
  encapsulation l2tpv3
  sequencing both
  ip local interface Loopback0

!
interface Serial4/0
  no ip address
  encapsulation hdlc
  dsu bandwidth 44210
  framing c-bit
  cablelength 10
  xconnect 172.18.255.1 600 pw-class L2TPv3_Default
!
...
```

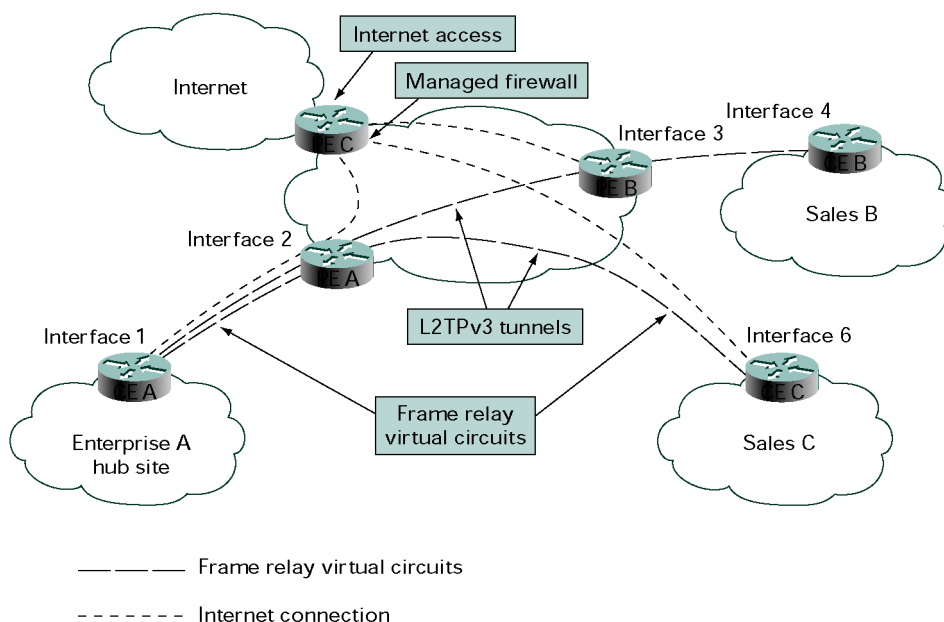
仮想専用線の利点

- サービスプロバイダーは、共通の IP パケット インフラストラクチャを使用して仮想専用線サービスを提供できるため、既存のサービスを拡張したり、あるいは1つに統合したりすることができます。
- ポート レベルのポリシングを使用することで、段階的な料金プランを実装できるため、顧客がネットワークで送信できる入力数を制限したり、帯域幅の使用率を最大限にすることができます。
- 企業は従来の設備基盤を利用できるため、ルーティングおよびネットワーク セキュリティ ポリシーの内容が維持されます。

フレーム リレーおよびインターネット

図 5 では、サービス プロバイダーがサポートする可能性がある拡張サービスの概要を表しています。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 リレーを使用している従来からある企業です。サービス プロバイダーは、管理されたファイアウォール 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
フレーム リレーおよびインターネット



企業は、従来のポイントツーポイントのサブインターフェイス フレーム リレーで構成されたシリアル 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。フレーム リレーでは、会社のイントラネットのサブインターフェイスやインターネット アクセスに使用されるサブインターフェイスが指定されています。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 アクセスの集中化や、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、拡張ネットワーク セキュリティ要件に対応した IPSec の暗号化を追加することもできます。サービス プロバイダーは、中央集中型のファイアウォール アーキテクチャを提供したり、オンデマンドによるビデオ サービスやビデオ会議のサービスを追加できます。これらのサービスは、Modular QoS CLI (MQC) を通じて割り当てられた Committed Information Rate (CIR; 認定情報速度) を増加させることで提供することができます。

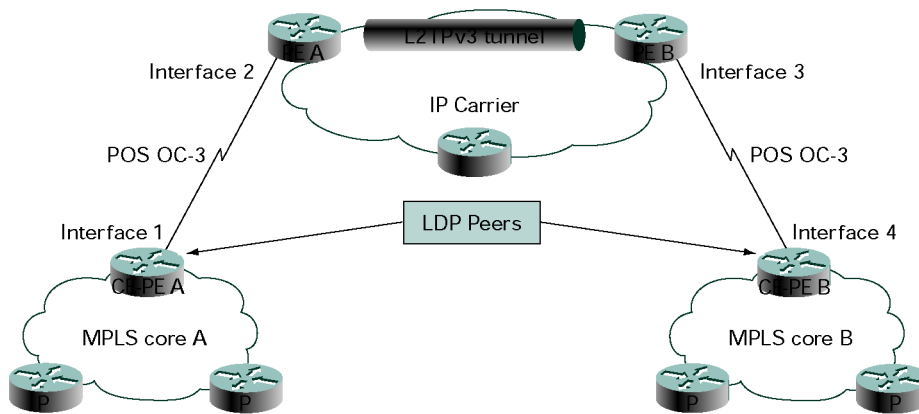
フレーム リレーおよびインターネットの利点

- サービス プロバイダーは、フレーム リレー専用の環境には存在しない IP インフラストラクチャ上で追加のサービスを提供できます。IP インフラストラクチャは、従来のレイヤ 2 ネットワークに追加の投資をすることなく、ネットワークを拡張するために使用されます。
- 企業は、ファイアウォールおよびインターネット アクセスのコストを外部委託することができ、それに関連するサポート コストを撤廃することで全体のコストが削減されます。
- 企業は、既存のフレーム リレー インフラストラクチャを利用することで、その設備投資を抑制することができます。
- ダイナミックな帯域幅のアップグレードを容易に設定することができ、最新のサービスおよび拡張要求をサポートします。

MPLS トランジット ネットワーク

サービス プロバイダーが IP および Multiprotocol Label Switching (MPLS) インフラストラクチャに移行しようとした場合、一度に一部分ずつ変更していくことで、アプローチを段階的に行うことができます。MPLS に対応したサービス プロバイダーは、異なる MPLS 間のトランジットとして、ネイティブ IP コアのインフラストラクチャが必要になる場合があります。この場合、MPLS を備えたサービス プロバイダーは IP コアを備えたサービス プロバイダーの顧客になります (図 6)。

図 6
MPLS ネットワークの IP コアへの接続



このシナリオでは、顧客は CE-PE A および CE-PE B を経由して IP トランジット プロバイダーに接続している MPLS サービス プロバイダーです。IP トランジット プロバイダーは、企業顧客がサービスを使用している場合と同様にこの接続を扱います。MPLS サービス プロバイダーは IP サービス プロバイダーのネットワークを使い、MPLS ベースのトラフィックを送信することができます。IP ネットワークが MPLS サービス プロバイダーにトランスペアレントなため、IP ネットワーク プロバイダーは Lightweight Directory Protocol (LDP) トラフィックを転送し、POS 接続が直接接続されているような、通常のラベル スワッピングを実行します。HDLC フレーム全体が IP ネットワークに転送されます。

MPLS トランジット ネットワークの利点

- IP ネットワークをトランジット ネットワークとして使用できます。トランジット ネットワークは個々の MPLS ネットワークを 1 つにリンクしたり、ピア関係の確立やキャリアがサポートする技術を実装することなく仮想 Network Access Point (NAP) を作成します。
- L2TPv3 を使用することで、MPLS 対応のコアに段階的に移行することができます。
- IP サービス プロバイダーは、ルーティング情報を管理したり、その情報を顧客のサービス プロバイダーのネットワークと交換したりする必要はありません。

構成例

L2TPv3 アプリケーションおよび設定例の詳細に関しては、次の URL を参照してください。

<http://www.univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s24/l2tpv3.htm>

参考資料

L2TP に関する詳細は、次の URL を参照してください。

<http://www.ietf.org/home.html>



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 International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

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 © 1992–2003 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, and the Cisco Systems logo are registered trademarks or 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.
(0403R) LS/JSI/05.03