

Technology

VPNs:A Case for VPLS VPN : VPLSの場合

VPLS(Virtual Private LAN Service)がマルチポイントイーサネットの代替技術として登場。

サンチャゴ・アルヴァレツ(Santiago Alvarez)による報告

イーサネットは他の技術に比べても低コストでシンプルなので、LANへの活用が図られてきた技術だ。また、最近では大都市圏で大規模に展開されている光ファイバーを活用したMAN(Metropolitan-Area Network)の技術としても人気を博している。そして今、VPLSがイーサネットをWANテクノロジーとしての活用を可能にするために貢献している。例えば、Ethernet over MPLS(Multiprotocol Label Switching)、Ethernet over SONET/SDH、Ethernet bridging over ATM、およびATM LAN Emulation(LANE)など、イーサネットをWAN全体でも使えるようにするためのいくつかの技術も存在しているが、これらは単にポイント・ツー・ポイントのコネクティビティを提供するだけであり、大規模な展開を図るためには、その複雑さからどうしても制限が出てきてしまう。あるいは、専用のネットワークアーキテクチャが必要なので、ネットワークの統合ができないという問題もある。

現在、大企業のWANは大きく変わりつつあり、それがVPLSテクノロジー開発の牽引力となっている。フレームリレーとATMは、パケットネットワークで好まれるテクノロジーとして長年にわたって広く利用されてきた。一般的に、大企業ではハブ・アンド・スポーク型または部分メッシュ型のトポロジーで、WANのコネクティビティが設計されてきた。このようなデザインは、フレー

ムリレーとATMの価格設定とポイント・ツー・ポイントという本来の性質に加えて、アプリケーションがネットワークインフラをどのように利用するのかという問題の結果として生み出されたものなのである。新しい世代のエンタープライズアプリケーションは、もっと柔軟なトポロジーと広帯域が提供できる企業WANアーキテクチャに対するニーズを生んだのだ。このような新しい要求に応えるために、サービスプロバイダもMPLSレイヤ3のVPN(Virtual Private Network)を基礎にしたプライベートIPを提供するようになってきた。また一方で、業界はイーサネットを基礎にしたWAN全体で広帯域のマルチポイントサービスを実施するための追加的選択肢としてVPLSを提案しているのである。

VPLSとは何か？

VPNテクノロジーの1つであるVPLSは、パケット交換網のインフラ上でイーサネットマルチポイントサービスを可能にするものである。VPNユーザーは、レイヤ2のプロードキャストドメインを提供するエミュレートされたLANセグメントを得る。エンドユーザーはVPN内のそれぞれの宛先にフレームを転送する仮想プライベートイーサネットスイッチとして、そのサービスを楽しむことができる。図1は、3つのサイトを接続しているVPLSの論理図である。各CE(Customer Edge)デバ

イスは、残りの全サイトへの接続性を得るためにそれぞれネットワークに対し単一接続されていればよい。マルチポイントのテクノロジーにより、ユーザーは物理的または論理的にひとつだけの接続で、複数の宛先に到達することが可能になる。ネットワークではパケットの宛先に基づいて転送を決定するだけである。これはVPLSにおいては、イーサネットフレームの宛先MACアドレスに基づいて、ネットワークがフォワーディングを決定することを意味している。エンドカスタマーの観点からもマルチポイントサービスは魅力的だ。というのも、複数のポイント間で全面的なコネクティビティを確立する際にも、多くのコネクションを必要としないからである。もしもポイント・ツー・ポイント技術に基づいて、同水準のコネクティビティを達成しようとするれば、はるかに多くのコネクションが必要になるか、あるいは最適ではないパケットフォワーディングを利用しなければならないのである。

VPLSテクノロジーコンポーネント

最もシンプルな形のVPLSは、LANサービスをエミュレートする数多くのPE(Provider Edge)デバイスに接続されたサイトの集合体でできている。各PEでは、各VPLSのフォワーディングを決定するためにVSI(Virtual Switching Instance)が使われている。PEデバイスはサイト間のフォワーディングを決定し、イーサネットのVC(Virtual Circuit)またはpseudo-wire(擬似ワイヤ)を使ってパケット交換網全体にわたって、イーサネットフレームをカプセル化するのである。PEはフルメッシュ型のイーサネットVCを使って、PE間でイーサネットフレームを転送する。VPLSは、ポイント・ツー・ポイントのEthernet over MPLSで定義されたのと同じカプセル化に依存している。ここではフレームブリアンブルとFCS(Frame Check Sequence)が外され、残りのペイロードはコントロールワード、VCラベル、およびInterior Gateway Protocol(IGP)またはトランスポートラベルをつけてカプセル化されることになる。VPLSは、元はMPLSトランスポート上で指定され、実行されていた。図2は、3つのサイトを接続しているVPLSのコンポーネントを示している。

PEは、VPLS内でフレームを交換するのに必要なフォ

VPLSの論理図

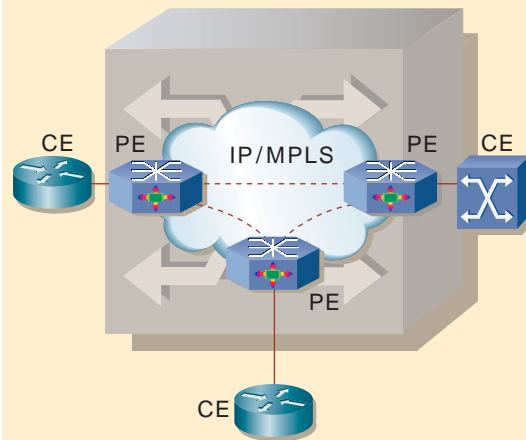


図1：各CEデバイスは、残りのサイトへの全面的なコネクティビティを得るために、ネットワークに対して単一の接続が必要である

VPLSのコンポーネント

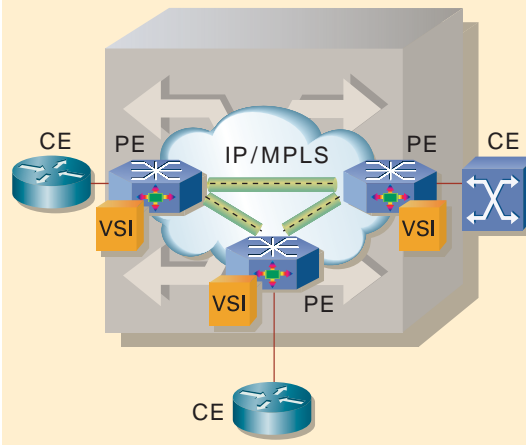


図2：この3つのサイトを接続しているVPLSには、各VPLSのフォワーディングの決定を行うために、各PEにそれぞれVSIが使われている。PEは、PE間でイーサネットフレームを転送するのにフルメッシュ型のイーサネットVCを使っている

ワーディング情報を持ったVSIを自動的に配布する。PEはスタンダードのMACアドレス学習とイーサネットスイッチングで使われているエージング機能で、この情報を取り込む。VSIのフォワーディング情報は、物理ポートおよびVCから学んだMACアドレスによって更新される。これらの機能は、ブロードキャスト、マルチキャスト、および宛先不明のMACアドレスがすべてのポートおよびVSIに関連するVCにフラディングすることを意味しているのである。PEは、ループフリーのトポロジーを形成するため、VC上でスプリットホライズンフォワーディングを使う。このようにして、フルメッシュ型VCはVPLSのPE間を直接接続し、ループフリーのトポロジーを実現するためにリソースを大量に消費するようなプロトコル(例えば、STP: Spanning Tree Protocol)を必要と

しない。

VPLSにはPE discovery(発見)およびVC setup(設定)というシグナリングに関わる2つの機能コンポーネントがある。Cisco VPLSは、現在はVPLS内のPEの関連付けをマニュアルの構成に頼っている。しかし、BGP(Border Gateway Protocol)、RADIUS、LDP(Label Distribution Protocol)およびDNS(Domain Name System)を含め、いくつかのdiscovery(発見)プロトコルをサポートするように、簡単にアーキテクチャを強化することができる。VC設定はポイント・ツー・ポイントのサービスのために定義されたLDPシグナリングメカニズムと同じものが用いられる。各PEは確立されたLDPセッションを使って、パケット転送中に入力側PEがイーサネットフレームにつけるラベルスタックの一部として使うVCラベルマッピングを配布する。

Cisco VPLSでは、シグナリングプロトコルを通じて到達可能性情報(MACアドレス)を交換する必要がない。この情報はイーサネットのブリッジ用に定義された標準のアドレス学習、エージング、およびフィルタリングメカニズムを使って、データプレーンから取得されるからである。しかし、VCの設定と削除に使われるLDPシグナリングは、リモートPEに対し、VCから取得したMACアドレスの一部または全部をVSIから取り消す通知をするためにも使うことができる。このメカニズムは、最終的に無効になったアドレスを消去する通常のアドレスエージングに対してコンバージェンスの最適化を提供してくれる。

ほとんどのVPLSサイトがイーサネット経由で接続されると仮定しても、それらはその他のレイヤ2の技術(例えば、ATM、フレームリレー、またはポイント・ツー・ポイントの protocols)を使って接続されるかも知れない。イーサネット以外のリンクで接続しているサイトはブリッジドカプセル化を使って、PEとパケットを交換する。CEデバイスの構成条件は、ポイント・ツー・ポイントのレイヤ2サービスにおけるイーサネットのインターワーキング要件と酷似している。

VPLSの拡張性の特徴

VPLSは、マルチポイントのイーサネットサービスを提供する業界初の試みというわけではない。以前は、企

業WAN全体にわたるイーサネットのトランスポートにはATMが使われていた。あるアプローチはイーサネットスイッチを接続しているATM VC上のブリッジングであり、また別のアプローチはATM LANEだった。これらの選択肢は複雑すぎて、拡張性にも限界があったことから、一般的に活用される機会を失ったのである。

VPLSの場合には、パケットの複製とアドレス情報の量がPEデバイスの拡張性を考える上での2つの主要な懸念材料である。(ブロードキャスト、マルチキャスト、または宛先不明のユニキャストアドレスのために)パケットがフラッドされる場合、入力側PEはパケットを複製しなければならない。VPLS内のPEの数が増加すれば、それだけ作成しなければならないパケットのコピーの数も増加することになる。

ハードウェアのアーキテクチャによっては、パケットの複製が処理能力とメモリーのリソースに重大な影響を与える可能性がある。さらに、非常に多くのホストがVPLSに接続されている場合には、データプレーンから学ぶMACアドレスの数が急速に増大するが、この状況はVPLS内でフラットなネットワークドメインが大きくなるようにすることで緩和できる。

VPLSの拡張性改善には階層型のモデルを使うことができる。H-VPLS(Hierarchical VPLS)は、シグナリングのオーバーヘッドとPEにおけるパケット複製の必要性を減らすことが可能だ。このモデルでは、ユーザー側PE(user-facing PE : u-PE)とネットワークPE(network PE : n-PE)という2種類のPEデバイスが定義されている。CEデバイスはu-PEに直接つながり、VSIに基づいてVPLSフォワーディングが行われるn-PEに到達する前にVPLSトラフィックを集約する。この階層型モデルでは、u-PEがレイヤ2のスイッチング機能をサポートし、通常のブリッジングを実行する。Cisco VPLSは、u-PEとn-PEの間でのトラフィックの集約に、IEEE 802.1Qトンネリング、ダブル802.1Q、またはQ-in-Qカプセル化を使っている。Q-in-Qトランクは、n-PE上のVPLSインスタンスに対するアクセスポートとなる。図3はH-VPLSのアーキテクチャを表している。

H-VPLSモデルでは、サービスプロバイダは分散したメトロイーサネットドメインを相互接続し、イーサネットサービスの地理的カバー範囲を拡大することができ

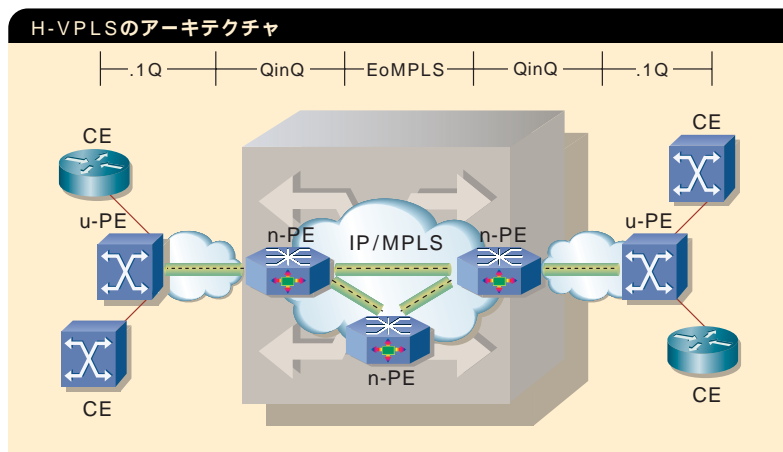
る。さらに、H-VPLSは、(VLANのアドレス空間によって決まる) 加入者数4000という制限を超えて、メトロイーサネットサービスを拡大するのにも役立つ。

逆に、イーサネットアクセスネットワークを持っていれば、パケットの複製を分散し、シグナリング要求を減らすことでVPLSの拡張性に貢献することもできるのである。メトロイーサネットとVPLSは相互補完的な技術であり、さらに高度なイーサネットサービスの提供を可能にするものである。

Cisco IOS MPLSのVPLS

Cisco IOS® MPLS VPLSはイーサネット、MPLS、およびエンド・ツー・エンド戦略を実現するために必要な管理コンポーネントを包括し、業界全体が支持するIETF Internet-Draft draft-ietf-pppvpn-vpls-ldpを基礎としている。シスコで最初にVPLSが実装されたCisco 7600シリーズルータは、世界中のサービスプロバイダがメトロイーサネットのアーキテクチャで幅広く展開している製品である。シスコはMPLS VPN、Any Transport over MPLS、QoS (Quality of Service) およびポイント・ツー・ポイントのイーサネットVPNに加え、Cisco ISQ IP Solution Center 3.1でもVPLSのサポートを導入した。Cisco ISQは、管理の自動化とインテリジェンスを提供すると同時に、ネットワークオペレータの生産性向上を支援するために設計されたプロビジョニングと管理のツールだ。これらのコンポーネントは、シスコのメトロイーサネット装置とともにイーサネットサービスのための完全なソリューションを提供している。

さらに、Cisco VPLSはMPLSを使ったコンバインドネットワークで提供することができるサービスポートフォリオの一部でもある。MPLSの展開でサービスプロバイダが期待するメリットの1つは、単一のネットワークインフラで複数のサービスを提供できることだ。MPLSが持つ本来の性質によって、コアデバイスはネットワークを通じて移動するパケットに関連するサービスを認知する必要がない。同様にコアデバイスはサービスに左右されることなく、トラフィックのスイッチングを行う。PEデバイスだけが、VPLSのシグナリングとカプセル化の詳細な情報を実行しなければならない。PEデバイスは、(たとえば、MPLS VPN、VPLS、フレームリレー、



またはATMなどの)ある特定のサービスのためだけのものではない。

イーサネットの高い普及率とVPLSの柔軟性は、一部の企業にとってマルチポイントのサービスのための魅力的な選択肢となっている。実際、MPLSインフラを使った完全なサービスポートフォリオの一環として、VPLSを考えているサービスプロバイダは多い。WANでマルチポイントのイーサネットサービスを提供しようとする試みは業界で初めてのものではないが、Cisco VPLSは従来のソリューションの改善に努力を重ねてきた。しかし、VPLSは依然として新しい技術であり、今後の取り組みが必要な分野(例えば、イーサネットOAMおよびイーサネットLMI)が存在しており、同時に実際の展開経験を積む中で、さらに利益が得られる分野も多い。サービスプロバイダや大企業の間でVPLSを基礎にしたサービスがどこまで普及するか、それは時間が証明してくれるに違いない。

図3: H-VPLSモデルでは、Cisco VPLSはu-PEとn-PEの間でトラフィックを集約するのにIEEE 802.1Qトンネリング、ダブル802.1Q、またはQ-in-Qカプセル化を使う。Q-in-Q トランクは、n-PE上のVPLSインスタンスに対するアクセスポートとなる

詳しい情報

Cisco IOS MPLS VPLS Statement of Direction :

cisco.com/packet/162_5b1

Cisco IOS MPLS VPLSアプリケーションノート (Cisco IOS MPLS VPLS Application Note) : cisco.com/packet/162_5b2

従来型のVPNを越えて前進するシスコのアリ・サジャーシとのQ&A (Moving Beyond Traditional VPNs, Q&A with Cisco's Ali Sajjasi) :

cisco.com/packet/162_5b3

Cisco ISCレイヤ2のVPNおよびVPLSのコンセプト (Cisco ISC Layer 2 VPN and VPLS concepts) : cisco.com/packet/162_5b4

Cisco ISCレイヤ2のVPN管理 (Cisco ISC Layer 2 VPN management) :

cisco.com/packet/162_5b5

Cisco Networking Professionals Connectionの“VPN (Virtual Private Networks)”フォーラムでシスコのエキスパートや同僚からVPNについてもっと多くのことを発見しよう。
cisco.com/discuss/vpn