LAN 拡張テクノロジーの比較：Cisco Overlay Transport Virtualization と Virtual Private LAN Service

このドキュメントの内容

データセンターが地理的に分散していると、アプリケーションの耐障害性が増し、ワークロードを柔軟に割り当てられます。これらの利点を引き出すには、ネットワークでデータセンター間のレイヤ 2、レイヤ 3、およびストレージ接続が可能でなければなりません。またそうした接続性はデータセンターの自律性やネットワーク全体の安定性を損なうことなく提供されている必要があります。

このドキュメントでは、Cisco® Overlay Transport Virtualization（OTV）、Virtual Private LAN Service（VPLS）、およびシスコの VPLS 拡張機能の特性を、企業の LAN 拡張を実現するときに生じる課題に関して比較します。ソリューションには次の機能が必要です。

- 透過性の確保（コアおよびサイト両方に対して透過的）
- トランスポート非依存
- マルチホームおよびマルチパスのサポート
- データセンター間の障害分離

このドキュメントは、OTV および VPLS の利点に興味のあるテクノロジーの意思決定者、IT 管理者、およびネットワーク アーキテクトを対象としています。

LAN 拡張の必要性

企業は、運用コストを低く抑えながらインフラストラクチャの使用率を最大まで引き上げ、アプリケーションの可用性を高めるという課題に直面しています。アプリケーションは、アクセスの場所や時間に関係なく、最短の応答時間で利用できなければなりません。

IT の設計時にデータセンターを地理的に分散して展開することにより、アプリケーションの可用性を高める効果的な災害回避および災害復旧のメカニズムを導入できます。また、地理的に分散することにより、施設の配置を改善してアプリケーションの応答を最適化することが可能になります。ワークロードをデータセンター間で柔軟に分散することにより、要求のホットスポットが発生するのを回避し、キャパシティをフルに利用できます。

データセンターを地理的に分散させ、それを最大限に活用するには、それらの場所をつなぐネットワークの全体でレイヤ 2 接続ができるようにする必要があります。Web、アプリケーション、およびデータベースの各レイヤにおいて各種アプリケーションにより実現される耐障害性およびクラスタ処理のメカニズムを有効にするには、データセンター内の各レイヤで LAN 拡張が必要です。さらに、レイヤ 3 接続とストレージ接続の要件も重要です。このドキュメントでは、レイヤ 2 接続の要件およびそれらを満たす最適な方法について解説します。

LAN 拡張とレイヤ 2 トランスポート サービスの比較

企業とサービス プロバイダーでは、レイヤ 2 VPN の使用に関して考え方が異なります。サービス プロバイダーは多数のお客様に対して大量のレイヤ 2 VPN をトランスポート サービスとして提供しなくてはなりません。一方で企業はデータセンター間の LAN 拡張を必要としており、二者の要件は大きく異なります。OTV は、データセンター間の LAN 拡張の課題に対処するように特別に設計されています。一方、シスコはプロバイダー ネットワークの技術的な課題に対処するために革新的で業界をリードするテクノロジーを提供し続けており、Multiprotocol Label Switching（MPLS）ベースのテクノロジーを最適化したトランスポート サービスを提供しています。

サービス プロバイダーと企業は、直面する課題が異なるのと同時に、必要なソリューションも異なります。

もちろん企業によっては構造がサービス プロバイダーに似ている場合があり、その場合にはサービス プロバイダーと同じような課題に直面することもあります。課題の一部は両者で共通であるため、シスコは、すべての MPLS ベースおよび IP ベースのトランスポート ソリューションを互換性のある補完的な設計にしています。プロバイダーに似た構造の企業の場合、組織全体にわたって MPLS テクノロジーを使用することは有益ですが、それでも一部のサービスは、OTV などの IP ベースのソリューションを使用した方が適切に対処できる場合があります。たとえば、企業がレイヤ 3 VPN およびトラフィック エンジニアリング サービスを提供する MPLS バックボーンを持ちながら、データセンター間の LAN 拡張を OTV で実現している場合があります。OTV トラフィックを含め、すべてのトラフィックが、バックボーン内で MPLS ベースのサービス（Traffic Engineering Fast Reroute（TE-FRR））の恩恵を受けると同時に、最適な LAN 拡張が OTV によって提供されます。

LAN 拡張の課題

LAN を複数のデータセンターにわたって拡張すると、トランスポート サービスを提供するサービス プロバイダーが直面する課題とは異なる一連の課題が生じます。

- **サイトの独立性の維持**：複数のデータセンターにわたってレイヤ 2 ドメインを拡張すると、IP ネットワークで相互接続したときには通常切り離されているプロトコルおよび障害が、データセンター間に波及する可能性があります。このような障害は、オープンなレイヤ 2 フラッディング ドメイン内に無制限に広がります。障害を封じ込め、複数データセンターの利用により実現される耐障害性を維持するには、フラッディング ドメインの範囲を制限したままレイヤ 2 接続を提供するソリューションが必要です。
- **トランスポートの独立性**：データセンター間のトランスポートの性質は、データセンターの場所および各地域でのサービスの可用性とコストに応じて変化します。データセンターの相互接続に対する費用対効果の高いソリューションは、トランスポートに非依存で、ネットワーク設計者がデータセンター間のトランスポートをビジネスおよび運用上の優先事項に基づいて柔軟に選択できるものでなければなりません。最も一般的な方法は IP 対応トランスポートで、これにより柔軟性が提供され、長距離接続が可能になります。IP トランスポートの使用に対応したソリューションは、最も高い柔軟性が得られると考えられます。
- **マルチホーミングおよびエンドツーエンドのループ防止**：LAN 拡張テクニックは高い耐障害性を実現する必要があり、そのため、VPN 上へのレイヤ 2 サイトのマルチホーミングが必要です。また、マルチホーミングされるブリッジ型ネットワークを接続するとループが発生する可能性があるため、それを防ぐメカニズムも必要になります。
- **レプリケーション、ロード バランシング、およびパス ダイバーシティによる帯域利用率**：レイヤ 2 ドメインをデータセンター間にわたって拡張する場合、最小のコストで最適な接続を実現するには、データセンター間で使用可能な帯域幅を最適化して使用する必要があります。冗長性のある接続をデータセンターとトランスポート ネットワークの間で提供しつつ、すべての使用可能なパスの間でロード バランシングを行うには、従来のイーサネット スイッチングおよびレイヤ 2 VPN で提供されている以上のインテリジェンスが必要です。マルチキャストおよびブロードキャストのトラフィックも、帯域幅の使用量を低減するように最適に複製される必要があります。
- **スケーラビリティおよびトポロジの独立性**：LAN 拡張はデータセンター内で展開されるので、ネットワーク設計に影響せず、結果としてトポロジ内のどのポイントでも展開可能なソリューションを提供することが重要です。一般にデータセンター アクセスの機能が強化されるにつれてエッジ デバイスの数は増加するため、このような柔軟性を実現するにはスケーラビリティの高い LAN 拡張ソリューションが必要になります。

- **VLAN および MAC アドレスのスケーラビリティ**:データセンター間の LAN の拡張では、複数の VLAN を同時に拡張する必要があります。さらに、アプリケーションによっては、重複する VLAN ID を使用するため、それらは共通の LAN 拡張上にありながら、互いに独立に伝送しなければなりません。MAC アドレス空間はサマライズできないため、サイトが相互接続されるにつれて関係する MAC アドレスの数が増加します。正しい対処がなされていない場合、これは問題発生の引き金となり、ソリューションの範囲が制限される可能性があります。
- **シンプルな運用**:レイヤ 2 VPN では、データセンター間全域で拡張されたレイヤ 2 接続が可能になります。しかし通常これには複雑なプロトコルの混在、プロビジョニングの分散、階層型スケーリング モデルに起因する運用の手間の増加が伴います。この接続の提供コストを削減するには、組み込み機能およびポイントツークラウド プロビジョニングを備えたシンプルなオーバーレイ プロトコルが不可欠です。

OTV および VPLS による LAN 拡張の課題の対処方法

表 1 に、OTV と VPLS がそれぞれ LAN 拡張の課題に対処する方法を示します。

表 1　OTV と VPLS の比較

サイトの独立性の保護	
OTV	**VPLS**
OTV では、MAC アドレス到着可能性情報がコントロール プロトコルによって伝送されます。MAC アドレス ラーニングが行われる必要がないので、オーバーレイでの未知のユニキャスト トラフィックのフラッディングを抑制できます。フラッディングの異常は、単一のサイト内に封じ込められます。	VPLS では、フラッディングによって MAC アドレス到着可能性情報を伝達します。したがって、フラッディングを防ぐことはできません。
OTV コントロール プロトコルにより、MAC アドレスから IP へのマッピングが伝送され、それらを使用して各エッジ デバイス上の Address Resolution Protocol（ARP）キャッシュにエントリを入力できます。エッジ デバイスは ARP プロキシとなり、オーバーレイを通過する ARP ブロードキャストを抑制できます。ARP ストームがサイト間で伝わることはなくなります。	VPLS には、情報を適切なスケールで特定の MAC アドレスに関連付けられるコントロール プロトコルはありません。ARP トラフィックおよびその他のネットワーク イベントの制御は、コントロール プロトコルを追加しなければ実用的ではありません。[1]
OTV には、最も一般的なリンクローカル ネットワーキング プロトコル（スパニング ツリー プロトコル、VLAN Trunking Protocol（VTP）、Hot Standby Router Protocol（HSRP）など）をローカライズし、それらがオーバーレイを通過するのを防止する組み込みフィルタリング機能があります。この機能により、プロトコルの障害がサイト間で伝わるのを防ぎます。First-Hop Resiliency Protocol（HSRP、Virtual Router Redundancy Protocol（VRRP; 仮想ルータ冗長プロトコル）など）のローカリゼーションは、障害を分離し、最適なルーティングの確保に役立ちます。	VPLS では、スパニング ツリー プロトコル、および VTP や Generic VLAN Registration Protocol（GVRP）などの VLAN 配布プロトコルを抑制できます。VPLS では、HSRP、VRRP、Gateway Load-Balancing Protocol（GLBP）などの First Hop Resiliency Protocol をローカライズされた状態に維持する統合メカニズムは提供されません。
トランスポートの独立性	
OTV	**VPLS**
OTV は、オーバーレイの特性から、IP パケットを転送できるものであればどのようなトランスポート上でも動作します。トランスポート内で実行される IP 向けのすべての最適化は、OTV でカプセル化されたトラフィックに効果があります。	VPLS では、ラベルスイッチド トランスポートが機能する必要があります。このアプローチは、MPLS トランスポートが使用可能なときに最も適しています。MPLS トランスポートを使用できない場合は、Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）での VPLS などといった改良型により、IP GRE トンネルのメッシュ上で VPLS ソリューションを展開できます。
マルチホーミングおよびエンドツーエンドのループ防止	
OTV	**VPLS**
OTV コントロール プロトコルの一部として、マルチホーミングの自動検出が含まれます。この機能により、設定やプロトコルを追加しなくてもサイトのマルチホーミングが可能になります。	VPLS では、マルチホーミングを提供するために、特定のプロトコルを追加する必要があります。VPLS に追加しなければならないプロトコルには、マルチホーミング拡張付きの Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）、Interchassis Communication Protocol（ICCP）と Multichassis Link Aggregation Control Protocol（MLACP）、Cisco IOS® ソフトウェア Embedded Event Manager（EEM）、および Multiple Spanning Tree（MST; 多重スパニング ツリー）などがあります。

[1] IP-only LAN Service（IPLS）は、その静的な性質から、LAN 拡張サービス内でサイトごとに大量のホストを扱わなければならない場合には適していません。

	シスコの VPLS では、VPLS クラウドに対して透過的なマルチホーミングを可能にするデバイス クラスタ処理ソリューションを使用することにより、これらのプロトコルは不要になります。Virtual Switching System（VSS; 仮想スイッチング システム）テクノロジーの使用により、プロバイダー エッジ デバイスのペアは、プロトコルを追加しなくても、VPLS サイトの二重アクティブ マルチホーミングを提供するための単一デバイスであると見なすことができます。
OTV では、VLAN 単位の単一アクティブ エッジ デバイス マルチホーミングがデフォルトで提供されます。virtual PortChannel（vPC）、シスコのレイヤ 2 マルチパス化、または Transparent Interconnection of Lots of Links（TRILL）テクノロジーと組み合わせると、OTV で全アクティブ マルチホーミングを提供できます。最大 16 台までのアクティブ エッジ デバイスを OTV 内のサイトごとに使用でき、それにより、シスコのレイヤ 2 マルチパス化および TRILL クラウドを OTV 上で拡張するときにそれらの連続性を維持できます。	VPLS 用のすべてのマルチホーミング スキームは、サイト上の複数のプロバイダーエッジ デバイスを単一のアクティブ デバイスに絞ることに重点が置かれています。
	シスコの VPLS では、アクティブ/アクティブ デュアル ホーミングを提供する VSS を使用して、2 つのプロバイダーエッジ デバイスを単一デバイスに統合できます。
帯域利用率：レプリケーション、ロード バランシング、およびパス ダイバーシティ	
OTV	**VPLS**
OTV では、マルチキャスト、ブロードキャスト、およびシグナリング トラフィックの最適なレプリケーションを行うために、ネイティブ IP マルチキャストが使用されます。	VPLS では、マルチキャスト トラフィックのヘッドエンド レプリケーションを防止するために、フル メッシュの point-to-multipoint（P2MP; ポイントツーマルチポイント）トンネルが使用されます。
OTV ヘッダーが定義されます。これにより、コアが 5 タプルのレイヤ 2、3、および 4 の情報に基づいてトラフィックをハッシュし、複数のパスにトラフィックを分散させて、カプセル化されたトラフィックの偏りを防ぐことができます。[2]	レイヤ 2 ～ 4 の情報に基づいてバックボーン内の複数のパスに負荷を分散し、それによりトンネルの偏りを回避するための効果的なメカニズムが、FAT-pseudowire（FAT-PW）の追加によってシスコの VPLS（およびすべての MPLS サービス）に提供されます。
OTV では、全アクティブ マルチホーム展開内で使用可能な複数のエッジ デバイス間でフローを効果的にロード バランシングできます。ロード バランシングは、OTV コントロール プロトコルによって提供される情報に基づいて Equal-Cost Multipath（ECMP）ルールに従います。ハッシングは、レイヤ 2 ～ 4 の情報に基づいて行われます。	VPLS では、すべてのアクティブパスの転送に対して本質的にシングル ホームになるので、フロー単位のロード バランシングはできません。
	シスコの VPLS では、VSS を使用してデュアルアクティブ プロバイダーエッジ マルチホーミングを提供することにより、この制約を克服します。
スケーラビリティおよびトポロジの独立性	
OTV	**VPLS**
OTV は、比較的密度の高い（百単位の）エッジ デバイスにまで拡張する設計になっています。この能力は、データセンター内のどこに機能を展開するかの決定を左右する重要な要素です。必要なエッジ デバイスを展開するのに都合の良い場所は、データセンター ネットワーク内のアグリゲーション レイヤです。この配置では、既存のレイヤ 2 ドメインを必要に応じて OTV オーバーレイに直接組み入れることにより、ネットワークの設計および運用が簡素化されます。エッジ デバイスをアグリゲーション レイヤに配置すると、多数のエッジ デバイスに対応できるソリューションが必要になりますが、OTV は、それに必要なスケーラビリティを提供します。エッジ デバイスをネットワーク内の他の場所（WAN エッジなど）に設置すると、レイヤ 2 ドメインをアグリゲーション レイヤからエッジ デバイスにまで拡張するための追加のハードウェアが必要になり、ネットワークの複雑さおよび運用の負荷が増します。	VPLS は、少数（40 ～ 60）のプロバイダー エッジ デバイスを含める設計になっています。プロバイダー エッジ デバイスの数が多くなると、Hierarchical VPLS（H-VPLS）などのスキームが必要になります。H-VPLS を使用することは、プロバイダー エッジ デバイスをデータセンター エッジに設置し、Ethernet over MPLS（EoMPLS）または IEEE QinQ を追加して、プロバイダー エッジ デバイスにトラフィックを集約することと同じです。このようなモデルでは、管理対象となる要素が多数存在することは明らかであり、それにより、VPLS の展開に対するトポロジの制約が厳しくなります。 VPLS で BGP シグナリングを使用すると、スケーラビリティが向上し、H-VPLS は必要なくなり、前述のトポロジに関する制約はなくなります。
VLAN および MAC アドレスのスケーラビリティ	
OTV	**VPLS**
OTV では、本質的に単一のオーバーレイ上で複数の VLAN に対するトラフィックが伝送されます。	VPLS では、VPLS インスタンスごとに 1 つの VLAN を伝送できます。単一のインスタンス上で複数の VLAN を多重伝送するには、VPLS で IEEE QinQ を使用します。
OTV は、VLAN ID 空間を、単一の 802.1Q ドメイン内で使用可能な 4,000 個の VLAN の範囲を超えて拡張できる組み込みの階層型 ID を備えています。	VPLS では、単一の VPLS インスタンスを使用して 4,000 個を超える VLAN に拡張するには、単一インスタンスで透過的に転送可能な追加の IEEE QinQ カプセル化を提供する外部デバイスの支援がサイト内で必要です。
	シスコの VPLS は、外部デバイスの支援がなくてもインスタンスごとに 4,000 個を超える VLAN を単純な設定モデルでサポートするように強化されています。
OTV の最初のリリースでは、オーバーレイ内の MAC アドレスがすべてのサイト上で学習されます。ただし、それらが関係するサイトに VLAN の範囲を限定することもできます。それにより、サイトに基づくテーブルのサイズが減少します。また、	VPLS はフラッディングに依存しています。そのため、すべての MAC アドレスがすべてのサイトで学習されます。複数 VLAN は IEEE QinQ カプセル化によって VPLS から隠蔽されなければならないので、VLAN スコーピングは選択肢に入

[2] OTV の User Datagram Protocol（UDP; ユーザ データグラム プロトコル）ヘッダーは、First Customer Shipment（FCS; お客様への最初の出荷）では使用できません。

OTV では、貴重なハードウェア メモリ空間を節約するために、フォワーディング テーブルの会話型プログラミングもできます。[3]	らず、すべての MAC アドレスがすべての場所で学習されます。
	シスコの VPLS では、IEEE 802.1Q ヘッダーをはるかに効率よく扱うことが可能になります。それにより、VLAN プルーニングが可能になり、MAC アドレスのスケーラビリティが向上します。
シンプルな運用	
OTV	**VPLS**
OTV では、LAN 拡張により生じるさまざま要件に対処する単一のプロトコルが提供されます。 OTV では、単一プロトコルに組み込まれ、既存のサイトに影響せずにポイントツークラウド プロビジョニングを実行可能な自動検出メカニズムが提供されます。	VPLS では、LAN 拡張の課題に対処するために多数のプロトコルが必要です。自動検出のための BGP、擬似回線の確立のための Label Distribution Protocol（LDP; ラベル配布プロトコル）、マルチホーミングのための BGP、ICCP、MLACP、および Cisco IOS EEM、マルチキャスト分散のための P2MP LDP、VPLS が GRE 上で使用される場合の GRE トンネルの確立のための BGP および Next-Hop Resolution Protocol（NHRP）などがあります。
	シスコの VPLS では、これらの追加プロトコルのいくつかを不要にし、エンタープライズクラスのプロビジョニング モデルの背後に他のプロトコルを隠すことにより、こうした複雑さの多くが簡素化されます。
OTV は、プロセスを自動化し、Command-Line Interface（CLI; コマンドライン インターフェイス）をほとんど使用しなくても済むように設計されています。	プロトコルの急増により、VPLS CLI を頻繁に使用することがあります。
	シスコの VPLS は、CLI 操作を統合し、運用を簡素化するための多くの拡張機能を備えています。
OTV の展開は、既存のネットワークに影響を与えません。そのため、サイトの独立性を損なうことや、コアまたはサイトのプロトコルの動作を変更することなく、OTV を透過的にかぶせることができます。	VPLS は、ネットワークに対して慎重に設計する必要があります。そのため、柔軟性は制限されます。

まとめ

シスコは VPLS を大幅に強化しており、VPLS 向けの革新的なテクノロジーの開発に投資し続けています。また同時に、長年の経験から生み出される OTV のような新しいテクノロジーによる革新も実現し続けています。どちらのテクノロジーも、Data Center Interconnect（DCI; データセンター相互接続）における LAN 拡張のアプリケーションとして利点および欠点がありますが、OTV の方がはるかにシンプルなアプローチを提供します。

関連情報

Cisco Nexus 7000 シリーズ スイッチ：
http://www.cisco.com/web/JP/product/hs/switches/nexus7000/index.html

[3] FCS 後に機能を使用できます。

お問い合わせ先

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

10.03