



概要

この章は、次の内容で構成されています。

- [ライセンス要件](#) (1 ページ)
- [サポートされるプラットフォーム](#) (1 ページ)
- [VXLAN の概要](#) (2 ページ)
- [ハードウェア ベースの VXLAN ゲートウェイとしての Cisco Nexus 9000](#) (2 ページ)
- [VXLAN のカプセル化およびパケット形式](#) (2 ページ)
- [VXLAN トンネル](#) (3 ページ)
- [VXLAN トンネル エンドポイント](#) (3 ページ)
- [アンダーレイ ネットワーク](#) (4 ページ)
- [オーバーレイ ネットワーク](#) (4 ページ)
- [分散型エニーキャスト ゲートウェイ](#) (4 ページ)
- [コントロールプレーン](#) (4 ページ)

ライセンス要件

Cisco NX-OS ライセンス方式の推奨の詳細と、ライセンスの取得および適用の方法については、『[Cisco NX-OS ライセンス ガイド](#)』および『[Cisco NX-OS ライセンス オプション ガイド](#)』を参照してください。

サポートされるプラットフォーム

Cisco NX-OS リリース 7.0(3)I7(1) 以降では、[Nexus スイッチ プラットフォーム サポート マトリクス](#)に基づいて、選択した機能をさまざまな Cisco Nexus 9000 および 3000 スイッチで使用するために、どの Cisco NX-OS リリースが必要かを確認してください。

VXLAN の概要

Virtual Extensible LAN (VXLAN) MAC-in-UDP のカプセル化とトンネリングを使用して、レイヤ3 インフラストラクチャを越えてレイヤ2 ネットワークを拡張する方法を提供します。この機能により、共有される共通の物理インフラストラクチャにおいて、仮想化され、マルチテナントのデータセンター デザインを可能にすることができます。

VXLAN には、次の利点があります。

- データセンター ファブリック全体でのワークロードの柔軟な配置。

これは、テナントのワークロードが単一のデータセンター内の物理ポッド全域に配置されるように、基盤となる共有ネットワーク インフラストラクチャでレイヤ2 セグメントを拡張する方法を提供します。または、地理的に多様な複数のデータセンターにまたがる場合もあります。

- より多くのレイヤ2 セグメントに対応するための高度なスケーラビリティ。

VXLAN は 24 ビットのセグメント ID、つまり VXLAN ネットワーク ID (VNID) を使用します。これにより、最大 1600 万個の VXLAN セグメントを同じ管理ドメイン内で共存させることができます。比較すると、従来の VLAN は最大 4096 個の VLAN をサポートできる 12 ビットのセグメント ID を使用します。

- 基盤となるインフラストラクチャにおける、有効なネットワーク パスの使用率。

VXLAN パケットは、レイヤ3 ヘッダーに基づいて、基盤となるネットワークを介して転送されます。これは、等コストマルチパス (ECMP) ルーティングおよびリンク集約プロトコルを使用して、有効なすべてのパスを使用します。対照的に、レイヤ2 ネットワークは、ループを回避するために有効な転送パスをブロックすることがあります。

ハードウェアベースの VXLAN ゲートウェイとしての Cisco Nexus 9000

Cisco Nexus 9000 シリーズスイッチは、ハードウェアベースの VXLAN のゲートウェイとして機能することが可能です。これは、レイヤ3 の境界を越えた 1 つの転送ドメインとして転送のパフォーマンスを低下させずに、VXLAN セグメントと VLAN セグメントをシームレスに接続します。Cisco Nexus 9000 Series ハードウェアベース VXLAN のカプセル化およびカプセル化解除により、すべてのフレーム サイズに対してラインレート パフォーマンスを提供します。

VXLAN のカプセル化およびパケット形式

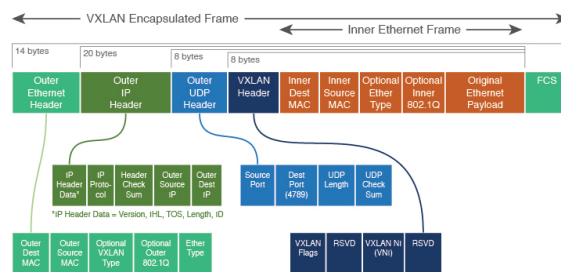
VXLAN は、レイヤ3 ネットワーク上のレイヤ2 オーバーレイ方式です。VXLAN は MAC Address-in-User Datagram Protocol (MAC-in-UDP) のカプセル化を使用して、データセンター ネットワークでレイヤ2 セグメントを拡張する方法を提供します。VXLAN は、共有される共

通の物理インフラストラクチャにおいて、柔軟で大規模なマルチテナント環境をサポートするためのソリューションです。物理データセンター ネットワークでの転送プロトコルは IP と UDP です。

VXLAN は MAC-in-UDP のカプセル化方式を定義します。この方式において、元のレイヤ 2 フレームに VXLAN ヘッダーが追加され、UDP-IP パケットに置かれます。この MAC-in-UDP のカプセル化によって、VXLAN はレイヤ 3 ネットワーク上でレイヤ 2 ネットワークをトンネルします。

VXLAN は、24 ビット VNID といくつかの予約ビットで構成される 8 バイト VXLAN ヘッダーを使用します。VXLAN ヘッダーおよび元のイーサネットフレームは、UDP ペイロードに入ります。24 ビット VNID は、レイヤ 2 セグメントを識別し、セグメント間でレイヤ 2 の分離を維持するために使用されます。VNID のすべての 24 ビットを使用して、VXLAN は 1600 万個の LAN セグメントをサポートできます。

図 1:



VXLAN トンネル

内部イーサネットフレームをカプセル化およびカプセル化解除する2つのデバイス間の VXLAN カプセル化通信は、VXLAN トンネルと呼ばれます。VXLAN トンネルは UDP カプセル化されているため、ステートレスです。

VXLAN トンネル エンドポイント

VXLAN トンネル エンドポイント (VTEP) は、VXLAN トンネルを終端するデバイスです。VXLAN カプセル化とカプセル化解除を実行します。各 VTEP 機能には、次の 2 つのインターフェイスがあります。1 つは、ブリッジングを介したローカルエンドポイント通信をサポートするローカル LAN セグメントのレイヤ 2 インターフェイスです。もう 1 つは、IP 転送ネットワーク上のレイヤ 3 インターフェイスです。

IP インターフェイスには、転送 IP ネットワークの VTEP を識別する一意の IP アドレスがあります。VTEP デバイスは、この IP アドレスを使用してイーサネットフレームをカプセル化し、カプセル化されたパケットを、IP インターフェイスを介して転送ネットワークへ送信します。VTEP は、ローカルに接続されている同じ VNID を共有する他の VTEP デバイスを検出します。ローカルに接続された MAC アドレスをピアにアドバタイズします。また、IP インターフェイスを介してリモート MAC アドレスから VTEP へのマッピングも学習します。

アンダーレイ ネットワーク

VXLAN セグメントは、基盤となる物理ネットワーク トポロジに依存しません。逆に、アンダーレイ ネットワークとも呼ばれる基盤となる IP ネットワークは、VXLAN オーバーレイから独立しています。アンダーレイ ネットワークは、外部 IP アドレス ヘッダーに基づいて VXLAN カプセル化パケットを転送します。カプセル化されたパケットは、発信元 IP アドレスとして開始 VTEP を持ち、宛先 IP アドレスとして終端 VTEP を持っており、外部 IP アドレス ヘッダーに基づいてルーティングされます。

VXLAN ファブリックのアンダーレイの主な目的は、仮想トンネルエンドポイント (VTEP) の到達可能性をアドバタイズすることです。アンダーレイは、VXLAN トラフィックの高速で信頼性の高い転送も提供します。

オーバーレイ ネットワーク

ブロードキャストの用語では、オーバーレイはアンダーレイ ネットワーク インフラストラクチャ上に構築される仮想ネットワークです。VXLAN ファブリックでは、オーバーレイ ネットワークはコントロール プレーンと VXLAN トンネルで構築されます。コントロール プレーンは、MAC アドレスの到達可能性をアドバタイズするために使用されます。VXLAN トンネルは、VTEP 間でイーサネット フレームを転送します。

分散型 エニーキャスト ゲートウェイ

分散型 エニーキャスト ゲートウェイとは、VNI の一部であるすべてのリーフで同じ IP アドレスと MAC アドレスを使用するデフォルト ゲートウェイ アドレッシングの使用を指します。そのため、直接接続されているワークロードのデフォルト ゲートウェイとしてすべての VTEP が機能します。分散型 エニーキャスト ゲートウェイ機能は、ワークロード配置の柔軟化および VXLAN ファブリック全体でのトラフィックの最適化を促進するために使用されます。

コントロール プレーン

VXLAN で使用される、広く採用されている 2 つのコントロール プレーンがあります。

フラiddiing および学習 マルチキャスト ベースの ラーニング コントロール プレーン

Cisco Nexus 9000 シリーズ スイッチは、フラiddiing およびマルチキャスト ベースのコントロール プレーン方式をサポートします。

- マルチキャスト ベースのコントロール プレーンで VXLAN を設定すると、特定の VXLAN VNI で設定されたすべての VTEP が同じマルチキャスト グループに参加します。各 VNI が独自のマルチキャスト グループを持つことも、複数の VNI が同じグループを共有することもできます。

- マルチキャストは、VNIに対して、ブロードキャスト、Unknownユニキャスト、およびマルチキャスト（BUM）トラフィックを転送するために使用されます。
- マルチキャスト設定は、Any-Source Multicast（ASM）またはPIM BiDirをサポートする必要があります。
- 最初、VTEPは、直接接続されているデバイスのMACアドレスのみを学習します。
- リモートMACアドレスからVTEPへのマッピングは、会話型学習によって学習されます。

VXLAN BGP EVPN コントロールプレーン

Cisco Nexus 9000 シリーズ スイッチは、Multiprotocol Border Gateway Protocol（MPBGP）イーサネットVPN（EVPN）コントロールプレーンを提供するように設定できます。コントロールプレーンは、レイヤ2およびレイヤ3 VXLAN オーバーレイ ネットワークを備えた分散型エニーキャスト ゲートウェイを使用します。

MPBGP EVPN コントロールプレーンでは、データセンター ネットワークについて、次のものが提供できます。

- データセンター ネットワークの物理 トポロジに制限されない、柔軟なワークロード配置。
 - データセンター ファブリック内の任意の場所に仮想マシンを配置します。
- データセンター内部およびデータセンター間における最適なサーバ間 East-West トラフィック。
 - サーバ/仮想マシン間の East-West トラフィックは、ファースト ホップ ルータでのほぼ特定されたルーティングで達成されます。ファースト ホップ ルーティングはアクセス レイヤで行われます。ホスト ルートの交換は、サーバまたはホストへの流入と送出に関するルーティングがほぼ特定されるようにする必要があります。仮想マシン（VM）モビリティは、新しいMAC アドレス/IP アドレスがローカル スイッチに直接接続されている場合に、新しいエンドポイント接続を検出することでサポートされます。ローカル スイッチは新しいMAC/IPを検出すると、ネットワークの残りの部分に新しいロケーションを通知します。
- データセンターでのフラッドイングの解消または削減。
 - フラッドイングの削減は、MAC 到達可能性情報を MP-BGP EVPN 経由で配信して L2 不明ユニキャストトラフィックに関連したフラッドイングを最適化することで行われます。ARP/IPv6 ネイバー要請に関連するブロードキャストの削減の最適化は、MPBGP EVPN を介して必要な情報を配信することによって実現されます。情報はアクセス スイッチでキャッシュされます。アドレス送信要求は、ファブリックの他の部分にブロードキャストを送信せずにローカルで応答できます。
- 特定のファブリック コントローラから独立して展開可能な標準ベースのコントロールプレーン。
 - MPBGP EVPN コントロールプレーンのアプローチで得られるもの：

- 特定のトンネルエンドポイントの背後にあるホストおよびセグメントに関連付けられたトンネルエンドポイントへの IP 到達可能性情報。
 - ホスト MAC への到達可能性の配信による不明ユニキャストフラッドイングの削減/削除。
 - ホスト IP/MAC バインディングの配信によるローカル ARP の抑制。
 - ホスト モビリティ。
 - シングルアドレス ファミリ (MPBGPEVPN) による L2 と L3 の両方のルート到達可能性情報の配信。
- レイヤ 2 およびレイヤ 3 トラフィックのセグメンテーション。
 - VXLAN カプセル化を使用したトラフィックセグメンテーションが行われ、そこでは VNI がセグメント識別子として機能します。

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。