Cisco Nexus 3600 スイッチ NX-OS VXLAN 構成ガイド、リリース 10.5(x)

最終更新：2025 年 12 月 12 日

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/

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次

はじめに

この前書きは、次の項で構成されています。

対象読者

このマニュアルは、Cisco Nexus スイッチの設置、設定、および維持に携わるネットワーク管理者を対象としています。

表記法

コマンドの説明には、次のような表記法が使用されます。

表記法	説明
bold	太字の文字は、表示どおりにユーザが入力するコマンドおよびキーワードです。
italic	イタリック体の文字は、ユーザが値を入力する引数です。
[x]	省略可能な要素（キーワードまたは引数）は、角かっこで囲んで示しています。
[x | y]	いずれか1つを選択できる省略可能なキーワードや引数は、角カッコで囲み、縦棒で区切って示しています。
{x | y}	必ずいずれか1つを選択しなければならない必須キーワードや引数は、波かっこで囲み、縦棒で区切って示しています。

表記法	説明
[x {y | z}]	角かっこまたは波かっこが入れ子になっている箇所は、任意または必須の要素内の任意または必須の選択肢であることを表します。角かっこ内の波かっこと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。
`variable`	ユーザが値を入力する変数であることを表します。イタリック体が使用できない場合に使用されます。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。

例では、次の表記法を使用しています。

表記法	説明
`screen フォント`	スイッチが表示する端末セッションおよび情報は、スクリーンフォントで示しています。
太字の screen フォント	ユーザが入力しなければならない情報は、太字のスクリーンフォントで示しています。
イタリック体の *screen* フォント	ユーザが値を指定する引数は、イタリック体の screen フォントで示しています。
<>	パスワードのように出力されない文字は、山カッコ（<>）で囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

Cisco Nexus 3600 プラットフォーム スイッチの関連資料

Cisco Nexus 3600 プラットフォーム スイッチ全体のマニュアル セットは、次の URL にあります。

http://www.cisco.com/c/en/us/support/switches/nexus-3000-series-switches/tsd-products-support-series-home.html

マニュアルに関するフィードバック

このマニュアルに関する技術的なフィードバック、または誤りや記載もれなどお気づきの点がございましたら、HTML ドキュメント内のフィードバック フォームよりご連絡ください。ご協力をよろしくお願いいたします。

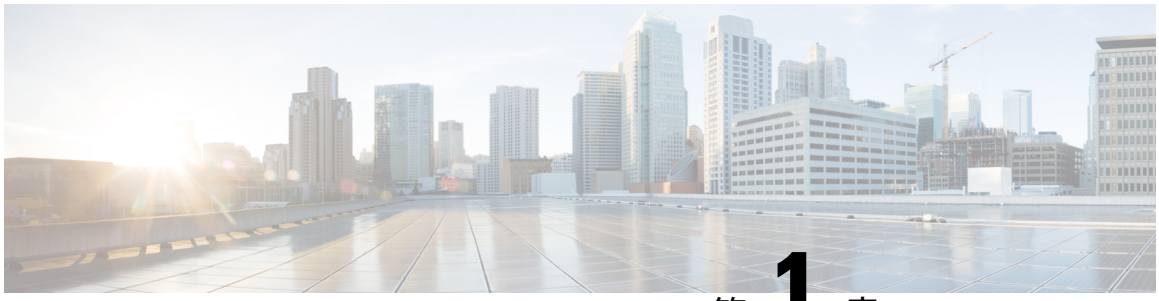
通信、サービス、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、Cisco Profile Manager でサインアップしてください。
- 重要な技術によって求めるビジネス成果を得るには、Cisco Services [英語] にアクセスしてください。
- サービス リクエストを送信するには、Cisco Support にアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、Cisco DevNet にアクセスしてください。
- 一般的なネットワーキング、トレーニング、認定関連の出版物を入手するには、Cisco Press にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、Cisco Warranty Finder にアクセスしてください。

Cisco バグ検索ツール

Cisco Bug Search Tool（BST）は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理する Cisco バグ追跡システムへのゲートウェイとして機能する、Web ベースのツールです。BST は、製品とソフトウェアに関する詳細な障害情報を提供します。

通信、サービス、およびその他の情報



第 1 章

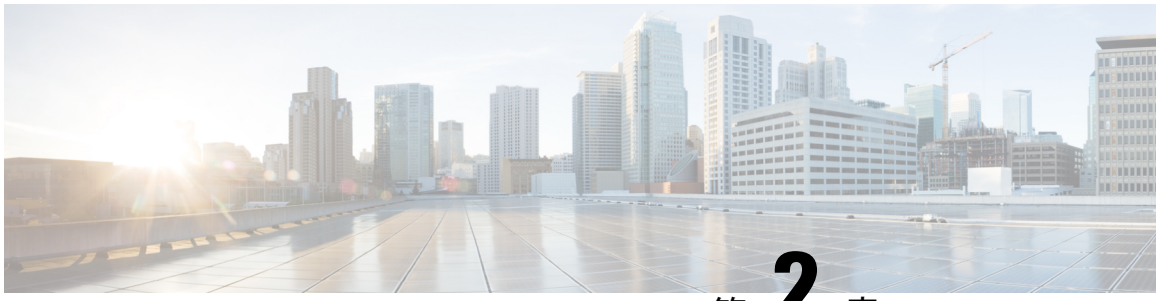
新機能および変更された機能に関する情報

新機能および変更された機能に関する情報

表 *1 : Cisco Nexus NX-OS* リリース *10.5(x)* の新機能および変更された機能

特長	説明	変更が行われたリリース	参照先
NA	このリリースで追加された新機能はありません。	10.5(1)F	N/A

新機能および変更された機能に関する情報



第 2 章

概要

ライセンス要件

Cisco NX-OS を動作させるには、機能とプラットフォームの要件に従って適切なライセンスを取得し、インストールする必要があります。

- 基本（Essential）ライセンスとアドオン ライセンスが、さまざまな機能セットに使用できます。
- ライセンスは、製品および購入オプションに応じて、永続的、一時的、または評価可能な場合があります。
- 高度な機能を使用するには、基本ライセンス以外の追加の機能ライセンスが必要です。
- 高度な機能を使用するには、基本ライセンス以外の追加ライセンスが必要です。
- ライセンスの適用と管理は、デバイスのコマンドライン インターフェイス（CLI）を介して行われます。

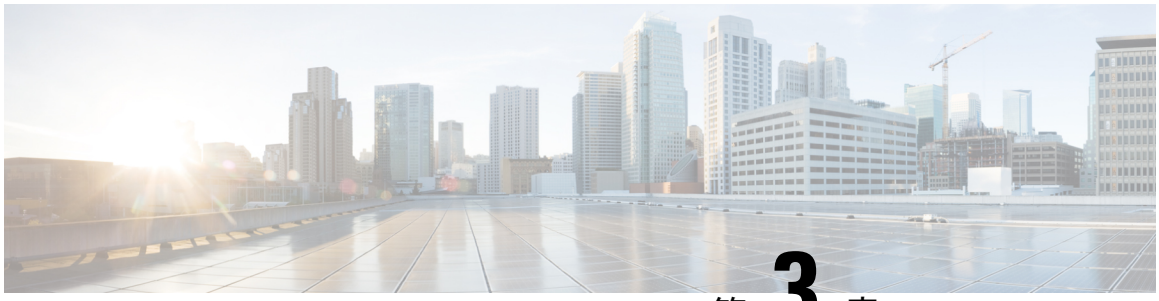
ハードウェアの取り付け手順の詳細については、次を参照してください。 *Cisco NX-OS ライセンシング ガイド* および *Cisco NX-OS ライセンシング オプション ガイド*。

サポートされるプラットフォーム

Nexus Switch プラットフォーム サポート マトリックスは、次をリストします：

- サポートされている Cisco Nexus 9000 および 3000 スイッチ モデル
- NX-OS ソフトウェア リリース バージョン

フル プラットフォーム機能マッピングは、「Nexus Switch プラットフォーム サポート マトリックス」 を参照します。



第 3 章

VXLAN の構成

この章は、次の内容で構成されています。

概要

VXLAN の概要

Cisco Nexus 3600 プラットフォーム スイッチは、ハードウェアベースの Virtual Extensible LAN（VXLAN）機能向けに設計されています。これらのスイッチは、レイヤ 3 境界を越えてレイヤ 2 接続を拡張することができます。そして、VXLAN と非 VXLAN のインフラストラクチャの間を統合します。仮想化されたそしてマルチテナントなデータ センター デザインは、共通の物理インフラストラクチャにおいて、共有することができます。

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有効にします。また、共有トランスポート

ネットワークからテナント レイヤ 2 セグメントを分離することで、マルチテナント データ センターを構築するために VXLAN を使用できます。

VXLAN ゲートウェイとして展開すると、Cisco Nexus 3600 プラットフォーム スイッチは VXLAN セグメントとクラシック VLAN セグメントを接続して共通の転送ドメインを作成し、テナント デバイスが両方の環境に存在できるようにできます。

VXLAN には、次の利点があります：

- データセンター全体でのマルチテナントセグメントの柔軟な配置。

  これは、テナントのワークロードが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 セグメントを拡張します。

- より多くのレイヤ 2 セグメントに対応できるより高い拡張性

  VXLAN は VXLAN ネットワーク ID（VNID）と呼ばれる 24 ビットのセグメント ID を使用します。VNID 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の有効なネットワーク パスの使用率。

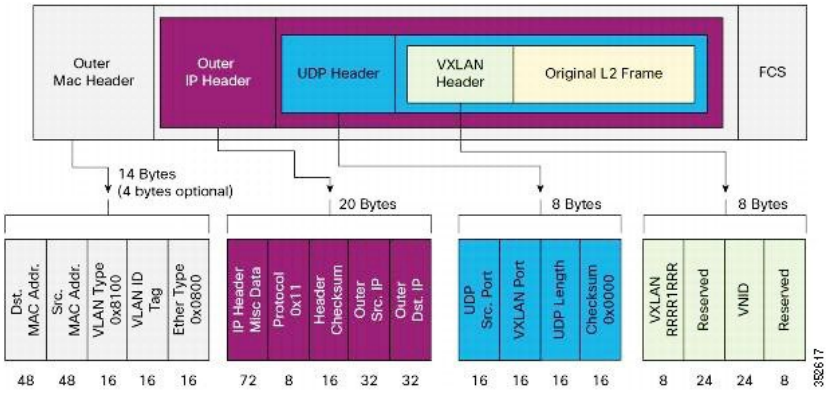
  VXLAN パケットは、レイヤ 3 ヘッダーに基づいて、基盤となるネットワークを介して転送されます。等コストマルチパス（ECMP）ルーティングおよびをリンク集約プロトコルを使用して、有効なすべてのパスを使用します。

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-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 セグメントを拡張します。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 のパケット形式を次の図に示します。

図 *1 : VXLAN* のパケット形式



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ペイロードにあります。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。VXLAN は 1600 万個の LAN セグメントをサポートできます。

VXLAN トンネル エンドポイント

VXLANはVXLANトンネルエンドポイント（VTEP）デバイスを使用してテナントのエンドデバイスを VXLAN セグメントへマッピングし、VXLAN のカプセル化およびカプセル化解除を実行します。各 VTEP デバイスには 2 つのインターフェイス タイプがあります :

- 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 セグメントのスイッチ ポート インターフェイス
- VXLAN カプセル化フレームが送信されるトランスポート ネットワークへの IP インターフェイス

VTEP デバイスは、ループバック インターフェイスの IP アドレスである一意の IP アドレスを使用して、 IP トランスポート ネットワークで識別されます。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 デバイスは、受信する VXLAN トラフィックのリモート VTEP IP アドレスとリモート MAC アドレスから VTEP IP へのマッピングを学習します。

VXLAN セグメントは基盤となるネットワーク トポロジに依存しません。逆に、VTEP 間の基盤となる IP ネットワークは、VXLAN オーバーレイに依存しません。IP ネットワークは、送信元 IP アドレスとして開始 VTEP を持ち、接続先 IP アドレスとして終端 VTEP または、マルチキャスト グループ IP アドレスを持つ外部 IP アドレス ヘッダーに基づいてカプセル化済みパケットをルーティングします。

VXLAN パケット転送フロー

VXLAN は VTEP 間のステートレス トンネルを使用して、レイヤ 3 トランスポート ネットワークを介してオーバーレイ レイヤ 2 ネットワークのトラフィックを送信します。

VXLAN との ECMP および LACP 負荷分散

カプセル化された VXLAN パケットは、転送ネットワークのネイティブの転送の決定に基づいて VTEP 間で転送されます。ほとんどのデータ センター トランスポート ネットワークは、さまざまなマルチパス ロード シェアリング テクノロジーを利用して使用可能なすべてのパスにトラフィックの負荷を分散する、複数の冗長パスで設計および展開されています。

一般的な VXLAN トランスポート ネットワークは、標準規格の IP 等コストマルチパス（ECMP）を使用して複数のベスト パス間でトラフィック負荷を分散する IP ルーティング ネットワークです。シーケンス外のパケット転送を避けるため、フローベースの ECMP が一般的に導入されています。ECMP フローは、送信元と接続先の IP アドレス、およびオプションで IP パケット ヘッダー内の送信元と接続先の TCP または UDP ポートによって定義されます。

VTEP ペア間の VXLAN パケットフローはすべて、同じ接続先送信元 IP アドレスと接続先 IP アドレスを持ちます。すべての VTEP デバイスは、インターネット Allocated Numbers Authority（IANA）が割り当てた UDP ポート 4789 かお客様構成のポート。トランスポート ネットワークの観点から VXLAN フローを区別できる ECMP フロー定義の唯一の変数要素は、送信元 UDP ポートです。ルーティングおよび ECMP の決定に基づいて解決された出力インターフェイスが LACP ポート チャネルである場合、Link Aggregation Control Protocol（LACP）ハッシュでは同様の状況が発生します。LACP は、 VXLAN 外部パケット ヘッダーをリンクのロードシェア ハッシュに使用します。これにより、送信元 UDP ポートが VXLAN フローを一意に識別できる唯一の要素になります。

VXLAN の Cisco Nexus 3600 プラットフォーム スイッチの実装では、内部フレームのヘッダーのハッシュが VXLAN 送信元 UDP ポートとして使用されます。その結果、 VXLAN フローを一意にすることができます。IP アドレスと UDP ポートの組み合わせは外部ヘッダーにあり、パケットはアンダーレイ トランスポート ネットワークを通過します。

プライマリ IP アドレスのアドバタイズ

vPC 対応リーフまたはボーダー リーフ スイッチでは、デフォルトで、すべてのレイヤ 3 ルートがリーフ スイッチ VTEP のセカンダリ IP アドレス（VIP）を BGP ネクスト ホップ IP アドレスとしてアドバタイズされます。プレフィックス ルートとリーフ スイッチで生成されたルートは、vPC リーフ スイッチ間で同期されません。これらのタイプのルートの BGP ネクスト ホップとして VIP を使用すると、トラフィックが誤った vPC リーフまたはボーダー リーフ スイッチに転送され、ブラック ホールになる可能性があります。vPC 対応リーフまたはボーダー リーフ スイッチで BGP のプレフィックス ルートまたはループバック インターフェイス ルートをアドバタイズするときにネクスト ホップとしてプライマリ IP アドレス（PIP）を使用するようにプロビジョニングすると、これらのタイプのアドバタイズ時に、BGP ネクスト ホップ

として PIP を選択できます。これにより、トラフィックは常に正しい vPC 対応リーフまたはボーダー リーフ スイッチに転送されます。

PIP をアドバタイズするための設定コマンドは **advertise-pip** です。

以下に設定サンプルを示します。

```
switch(config)# router bgp 65536
  address-family 12vpn evpn
    advertise-pip
interface nve 1
    advertise virtual-rmac
```

advertise-pip コマンドは、vPC がイネーブルの場合にプレフィックスルートまたはリーフ生成ルートをアドバタイズするときに、BGP がネクスト ホップとして PIP を使用できるようにします。

VIP で VMAC（仮想 MAC）が使用され、VIP/PIP 機能が有効になっている場合は、システム MAC が PIP で使用されます。

advertise-pip および **advertise virtual-rmac** コマンドをイネーブルにすると、タイプ 5 ルートは PIP でアドバタイズされ、タイプ 2 ルートは引き続き VIP でアドバタイズされます。さらに、VMAC は VIP で使用され、システム MAC は PIP で使用されます。

（注） この機能を正しく動作させるには、**advertise-pip** および **advertise-virtual-rmac** コマンドを同時に有効または無効にする必要があります。一方を有効または無効にすると、無効な設定と見なされます。

VXLAN の注意事項と制約事項

VXLAN には、次の注意事項と制限事項があります。

- IGMP スヌーピングは VXLAN VLAN ではサポートされています。
- VXLAN レイヤ 2 ゲートウェイ機能は、サポートされています。
- VXLANフラッドおよび学習機能はサポートされていません。
- ネットワークが VXLAN ヘッダーの追加の 50 バイトに対応できることを確認します。
- スイッチでは 1 つの網仮想化 Edge（NVE）インターフェイスのみがサポートされます。
- 非デフォルト仮想およびルーティング転送（VRF）インスタンス内のレイヤ 3 VLAN アップリンクは、サポートされいません。
- VXLANカプセル化されたトラフィックを伝送するポートのスイッチドポートアナライザ（SPAN）はサポートされていません。
- レイヤ 3 VPN 付きの VXLAN は、サポートされていません。

- 入力レプリケーションを使用した VXLAN はサポートされていません。
- MLD スヌーピングは VXLAN VLAN ではサポートされていません。
- ACL、QoS ポリシーは VXLAN VLAN ではサポートされません。
- DHCP スヌーピングは VXLAN VLAN ではサポートされません。
- L3VNI の VLAN を vPC ピアリンク トランクの許可 VLAN リストに追加する必要があります。

VXLAN 展開の考慮事項

次に、VXLAN 展開時の考慮事項の一部を示します：

- ループバック インターフェイスIPは、転送ネットワークでVTEPデバイスを一意に識別するために使用されます。
- コアでIPマルチキャストのルーティングを確立するには、IPマルチキャストの構成、PIMの構成、およびランデブーポイント（RP）の構成が必要です。
- VTEP-to-VTEP ユニキャストの到達可能性は、いずれかの IGP プロトコルを介して構成できます。
- VXLAN マルチキャスト トラフィックは、常に RPT 共有ツリーを使用する必要があります。
- VTEP でのマルチキャスト グループの RP がサポートされている設定です。ただし、スパイン レイヤ/アップストリーム デバイスでマルチキャスト グループの RP を構成する必要があります。すべてのマルチキャストトラフィックがRPを通過するので、このトラフィックをスパイン レイヤ/アップストリーム デバイスに転送する方が効率的です。

VXLAN の有効化

VXLAN の有効化には、次の操作が含まれます：

- VXLAN 機能をイネーブルにします。
- VLAN から VN セグメントへのマッピングの有効化

始める前に

VXLAN Enterprise ライセンスがインストールされていることを確認してください。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **[no] feature nv overlay**

3. switch (config)# **[no] feature vn-segment-vlan-based**
4. （任意） switch(config)# **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **[no] feature nv overlay**	VXLAN 機能をイネーブルにします。
ステップ 3	switch (config)# **[no] feature vn-segment-vlan-based**	すべての VXLAN ブリッジ ドメインにグローバル モードを設定します。 VLAN から VN-Segment へのマッピングの有効化 VLAN から VN セグメントへのマッピングは、常に 1 対 1 です。
ステップ 4	（任意） switch(config)# **copy running-config startup-config**	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

例

次に、 VXLAN をイネーブルにし、 VLAN から VN セグメントへのマッピングを構成する例を示します。

```
switch# configure terminal
switch(config)# feature nv overlay
switch(config)# feature vn-segment-vlan-based
switch(config)# copy running-config startup-config
```

VLAN から VXLAN VNI へのマッピング

手順の概要

1. switch# **configure terminal**
2. switch(config)# **vlan** *vlan-id*
3. switch(config-vlan)# **vn-segment** *vnid*

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **vlan** *vlan-id*	VLAN を指定します。
ステップ 3	switch(config-vlan)# **vn-segment** *vnid*	VXLAN 仮想ネットワーク ID（VNID）を指定します。vnid の値の範囲は 1 ～ 16777214 です。

例

次に、VLAN を VXLAN VNI にマッピングする例を示します：

```
switch# configure terminal
switch(config)# vlan 3100
switch(config-vlan)# vn-segment 5000
```

NVE ユニキャスト アドレスのルーティング プロトコルの構成

NVE ユニキャスト アドレスのルーティング プロトコルの構成

- NVE の到達可能性のための専用ループバック インターフェイスの設定。
- ルーティング プロトコル ネットワーク タイプの構成。
- インターフェイスのルーティング プロトコル インスタンスとエリアの指定。
- マルチキャスト レプリケーションの場合に PIM スパース モードを有効化します。

（注） Open Shortest Path First（OSPF）は、例では、ルーティング プロトコルとして使用されます。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface loopback** *instance*
3. switch(config-if)# **ip address** *ip-address/length*
4. switch(config-if)# **ip ospf network** {**broadcast** | **point-to-point**}
5. switch(config-if)# **ip router ospf** *instance-tag* **area** *area-id*

6. switch(config-if)# **ip pim sparse-mode**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface loopback** *instance*	NVE インターフェイスの専用のループバック インターフェイスを作成します。instance の範囲は 0 ～ 1023 です。
ステップ 3	switch(config-if)# **ip address** *ip-address/length*	このインターフェイスのIPアドレスを設定します。
ステップ 4	switch(config-if)# **ip ospf network** {**broadcast** | **point-to-point**}	OSPF ネットワーク タイプをインターフェイスのデフォルト以外のタイプに構成します。
ステップ 5	switch(config-if)# **ip router ospf** *instance-tag* **area** *area-id*	インターフェイスにOSPFインスタンスとエリアを指定します。
ステップ 6	switch(config-if)# **ip pim sparse-mode**	現在のインターフェイスで PIM スパース モードをイネーブルにします。デフォルトではディセーブルになっています。 マルチキャスト レプリケーションの場合は、PIM スパース モードを有効にします。

例

NVE ユニキャスト アドレスのルーティング プロトコルの構成

```
switch# configure terminal
switch(config)# interface loopback 10
switch(config-if)# ip address 222.2.2.1/32
switch(config-if)# ip ospf network point-to-point
switch(config-if)# ip router ospf 1 area 0.0.0.0
```

NVE インターフェイスの作成および構成

NVEインターフェイスは、VXLANトンネルを開始および終了するオーバーレイ インターフェイスです。NVE（オーバーレイ）インターフェイスを作成および構成できます。

手順の概要

1. switch# **configure terminal**

2. switch(config)# **interface nve** *instance*
3. switch(config-if-nve)# **source-interface loopback** *instance*

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface nve** *instance*	VXLAN トンネルを開始および終了する VXLAN オーバーレイ インターフェイスを作成します。 （注） スイッチでは 1 つの NVE インターフェイスのみ使用できます。
ステップ 3	switch(config-if-nve)# **source-interface loopback** *instance*	送信元インターフェイスを指定します。 送信元インターフェイスは、有効な/32 IP アドレスを持つスイッチ上に設定されているループバック インターフェイスにする必要があります。この/32 IP アドレスは、転送ネットワークの中継ルータおよびリモート VTEP によって認識される必要があります。

例

次の例は、NVE インターフェイスを作成と構成する方法を示しています：

```
switch# configure terminal
switch(config)# interface nve 1
switch(config-if-nve)# source-interface loopback 10
```

vPC での VXLAN VTEP の設定

手順の概要

1. グローバル コンフィギュレーション モードを開始します。
2. デバイスの vPC 機能を有効にします。
3. デバイスのインターフェイス VLAN 機能を有効にします。
4. デバイスの LACP 機能を有効にします。
5. デバイスの PIM 機能を有効にします。

6. デバイスの OSPF 機能を有効にします。
7. アンダーレイ マルチキャスト グループ範囲の PIM RP アドレスを定義します
8. バックアップリンクとして使用する VLAN を作成します。
9. ACL データベースの TCAM リージョンをカービングします。
10. VXLAN で使用する TCAM リージョンを割り当てます。
11. vPC ピアリンク上のバックアップ ルーテッド パスに使用する SVI を作成します。
12. プライマリおよびセカンダリ IP アドレスを作成します。
13.
14. vPC ドメインを作成します。
15. vPC ピア キープアライブ リンクのリモート エンドの IPv4 アドレスを設定します。
16. vPC ドメインでピアゲートウェイを有効にします。
17. vPC ドメインでピアスイッチを有効にします。
18. vPC ドメインで IP ARP 同期を有効にして、デバイスのリロード後の ARP テーブルの生成を高速化します。
19. （任意） vPC ドメインで IPv6 nd 同期を有効にして、デバイスのリロード後の nd テーブルの設定を高速化します。
20. vPC ピアリンク ポート チャネル インターフェイスを作成し、2 つのメンバー インターフェイスを追加します。
21. STP hello-time、forward-time、および max-age time を変更します。
22. （任意） SVI の遅延復元タイマーを有効にします。

手順の詳細

手順

ステップ 1 グローバル コンフィギュレーション モードを開始します。

```
switch# configure terminal
```

ステップ 2 デバイスの vPC 機能を有効にします。

```
switch(config)# feature vpc
```

ステップ 3 デバイスのインターフェイス VLAN 機能を有効にします。

```
switch(config)# feature interface-vlan
```

ステップ 4 デバイスの LACP 機能を有効にします。

```
switch(config)# feature lacp
```

ステップ 5 デバイスの PIM 機能を有効にします。

```
switch(config)# feature pim
```

ステップ 6 デバイスの OSPF 機能を有効にします。

```
switch(config)# feature ospf
```

ステップ 7 アンダーレイ マルチキャスト グループ範囲の PIM RP アドレスを定義します

```
switch(config)# ip pim rp-address 192.168.100.1 group-list 224.0.0.0/4
```

ステップ 8 バックアップリンクとして使用する VLAN を作成します。

```
switch(config)# vlan 10
```

ステップ 9 ACL データベースの TCAM リージョンをカービングします。

```
switch(config)# hardware access-list tcam region mac-ifacl 0
```

（注）
このコマンドは、Cisco Nexus 36180YC-R および 3636C-R vPC リーフ スイッチにのみ適用されます。

ステップ 10 VXLAN で使用する TCAM リージョンを割り当てます。

```
switch(config)# hardware access-list tcam region vxlan 10
```

（注）
このコマンドは、Cisco Nexus 36180YC-R および 3636C-R vPC リーフ スイッチにのみ適用されます。

ステップ 11 vPC ピアリンク上のバックアップ ルーテッド パスに使用する SVI を作成します。

```
switch(config)# interface vlan 10
switch(config-if)# ip address 10.10.10.1/30
switch(config-if)# ip router ospf UNDERLAY area 0
switch(config-if)# ip pim sparse-mode
switch(config-if)# no ip redirects
switch(config-if)# mtu 9216
```

ステップ 12 プライマリおよびセカンダリ IP アドレスを作成します。

```
switch(config)# interface loopback 0
switch(config-if)# description Control_plane_Loopback
switch(config-if)# ip address x.x.x.x/32
switch(config-if)# ip address y.y.y.y/32 secondary
switch(config-if)# ip router ospf process tag area area id
switch(config-if)# ip pim sparse-mode
switch(config-if)# no shutdown
```

ステップ 13

```
switch(config)# interface loopback 1
switch(config-if)# description Data_Plane_loopback
switch(config-if)# ip address z.z.z.z/32
switch(config-if)# ip router ospf process tag area area id
switch(config-if)# ip pim sparse-mode
switch(config-if)# no shutdown
```

ステップ 14 vPC ドメインを作成します。

```
switch(config)# vpc domain 10
```

ステップ 15 vPC ピア キープアライブ リンクのリモート エンドの IPv4 アドレスを設定します。

```
switch(config-vpc-domain)# peer-keepalive destination 172.28.x.x
```

（注）
vPC ピアキープアライブ リンクを設定するまで、vPC ピア リンクは構成されません。

管理ポートと VRF がデフォルトです。

（注）
独立した VRF を設定し、vPC ピアキープアライブ リンクのための VRF 内の各 vPC ピア デバイスからのレイヤ 3 ポートを使用することを推奨します。VRF の作成および設定の詳細については、『Cisco Nexus 3600 Series NX-OS Unicast Routing Configuration Guide』を参照してください。

ステップ 16 vPC ドメインでピアゲートウェイを有効にします。

```
switch(config-vpc-domain)# peer-gateway
```

（注）
この機能を正常に動作させるために、この vPC ドメインのすべてのインターフェイス VLAN 上で IP リダイレクトをディセーブルにします。

ステップ 17 vPC ドメインでピアスイッチを有効にします。

```
switch(config-vpc-domain)# peer-switch
```

（注）
この機能を正常に動作させるために、この vPC ドメインのすべてのインターフェイス VLAN 上で IP リダイレクトをディセーブルにします。

ステップ 18 vPC ドメインで IP ARP 同期を有効にして、デバイスのリロード後の ARP テーブルの生成を高速化します。

```
switch(config-vpc-domain)# ip arp synchronize
```

ステップ 19 （任意） vPC ドメインで IPv6 nd 同期を有効にして、デバイスのリロード後の nd テーブルの設定を高速化します。

```
switch(config-vpc-domain)# ipv6 nd synchronize
```

ステップ 20 vPC ピアリンク ポート チャネル インターフェイスを作成し、2 つのメンバー インターフェイスを追加します。

```
switch(config)# interface port-channel 1
switch(config-if)# switchport
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk allowed vlan 1,100-200
switch(config-if)# mtu 9216
switch(config-if)# vpc peer-link
switch(config-if)# no shutdown
switch(config-if)# interface Ethernet 1/1, 1/20
switch(config-if)# switchport
switch(config-if)# mtu 9216
switch(config-if)# channel-group 1 mode active
switch(config-if)# no shutdown
```

ステップ 21 STP hello-time、forward-time、および max-age time を変更します。

ベスト プラクティスとして、vPC ロールの変更が発生したときに不要な TCN 生成を回避するために、**hello-time** を 4 秒に変更することを推奨します。**hello-time** を変更した結果、**max-age** と **forward-time** を適宜変更することも推奨されます。

```
switch(config)# spanning-tree vlan 1-3967 hello-time 4
switch(config)# spanning-tree vlan 1-3967 forward-time 30
switch(config)# spanning-tree vlan 1-3967 max-age 40
```

ステップ 22 （任意） SVI の遅延復元タイマーを有効にします。

SVI または VNI スケールが大きい場合は、この値を調整することをお勧めします。たとえば、SVI カウントが 1000 の場合、interface-vlan の delay restore を 45 秒に設定することを推奨します。

```
switch(config-vpc-domain)# delay restore interface-vlan 45
```

VNI 複製の構成

VXLAN ネットワーク識別子（VNI）の複製は、次の 2 つの方法のいずれかで構成できます：

- マルチキャスト レプリケーション

マルチキャスト レプリケーションの構成

始める前に

- NVE インターフェイスが作成され、構成されていることを確認します。
- 送信元インターフェイスが指定されていることを確認します。

手順の概要

1. switch(config-if-nve)# **member vni** {*vnid* **mcast-group** *multicast-group-addr* | *vnid- range* **mcast-group** *start-addr* [*end-addr*]}

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	switch(config-if-nve)# **member vni** {*vnid* **mcast-group** *multicast-group-addr* | *vnid- range* **mcast-group** *start-addr* [*end-addr*]}	VXLAN VNI を NVE インターフェイスにマッピングし、マルチキャストグループを VNI に割り当てます。

例

次に、 VNIを NVE インターフェイスにマッピングし、マルチキャスト グループに割り当てる例を示します：

```
switch(config-if-nve)# member vni 5000 mcast-group 225.1.1.1
```

VXLAN を介した IGMP スヌーピングの設定

VXLAN を介した IGMP スヌーピングの概要

Cisco NX-OSリリース 7.0(3)F3(4) 以降、 VXLAN を介した IGMP スヌーピングを構成できます。IGMP スヌーピングの構成は、通常の VLAN ドメインでの IGMP スヌーピングの構成と VXLAN で同じです。IGMP スヌーピングの詳細は、『*Cisco Nexus 3600 NX-OS* マルチキャスト ルーティング構成ガイド、リリース *7.x*』の「IGMP スヌーピングを構成」章を参照してください。

VXLAN を介した IGMP スヌーピングに関する注意事項と制限事項

VXLAN を介した IGMP スヌーピングに関する注意事項と制限事項は次のとおりです。

- VXLAN を介した IGMP スヌーピングに関する注意事項と制限事項
- VXLAN を介した IGMP スヌーピングは、 FEX 対応プラットフォームおよび FEX ポートではサポートされません。

VXLAN を介した IGMP スヌーピングの設定

手順の概要

1. switch(config)# **ip igmp snooping vxlan**
2. switch(config)# **ip igmp snooping disable-nve-static-router-port**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	switch(config)# **ip igmp snooping vxlan**	VXLAN VLAN の IGMP スヌーピングを有効にします。VXLAN VLANのスヌーピングを有効にするには、このコマンドを明示的に設定する必要があります。
ステップ 2	switch(config)# **ip igmp snooping disable-nve-static-router-port**	このグローバル CLI コマンドを使用して、VXLAN 経由の IGMP スヌーピングを設定し、静的 mrouter ポートとしてNVEを含めないようにします。VXLAN を介した IGMP スヌーピングには、デフォルトで

	コマンドまたはアクション	目的
		mrouter ポートとして NVE インターフェイスがあります。

VXLAN QoS 構成の確認

次のいずれかのコマンドを活用、 VXLAN 構成を確認し、 MAC アドレスを表示し、 MAC アドレスをクリアします：

コマンド	目的
show nve interface nve *id*	NVE インターフェイスの構成を表示します。
show nve vni	NVE インターフェイスにマッピングされている VNI を表示します。
show nve peers	NVE インターフェイスのピアを表示します。
show nve vxlan-params	構成された VXLAN UDP ポートを表示します。
show mac address-table	VLAN と VXLAN の両方の MAC アドレスを表示します。
clear mac address-table dynamic	MAC アドレステーブルの全ての MAC アドレスエントリをクリアにします。

例

次の例は、NVE インターフェイスの構成を表示する方法を示しています。

```
switch# show nve interface nve 1
Interface: nve1, State: up, encapsulation: VXLAN
Source-interface: loopback10 (primary: 111.1.1.1, secondary: 0.0.0.0)
```

この例は、マルチキャスト レプリケーションの NVE インターフェイスにマッピングされている VNI を表示する方法を示しています：

```
switch# show nve vni
Interface          VNI        Multicast-group   VNI State
-----------------  ---------  ---------------   ---------
nve1               5000       225.1.1.1          Up
```

次に、入力レプリケーションの NVE インターフェイスにマッピングされている VNI を表示する例を示します：

```
switch# show nve vni
Interface          VNI        Multicast-group   VNI State
-----------------  ---------  ---------------   ---------
nve1               5000       0.0.0.0           Up
```

次に、NVE インターフェイスのピアを表示する例を示します。

```
switch# show nve peers
Interface          Peer-IP           Peer-State
----------------   ---------------   -------------
nve1               111.1.1.1          Up
```

次に、構成された VXLAN UDP ポートを表示する例を示します：

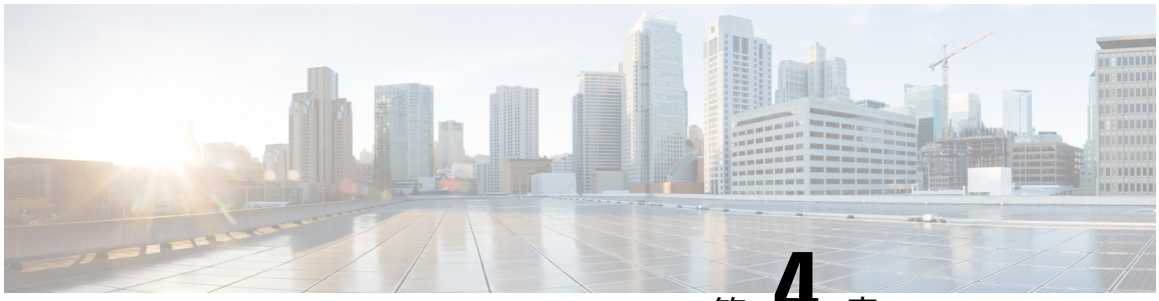
```
switch# show nve vxlan-params
VxLAN Dest. UDP Port: 4789
```

次の例は、VLAN と VXLAN の両方の MAC アドレスを表示する方法を示しています：

```
Added draft comment: hidden contentswitch# show mac address-table
Legend:
        * - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
        age - seconds since first seen,+ - primary entry using vPC Peer-Link
   VLAN     MAC Address      Type      age     Secure NTFY   Ports/SWID.SSID.LID
---------+-----------------+--------+---------+------+----+------------------
* 109      0000.0410.0902    dynamic   470        F    F  Po2233
* 109      0000.0410.0912    dynamic   470        F    F  Po2233
* 109      0000.0410.0912    dynamic   470        F    F  nve1(1.1.1.200)
* 108      0000.0410.0802    dynamic   470        F    F  Po2233
* 108      0000.0410.0812    dynamic   470        F    F  Po2233
* 107      0000.0410.0702    dynamic   470        F    F  Po2233
* 107      0000.0410.0712    dynamic   470        F    F  Po2233
* 107      0000.0410.0712    dynamic   470        F    F  nve1(1.1.1.200)
* 106      0000.0410.0602    dynamic   470        F    F  Po2233
* 106      0000.0410.0612    dynamic   470        F    F  Po2233
* 105      0000.0410.0502    dynamic   470        F    F  Po2233
* 105      0000.0410.0512    dynamic   470        F    F  Po2233
* 105      0000.0410.0512    dynamic   470        F    F  nve1(1.1.1.200)
* 104      0000.0410.0402    dynamic   470        F    F  Po2233
* 104      0000.0410.0412    dynamic   470        F    F  Po2233
```

次に、MAC アドレス テーブル内の全ての MAC アドレス エントリを消去する例を示します：

```
switch# clear mac address-table dynamic
switch#
```



第 4 章

VXLAN BGP EVPN の設定

この章は、次の内容で構成されています。

VXLAN BGP EVPN に関する情報

VXLAN BGP EVPN の注意事項と制約事項

VXLAN BGP EVPN には、次の注意事項と制約事項があります。

- コア リンクとしての SVI およびサブインターフェイスは、レイヤ 2 GW 構成ではサポートされていません。
- VXLAN EVPN セットアップでは、できれば **auto rd** コマンドを使用して、ボーダー リーフに一意のルート識別子を使用する必要があります。異なるボーダー リーフに同じルート識別子を設定することはサポートされていません。
- ARP 抑制は、VTEP がこの VNI のファーストホップ ゲートウェイ（Distributed Anycast Gateway）をホストしている場合にのみ、VNI でサポートされます。この VLAN の VTEP

とSVIは、分散型エニーキャスト ゲートウェイ動作用に適切に設定する必要があります。たとえば、グローバル エニーキャストゲートウェイ MAC アドレスが設定され、エニーキャスト ゲートウェイ機能が SVI の仮想 IP アドレスに設定されている必要があります。

- **internal** キーワードが付いている **show** コマンドはサポートされていません。
- DHCP スヌーピング（Dynamic Host Configuration Protocol スヌーピング）は VXLAN VLAN ではサポートされません。
- VXLAN アップリンク インターフェイスの SPAN はサポートされていません。
- RACL は VXLAN トラフィックのレイヤ 3 のアップリンクでサポートされません。
- RACLS および PACL はVXLAN VLAN ではサポートされません。
- QoS 分類は、 VXLAN VLAN ではサポートされていません。
- アップリンク ポートのタイプは、レイヤ3インターフェイス、サブインターフェイス、またはレイヤ3ポートチャネル インターフェイスにできます。ただし、レイヤ2では、サブインターフェイスのアップリンク ポートはサポートされていません。
- EBGP では、シングル オーバーレイ EBGP EVPN セッションをループバック間で使用することを推奨します。
- NVE を、レイヤ 3 プロトコルで必要な他のループバック アドレスとは別のループバック アドレスにバインドします。VXLANに対して専用のループバック アドレスを使用することがベスト プラクティスです。
- VXLAN BGP EVPN は、非デフォルト VRF にある NVE インターフェイスをサポートしません。
- オーバーレイ BGP セッションのループバックで単一 BGP セッションを設定することを推奨します。
- VXLAN UDP ポート番号はVXLAN カプセル化に使用されます。Cisco Nexus NX-OS では、UDP ポート番号は 4789 です。これは IETF 標準に準拠しており、変更できません。
- VXLAN は、 MPLS 機能との共存をサポートしません。
- レイヤ 3 VPN 付きの VXLAN は、サポートされていません。
- 入力レプリケーションを使用した VXLAN はサポートされていません。
- MLD スヌーピングは VXLAN VLAN ではサポートされていません。
- DHCP スヌーピングは VXLAN VLAN ではサポートされません。

VXLAN BGP EVPN 展開の考慮事項

- **source-interface config**を使用する場合は、ループバック アドレスが必要です。ループバック アドレスは、ローカル VTEP IP を表します。

- コアで IP マルチキャストのルーティングを確立するには、IP マルチキャストの設定、PIM の設定、および RP の設定が必要です。
- VTEP to VTEP ユニキャストの到達可能性は、任意の IGP/BGP プロトコルを介して設定できます。
- VTEP デバイスの IP アドレスを変更するときのベストプラクティスとして、NVE インターフェイスで使用されるループバック インターフェイスで **shut** コマンドを入力し、 IP アドレスを変更する前に **no shut** コマンドを入力します。
- 各テナント VRF は、VRF オーバーレイ、VLAN および SVI を VXLAN ルーティングに必要とします。

VXLAN 展開に対するネットワークの考慮事項

- 転送ネットワークの MTU サイズ

  MAC-to-UDP のカプセル化に起因して、VXLAN は元のフレームに 50 バイトのオーバーヘッドを導入しています。このため、転送ネットワークの最大転送単位（MTU）は 50 バイト増やす必要があります。オーバーレイで 1500 バイトの MTU を使用する場合、転送ネットワークは、最低でも 1550 バイトのパケットに対応できるように設定する必要があります。オーバーレイ アプリケーションで 1500 バイトを超えるフレーム サイズを頻繁に使用する場合は、転送ネットワークでジャンボ フレームのサポートが必要になります。

- 転送ネットワークの ECMP および LACP ハッシュ アルゴリズム

  前のセクションで説明したように、Cisco Nexus 3600 プラットフォーム スイッチは、転送ネットワークの ECMP および LACP ハッシュに対する送信元 UDP ポートのエントロピー レベルを導入しています。この実装を強化する方法として、転送ネットワークは ECMP または LACP のハッシュ アルゴリズムを使用します。これらのアルゴリズムはハッシュの入力として UDP 送信元ポートを使用し、これにより VXLAN のカプセル化されたトラフィックに対して最適なロード シェアリングを実現します。

- マルチキャスト グループの拡張

  Cisco Nexus 3600 プラットフォーム スイッチの VXLAN の実装では、ブロードキャスト、未知のユニキャスト、およびマルチキャスト トラフィックの転送に対してマルチキャスト トンネルを使用します。マルチキャスト転送を提供するには、1 つの VXLAN セグメントを 1 つの IP マルチキャスト グループにマッピングする方法が理想的です。ただし、複数の VXLAN セグメントは、コア ネットワーク内で 1 つの IP マルチキャスト グループを共有することが可能です。VXLAN は、ヘッダーの 24 ビット VNID フィールドを使用して最大 1600 万個の論理レイヤ 2 セグメントをサポートできます。VXLAN セグメントと IP マルチキャスト グループ間の 1 対 1 マッピングにより、VXLAN のセグメント数の増加に起因して、必要なマルチキャスト アドレス空間とコア ネットワーク デバイスのフォワーディング ステートの量がパラレルに増加します。ある時点で、転送ネットワークにおけるマルチキャスト スケーラビリティが問題になることがあります。この場合には、複数の VXLAN セグメントを 1 つのマルチキャスト グループにマッピングすると、コア デバイス上のマルチキャスト コントロール プレーンのリソースが節約され、目的の VXLAN のスケーラ

ビリティを実現できるようになります。ただしこのマッピングは、次善のマルチキャスト転送を犠牲にして実現されます。1つのテナントのマルチキャスト グループに転送されたパケットは、同じマルチキャスト グループを共有する他のテナントのVTEPに送信されます。このため、マルチキャストデータのプレーン リソースの使用が非効率的になります。したがってこのソリューションは、コントロール プレーンのスケーラビリティとデータ プレーンの効率性との二者択一になります。

次善のマルチキャスト複製と転送を実現しているにも関わらず、複数テナントの VXLAN ネットワークで 1 つのマルチキャスト グループを共有することで、テナント ネットワーク間のレイヤ2分離に影響をもたらすことはありません。マルチキャスト グループからカプセル化されたパケットを受信すると、VTEP はパケットの VXLAN ヘッダー内の VNID をチェックし、検証します。VTEPは、不明なVNIDが見つかるとパケットを廃棄します。VNID が VTEP のローカル VXLAN VNID のいずれかに一致する場合のみ、パケットを VXLAN セグメントに転送します。別のテナントのネットワークはパケットを受信しません。したがって、VXLAN セグメント間の分離は低下しません。

転送ネットワークの考慮事項

転送ネットワークの設定に関する考慮事項は次のとおりです。

- VTEP デバイス：
  - IP マルチキャストを有効にして、設定します。
  - /32 IP アドレスで、ループバック インターフェイスを作成および設定します。
  - ループバック インターフェイスで IP マルチキャストを有効にします。
  - 転送ネットワークで実行されるルーティング プロトコル（スタティック ルート）を通じて、ループバック インターフェイス /32 アドレスをアドバタイズします。
  - アップリンクの出力物理インターフェイス上で IP マルチキャストを有効にします。
- 転送ネットワーク全体：
  - IP マルチキャストを有効にして、設定します。

VXLAN 展開の BGP EVPN 考慮事項

VXLAN BGP EVPN の設定

VXLAN のイネーブル化

VXLAN および EVPN をイネーブルにします。

手順の概要

1. **feature vn-segment**
2. **feature nv overlay**
3. **nv overlay evpn**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**feature vn-segment**	VLAN ベースの VXLAN をイネーブルにします。
ステップ 2	**feature nv overlay**	VXLAN をイネーブルにします。
ステップ 3	**nv overlay evpn**	EVPN コントロール プレーンを VXLAN 用にイネーブルにします。

VLAN および VXLAN VNI の設定

手順の概要

1. **vlan** *number*
2. **vn-segment** *number*

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**vlan** *number*	VLAN を指定します。
ステップ 2	**vn-segment** *number*	VXLAN VLAN でのレイヤ 2 VNI を設定するために VLAN を VXLAN VNI にマッピングします。

VXLAN ルーティングの VRF の設定

テナント VRF を設定します。

手順の概要

1. **vrf context** *vxlan*
2. **vni** *number*
3. **rd auto**

4. **address-family ipv4 unicast**
5. **route-target both auto**
6. **route-target both auto evpn**
7. **address-family ipv6 unicast**
8. **route-target both auto**
9. **route-target both auto evpn**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**vrf context** *vxlan*	VRF を設定します。
ステップ 2	**vni** *number*	VNI を指定します。
ステップ 3	**rd auto**	VRF RD （ルート識別子）を指定します。
ステップ 4	**address-family ipv4 unicast**	IPv4 のアドレス ファミリを設定します。
ステップ 5	**route-target both auto**	（注） **auto** オプションの指定は IBGP のみに適用されます。 EBGP では手動で構成されたルート ターゲットが必要です。
ステップ 6	**route-target both auto evpn**	（注） **auto** オプションの指定は IBGP のみに適用されます。 EBGP では手動で構成されたルート ターゲットが必要です。
ステップ 7	**address-family ipv6 unicast**	IPv6 のアドレス ファミリを設定します。
ステップ 8	**route-target both auto**	（注） **auto** オプションの指定は IBGP のみに適用されます。 EBGP では手動で構成されたルート ターゲットが必要です。
ステップ 9	**route-target both auto evpn**	（注） **auto** オプションの指定は IBGP のみに適用されます。

	コマンドまたはアクション	目的
		EBGP では手動で構成されたルート ターゲットが必要です。

VXLAN ルーティングのホストの SVI の構成

ホストの SVI を構成します。

手順の概要

1. **vlan** *number*
2. **interface** *vlan-number*
3. **vrf member** *vxlan-number*
4. **ip address** *address*

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**vlan** *number*	VLAN を指定します
ステップ 2	**interface** *vlan-number*	VLAN インターフェイスを指定します。
ステップ 3	**vrf member** *vxlan-number*	ホストの SVI を設定します。
ステップ 4	**ip address** *address*	IP アドレスを指定します。

VXLAN ルーティングの VRF オーバーレイ VLAN の構成

手順の概要

1. **vlan** *number*
2. **vn-segment** *number*

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**vlan** *number*	VLAN を指定します。
ステップ 2	**vn-segment** *number*	vn-segment を指定します。

VXLAN ルーティングの VRF の下の VNI の構成

VRF オーバーレイ VLAN でレイヤ 3 VNI を構成します。（VRF オーバーレイ VLAN は、ポート側のサーバーに関連付けられていない VLAN です。VRF にマッピングされるすべての VXLAN VNI には、独自の内部 VLAN が割り当てられている必要があります）。

手順の概要

1. **vrf context** *vxlan*
2. **vni** *number*

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**vrf context** *vxlan*	VXLAN テナント VRF を作成します。
ステップ 2	**vni** *number*	VRF の下のレイヤ 3 VNI を構成します。

エニーキャストゲートウェイの VXLAN ルーティングの構成

手順の概要

1. **fabric forwarding anycast-gateway-mac** *address*
2. **fabric forwarding mode anycast-gateway**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**fabric forwarding anycast-gateway-mac** *address*	分散ゲートウェイの仮想 MAC アドレスを構成します （注） VTEP ごとの仮想 MAC は 1 つです （注） すべての VTEP が同じ仮想 MAC アドレスを持っている必要があります

	コマンドまたはアクション	目的
ステップ 2	**fabric forwarding mode anycast-gateway**	VLAN コンフィギュレーション モードで SVI をエニーキャスト ゲートウェイと関連付けます。

NVE インターフェイスと VNI の設定

手順の概要

1. **interface** *nve-interface*
2. **host-reachability protocol bgp**
3. **member vni** *vni* **associate-vrf**
4. **member vni** *vni*
5. **mcast-group** *address*

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**interface** *nve-interface*	NVE インターフェイスを設定します。
ステップ 2	**host-reachability protocol bgp**	これはホスト到達可能性のアドバタイズメント機構として BGP を定義します。
ステップ 3	**member vni** *vni* **associate-vrf**	レイヤ 3 VNI を、テナント VRF ごとに 1 つずつ、オーバーレイに追加します。 （注） VXLAN ルーティングのみで必要です。
ステップ 4	**member vni** *vni*	レイヤ 2 VNI をトンネル インターフェイスに追加します。 switch# member vni 900001 associate-vrf
ステップ 5	**mcast-group** *address*	mcast group を VNI 単位で構成します

VTEP での BGP の設定

手順の概要

1. **router bgp** *number*
2. **router-id** *address*

3. **neighbor** *address* **remote-as** *number*
4. **address-family ipv4 unicast**
5. **address-family l2vpn evpn**
6. （任意） **Allowas-in**
7. **send-community extended**
8. **vrf** *vrf-name*
9. **address-family ipv4 unicast**
10. **advertise** *l2vpn* **evpn**
11. **address-family ipv6 unicast**
12. **advertise** *l2vpn* **evpn**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**router bgp** *number*	BGP を設定します。
ステップ 2	**router-id** *address*	ルータ アドレスを指定します。
ステップ 3	**neighbor** *address* **remote-as** *number*	MP-BGP ネイバーを定義します。各ネイバーの下に l2vpn evpn を定義します。
ステップ 4	**address-family ipv4 unicast**	IPv4 のアドレス ファミリを設定します。
ステップ 5	**address-family l2vpn evpn**	BGP ネイバーにある VPN EVPN アドレス ファミリのレイヤ 2 を設定します。 （注） vxlan ホスト ベースのルーティング用のアドレス ファミリ ipv4 evpn
ステップ 6	（任意） **Allowas-in**	AS パスでの AS 番号の重複を許可します。すべてのリーフが同じ AS を使用しているが、スパインがリーフと異なる AS を使用している場合、このパラメータを eBGP 用のリーフに設定します。
ステップ 7	**send-community extended**	BGP ネイバーのコミュニティを設定します。
ステップ 8	**vrf** *vrf-name*	VRF を指定します。
ステップ 9	**address-family ipv4 unicast**	IPv4 のアドレス ファミリを設定します。
ステップ 10	**advertise** *l2vpn* **evpn**	EVPN ルートのアドバタイジングをイネーブルにします。
ステップ 11	**address-family ipv6 unicast**	IPv6 のアドレス ファミリを設定します。

	コマンドまたはアクション	目的
ステップ 12	**advertise** *l2vpn* **evpn**	EVPN ルートのアドバタイジングをイネーブルにします。

VXLAN ブリッジングのルート ターゲットおよび RD を構成します。

手順の概要

1. **evpn**
2. **vni** *number* **l2**
3. **rd auto**
4. **route-target import auto**
5. **route-target export auto**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**evpn**	VRF を設定する。
ステップ 2	**vni** *number* **l2**	（注） レイヤ 2 VNI のみを指定する必要があります。
ステップ 3	**rd auto**	VRF コンテキストを構成するために VRF RD（ルート識別子）を定義します。
ステップ 4	**route-target import auto**	VRF ルート ターゲットとインポート ポリシーを定義します。
ステップ 5	**route-target export auto**	VRF ルート ターゲットとエクスポート ポリシーを定義します。

スパインでの EVPN の BGP 構成

手順の概要

1. **route-map permitall permit 10**
2. **set ip next-hop unchanged**

3. **router bgp** *autonomous system number*
4. **address-family l2vpn evpn**
5. **retain route-target all**
6. **neighbor** *address* **remote-as** *number*
7. **address-family l2vpn evpn**
8. **disable-peer-as-check**
9. **send-community extended**
10. **route-map permitall out**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**route-map permitall permit 10**	ルートマップの構成 （注） ルート マップでは、EVPN ルート用にネクストホップを変更しないまま保持します。 • eBGP では必須です。 • iBGP ではオプションです。
ステップ 2	**set ip next-hop unchanged**	ネクストホップ アドレスを設定します。 （注） ルート マップでは、EVPN ルート用にネクストホップを変更しないまま保持します。 • eBGP では必須です。 • iBGP ではオプションです。
ステップ 3	**router bgp** *autonomous system number*	BGP を指定します。
ステップ 4	**address-family l2vpn evpn**	BGP ネイバーにある VPN EVPN アドレス ファミリのレイヤ 2 を設定します。
ステップ 5	**retain route-target all**	アドレス ファミリのレイヤ 2 VPN EVPN で、すべてのルート ターゲットの保持を [global] で設定します。 （注） eBGP では必須です。インポート ルート ターゲットに一致するように設定されたローカル VNI が存在しない場合、スパインがすべての EVPN ルートを保持およびアドバタイズできるようにします。

	コマンドまたはアクション	目的
ステップ 6	**neighbor** *address* **remote-as** *number*	ネイバーを定義します。
ステップ 7	**address-family l2vpn evpn**	BGP ネイバーにある VPN EVPN アドレス ファミリのレイヤ 2 を設定します。
ステップ 8	**disable-peer-as-check**	ルート アドバタイズメント時のピア AS 番号のチェックをディセーブルにします。すべてのリーフが同じASを使用しているが、スパインがリーフと異なるASを使用している場合、このパラメータをeBGP 用のスパインに設定します。 （注） eBGP では必須です。
ステップ 9	**send-community extended**	BGP ネイバーのコミュニティを設定します。
ステップ 10	**route-map permitall out**	ルート マップを適用してネクストホップを変更しないまま保持します。 （注） eBGP では必須です。

VXLAN のディセーブル化

手順の概要

1. **configure terminal**
2. **no nv overlay evpn**
3. **no feature vn-segment-vlan-based**
4. **no feature nv overlay**
5. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	コンフィギュレーション モードに入ります。
ステップ 2	**no nv overlay evpn**	EVPN コントロール プレーンをディセーブルにします。

	コマンドまたはアクション	目的
ステップ 3	**no feature vn-segment-vlan-based**	すべての VXLAN ブリッジ ドメインのグローバル モードをディセーブルにします。
ステップ 4	**no feature nv overlay**	VXLAN 機能をディセーブルにします。
ステップ 5	（任意） **copy running-config startup-config**	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

IP アドレスと MAC アドレスの重複データ検出

Cisco NX-OS は、IP と MAC アドレスの重複データ検出をサポートしています。これにより、特定のタイムインターバル（秒）内での移動回数に基づいた、IP または MAC アドレスの重複検出が行えます。

デフォルトは 180 秒以内に 5 つの移動です（移動数のデフォルトは 5 つです。タイム インターバルのデフォルトは 180 秒です）。

- IP アドレスの場合：
  - 180 秒以内に 5 つ目の移動が行われると、重複がまだ残っているかをチェックする前に、スイッチが 30 秒のロック（ホールドダウン タイマー）をスタートさせます（シーケンス ビット増加の防止措置）。こうした 30 秒ロックの実施は、最大 5 回までで（つまり 180 秒以内に 5 つの移動を 5 回分）、これを超えるとスイッチは重複エントリを恒久的にロックまたはフリーズさせます。
- MAC アドレスの場合：
  - 180 秒以内に 5 つ目の移動が行われると、重複がまだ残っているかをチェックする前に、スイッチが 30 秒のロック（ホールドダウン タイマー）をスタートさせます（シーケンス ビット増加の防止措置）。こうした 30 秒ロックの実施は、最大 3 回までで（つまり 180 秒以内に 5 つの移動を 3 回分）、これを超えるとスイッチは重複エントリを恒久的にロックまたはフリーズさせます。

次に示すのは、重複 IP 検出用に特定のタイム インターバル（秒）内での VM 移動回数を設定する場合に参考になるコマンドの例です。

コマンド	説明

`switch(config)# fabric forwarding ?`
`anycast-gateway-mac`
`dup-host-ip-addr-detection`
	使用可能なサブコマンド：
	• スイッチのエニーキャスト ゲートウェイ MAC。
	• n 秒以内の重複するホスト アドレスを検出。

コマンド	説明
`switch(config)# fabric forwarding dup-host-ip-addr-detection ?` `<1-1000>`	n秒以内に許可されるホストの移動回数。指定できる移動回数の範囲は 1 ～ 1000 です。デフォルトは、5 回です。
`switch(config)# fabric forwarding dup-host-ip-addr-detection 100 ?` `<2-36000>`	ホストの移動回数における重複データ検出のタイムアウトの秒数。指定できる範囲は 2 ～ 36000 秒で、デフォルトは 180 秒です。
`switch(config)# fabric forwarding dup-host-ip-addr-detection 100 10`	10 秒間以内での重複するホスト アドレスを検出（100 個の移動までに制限）。

次に示すのは、重複 MAC 検出用に特定のタイム インターバル（秒）内での VM 移動回数を設定する場合に参考になるコマンドの例です。

コマンド	説明

`switch(config)# l2rib dup-host-mac-detection ?`
`<1-1000>`
`default`
	L2RIB で利用可能なサブコマンド：
	• n秒以内に許可されるホストの移動回数。有効な移動回数の範囲は 1 ～ 1000 です。
	• デフォルト設定（180 秒以内に 5 つの移動）。

`switch(config)# l2rib dup-host-mac-detection 100 ?` `<2-36000>`	ホストの移動回数における重複データ検出のタイムアウトの秒数。指定できる範囲は 2 ～ 36000 秒で、デフォルトは 180 秒です。
`switch(config)# l2rib dup-host-mac-detection 100 10`	10 秒間以内での重複するホスト アドレスを検出（100 個の移動までに制限）。

VXLAN QoS 構成の確認

VXLAN の構成情報を表示するには、次のいずれかのコマンドを入力します：

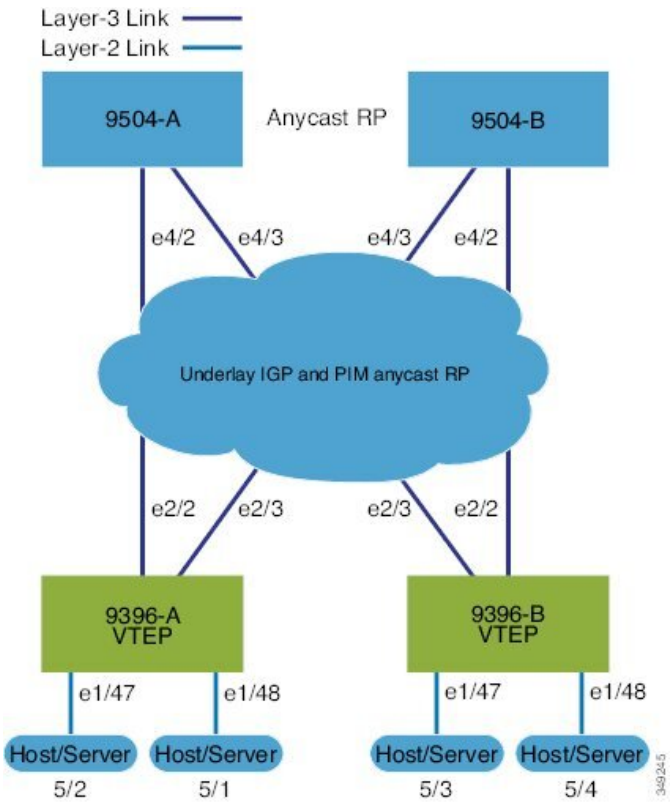
コマンド	目的
show tech-support vxlan	関連する VXLAN テクニカル サポート情報を表示します。

コマンド	目的
show logging level nve	ロギング レベルを表示します。
show tech-support nve	関連する NVE テクニカル サポート情報を表示します。
show tech-support vxlan-evpn	関連する VXLAN EVPN テクニカル サポート情報を表示します。
show tech-support vxlan platform	VXLANプラットフォームに関連したテクニカル サポート情報を表示します。
show run interface nve	NVEオーバーレイ インターフェイスの構成を表示します。
show nve interface	NVEオーバーレイ インターフェイスのステータスを表示します。
show nve peers	NVE ピアのステータスを表示します。
show nve peers *peer_IP_address* **interface** *interface_ID* **counters**	NVE ピア統計ごとに表示します。
clear nve peers *peer_IP_address* **interface** *interface_ID* **counters**	NVE ピア統計ごとにクリアします。
show nve vni	VXLAN VNI ステータスを表示します。
show nve vxlan-params	VXLAN 接続先や UDP ポートなどの VXLAN パラメータを表示します。

VXLAN BGP EVPN の例（EBGP）

VXLAN BGP EVPN の例（EBGP）。

図 *2 : VXLAN BGP EVPN* のトポロジ（*EBGP*）



スパインとリーフ間の EBGP

- スパイン（9504-A）
  - EVPN コントロール プレーンを有効にします。

    ```
    nv overlay evpn
    ```

  - 関連するプロトコルを有効にします。

    ```
    feature bgp
    feature pim
    ```

  - ローカル VTEP IP、および BGP のループバックを設定します。

    ```
    interface loopback0
      ip address 10.1.1.1/32
      ip pim sparse-mode
    ```

  - エニーキャスト RP のループバックを設定します。

    ```
    interface loopback1
      ip address 100.1.1.1/32
      ip pim sparse-mode
    ```

  - エニーキャスト RP を設定します。

```
ip pim rp-address 100.1.1.1 group-list 225.0.0.0/8
ip pim rp-candidate loopback1 group-list 225.0.0.0/8
ip pim log-neighbor-changes
ip pim ssm range 232.0.0.0/8
ip pim anycast-rp 100.1.1.1 10.1.1.1
ip pim anycast-rp 100.1.1.1 20.1.1.1
```

- スパインで EBGP が使用する route-map を設定します。

```
route-map permitall permit 10
  set ip next-hop unchanged
```

- アンダーレイ ルーティング用の OSPF を有効にします。

```
router ospf 1
  log-adjacency-changes detail
```

- スパインとリーフの相互接続用のインターフェイスを設定します。

```
interface Ethernet4/2
  ip address 192.168.1.42/24
  ip pim sparse-mode
  no shutdown

interface Ethernet4/3
  ip address 192.168.2.43/24
  ip pim sparse-mode
  no shutdown
```

- EVPN アドレス ファミリ用の BGP オーバーレイを設定します。

```
router bgp 100
  router-id 10.1.1.1
  address-family l2vpn evpn
    nexthop route-map permitall
    retain route-target all
  neighbor 30.1.1.1 remote-as 200
    update-source loopback0
    ebgp-multihop 3
    address-family l2vpn evpn
      disable-peer-as-check
      send-community extended
      route-map permitall out
  neighbor 40.1.1.1 remote-as 200
    update-source loopback0
    ebgp-multihop 3
    address-family l2vpn evpn
      disable-peer-as-check
      send-community extended
      route-map permitall out
```

- BGP アンダーレイを構成します。

```
neighbor 192.168.1.43 remote-as 200
    address-family ipv4 unicast
      allowas-in
      disable-peer-as-check
```

- スパイン（9504-B）
  - EVPN コントロール プレーンおよび関連プロトコルを有効にします

```
feature telnet
feature nxapi
feature bash-shell
feature scp-server
nv overlay evpn
feature bgp
feature pim
feature lldp
```

  - エニーキャスト RP を設定します。

```
ip pim rp-address 100.1.1.1 group-list 225.0.0.0/8
ip pim rp-candidate loopback1 group-list 225.0.0.0/8
ip pim log-neighbor-changes
ip pim ssm range 232.0.0.0/8
ip pim anycast-rp 100.1.1.1 10.1.1.1
ip pim anycast-rp 100.1.1.1 20.1.1.1
vlan 1-1002
route-map permitall permit 10
  set ip next-hop unchanged
```

  - スパインとリーフの相互接続用のインターフェイスを設定します。

```
interface Ethernet4/2
  ip address 192.168.4.42/24
  no shutdown

interface Ethernet4/3
  ip address 192.168.3.43/24
  no shutdown
```

  - ローカル VTEP IP、および BGP のループバックを設定します。

```
interface loopback0
  ip address 20.1.1.1/32
```

  - EVPN アドレス ファミリ用の BGP オーバーレイを設定します。

```
router bgp 100
  router-id 20.1.1.1
  address-family l2vpn evpn
    retain route-target all
  neighbor 30.1.1.1 remote-as 200
    update-source loopback0
    ebgp-multihop 3
    address-family l2vpn evpn
      disable-peer-as-check
      send-community extended
      route-map permitall out
  neighbor 40.1.1.1 remote-as 200
    ebgp-multihop 3
    address-family l2vpn evpn
      disable-peer-as-check
```

```
      send-community extended
      route-map permitall out
```

- BGP アンダーレイを構成します。

```
neighbor 192.168.1.43 remote-as 200
    address-family ipv4 unicast
      allowas-in
      disable-peer-as-check
```

- リーフ（9396-A）
  - EVPN コントロール プレーンを有効にします。

```
nv overlay evpn
```

  - 関連するプロトコルを有効にします。

```
feature bgp
feature interface-vlan
feature dhcp
```

  - BGP EVPN を使用して分散エニーキャスト ゲートウェイの配置された VxLAN を有効にします。

```
feature vn-segment-vlan-based
feature nv overlay
fabric forwarding anycast-gateway-mac 0000.2222.3333
```

  - PIM RP をイネーブルにします。

```
ip pim rp-address 100.1.1.1 group-list 225.0.0.0/8
```

  - BGP のループバックを構成します。

```
interface loopback0
  ip address 30.1.1.1/32
```

  - ローカル VTEP IP のループバックを設定します。

```
interface loopback1
  ip address 50.1.1.1/32
```

  - スパインとリーフの相互接続用のインターフェイスを設定します。

```
interface Ethernet2/2
  no switchport
  load-interval counter 1 5
  ip address 192.168.1.22/24
  no shutdown

interface Ethernet2/3
  no switchport
  load-interval counter 1 5
```

```
  ip address 192.168.3.23/24
  no shutdown
```

- VRF オーバーレイ VLAN を作成し、vn-segment を構成します。

```
vlan 101
  vn-segment 900001
```

- VRF 用の VRF オーバーレイ VLAN/SVI を構成：

```
interface Vlan101
  no shutdown
  vrf member vxlan-900001
```

- VLAN を作成し、VXLAN のマッピングを割り当てます。

```
vlan 1001
  vn-segment 2001001
vlan 1002
  vn-segment 2001002
```

- VRF を作成し、VNI を設定します。

```
vrf context vxlan-900001
  vni 900001
```

（注） オーバーライドとして 1 つ以上を入力しない限り、 **rd auto** および **route-target** コマンドは自動的に構成されます。

```
  rd auto
  address-family ipv4 unicast
    route-target import 65535:101 evpn
    route-target export 65535:101 evpn
    route-target import 65535:101
    route-target export 65535:101
  address-family ipv6 unicast
    route-target import 65535:101 evpn
    route-target export 65535:101 evpn
    route-target import 65535:101
    route-target export 65535:101
```

- サーバ側 SVI を作成し、分散エニーキャスト ゲートウェイを有効にします。

```
interface Vlan1001
  no shutdown
  vrf member vxlan-900001
  ip address 4.1.1.1/24
  ipv6 address 4:1:0:1::1/64
  fabric forwarding mode anycast-gateway
  ip dhcp relay address 192.168.100.1 use-vrf default

interface Vlan1002
  no shutdown
```

```
  vrf member vxlan-900001
  ip address 4.2.2.1/24
  ipv6 address 4:2:0:1::1/64
  fabric forwarding mode anycast-gateway
```

-

（注） NVEインターフェイスを作成するには、次の2つのオプションのいずれかを選択できます。少数のVNIにはオプション1を使用します。多数のVNIを構成するには、オプション2を使用します。

ネットワーク仮想化エンドポイント（NVE）インターフェイスを作成します。

オプション1

```
interface nve1
  no shutdown
  source-interface loopback1
  host-reachability protocol bgp
  member vni 10000 associate-vrf
  mcast-group 224.1.1.1
  member vni 10001 associate-vrf
  mcast-group 224.1.1.1
  member vni20000
  suppress-arp
  mcast-group 225.1.1.1
  member vni 20001
  suppress-arp
  mcast-group 225.1.1.1
```

オプション2

```
interface nve1
  no shutdown
  source-interface loopback 1
  host-reachibility protocol bgp
  global suppress-arp
  global mcast-group 224.1.1.1 L3
  global mcast-group 255.1.1.1 L2
  member vni 10000 associate-vrf
  member vni 10001 associate-vrf
  member vni 10002 associate-vrf
  member vni 10003 associate-vrf
  member vni 10004 associate-vrf
  member vni 10005 associate-vrf
  member vni 20000
  member vni 20001
  member vni 20002
  member vni 20003
  member vni 20004
  member vni 20005
```

- ホスト/サーバのインターフェイスを設定します。

```
interface Ethernet1/47
  switchport access vlan 1002
```

```
interface Ethernet1/48
  switchport access vlan 1001
```

- BGP を設定します。

```
router bgp 200
router-id 30.1.1.1
  neighbor 10.1.1.1 remote-as 100
    update-source loopback0
    ebgp-multihop 3
      allowas-in
      send-community extended
    address-family l2vpn evpn
      allowas-in
      send-community extended
  neighbor 20.1.1.1 remote-as 100
    update-source loopback0
    ebgp-multihop 3
      allowas-in
      send-community extended
    address-family l2vpn evpn
      allowas-in
      send-community extended
  vrf vxlan-900001

      advertise l2vpn evpn
```

（注） EVPN モードで次のコマンドを入力する必要はありません。

```
evpn
  vni 2001001 l2
  vni 2001002 l2
```

（注） オーバーライドとして 1 つ以上を入力しない限り、 **rd auto** および **route-target auto** コマンドは自動的に構成されます。

```
rd auto
route-target import auto
route-target export auto



router bgp 200
router-id 30.1.1.1
  neighbor 10.1.1.1 remote-as 100
    update-source loopback0
    ebgp-multihop 3
      allowas-in
      send-community extended
    address-family l2vpn evpn
      allowas-in
      send-community extended
  neighbor 20.1.1.1 remote-as 100
    update-source loopback0
    ebgp-multihop 3
      allowas-in
```

```
      send-community extended
    address-family l2vpn evpn
      allowas-in
      send-community extended
  vrf vxlan-900001
advertise l2vpn evpn
```

（注） 次の **advertise** コマンドはオプションです。

```
advertise l2vpn evpn
```

（注） オーバーライドとして 1 つ以上を入力しない限り、 **rd auto** および **route-target** コマンドは自動的に構成されます。

（注） 次の EVPN モード コマンドは、オプションです。

```
evpn
  vni 2001001 l2
  vni 2001002 l2
```

- リーフ（9396-B）
  - EVPN コントロール プレーンおよび関連プロトコルを有効にします

```
feature telnet
feature nxapi
feature bash-shell
feature scp-server
nv overlay evpn
feature bgp
feature pim
feature interface-vlan
feature vn-segment-vlan-based
feature lldp
feature nv overlay
```

  - BGP EVPN を使用して分散エニーキャスト ゲートウェイの配置された VxLAN を有効にします。

```
fabric forwarding anycast-gateway-mac 0000.2222.3333
```

  - VRF オーバーレイ VLAN を作成し、vn-segment を構成します

```
vlan 1-1002
vlan 101
  vn-segment 900001
```

- VLAN を作成し、VXLAN のマッピングを割り当てます。

```
vlan 1001
  vn-segment 2001001
vlan 1002
  vn-segment 2001002
```

- VRF を作成し、VNI を設定します。

```
vrf context vxlan-900001
  vni 900001
```

（注） 次のコマンドは、1 つ以上がオーバーライドとして入力されない限り、自動的に設定されます。

```
  rd auto
  address-family ipv4 unicast
    route-target import 65535:101 evpn
    route-target export 65535:101 evpn
    route-target import 65535:101
    route-target export 65535:101
  address-family ipv6 unicast
    route-target import 65535:101 evpn
    route-target export 65535:101 evpn
    route-target import 65535:101 evpn
    route-target export 65535:101 evpn
```

- VRF の内部コントロール VLAN/SVI を構成します

```
interface Vlan1

interface Vlan101
  no shutdown
  vrf member vxlan-900001
```

- サーバ側 SVI を作成し、分散エニーキャスト ゲートウェイを有効にします。

```
interface Vlan1001
  no shutdown
  vrf member vxlan-900001
  ip address 4.1.1.1/24
  ipv6 address 4:1:0:1::1/64
  fabric forwarding mode anycast-gateway

interface Vlan1002
  no shutdown
  vrf member vxlan-900001
  ip address 4.2.2.1/24
  ipv6 address 4:2:0:1::1/64
  fabric forwarding mode anycast-gateway
```

- ネットワーク仮想化エンドポイント（NVE）インターフェイスを作成します。

（注） NVEインターフェイスを作成するには、次の2つの手順のいずれかを選択できます。少数のVNIにはオプション1を使用します。多数の VNI を構成するには、オプション 2 を使用します。

オプション 1

```
interface nve1
  no shutdown
  source-interface loopback1
  host-reachability protocol bgp
  member vni 10000 associate-vrf
  mcast-group 224.1.1.1
  member vni 10001 associate-vrf
  mcast-group 224.1.1.1
  member vni20000
  suppress-arp
  mcast-group 225.1.1.1
  member vni 20001
  suppress-arp
  mcast-group 225.1.1.1
```

オプション 2

```
interface nve1
  no shutdown
  source-interface loopback 1
  host-reachibility protocol bgp
  global suppress-arp
  global mcast-group 224.1.1.1 L3
  global mcast-group 255.1.1.1 L2
  member vni 10000 associate-vrf
  member vni 10001 associate-vrf
  member vni 10002 associate-vrf
  member vni 10003 associate-vrf
  member vni 10004 associate-vrf
  member vni 10005 associate-vrf
  member vni 20000
  member vni 20001
  member vni 20002
  member vni 20003
  member vni 20004
  member vni 20005
```

- ホスト/サーバのインターフェイスを設定します。

```
interface Ethernet1/47
  switchport access vlan 1002

interface Ethernet1/48
  switchport access vlan 1001
```

- スパインとリーフの相互接続用のインターフェイスを設定します。

```
interface Ethernet2/1
```

```
interface Ethernet2/2
  no switchport
  load-interval counter 1 5
  ip address 192.168.4.22/24
  ip pim sparse-mode
  no shutdown

interface Ethernet2/3
  no switchport
  load-interval counter 1 5
  ip address 192.168.2.23/24
  ip pim sparse-mode
  no shutdown
```

- BGP のループバックを構成します。

```
interface loopback0
  ip address 40.1.1.1/32
```

- ローカル VTEP IP のループバックを設定します。

```
interface loopback1
  ip address 51.1.1.1/32
  ip pim sparse-mode
```

- BGP の設定

```
router bgp 200
router-id 40.1.1.1
  neighbor 10.1.1.1 remote-as 100
    update-source loopback0
    ebgp-multihop 3
      allowas-in
      send-community extended
    address-family l2vpn evpn
      allowas-in
      send-community extended
  neighbor 20.1.1.1 remote-as 100
    update-source loopback0
    ebgp-multihop 3
      allowas-in
      send-community extended
    address-family l2vpn evpn
      allowas-in
      send-community extended
  vrf vxlan-900001
      advertise l2vpn evpn
```

（注） 次の **advertise** コマンドはオプションです。

```
advertise l2vpn evpn
```

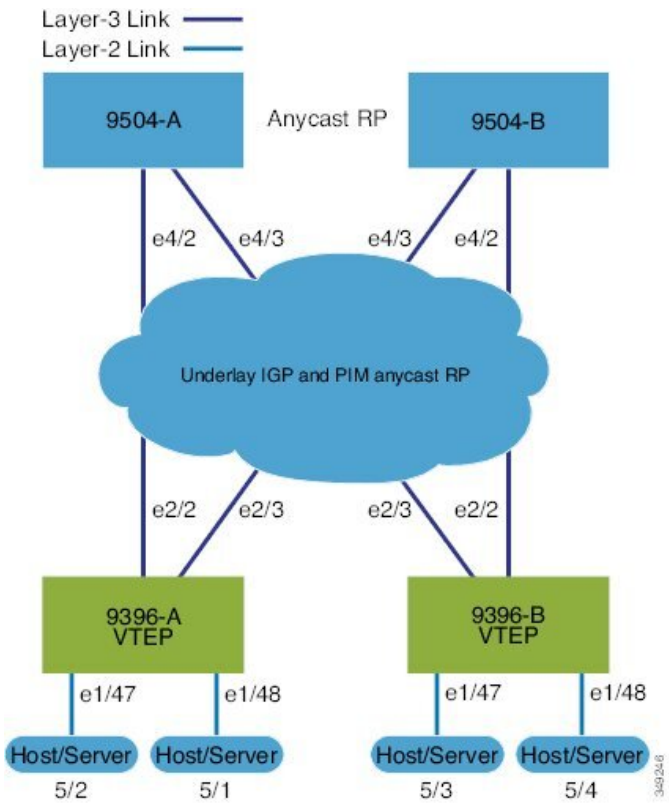
（注） **rd auto** および **route-target** コマンドは、**import** または **export** オプションを上書きするために使用しない限り、オプションです。

```
evpn
  vni 2001001 l2
    rd auto
    route-target import auto
    route-target export auto
  vni 2001002 l2
    rd auto
    route-target import auto
    route-target export auto
```

VXLAN BGP EVPN の例（IBGP）

VXLAN BGP EVPN の例（IBGP）。

図 *3 : VXLAN BGP EVPN* のトポロジ（*IBGP*）



スパインとリーフ間の IBGP

- スパイン（9504-A）

- EVPN コントロール プレーンを有効にします。

```
nv overlay evpn
```

- 関連するプロトコルを有効にします。

```
feature ospf
feature bgp
```

- ローカル VTEP IP、および BGP のループバックを設定します。

```
interface loopback0
  ip address 10.1.1.1/32
  ip router ospf 1 area 0.0.0.0
```

- アンダーレイ ルーティング用の OSPF を有効にします。

```
router ospf 1
```

- スパインとリーフの相互接続用のインターフェイスを設定します。

```
interface Ethernet4/2
  ip address 192.168.1.42/24
  ip router ospf 1 area 0.0.0.0
  no shutdown

interface Ethernet4/3
  ip address 192.168.2.43/24
  ip router ospf 1 area 0.0.0.0
  no shutdown
```

- BGP を設定します。

```
router bgp 65535
router-id 10.1.1.1
  neighbor 30.1.1.1 remote-as 65535
    update-source loopback0
    address-family l2vpn evpn
      send-community both
      route-reflector-client
  neighbor 40.1.1.1 remote-as 65535
    update-source loopback0
    address-family l2vpn evpn
      send-community both
      route-reflector-client
```

- スパイン（9504-B）
  - EVPN コントロール プレーンおよび関連プロトコルを有効にします

```
feature telnet
feature nxapi
feature bash-shell
feature scp-server
nv overlay evpn
feature ospf
```

```
feature bgp
feature lldp
```

- スパインとリーフの相互接続用のインターフェイスを設定します。

```
interface Ethernet4/2
  ip address 192.168.4.42/24
  ip router ospf 1 area 0.0.0.0
  no shutdown

interface Ethernet4/3
  ip address 192.168.3.43/24
  ip router ospf 1 area 0.0.0.0
  no shutdown
```

- ローカル VTEP IP、および BGP のループバックを設定します。

```
interface loopback0
  ip address 20.1.1.1/32
  ip router ospf 1 area 0.0.0.0
```

- エニーキャスト RP のループバックを設定します。

```
interface loopback1
  ip address 100.1.1.1/32
  ip router ospf 1 area 0.0.0.0
```

- アンダーレイ ルーティング用の OSPF を有効にします。

```
router ospf 1
```

- BGP を設定します。

```
router bgp 65535
router-id 20.1.1.1
  neighbor 30.1.1.1 remote-as 65535
    update-source loopback0
    address-family l2vpn evpn
      send-community both
      route-reflector-client
  neighbor 40.1.1.1 remote-as 65535
    update-source loopback0
     address-family l2vpn evpn
      send-community both
      route-reflector-client
```

- リーフ（9396-A）
  - EVPN コントロール プレーンを有効にします。

```
nv overlay evpn
```

  - 関連するプロトコルを有効にします。

```
feature ospf
```

```
feature bgp
feature interface-vlan
```

- アンダーレイ ルーティング用の OSPF を有効にします。

```
router ospf 1
```

- ローカル VTEP IP、および BGP のループバックを設定します。

```
interface loopback0
  ip address 30.1.1.1/32
  ip router ospf 1 area 0.0.0.0
```

- スパインとリーフの相互接続用のインターフェイスを設定します。

```
interface Ethernet2/2
  no switchport
  ip address 192.168.1.22/24
  ip router ospf 1 area 0.0.0.0
  no shutdown

interface Ethernet2/3
  no switchport
  ip address 192.168.3.23/24
  ip router ospf 1 area 0.0.0.0
  no shutdown
```

- オーバーレイ VRF VLAN を作成し、vn-segment を設定します。

```
vlan 101
  vn-segment 900001
```

- VRF 用の VRF オーバーレイ VLAN/SVI を構成：

```
interface Vlan101
  no shutdown
  vrf member vxlan-900001
```

- VLAN を作成し、VXLAN のマッピングを割り当てます。

```
vlan 1001
  vn-segment 2001001
vlan 1002
  vn-segment 2001002
```

- VRF を作成し、VNI を設定します。

```
vrf context vxlan-900001
  vni 900001
```

（注） オーバーライドとして 1 つ以上を入力しない限り、 **rd auto** および **route-target** コマンドは自動的に構成されます。

```
rd auto
  address-family ipv4 unicast
    route-target both auto
    route-target both auto evpn
  address-family ipv6 unicast
    route-target both auto
    route-target both auto evpn
```

- サーバ側 SVI を作成し、分散エニーキャスト ゲートウェイを有効にします。

```
interface Vlan1001
  no shutdown
  vrf member vxlan-900001
  ip address 4.1.1.1/24
  ipv6 address 4:1:0:1::1/64
  fabric forwarding mode anycast-gateway

interface Vlan1002
  no shutdown
  vrf member vxlan-900001
  ip address 4.2.2.1/24
  ipv6 address 4:2:0:1::1/64
  fabric forwarding mode anycast-gateway
```

-

（注） NVEインターフェイスを作成するには、次の2つのオプションのいずれかを選択できます。少数のVNIにはオプション1を使用します。多数のVNIを構成するには、オプション2を使用します。

ネットワーク仮想化エンドポイント（NVE）インターフェイスを作成します。

オプション 1

```
interface nve1
  no shutdown
  source-interface loopback0
  host-reachability protocol bgp
  member vni 900001 associate-vrf
  member vni 2001001
    suppress-arp
    mcast-group 225.4.0.1
  member vni 2001002
    suppress-arp
    mcast-group 225.4.0.1
```

オプション 2

```
Interface nve1
  source-interface loopback 1
  host-reachability protocol bgp
  global suppress-arp
  global mcast-group 255.1.1.1 L2
  global mcast-group 255.1.1.2 L3
  member vni 10000
  member vni 20000
  member vni 30000
```

• BGP を設定します。

```
router bgp 65535
router-id 30.1.1.1
  neighbor 10.1.1.1 remote-as 65535
    update-source loopback0
    address-family l2vpn evpn
      send-community both
  neighbor 20.1.1.1 remote-as 65535
    update-source loopback0
    address-family l2vpn evpn
      send-community both
  vrf vxlan-900001
    address-family ipv4 unicast
      advertise l2vpn evpn
```

（注） EVPN モードで次のコマンドを入力する必要はありません。

```
evpn
  vni 2001001 l2
  vni 2001002 l2
```

（注） オーバーライドとして 1 つ以上を入力しない限り、 **rd auto** および **route-target auto** コマンドは自動的に構成されます。

```
rd auto
    route-target import auto
    route-target export auto
```

（注） **rd auto** および **route-target** コマンドは、 **import** または **export** オプションを上書きするために使用しない限り、自動的に構成されます。

（注） 次の EVPN モード コマンドは、オプションです。

```
evpn
  vni 2001001 l2
    rd auto
    route-target import auto
    route-target export auto
  vni 2001002 l2
    rd auto
    route-target import auto
    route-target export auto
```

• リーフ（9396-B）

- EVPN コントロール プレーン機能および関連プロトコルを有効にします

```
feature telnet
feature nxapi
feature bash-shell
feature scp-server
nv overlay evpn
feature ospf
feature bgp
feature interface-vlan
feature vn-segment-vlan-based
feature lldp
feature nv overlay
```

- BGP EVPN を使用して分散エニーキャスト ゲートウェイの配置された VxLAN を有効にします。

```
fabric forwarding anycast-gateway-mac 0000.2222.3333
```

- オーバーレイ VRF VLAN を作成し、vn-segment を設定します。

```
vlan 1-1002
vlan 101
  vn-segment 900001
```

- VLAN を作成し、VXLAN のマッピングを割り当てます。

```
vlan 1001
  vn-segment 2001001
vlan 1002
  vn-segment 2001002
```

- VRF を作成し、VNI を設定します。

```
vrf context vxlan-900001
  vni 900001
```

（注） **rd auto** および **route-target** コマンドは、 **import** または **export** オプションを上書きするために使用しない限り、自動的に構成されます。

```
rd auto
  address-family ipv4 unicast
    route-target both auto
    route-target both auto evpn
  address-family ipv6 unicast
    route-target both auto
    route-target both auto evpn
```

- VRF の内部コントロール VLAN/SVI を構成します

```
interface Vlan101
  no shutdown
  vrf member vxlan-900001
```

- サーバ側 SVI を作成し、分散エニーキャスト ゲートウェイを有効にします。

```
interface Vlan1001
  no shutdown
  vrf member vxlan-900001
  ip address 4.1.1.1/24
  ipv6 address 4:1:0:1::1/64
  fabric forwarding mode anycast-gateway

interface Vlan1002
  no shutdown
  vrf member vxlan-900001
  ip address 4.2.2.1/24
  ipv6 address 4:2:0:1::1/64
  fabric forwarding mode anycast-gateway
```

-

（注） NVE インターフェイスを作成するには、次の 2 つのコマンド プロシージャのいずれかを選択できます。少数の VNI にはオプション 1 を使用します。多数の VNI を構成するには、オプション 2 を使用します。

ネットワーク仮想化エンドポイント（NVE）インターフェイスを作成します。

オプション 1

```
interface nve1
  no shutdown
  source-interface loopback0
  host-reachability protocol bgp
  member vni 900001 associate-vrf
  member vni 2001001
    suppress-arp
    mcast-group 225.4.0.1
  member vni 2001002
    suppress-arp
    mcast-group 225.4.0.1
```

オプション 2

```
Interface nve1
  source-interface loopback0
  host-reachability protocol bgp
  global suppress-arp
  global mcast-group 255.4.0.1
  member vni 900001
  member vni 2001001
```

- ホスト/サーバのインターフェイスを設定します。

```
interface Ethernet1/47
  switchport access vlan 1002

interface Ethernet1/48
  switchport access vlan 1001
```

- スパインとリーフの相互接続用のインターフェイスを設定します。

```
interface Ethernet2/1

interface Ethernet2/2
  no switchport
  ip address 192.168.4.22/24
  ip router ospf 1 area 0.0.0.0
  no shutdown

interface Ethernet2/3
  no switchport
  ip address 192.168.2.23/24
  ip router ospf 1 area 0.0.0.0
  no shutdown
```

- ローカル VTEP IP、および BGP のループバックを設定します。

```
interface loopback0
  ip address 40.1.1.1/32
  ip router ospf 1 area 0.0.0.0
```

- アンダーレイ ルーティング用の OSPF を有効にします。

```
router ospf 1
```

- BGP の設定

```
router bgp 65535
router-id 40.1.1.1
  neighbor 10.1.1.1 remote-as 65535
    update-source loopback0
    address-family l2vpn evpn
      send-community both
  neighbor 20.1.1.1 remote-as 65535
    update-source loopback0
    address-family l2vpn evpn
      send-community both
  vrf vxlan-900001
    address-family ipv4 unicast
      advertise l2vpn evpn
evpn
  vni 2001001 l2
    rd auto
    route-target import auto
    route-target export auto
  vni 2001002 l2
    rd auto
    route-target import auto
    route-target export auto
```

（注） **rd auto** および **route-target** コマンドは、**import** または **export** オプションを上書きするために使用しない限り、オプションです。

```
evpn
  vni 2001001 l2
    rd auto
    route-target import auto
    route-target export auto
  vni 2001002 l2
    rd auto
    route-target import auto
    route-target export auto
```

show コマンドの例

- **show nve peers**

```
9396-B# show nve peers
Interface Peer-IP          Peer-State
--------- ---------------  ----------
nve1      30.1.1.1         Up
```

- **show nve vni**

```
9396-B# show nve vni
Codes: CP - Control Plane        DP - Data Plane
       UC - Unconfigured         SA - Suppress ARP

Interface VNI      Multicast-group   State Mode Type [BD/VRF]      Flags
--------- -------- ----------------- ----- ---- ------------------ -----
nve1      900001   n/a               Up    CP   L3 [vxlan-900001]
nve1      2001001  225.4.0.1         Up    CP   L2 [1001]          SA
nve1      2001002  225.4.0.1         Up    CP   L2 [1002]          SA
```

- **show vxlan interface**

```
9396-B# show vxlan interface
Interface       Vlan    VPL Ifindex     LTL             HW VP
=========       ====    ===========     ===             =====
Eth1/47         1002    0x4c07d22e      0x10000         5697
Eth1/48         1001    0x4c07d02f      0x10001         5698
```

- **show bgp l2vpn evpn summary**

```
leaf3# show bgp l2vpn evpn summary
BGP summary information for VRF default, address family L2VPN EVPN
BGP router identifier 40.0.0.4, local AS number 10
BGP table version is 60, L2VPN EVPN config peers 1, capable peers 1
21 network entries and 21 paths using 2088 bytes of memory
BGP attribute entries [8/1152], BGP AS path entries [0/0]
BGP community entries [0/0], BGP clusterlist entries [1/4]

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down
State/PfxRcd
40.0.0.1        4    10    8570    8565       60    0    0    5d22h 6
```

- **show bgp l2vpn evpn**

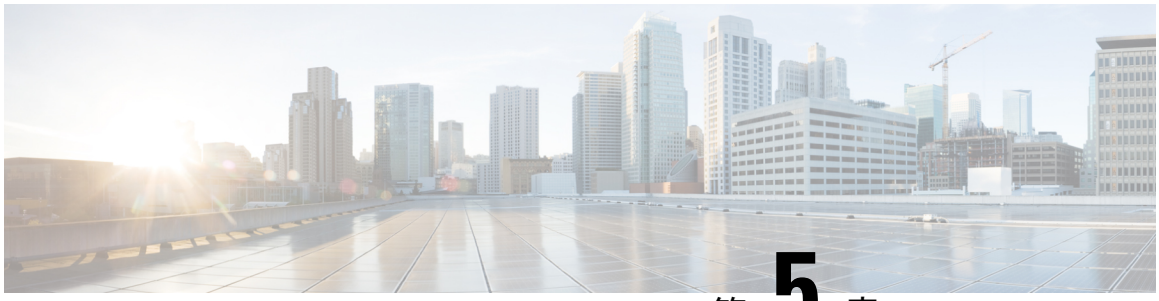
```
leaf3# show bgp l2vpn evpn
BGP routing table information for VRF default, address family L2VPN EVPN
BGP table version is 60, local router ID is 40.0.0.4
Status: s-suppressed, x-deleted, S-stale, d-dampened, h-history, *-valid,
>-best
Path type: i-internal, e-external, c-confed, l-local, a-aggregate, r-redist,
I-injected
Origin codes: i - IGP, e - EGP, ? - incomplete, | - multipath, & - backup

   Network            Next Hop            Metric     LocPrf     Weight Path
Route Distinguisher: 40.0.0.2:32868
*>i[2]:[0]:[10001]:[48]:[0000.8816.b645]:[0]:[0.0.0.0]/216
                      40.0.0.2                           100          0 i
*>i[2]:[0]:[10001]:[48]:[0011.0000.0034]:[0]:[0.0.0.0]/216
                      40.0.0.2                           100          0 i
```

- **show l2route evpn mac all**

```
leaf3# show l2route evpn mac all
Topology    Mac Address    Prod   Next Hop (s)
----------- -------------- ------ ---------------
101         0000.8816.b645 BGP    40.0.0.2
101         0001.0000.0033 Local  Ifindex 4362086
101         0001.0000.0035 Local  Ifindex 4362086
101         0011.0000.0034 BGP    40.0.0.2
```

- **show l2route evpn mac-ip all**

```
leaf3# show l2route evpn mac-ip all
Topology ID Mac Address    Prod Host IP                 Next Hop (s)
----------- -------------- ---- ------------------------------------------------------
101         0011.0000.0034 BGP  5.1.3.2                      40.0.0.2
102         0011.0000.0034 BGP  5.1.3.2                      40.0.0.2
```



第 5 章

テナント ルーテッド マルチキャストの設定

この章は、次の項で構成されています。

テナント ルーテッド マルチキャストについて

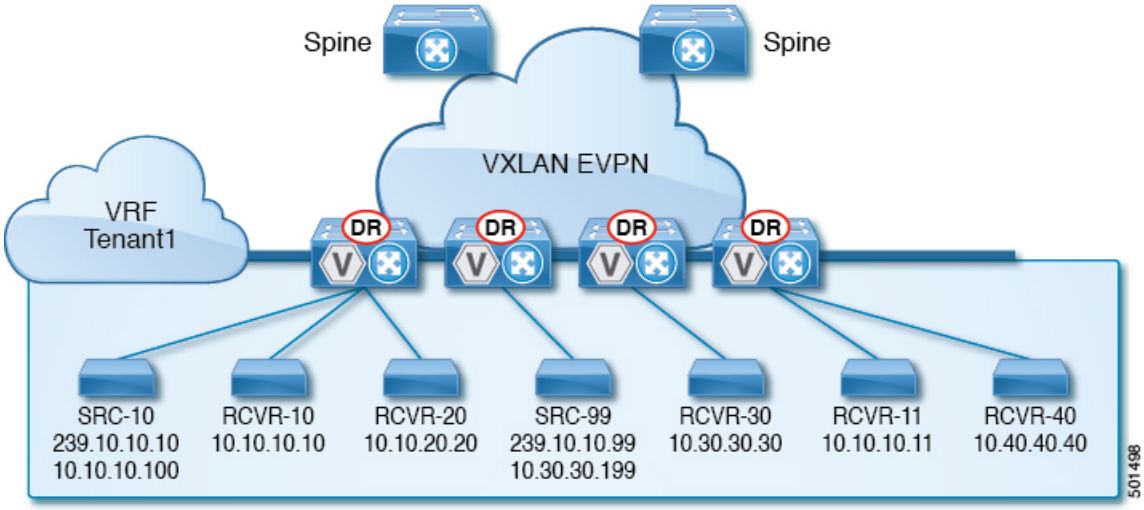
テナント ルーテッド マルチキャスト（TRM）は、BGP ベースの EVPN コントロール プレーンを使用する VXLAN ファブリック内でのマルチキャスト転送を有効にします。TRM は、ローカルまたは VTEP 間で同じサブネット内または異なるサブネット内の送信元と受信側の間にマルチテナント対応のマルチキャスト転送を実装します。

この機能により、VXLAN オーバーレイへのマルチキャスト配信の効率が向上します。これは、IETF RFC 6513、6514 で説明されている標準ベースの次世代コントロール プレーン（ngMVPN）に基づいています。TRM は、効率的かつ復元力のある方法で、マルチテナント ファブリック内で顧客の IP マルチキャスト トラフィックを配布できるようにします。TRM の配布により、ネットワーク内のレイヤ 3 オーバーレイ マルチキャスト機能が向上します。

BGP EVPN はユニキャスト ルーティングのコントロール プレーンを提供しますが、ngMVPN はスケーラブルなマルチキャスト ルーティング機能を提供します。これは、ユニキャスト用の分散型 IP エニーキャスト ゲートウェイを持つすべてのエッジ デバイス（VTEP）がマルチキャスト用の指定ルータ（DR）になる「常時ルート」アプローチに従います。ブリッジ型マルチ

キャスト転送は、エッジ デバイス（VTEP）にのみ存在し、IGMP スヌーピングは該当する受信者へのマルチキャスト転送を最適化します。ローカル配信以外のすべてのマルチキャスト トラフィックは効率的にルーティングされます。

図 *4 : VXLAN EVPN TRM*



TRM を有効にすると、アンダーレイでのマルチキャスト転送が活用され、VXLAN でカプセル化されたルーテッド マルチキャストトラフィックが複製されます。デフォルト マルチキャスト配信ツリー（デフォルト MDT）は、VRF ごとに構築されます。これは、レイヤ 2 仮想ネットワーク インスタンス（VNI）のブロードキャストおよび不明ユニキャスト トラフィック、およびレイヤ 2 マルチキャスト複製グループの既存のマルチキャスト グループに追加されます。オーバーレイ内の個々のマルチキャスト グループ アドレスは、複製および転送のためにそれぞれのアンダーレイ マルチキャスト アドレスにマッピングされます。BGP ベースのアプローチを使用する利点は、TRM を備えた BGP EVPN VXLAN ファブリックが、すべてのエッジ デバイスまたは VTEP に RP が存在する完全な分散型オーバーレイ ランデブー ポイント（RP）として動作できることです。

マルチキャスト対応のデータセンターファブリックは、通常、マルチキャストネットワーク全体の一部です。マルチキャスト送信元、受信側、およびマルチキャスト ランデブー ポイントはデータセンター内に存在する可能性がありますが、キャンパス内にある場合や WAN 経由で外部から到達可能である場合もあります。TRM を使用すると、既存のマルチキャスト ネットワークをシームレスに統合できます。ファブリック外部のマルチキャスト ランデブー ポイントを活用できます。さらに、TRM では、レイヤ 3 物理インターフェイスまたはサブインターフェイスを使用したテナント対応外部接続が可能です。

テナントルーテッドマルチキャストに関する注意事項と制限事項

テナント ルーテッド マルチキャスト（TRM）には、次の注意事項と制約事項があります。

- FEX のサポートは、Cisco Nexus 3600 プラットフォーム スイッチでは使用されません。
- VXLAN の注意事項と制約事項 （9 ページ） は TRM にも適用されます。
- TRM が有効になっている場合、コアリンクとしての SVI はサポートされません。
- TRM は IPv4 マルチキャストのみをサポートします。
- TRM には、スパース モードとも呼ばれる PIM Any Source Multicast（ASM）を使用した IPv4 マルチキャスト ベースのアンダーレイが必要です。
- TRM は、オーバーレイ PIM ASM および PIM SSM のみをサポートします。PIM BiDir はオーバーレイではサポートされていません。
- RP は、ファブリックの内部または外部のいずれかに設定する必要があります。
- 内部 RP は、ボーダー ノードを含むすべての TRM 対応 VTEP で設定する必要があります。
- 外部 RP は、ボーダー ノードの外部にある必要があります。
- RP は、外部 RP IP アドレス（スタティック RP）を指す VRF 内で設定する必要があります。これにより、特定の VRF の外部 RP に到達するためのユニキャストおよびマルチキャスト ルーティングが有効になります。
- TRM は複数のボーダー ノードをサポートします。複数のボーダー リーフ スイッチを介した外部 RP への到達可能性がサポートされています（ECMP）。
- VXLAN vPC セットアップで L3 VNI の VLAN で PIM と **ip igmp snooping vxlan** の両方を有効にする必要があります。

レイヤ3テナントルーテッドマルチキャストの注意事項と制約事項

レイヤ3テナントルーテッドマルチキャスト（TRM）には次の設定の注意事項と制限事項があります。

- Cisco NX-OS リリース 9.3(3) 以降、Cisco Nexus 3600 プラットフォーム スイッチは、レイヤ 3 モードで TRM をサポートします。この機能は、IPv4 オーバーレイでのみサポートされます。レイヤ 2 モードと L2/L3 混合モードはサポートされていません。

  Cisco Nexus 3600 プラットフォーム スイッチは、L3 ユニキャストトラフィックの BL として機能できます。エニーキャスト機能の場合、RP は内部、外部、またはあらゆる場所の RP にすることができます。

- Cisco NX-OS リリース 9.3(3)以降、Cisco Nexus 3600 プラットフォーム スイッチは、レイヤ 3 モードで TRM をサポートします。この機能をサポートするには、ボーダー リーフで **advertise-pip** コマンドと **advertise virtual-rmac** コマンドを有効にする必要があります。詳細については、「VIP/PIP の構成」セクションを参照してください。

- 既知のローカル スコープ マルチキャスト（224.0.0.0/24）はTRMから除外され、ブリッジされます。
- インターフェイス NVE がボーダー リーフでダウンした場合、VRF ごとの内部オーバーレイ RP をダウンする必要があります。
- 一方または両方の VTEP が Cisco Nexus 3600 プラットフォーム スイッチである場合、パケット TTL は 2 回デクリメントされます。1 回は送信元リーフの L3 VNI にルーティングするため、もう 1 回は宛先 L3 VNI から宛先リーフの宛先 VLAN に転送するためです。
- Cisco Nexus 3600 プラットフォーム スイッチは、TRM マルチサイト をサポートしていません。

テナント ルーテッド マルチキャストのランデブー ポイント

TRM を有効にすると、内部および外部 RP がサポートされます。次の表に、RP の位置付けがサポートされているか、サポートされていない最初のリリースを示します。

	RP 内部	**RP 外部**	**PIM ベースの RP Everywhere**
TRM L3 モード	9.3(3)	9.3(3)	9.3(3)

	RP 内部	**RP 外部**
TRM L2 モード	なし	なし
TRM L3 モード	7.0(3)I7(1)	7.0(3)I7(4)
TRM L2L3 モード	7.0(3)I7(1)	N/A

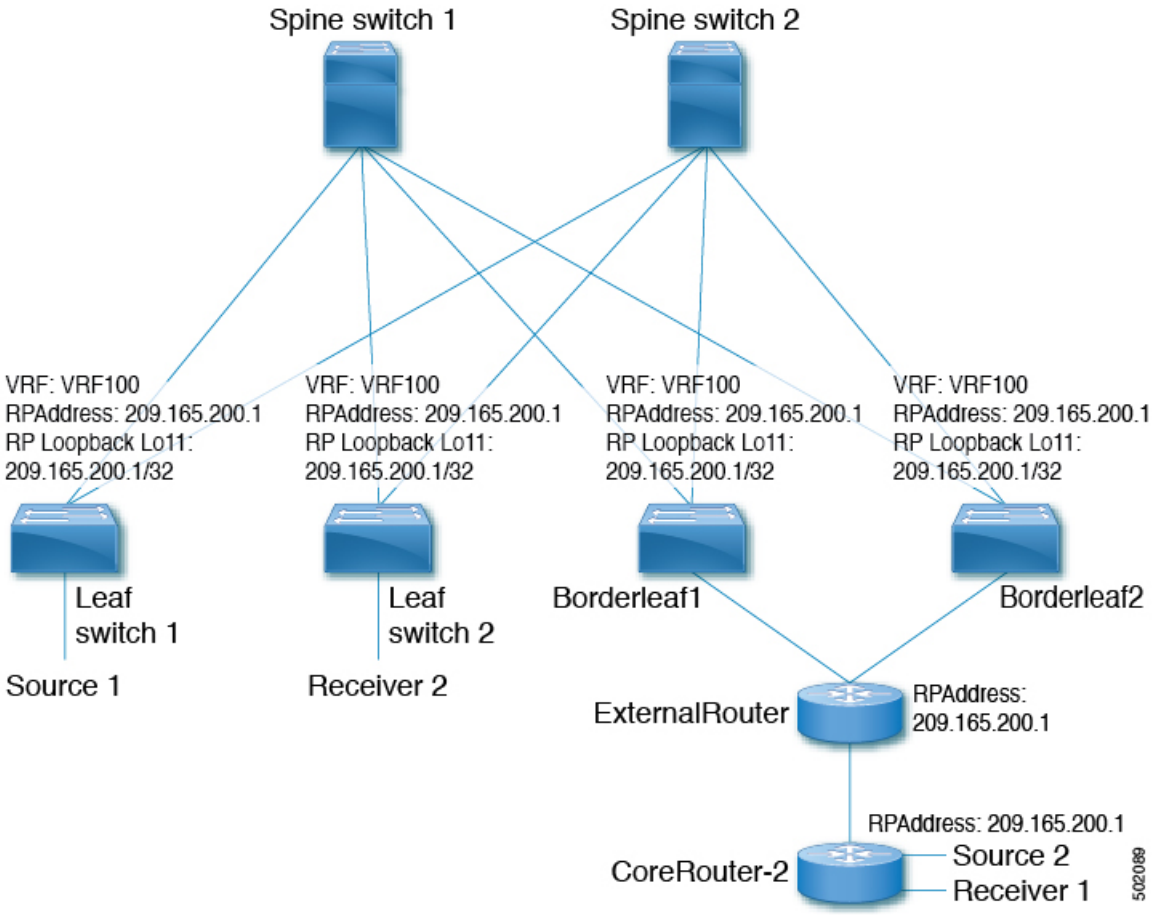
テナント ルーテッド マルチキャストのランデブー ポイントの設定

テナント ルーテッド マルチキャストでは、次のランデブー ポイント オプションがサポートされています。

- VXLAN ファブリック内のランデブー ポイントの設定 （65 ページ）
- 外部ランデブー ポイントの設定 （66 ページ）

VXLAN ファブリック内のランデブー ポイントの設定

すべてのデバイス（VTEP）で次のコマンドを使用して、TRM VRF のループバックを設定します。EVPN 内で到達可能であることを確認します（アドバタイズ/再配布）。



手順の概要

1. **configure terminal**
2. **interface loopback** *loopback_number*
3. **vrf member** *vxlan-number*
4. **ip address** *ip-address*
5. **ip pim sparse-mode**
6. **vrf context** *vrf-name*
7. **ip pim rp-address** *ip-address-of-router* **group-list** *group-range-prefix*

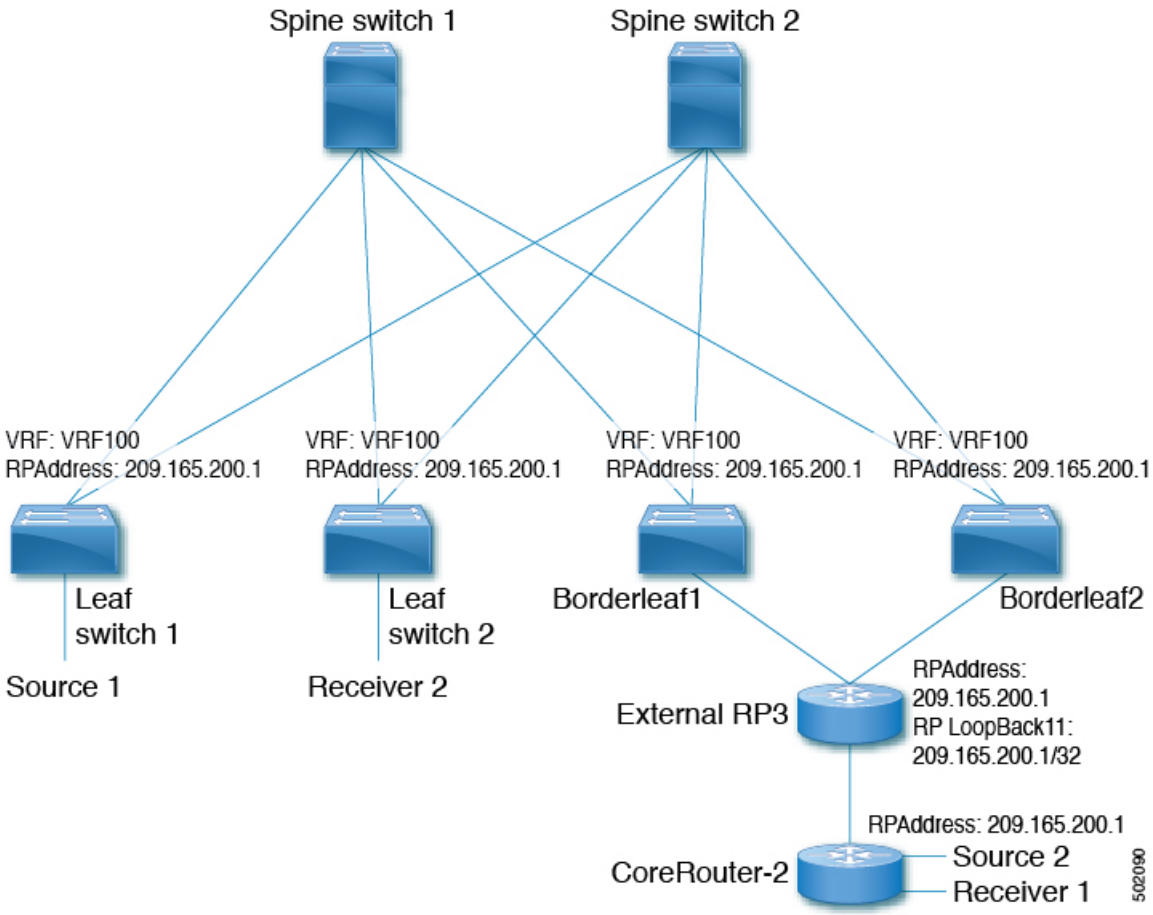
手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface loopback** *loopback_number* 例： `switch(config)# interface loopback 11`	すべての TRM 対応ノードでループバック インターフェイスを設定します。これにより、ファブリック内のランデブー ポイントが有効になります。
ステップ 3	**vrf member** *vxlan-number* 例： `switch(config-if)# vrf member vrf100`	VRF 名を設定します。
ステップ 4	**ip address** *ip-address* 例： `switch(config-if)# ip address 209.165.200.1/32`	IP アドレスを指定します。
ステップ 5	**ip pim sparse-mode** 例： `switch(config-if)# ip pim sparse-mode`	インターフェイスでスパースモード PIM を設定します。
ステップ 6	**vrf context** *vrf-name* 例： `switch(config-if)# vrf context vrf100`	VXLAN テナント VRF を作成します。
ステップ 7	**ip pim rp-address** *ip-address-of-router* **group-list** *group-range-prefix* 例： `switch(config-vrf# ip pim rp-address 209.165.200.1 group-list 224.0.0.0/4`	*ip-address-of-router* パラメータの値は RP の値です。完全に分散された RP の場合、すべてのエッジ デバイス（VTEP）に同じ IP アドレスが必要です。

外部ランデブー ポイントの設定

すべてのデバイス（VTEP）の TRM VRF 内の外部ランデブー ポイント（RP）IP アドレスを設定します。さらに、ボーダー ノードを介した VRF 内の外部 RP の到達可能性を確認します。TRM が有効で、外部 RP が使用されている場合は、1 つのルーティング パスだけがアクティブであることを確認します。TRM ファブリックと外部 RP 間のルーティングは、単一のボーダー リーフ（非 ECMP）を経由する必要があります。



手順の概要

1. **configure terminal**
2. **vrf context vrf100**
3. **ip pim rp-address** *ip-address-of-router* **group-list** *group-range-prefix*

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal`	コンフィギュレーション モードを入力します。
ステップ 2	**vrf context vrf100** 例： `switch(config)# vrf context vrf100`	コンフィギュレーション モードを入力します。

	コマンドまたはアクション	目的
ステップ 3	**ip pim rp-address** *ip-address-of-router* **group-list** *group-range-prefix* 例： `switch(config-vrf)# ip pim rp-address 209.165.200.1 group-list 224.0.0.0/4`	*ip-address-of-router* パラメータの値は RP の値です。完全に分散された RP のすべてのエッジデバイス（VTEP）に同じ IP アドレスが必要です。

レイヤ 3 テナント ルーテッド マルチキャストの設定

この手順では、テナントルーテッドマルチキャスト（TRM）機能を有効にします。TRM は、BGP MVPN シグナリングを使用して、主に IP マルチキャストのレイヤ 3 転送モードで動作します。レイヤ 3 モードの TRM は、TRM 対応 VXLAN BGP EVPN ファブリックの主要な機能であり、唯一の要件です。非 TRM 対応エッジ デバイス（VTEP）が存在する場合は、レイヤ 2/レイヤ 3 モードとレイヤ 2 モードを相互運用性について考慮する必要があります。

レイヤ 3 クラウドの送信者と受信者、および TRM vPC 境界リーフの VXLAN ファブリック間でマルチキャストを転送するには、VIP/PIP 設定を有効にする必要があります。詳細については、VIP/PIP の設定を参照してください。

（注） TRMは、always-routeアプローチに従って、転送されるIPマルチキャストトラフィックの存続可能時間（TTL）を減らします。

始める前に

VXLAN EVPN **feature nv overlay** および **nv overlay evpn** を設定する必要があります。

ランデブー ポイント（RP）を設定する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal`	コンフィギュレーション モードを入力します。
ステップ 2	**feature ngmvpn** 例： `switch(config)# feature ngmvpn`	次世代マルチキャストVPN（ngMVPN）コントロール プレーンを有効にします。BGP で新しいアドレス ファミリ コマンドが使用可能になります。
ステップ 3	**ip igmp snooping vxlan** 例：	VXLAN VLAN の IGMP スヌーピングを設定します。

	コマンドまたはアクション	目的
	`switch(config)# ip igmp snooping vxlan`	
ステップ 4	**interface nve1** 例： `switch(config)# interface nve 1`	NVE インターフェイスを設定します。
ステップ 5	**member vni** *vni-range* **associate-vrf** 例： `switch(config-if-nve)# member vni 200100 associate-vrf`	レイヤ 3 仮想ネットワーク識別子を設定します。*vni-range* の範囲は 1 ～ 16,777,214 です。
ステップ 6	**mcast-group** *ip-prefix* 例： `switch(config-if-nve-vni)# mcast-group 225.3.3.3`	VRF VNI（レイヤ 3 VNI）のデフォルト マルチキャスト配信ツリーを構築します。 マルチキャスト グループは、関連付けられているレイヤ 3 VNI（VRF）内のすべてのマルチキャスト ルーティングのアンダーレイ（コア）で使用されます。 （注） レイヤ 2 VNI、デフォルト MDT、およびデータ MDT のアンダーレイ マルチキャスト グループは共有しないことを推奨します。重複しない個別のグループを使用します。
ステップ 7	**exit** 例： `switch(config-if-nve-vni)# exit`	コマンド モードを終了します。
ステップ 8	**exit** 例： `switch(config-if)# exit`	コマンド モードを終了します。
ステップ 9	**router bgp 100** 例： `switch(config)# router bgp 100`	自律システム番号の設定
ステップ 10	**exit** 例： `switch(config-router)# exit`	コマンド モードを終了します。
ステップ 11	**neighbor** *ip-addr* 例： `switch(config-router)# neighbor 1.1.1.1`	ネイバーの IP アドレスを設定します。

	コマンドまたはアクション	目的
ステップ 12	**address-family ipv4 mvpn** 例： `switch(config-router-neighbor)# address-family ipv4 mvpn`	マルチキャスト VPN を設定します。
ステップ 13	**send-community extended** 例： `switch(config-router-neighbor-af)# send-community extended`	アドレス ファミリ シグナリングの ngMVPN をイネーブルにします。**send community extended** コマンドにより、拡張コミュニティがこのアドレス ファミリに確実に交換されます。
ステップ 14	**exit** 例： `switch(config-router-neighbor-af)# exit`	コマンド モードを終了します。
ステップ 15	**exit** 例： `switch(config-router)# exit`	コマンド モードを終了します。
ステップ 16	**vrf context** *vrf_name* 例： `switch(config-router)#vrf context vrf100`	VRF 名を設定します。
ステップ 17	**ip pim rp-address** *ip-address-of-router* **group-list** *group-range-prefix* 例： `switch(config-vrf)# ip pim rp-address 209.165.201.1 group-list 226.0.0.0/8`	*ip-address-of-router* パラメータの値は RP の値です。完全に分散された RP のすべてのエッジデバイス（VTEP）に同じ IP アドレスが必要です。 オーバーレイ RP の配置オプションについては、テナント ルーテッド マルチキャストのランデブー ポイントの設定 （64 ページ） セクションを参照してください。
ステップ 18	**address-family ipv4 unicast** 例： `switch(config-vrf)# address-family ipv4 unicast`	ユニ キャスト アドレス ファミリを設定します。
ステップ 19	**route-target both auto mvpn** 例： `switch(config-vrf-af-ipv4)# route-target both auto mvpn`	カスタマー マルチキャスト（C_Multicast）ルート（ngMVPN ルートタイプ 6 および 7）に拡張コミュニティ属性として追加される BGP ルート ターゲットを定義します。 自動ルート ターゲットは、2 バイトの自律システム番号（ASN）とレイヤ 3 VNI によって構築されます。

	コマンドまたはアクション	目的
ステップ 20	**ip multicast overlay-spt-only** 例： `switch(config)# ip multicast overlay-spt-only`	送信元がローカルに接続されている場合の Gratuitally Originate（S、A）ルート。**ip multicast overlay-spt-only** コマンドは、すべての MVPN 対応スイッチ（通常はリーフ ノード）でデフォルトで有効になっています。
ステップ 21	**interface***vlan_id* 例： `switch(config)# interface vlan11`	ファーストホップ ゲートウェイ（レイヤ 2 VNI の分散エニーキャスト ゲートウェイ）を設定します。このインターフェイスでは、ルータ PIM ピアリングは発生しません。
ステップ 22	**no shutdown** 例： `switch(config-if)# no shutdown`	インターフェイスをディセーブルにします。
ステップ 23	**vrf member** *vrf-num* 例： `switch(config-if)# vrf member vrf100`	VRF 名を設定します。
ステップ 24	**ip address** *ip_address* 例： `switch(config-if)# ip address 11.1.1.1/24`	IP アドレスを設定します。
ステップ 25	**ip pim sparse-mode** 例： `switch(config-if)# ip pim sparse-mode`	SVI で IGMP および PIM をイネーブルにします。これは、この VLAN にマルチキャスト送信元や受信者が存在する場合に必要です。
ステップ 26	**fabric forwarding mode anycast-gateway** 例： `switch(config-if)# fabric forwarding mode anycast-gateway`	エニーキャスト ゲートウェイ転送モードを設定します。
ステップ 27	**ip pim neighbor-policy NONE*** 例： `switch(config-if)# ip pim neighbor-policy NONE*`	IP PIM ネイバー ポリシーを作成して、VLAN 内の PIM ルータとの PIM ネイバーシップを回避します。**none** キーワードは、すべての ipv4 アドレスを拒否するように設定されたルートマップで、大文字と小文字を区別しない IP を使用した PIM ネイバーシップ ポリシーの確立を回避します。 （注） PIM ピアリングに分散型エニーキャスト ゲートウェイを使用しないでください。

	コマンドまたはアクション	目的
ステップ 28	**exit** 例： `switch(config-if)# exit`	コマンド モードを終了します。
ステップ 29	**interface** *vlan_id* 例： `switch(config)# interface vlan100`	VRF およびレイヤ 3 VNI を設定します。
ステップ 30	**no shutdown** 例： `switch(config-if)# no shutdown`	インターフェイスを無効にします。
ステップ 31	**vrf member vrf100** 例： `switch(config-if)# vrf member vrf100`	VRF 名を設定します。
ステップ 32	**ip forward** 例： `switch(config-if)# ip forward`	インターフェイスで IP 転送を有効にします。
ステップ 33	**ip pim sparse-mode** 例： `switch(config-if)# ip pim sparse-mode`	インターフェイスでスパース モード PIM を設定します。レイヤ 3 VNI で発生する PIM ピアリングはありませんが、転送にはこのコマンドが必要です。

VXLAN EVPN スパインでの TRM の設定

この手順では、VXLAN EVPN スパイン スイッチでテナント ルーテッド マルチキャスト（TRM）を有効にします。

始める前に

VXLAN BGP EVPN スパインを設定する必要があります。スパインでの EVPN の BGP 構成（33 ページ）を参照してください。

手順の概要

1. **configure terminal**
2. **route-map permitall permit 10**
3. **set ip next-hop unchanged**
4. **exit**
5. **router bgp [autonomous system]** *number*
6. **address-family ipv4 mvpn**

7. **retain route-target all**
8. **neighbor** *ip-address* [**remote-as** *number*]
9. **address-family ipv4 mvpn**
10. **disable-peer-as-check**
11. **rewrite-rt-asn**
12. **send-community extended**
13. **route-reflector-client**
14. **route-map permitall out**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal`	コンフィギュレーション モードを入力します。
ステップ 2	**route-map permitall permit 10** 例： `switch(config)# route-map permitall permit 10`	ルート マップを設定します。 （注） ルート マップでは、EVPN ルート用にネクスト ホップを変更しないまま保持します。 • eBGP では必須です。 • iBGP ではオプションです。
ステップ 3	**set ip next-hop unchanged** 例： `switch(config-route-map)# set ip next-hop unchanged`	ネクスト ホップ アドレスを設定します。 （注） ルート マップでは、EVPN ルート用にネクスト ホップを変更しないまま保持します。 • eBGP では必須です。 • iBGP ではオプションです。
ステップ 4	**exit** 例： `switch(config-route-map)# exit`	EXEC モードに戻ります。
ステップ 5	**router bgp [autonomous system]** *number* 例： `switch(config)# router bgp 65002`	BGP を指定します。

	コマンドまたはアクション	目的
ステップ 6	**address-family ipv4 mvpn** 例： `switch(config-router)# address-family ipv4 mvpn`	BGP でアドレス ファミリ IPv4 MVPN を設定します。
ステップ 7	**retain route-target all** 例： `switch(config-router-af)# retain route-target all`	アドレス ファミリ IPv4 MVPN [global] で、すべてのルート ターゲットの保持を設定します。 （注） eBGP では必須です。インポート ルート ターゲットに一致するように設定されたローカル VNI が存在しない場合、スパインがすべての MVPN ルートを保持およびアドバタイズできるようにします。
ステップ 8	**neighbor** *ip-address* [**remote-as** *number*] 例： `switch(config-router-af)# neighbor 100.100.100.1`	ネイバーを定義します。
ステップ 9	**address-family ipv4 mvpn** 例： `switch(config-router-neighbor)# address-family ipv4 mvpn`	BGP ネイバーでアドレス ファミリ IPv4 MVPN を設定します。
ステップ 10	**disable-peer-as-check** 例： `switch(config-router-neighbor-af)# disable-peer-as-check`	ルート アドバタイズメント時のピア AS 番号のチェックをディセーブルにします。すべてのリーフが同じ AS を使用しているが、スパインがリーフと異なる AS を使用している場合、このパラメータを eBGP 用のスパインに設定します。 （注） eBGP では必須です。
ステップ 11	**rewrite-rt-asn** 例： `switch(config-router-neighbor-af)# rewrite-rt-asn`	発信ルート ターゲットの AS 番号をリモート AS 番号と一致するように正規化します。BGP で設定されたネイバーのリモート AS を使用します。**rewrite-rt-asn** コマンドは、Route Target Auto 機能を使用して EVPN ルート ターゲットを設定する場合に必要です。
ステップ 12	**send-community extended** 例： `switch(config-router-neighbor-af)# send-community extended`	BGP ネイバーのコミュニティを設定します。

	コマンドまたはアクション	目的
ステップ 13	**route-reflector-client** 例： `switch(config-router-neighbor-af)# route-reflector-client`	ルート リフレクタを設定します。 （注） ルート リフレクタを使用する iBGP に必要です。
ステップ 14	**route-map permitall out** 例： `switch(config-router-neighbor-af)# route-map permitall out`	ルート マップを適用してネクストホップを変更しないまま保持します。 （注） eBGP では必須です。

vPC サポートを使用した TRM の設定

手順の概要

1. **configure terminal**
2. **feature vpc**
3. **feature interface-vlan**
4. **feature lacp**
5. **feature pim**
6. **feature ospf**
7. **ip pim rp-address** *address* **group-list** *range*
8. **vpc domain** *domain-id*
9. **hardware access-list tcam region mac-ifacl**
10. **hardware access-list tcam region vxlan 10**
11. **reload**
12. **peer switch**
13. **peer gateway**
14. **peer-keepalive destination** *ipaddress*
15. **ip arp synchronize**
16. **ipv6 nd synchronize**
17. vPC ピアリンクを作成します。
18. **system nve infra-vlans** *range*
19. **vlan** *number*
20. SVI を作成します。
21. （任意） **delay restore interface-vlan** *seconds*

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**feature vpc** 例： `switch(config)# feature vpc`	デバイス上で vPC をイネーブルにします。
ステップ 3	**feature interface-vlan** 例： `switch(config)# feature interface-vlan`	デバイスのインターフェイス VLAN 機能をイネーブルにします。
ステップ 4	**feature lacp** 例： `switch(config)# feature lacp`	デバイスの LACP 機能をイネーブルにします。
ステップ 5	**feature pim** 例： `switch(config)# feature pim`	デバイスの PIM 機能をイネーブルにします。
ステップ 6	**feature ospf** 例： `switch(config)# feature ospf`	デバイスの OSPF 機能をイネーブルにします。
ステップ 7	**ip pim rp-address** *address* **group-list** *range* 例： `switch(config)# ip pim rp-address 100.100.100.1 group-list 224.0.0/4`	アンダーレイ マルチキャスト グループ範囲に、PIM RP アドレスを設定します。
ステップ 8	**vpc domain** *domain-id* 例： `switch(config)# vpc domain 1`	デバイス上に vPC ドメインを作成し、設定目的で vpc-domain 設定モードを開始します。デフォルトはありません。範囲は 1 ～ 1000 です。
ステップ 9	**hardware access-list tcam region mac-ifacl** 例： `switch(config)# hardware access-list tcam region mac-ifacl 0`	ACL データベースの TCAM リージョンをカービングします。

	コマンドまたはアクション	目的
ステップ 10	**hardware access-list tcam region vxlan 10** 例： `switch(config)# hardware access-list tcam region vxlan 10`	VXLAN で使用する TCAM リージョンを割り当てます。
ステップ 11	**reload** 例： `switch(config)# reload`	TCAM 割り当てのスイッチ設定をリロードして、アクティブにします。
ステップ 12	**peer switch** 例： `switch(config-vpc-domain)# peer switch`	ピア スイッチを定義します。
ステップ 13	**peer gateway** 例： `switch(config-vpc-domain)# peer gateway`	仮想ポート チャネル（vPC）のゲートウェイ MAC アドレスを宛先とするパケットのレイヤ3転送をイネーブルにするには、**peer-gateway** コマンドを使用します。
ステップ 14	**peer-keepalive destination** *ipaddress* 例： `switch(config-vpc-domain)# peer-keepalive destination 172.28.230.85`	vPC ピアキープアライブ リンクのリモート エンドの IPv4 アドレスを設定します。 （注） vPC ピアキープアライブ リンクを設定するまで、vPC ピア リンクは構成されません。 管理ポートと VRF がデフォルトです。 （注） 独立した VRF を設定し、vPC ピアキープアライブ リンクのための VRF 内の各 vPC ピア デバイスからのレイヤ3ポートを使用することを推奨します。 VRF の作成および構成の詳細については、『Cisco Nexus 3600 シリーズ NX-OS シリーズ ユニキャスト ルーティング 構成ガイド、リリース 9.3(x)』を参照してください。
ステップ 15	**ip arp synchronize** 例： `switch(config-vpc-domain)# ip arp synchronize`	vPC ドメインで IP ARP 同期を有効にして、デバイスのリロード後の ARP テーブルの生成を高速化します。
ステップ 16	**ipv6 nd synchronize** 例： `switch(config-vpc-domain)# ipv6 nd synchronize`	vPC ドメインで IPv6 と同期を有効にして、デバイスのリロード後のテーブルの作成を高速化します。

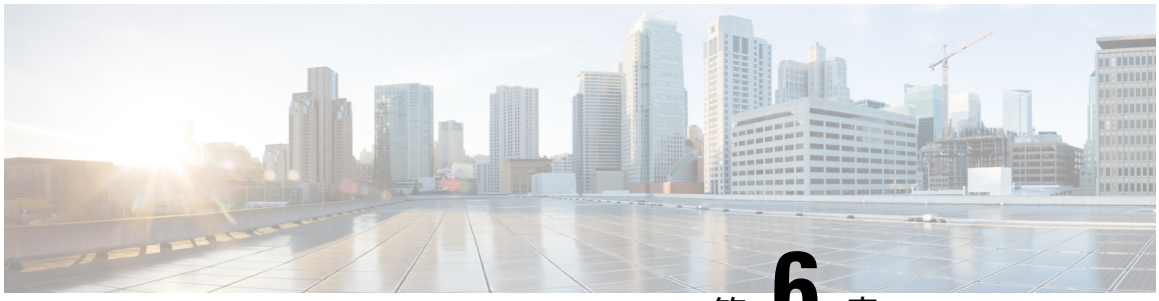
	コマンドまたはアクション	目的

ステップ 17	vPC ピアリンクを作成します。
	例：
	`switch(config)# interface port-channel 1`
	`switch(config)# switchport`
	`switch(config)# switchport mode trunk`
	`switch(config)# switchport trunk allowed vlan 1,10,100-200`
	`switch(config)# mtu 9216`
	`switch(config)# vpc peer-link`
	`switch(config)# no shut`
	
	`switch(config)# interface Ethernet 1/1, 1/21`
	`switch(config)# switchport`
	`switch(config)# mtu 9216`
	`switch(config)# channel-group 1 mode active`
	`switch(config)# no shutdown`
		vPC ピアリンク ポート チャネル インターフェイスを作成し、2つのメンバーインターフェイスを追加します。

ステップ 18	**system nve infra-vlans** *range* 例： `switch(config)# system nve infra-vlans 10`	バックアップ ルーテッド パスとして非 VXLAN 対応 VLAN を定義します。
ステップ 19	**vlan** *number* 例： `switch(config)# vlan 10`	インフラ VLAN として使用する VLAN を作成します。

ステップ 20	SVI を作成します。
	例：
	`switch(config)# interface vlan 10`
	`switch(config)# ip address 10.10.10.1/30`
	`switch(config)# ip router ospf process UNDERLAY area 0`
	`switch(config)# ip pim sparse-mode`
	`switch(config)# no ip redirects`
	`switch(config)# mtu 9216`
	`switch(config)# no shutdown`
		vPC ピアリンク上のバックアップルーテッドパスに使用される SVI を作成します。

ステップ 21	（任意） **delay restore interface-vlan** *seconds* 例： `switch(config-vpc-domain)# delay restore interface-vlan 45`	SVI の遅延復元タイマーをイネーブルにします。SVI/VNI スケールが大きい場合は、この値を調整することを推奨します。たとえば、SCIカウントが1000の場合、delay restoreを **interface-vlan** から 45 秒に設定することを推奨します。



第 6 章

外部 VRF 接続とルート リークの設定

この章は、次の内容で構成されています。

外部 VRF 接続の設定

VXLAN BGP EVPN ファブリックの外部レイヤ 3 接続について

VXLAN BGP EVPN ファブリックは、外部接続を実現するために VRF 単位の IP ルーティングを使用して拡張できます。レイヤ 3 拡張に使用されるアプローチは一般に VRF Lite と呼ばれ、機能自体はより正確に Inter-AS オプション A またはバックツーバック VRF 接続として定義されます。

外部 VRF 接続とルート リークの注意事項と制約事項

VXLAN BGP EVPN ファブリックの外部レイヤ 3 接続には、次のガイドラインと制限事項が適用されます。

- Cisco Nexus 3600 プラットフォーム スイッチの追加されたサポート。
- 物理レイヤ 3 インターフェイス（親インターフェイス）は、外部レイヤ 3 接続（つまり、VRF デフォルト）に使用できます。
- 複数のサブインターフェイスへの親インターフェイスは、外部レイヤ 3 接続（つまり、VRF デフォルトのイーサネット 1/1）には使用できません。代わりにサブインターフェイスを使用できます。
- サブインターフェイスが構成されている場合、VTEP は親インターフェイス上の VXLAN カプセル化トラフィックをサポートしません。これは、VRF 参加に関係ありません。
- VTEP は、サブインターフェイス上の VXLAN カプセル化トラフィックをサポートしません。これは、VRF 参加または IEEE 802.1q カプセル化に関係ありません。

- VXLAN VLAN と非 VXLAN が有効化された VLAN のサブインターフェイスの混在はサポートされていません。

ルート リークの設定

VXLAN BGP EVPN ファブリックの一元管理型 VRF ルート リークについて

VXLAN BGP EVPN は、MP-BGP とそのルート ポリシーの概念を使用して、プレフィックスをインポートおよびエクスポートします。この非常に広範なルート ポリシー モデルの機能により、ある VRF から別の VRF へ、またはその逆にルートをリークできます。カスタム VRF または VRF デフォルトの任意の組み合わせを使用できます。VRF ルート リークは、クロス VRF ルート ターゲットのインポート/エクスポート設定が行われる（リークポイント）ネットワーク内の特定の場所でのスイッチ ローカル機能です。異なる VRF 間の転送は、コントロール プレーン、つまり、ルートリークの設定が実行される場所、つまり集中型 VRF ルートリークに従います。VXLAN BGP EVPN の追加により、漏出ポイントはクロス VRF インポート/エクスポートされたルートをアドバタイズし、それらをリモート VTEP または外部ルータにアドバタイズする必要があります。

中央集中型 VRF ルート リークの利点は、リーク ポイントとして機能する VTEP だけが必要な特別な機能を必要とすることです。一方、ネットワーク内の他のすべての VTEP はこの機能に対して中立です。

外部 VRF 接続とルート リークの注意事項と制約事項

VXLAN BGP EVPN ファブリックの外部レイヤ 3 接続には、次のガイドラインと制限事項が適用されます。

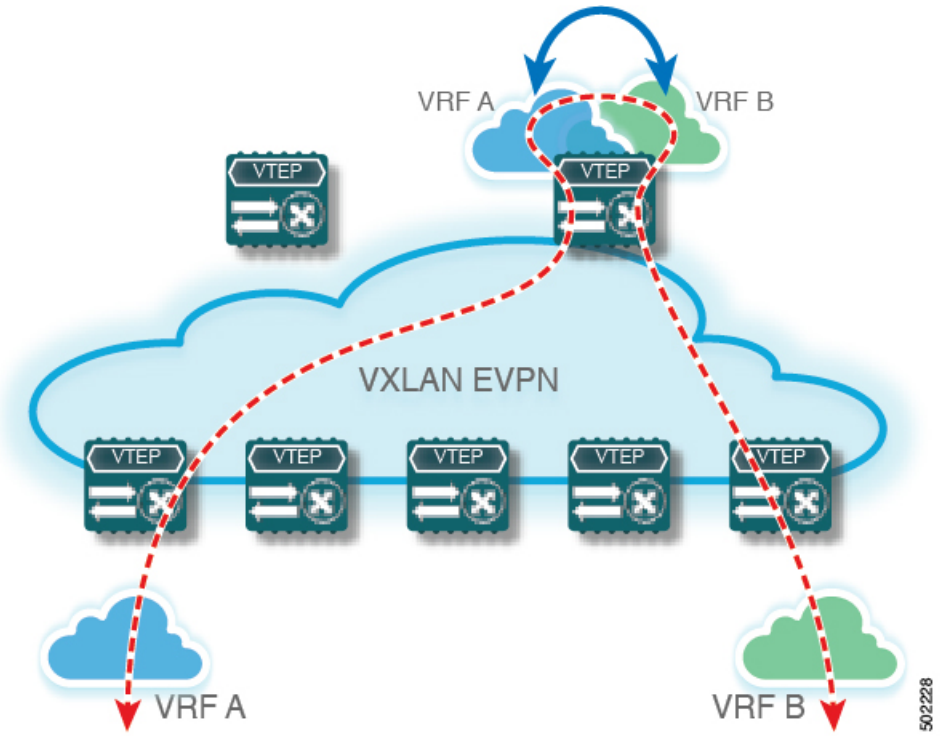
- Cisco Nexus 3600 プラットフォーム スイッチの追加されたサポート。
- 物理レイヤ 3 インターフェイス（親インターフェイス）は、外部レイヤ 3 接続（つまり、VRF デフォルト）に使用できます。
- 複数のサブインターフェイスへの親インターフェイスは、外部レイヤ 3 接続（つまり、VRF デフォルトのイーサネット 1/1）には使用できません。代わりにサブインターフェイスを使用できます。
- サブインターフェイスが構成されている場合、VTEP は親インターフェイス上の VXLAN カプセル化トラフィックをサポートしません。これは、VRF 参加に関係ありません。
- VTEP は、サブインターフェイス上の VXLAN カプセル化トラフィックをサポートしません。これは、VRF 参加または IEEE 802.1q カプセル化に関係ありません。
- VXLAN VLAN と非 VXLAN が有効化された VLAN のサブインターフェイスの混在はサポートされていません。

中央集中型 VRF ルート リーク ブリーフ：カスタム VRF による共有インターネット

次に、いくつかのポイントを示します。

- VXLAN BGP EVPN ファブリックの VRF ルート リークを使用した共有インターネットを次の図に示します。
- デフォルト ルートは共有インターネット VRF からエクスポートされ、ボーダー ノードの VRF Blue および VRF Red 内で再アドバタイズされます。
- VRF Blue および VRF Red のデフォルト ルートが共有インターネット VRF にリークされていないことを確認します。
- VRF Blue および VRF Red の限定的でないプレフィックスは、共有インターネット VRF にエクスポートされ、必要に応じて再アドバタイズされます。
- 境界ノードから残りの VTEP に宛先 VRF（青または赤）にアドバタイズされる、より具体性の低いプレフィックス（集約）。
- BGP EVPN は、ルーティングループの発生を防ぐために以前にインポートされたプレフィックスをエクスポートしません。

図 *5 :* 中央集中型 *VRF* ルートリーク：カスタム *VRF* による共有インターネット



一元管理型 VRF ルート リーキングの構成：カスタム VRF 間の特定のプレフィックス

ルーティング ブロック VTEP での VRF コンテキストの設定

この手順は、IPv6 にも同様に適用されます。

手順の概要

1. **configure terminal**
2. **vrf context** *vrf-name*
3. **vni** *number*
4. **rd auto**
5. **address-family ipv4 unicast**
6. **route-target both {auto** | *as:vni*}
7. **route-target both {auto** | *as:vni* }**evpn**
8. **route-target import** *rt-from-different-vrf*
9. **route-target import** *rt-from-different-vrf* **evpn**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vrf context** *vrf-name*	VRF を設定します。
ステップ 3	**vni** *number*	VNI を指定します。 VRF に関連付けられている VNI は、多くの場合、Layer-3 VNI、L3VNI、または L3VPN と呼ばれます。L3VNI は、参加する VTEP 間で共通の ID として構成されます。
ステップ 4	**rd auto**	VRF のルート識別子（RD）を指定します。 RD は、L3VNI 内の VTEP を一意に識別します。
ステップ 5	**address-family ipv4 unicast**	IPv4 ユニキャスト アドレス ファミリを設定します。 IPv4 アンダーレイを使用した IPv4 over VXLAN に必要です。
ステップ 6	**route-target both {auto** | *as:vni*}	IPv4 ユニキャスト address-family 内の IPv4 プレフィックスのインポート/エクスポートのルート ターゲッ

	コマンドまたはアクション	目的
		ト（RT）を構成します。ルート ターゲット（RT）は、各プレフィックス インポート/エクスポート ポリシーに使用されます。*as:vni* が入力されると値は、ASN:NN、ASN4:NN、または、IPv4:NN のフォーマットです。
ステップ 7	**route-target both {auto** | *as:vni* }**evpn**	IPv4 ユニキャスト address-family 内の IPv4 プレフィックスのインポート/エクスポートのルート ターゲット（RT）を構成します。ルート ターゲット（RT）は、各プレフィックス インポート/エクスポート ポリシーに使用されます。*as:vni* が入力されると値は、ASN:NN、ASN4:NN、または、IPv4:NN のフォーマットです。
ステップ 8	**route-target import** *rt-from-different-vrf*	leaked-from VRF（AS:VNI など）から IPv4 プレフィックスをインポートするようにルート ターゲット（RT）を構成します。
ステップ 9	**route-target import** *rt-from-different-vrf* **evpn**	leaked-from VRF（AS:VNI など）から IPv4 プレフィックスをインポートするようにルート ターゲット（RT）を構成します。

ルーティング ブロックでの BGP VRF インスタンスの設定

この手順は、IPv6 にも同様に適用されます。

手順の概要

1. **configure terminal**
2. **router bgp** *autonomous-system number*
3. **vrf** *vrf-name*
4. **address-family ipv4 unicast**
5. **advertise l2vpn evpn**
6. **aggregate-address** *prefix/mask*
7. **maximum-paths ibgp** *number*
8. **maximum-paths** *number*

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**router bgp** *autonomous-system number*	BGP を設定します。
ステップ 3	**vrf** *vrf-name*	VRF を指定します。
ステップ 4	**address-family ipv4 unicast**	IPv4 のアドレス ファミリの設定
ステップ 5	**advertise l2vpn evpn**	IPv4 アドレス ファミリ内の EVPN ルートのアドバタイズメントを有効にします。
ステップ 6	**aggregate-address** *prefix/mask*	宛先 VRF に特定性の低いプレフィックス集約を作成します。
ステップ 7	**maximum-paths ibgp** *number*	iBGP プレフィックスの等コスト マルチパス（ECMP）の有効化。
ステップ 8	**maximum-paths** *number*	eBGP プレフィックスの等コスト マルチパス（ECMP）の有効化

例：一元管理型 VRF ルート リークの設定：カスタム VRF 間の特定のプレフィックス

VXLAN BGP EVPN ルーティング ブロックの設定

VXLAN BGP EVPN ルーティング ブロックは、集中型ルート リーク ポイントとして機能します。漏洩設定は、コントロールプレーンの漏洩とデータパスの転送が同じパスをたどるようにローカライズされます。最も重要なのは、ルーティング ブロックの VRF 設定と、それぞれの宛先 VRF への特定性の低いプレフィックス（集約）のアドバタイズメントです。

```
vrf context Blue
  vni 51010
  rd auto
  address-family ipv4 unicast
    route-target both auto
    route-target both auto evpn
    route-target import 65002:51020
    route-target import 65002:51020 evpn
!
vlan 2110
  vn-segment 51010
!
interface Vlan2110
  no shutdown
  mtu 9216
  vrf member Blue
  no ip redirects
  ip forward
!
vrf context Red
  vni 51020
  rd auto
  address-family ipv4 unicast
    route-target both auto
    route-target both auto evpn
    route-target import 65002:51010
    route-target import 65002:51010 evpn
```

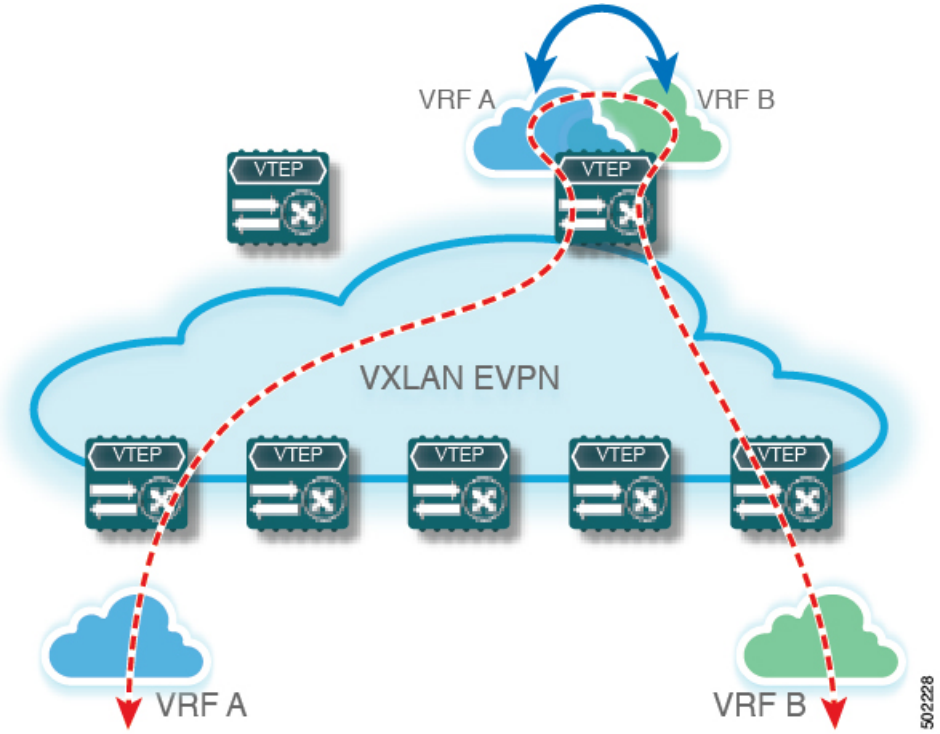
```
!
vlan 2120
  vn-segment 51020
!
interface Vlan2120
  no shutdown
  mtu 9216
  vrf member Blue
  no ip redirects
  ip forward
!
interface nve1
  no shutdown
  host-reachability protocol bgp
  source-interface loopback1
  member vni 51010 associate-vrf
  member vni 51020 associate-vrf
!
router bgp 65002
  vrf Blue
    address-family ipv4 unicast
      advertise l2vpn evpn
      aggregate-address 10.20.0.0/16
      maximum-paths ibgp 2
      Maximum-paths 2
  vrf Red
    address-family ipv4 unicast
      advertise l2vpn evpn
      aggregate-address 10.10.0.0/16
      maximum-paths ibgp 2
      Maximum-paths 2
```

中央集中型 VRF ルート リーク ブリーフ：カスタム VRF による共有インターネット

次に、いくつかのポインタを示します。

- VXLAN BGP EVPN ファブリックの VRF ルート リークを使用した共有インターネットを次の図に示します。
- デフォルト ルートは共有インターネット VRF からエクスポートされ、ボーダー ノードの VRF Blue および VRF Red 内で再アドバタイズされます。
- VRF Blue および VRF Red のデフォルト ルートが共有インターネット VRF にリークされていないことを確認します。
- VRF Blue および VRF Red の限定的でないプレフィックスは、共有インターネット VRF にエクスポートされ、必要に応じて再アドバタイズされます。
- 境界ノードから残りの VTEP に宛先 VRF（青または赤）にアドバタイズされる、より具体性の低いプレフィックス（集約）。
- BGP EVPN は、ルーティング ループの発生を防ぐために以前にインポートされたプレフィックスをエクスポートしません。

図 *6 :* 中央集中型 *VRF* ルートリーク：カスタム *VRF* による共有インターネット



一元管理型 VRF ルートリークの設定：カスタム VRF による共有インターネット

ボーダー ノードでのインターネット VRF の設定

この手順は、IPv6 にも同様に適用されます。

手順の概要

1. **configure terminal**
2. **vrf context** *vrf-name*
3. **vni** *number*
4. **ip route 0.0.0.0/0** *next-hop*
5. **rd auto**
6. **address-family ipv4 unicast**
7. **route-target both {auto** | *as:vni*}
8. **route-target both** *shared-vrf-rt* **evpn**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vrf context** *vrf-name*	VRF を設定します。
ステップ 3	**vni** *number*	VNI を指定します。 VRF に関連付けられている VNI は、多くの場合、Layer-3 VNI、L3VNI、または L3VPN と呼ばれます。L3VNI は、参加する VTEP 間で共通の ID として構成されます。
ステップ 4	**ip route 0.0.0.0/0** *next-hop*	外部ルータ（例）への共有インターネット VRF のデフォルトルートを構成します。
ステップ 5	**rd auto**	VRF のルート識別子（RD）を指定します。 RD は、L3VNI 内の VTEP を一意に識別します。
ステップ 6	**address-family ipv4 unicast**	IPv4 ユニキャスト アドレス ファミリを設定します。 IPv4 アンダーレイを使用した IPv4 over VXLAN に必要です。
ステップ 7	**route-target both {auto** | *as:vni*}	IPv4 ユニキャスト アドレスファミリ内の EVPN および IPv4 プレフィックスのインポート/エクスポート用のルート ターゲット（RT）を構成します。
ステップ 8	**route-target both** *shared-vrf-rt* **evpn**	共有 IPv4 プレフィックスのインポート/エクスポート用の特別なルート ターゲット（RT）を構成します。 さらなる認定のための追加のインポート/エクスポート マップがサポートされます。

ボーダー ノードでの共有インターネット BGP インスタンスの設定

この手順は、IPv6 にも同様に適用されます。

手順の概要

1. **configure terminal**
2. **router bgp** *autonomous-system number*
3. **vrf** *vrf-name*

4. **address-family ipv4 unicast**
5. **advertise l2vpn evpn**
6. **aggregate-address** *prefix/mask*
7. **maximum-paths ibgp** *number*
8. **maximum-paths** *number*

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router bgp** *autonomous-system number*	BGP を設定します。
ステップ 3	**vrf** *vrf-name*	VRF を指定します。
ステップ 4	**address-family ipv4 unicast**	IPv4 のアドレス ファミリの設定
ステップ 5	**advertise l2vpn evpn**	IPv4 アドレス ファミリ内の EVPN ルートのアドバタイズメントを有効にします。
ステップ 6	**aggregate-address** *prefix/mask*	宛先 VRF に特定性の低いプレフィックス集約を作成します。
ステップ 7	**maximum-paths ibgp** *number*	iBGP プレフィックスの等コスト マルチパス（ECMP）の有効化。
ステップ 8	**maximum-paths** *number*	eBGP プレフィックスの等コスト マルチパス（ECMP）の有効化。

ボーダーノードでのカスタム VRF コンテキストの設定 - 1

この手順は、IPv6 にも同様に適用されます。

手順の概要

1. **configure terminal**
2. **vrf context** *vrf-name*
3. **vni** *number*
4. **rd auto**
5. **ip route 0.0.0.0/0 Null0**
6. **address-family ipv4 unicast**
7. **route-target both {auto** | *as:vni***}**
8. **route-target both {auto** | *as:vni***} evpn**
9. **import map** *name*

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vrf context** *vrf-name*	VRF を設定します。
ステップ 3	**vni** *number*	VNI を指定します。 VRF に関連付けられている VNI は、多くの場合、Layer-3 VNI、L3VNI、または L3VPN と呼ばれます。L3VNI は、参加する VTEP 間で共通の識別子として設定されます。
ステップ 4	**rd auto**	VRF のルート識別子（RD）を指定します。 ルート識別子（RD）は、L3VNI 内の VTEP を一意に識別します。
ステップ 5	**ip route 0.0.0.0/0 Null0**	共通 VRF でデフォルト ルートを設定し、共有インターネット VRF を持つボーダーノードにトラフィックを引き付けます。
ステップ 6	**address-family ipv4 unicast**	IPv4 ユニキャスト アドレス ファミリを設定します。 IPv4 アンダーレイを使用した IPv4 over VXLAN に必要です。
ステップ 7	**route-target both {auto** | *as:vni***}**	IPv4 ユニキャスト address-family 内の IPv4 プレフィックスのインポート/エクスポートのルート ターゲット（RT）を構成します。ルート ターゲット（RT）は、各プレフィックス インポート/エクスポート ポリシーに使用されます。*as:vni* が入力されると値は、ASN:NN、ASN4:NN、または、IPv4:NN のフォーマットです。
ステップ 8	**route-target both {auto** | *as:vni***} evpn**	IPv4 ユニキャスト address-family 内の IPv4 プレフィックスのインポート/エクスポートのルート ターゲット（RT）を構成します。ルート ターゲット（RT）は、各プレフィックス インポート/エクスポート ポリシーに使用されます。*as:vni* が入力されると値は、ASN:NN、ASN4:NN、または、IPv4:NN のフォーマットです。

	コマンドまたはアクション	目的
ステップ 9	**import map** *name*	このルーティング テーブルにインポートされるルートにルート マップを適用します。

ボーダー ノードでの BGP でのカスタム VRF インスタンスの設定

この手順は、IPv6 にも同様に適用されます。

手順の概要

1. **configure terminal**
2. **router bgp** *autonomous-system-number*
3. **vrf** *vrf-name*
4. **address-family ipv4 unicast**
5. **advertise l2vpn evpn**
6. **network 0.0.0.0/0**
7. **maximum-paths ibgp** *number*
8. **maximum-paths** *number*

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router bgp** *autonomous-system-number*	BGP を設定します。
ステップ 3	**vrf** *vrf-name*	VRF を指定します。
ステップ 4	**address-family ipv4 unicast**	IPv4 のアドレス ファミリを設定します。
ステップ 5	**advertise l2vpn evpn**	IPv4 アドレス ファミリ内の EVPN ルートのアドバタイズメントを有効にします。
ステップ 6	**network 0.0.0.0/0**	IPv4 デフォルト ルート ネットワーク ステートメントを作成しています。
ステップ 7	**maximum-paths ibgp** *number*	iBGP プレフィックスの等コスト マルチパス（ECMP）の有効化。
ステップ 8	**maximum-paths** *number*	eBGP プレフィックスの等コスト マルチパス（ECMP）の有効化。

例：一元管理型 VRF ルート リークの設定：カスタム VRF による共有インターネット

共有インターネット VRF による中央集中型 VRF ルート リークの例

共有インターネット VRF の VXLAN BGP EVPN ボーダー ノードの設定

VXLAN BGP EVPN ボーダー ノードは、集中型共有インターネット VRF を提供します。漏出設定は、コントロール プレーンの漏出とデータ パス転送が同じパスをたどるようにローカライズされます。最も重要な点は、ボーダー ノードの VRF 設定と、デフォルト ルートと特定性の低いプレフィックス（集約）をそれぞれの宛先 VRF にアドバタイズすることです。

```
vrf context Shared
  vni 51099
  ip route 0.0.0.0/0 10.9.9.1
  rd auto
  address-family ipv4 unicast
    route-target both auto
    route-target both auto evpn
    route-target both 99:99
    route-target both 99:99 evpn
!
vlan 2199
  vn-segment 51099
!
interface Vlan2199
  no shutdown
  mtu 9216
  vrf member Shared
  no ip redirects
  ip forward
!
ip prefix-list PL_DENY_EXPORT seq 5 permit 0.0.0.0/0
!
route-map RM_DENY_IMPORT deny 10
 match ip address prefix-list PL_DENY_EXPORT
route-map RM_DENY_IMPORT permit 20
!
vrf context Blue
  vni 51010
  ip route 0.0.0.0/0 Null0
  rd auto
  address-family ipv4 unicast
    route-target both auto
    route-target both auto evpn
    route-target both 99:99
    route-target both 99:99 evpn
    import map RM_DENY_IMPORT
!
vlan 2110
  vn-segment 51010
!
interface Vlan2110
  no shutdown
  mtu 9216
  vrf member Blue
  no ip redirects
  ip forward
!
vrf context Red
  vni 51020
  ip route 0.0.0.0/0 Null0
```

```
  rd auto
  address-family ipv4 unicast
    route-target both auto
    route-target both auto evpn
    route-target both 99:99
    route-target both 99:99 evpn
    import map RM_DENY_IMPORT
!
vlan 2120
  vn-segment 51020
!
interface Vlan2120
  no shutdown
  mtu 9216
  vrf member Blue
  no ip redirects
  ip forward
!
interface nve1
  no shutdown
  host-reachability protocol bgp
  source-interface loopback1
  member vni 51099 associate-vrf
  member vni 51010 associate-vrf
  member vni 51020 associate-vrf
!
router bgp 65002
  vrf Shared
    address-family ipv4 unicast
      advertise l2vpn evpn
      aggregate-address 10.10.0.0/16
      aggregate-address 10.20.0.0/16
      maximum-paths ibgp 2
      maximum-paths 2
  vrf Blue
    address-family ipv4 unicast
      advertise l2vpn evpn
      network 0.0.0.0/0
      maximum-paths ibgp 2
      maximum-paths 2
  vrf Red
    address-family ipv4 unicast
      advertise l2vpn evpn
      network 0.0.0.0/0
      maximum-paths ibgp 2
      maximum-paths 2
```

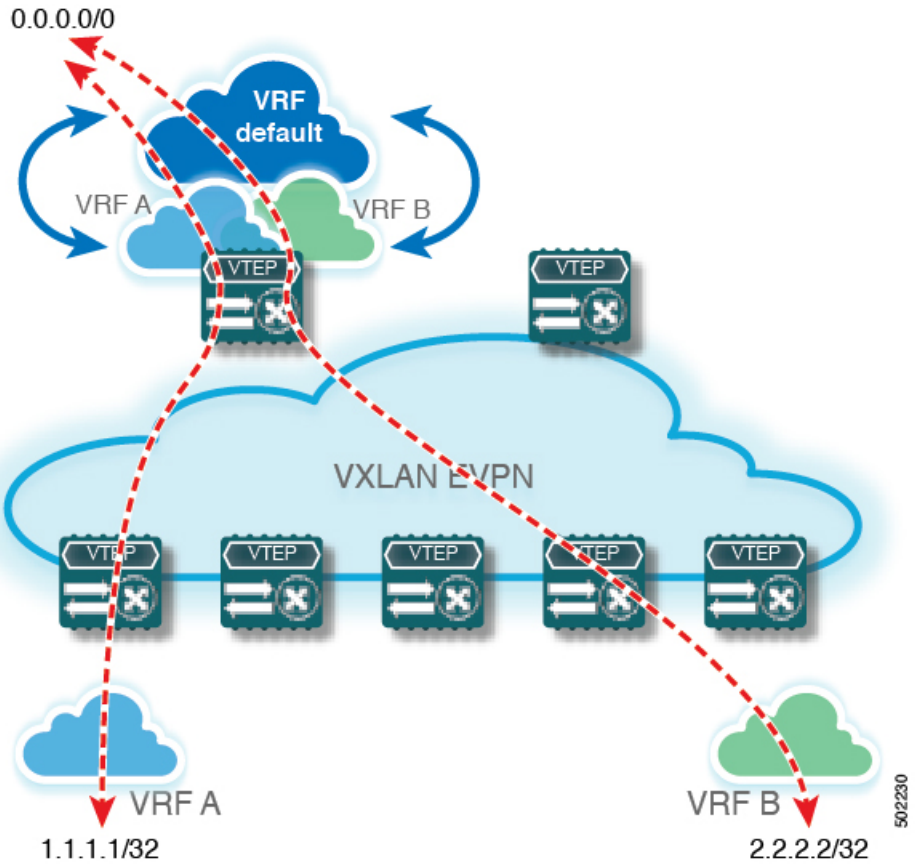
一元管理型 VRF ルート リーク ブリーフ：VRF デフォルトでの共有インターネット

いくつかのポイントを次に示します。

- VXLAN BGP EVPN ファブリックの VRF ルート漏洩を伴う共有インターネットを図 4 に示します。
- default-route は VRF default からエクスポートされ、ボーダーノードの VRF Blue および VRF Red 内で再アドバタイズされます。
- VRF Blue および VRF Red のデフォルト ルートが共有インターネット VRF にリークされていないことを確認します。

- VRF Blue および VRF Red の限定的でないプレフィックスは、VRF デフォルトにエクスポートされ、必要に応じて再アドバタイズされます。
- 境界ノードから残りの VTEP に宛先 VRF（青または赤）にアドバタイズされる、より具体性の低いプレフィックス（集約）。
- BGP EVPN は、ルーティングループの発生を防ぐために以前にインポートされたプレフィックスをエクスポートしません。

図 *7:* 中央集中型 *VRF* ルートリーク：*VRF* デフォルトでの共有インターネット



一元管理型 VRF ルート リークの設定：VRF デフォルトでの共有インターネット

ボーダー ノードでの VRF デフォルトの設定

この手順は、IPv6 にも同様に適用されます。

手順の概要

1. **configure terminal**

2. **ip route 0.0.0.0/0** *next-hop*

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ip route 0.0.0.0/0** *next-hop*	VRF のデフォルト ルートを外部ルータに設定する（例）

ボーダー ノードでの VRF デフォルトの BGP インスタンスの設定

この手順は、IPv6 にも同様に適用されます。

手順の概要

1. **configure terminal**
2. **router bgp** *autonomous-system number*
3. **address-family ipv4 unicast**
4. **aggregate-address** *prefix/mask*
5. **maximum-paths** *number*

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router bgp** *autonomous-system number*	BGP を設定します。
ステップ 3	**address-family ipv4 unicast**	IPv4 のアドレス ファミリを設定します。
ステップ 4	**aggregate-address** *prefix/mask*	VRF のデフォルトで、より限定的なプレフィックス集約を作成します。
ステップ 5	**maximum-paths** *number*	eBGP プレフィックスの等コスト マルチパス（ECMP）の有効化。

ボーダー ノードでのカスタム VRF の設定

この手順は、IPv6 にも同様に適用されます。

手順の概要

1. **configure terminal**
2. **ip prefix-list** *name* **seq 5 permit 0.0.0.0/0**
3. **route-map** *name* **deny 10**
4. **match ip address prefix-list** *name*
5. **route-map** *name* **permit 20**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル構成モードを開始します。
ステップ 2	**ip prefix-list** *name* **seq 5 permit 0.0.0.0/0**	デフォルトルートフィルタリングの IPv4 プレフィックス リストを設定します。
ステップ 3	**route-map** *name* **deny 10**	default-route がリークされるのを防ぐために、先行する deny ステートメントを使用してルートマップを作成します。
ステップ 4	**match ip address prefix-list** *name*	default-route を含む IPv4 プレフィックスリストと照合します。
ステップ 5	**route-map** *name* **permit 20**	ルートリークを介して一致しないルートをアドバタイズする後続の allow ステートメントを使用してルートマップを作成します。

ボーダー ノードでの VRF デフォルトから許可されるプレフィックスのフィルタの設定

この手順は、IPv6 にも同様に適用されます。

手順の概要

1. **configure terminal**
2. **route-map** *name* **permit 10**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル構成モードを開始します。
ステップ 2	**route-map** *name* **permit 10**	allow ステートメントを使用してルートマップを作成し、カスタマー VRF およびその後のリモート VTEP にルートリークを介してルートをアドバタイズします。

ボーダーノードでのカスタム VRF コンテキストの設定 - 2

この手順は、IPv6 にも同様に適用されます。

手順の概要

1. **configure terminal**
2. **vrf context** *vrf-name*
3. **vni** *number*
4. **rd auto**
5. **ip route 0.0.0.0/0 Null0**
6. **address-family ipv4 unicast**
7. **route-target both auto** | *AS:VNI*
8. **route-target both auto** | *AS:VNI* **evpn**
9. **route-target both** *shared-vrf-rt*
10. **route-target both** *shared-vrf-rt* **evpn**
11. **import vrf default map** *name*

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vrf context** *vrf-name*	VRF を設定します。
ステップ 3	**vni** *number*	VNI を指定します。 VRF に関連付けられている VNI は、多くの場合、Layer-3 VNI、L3VNI、または L3VPN と呼ばれま

	コマンドまたはアクション	目的
		す。L3VNI は、参加する VTEP 間で共通の ID として構成されます。
ステップ 4	**rd auto**	VRF のルート識別子（RD）を指定します。 ルート識別子（RD）は、L3VNI 内の VTEP を一意に識別します。
ステップ 5	**ip route 0.0.0.0/0 Null0**	共通 VRF でデフォルト ルートを設定し、共有インターネット VRF を持つボーダーノードにトラフィックを引き付けます。
ステップ 6	**address-family ipv4 unicast**	IPv4 ユニ キャスト アドレス ファミリを設定します。 IPv4 アンダーレイを使用した IPv4 over VXLAN に必要です。
ステップ 7	**route-target both auto** | *AS:VNI*	IPv4 ユニキャスト アドレスファミリ内の EVPN および IPv4 プレフィックスのインポート/エクスポート用のルート ターゲット（RT）を構成します。
ステップ 8	**route-target both auto** | *AS:VNI* **evpn**	IPv4 ユニキャスト アドレスファミリ内の EVPN および IPv4 プレフィックスのインポート/エクスポート用のルート ターゲット（RT）を構成します。
ステップ 9	**route-target both** *shared-vrf-rt*	共有 IPv4 プレフィックスのインポート/エクスポート用の特別なルート ターゲット（RT）を構成します。 さらなる認定のための追加のインポート/エクスポート マップがサポートされます。
ステップ 10	**route-target both** *shared-vrf-rt* **evpn**	共有 IPv4 プレフィックスのインポート/エクスポート用の特別なルート ターゲット（RT）を構成します。 さらなる認定のための追加のインポート/エクスポート マップがサポートされます。
ステップ 11	**import vrf default map** *name*	VRF デフォルトからのすべてのルートが、特定のルート マップに従ってカスタム VRF にインポートされることを許可します。

ボーダー ノードでの BGP でのカスタム VRF インスタンスの設定

この手順は、IPv6 にも同様に適用されます。

手順の概要

1. **configure terminal**
2. **router bgp** *autonomous-system-number*
3. **vrf** *vrf-name*
4. **address-family ipv4 unicast**
5. **advertise l2vpn evpn**
6. **network 0.0.0.0/0**
7. **maximum-paths ibgp** *number*
8. **maximum-paths** *number*

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**router bgp** *autonomous-system-number*	BGP を設定します。
ステップ 3	**vrf** *vrf-name*	VRF を指定します。
ステップ 4	**address-family ipv4 unicast**	IPv4 のアドレス ファミリを設定します。
ステップ 5	**advertise l2vpn evpn**	IPv4 アドレス ファミリ内の EVPN ルートのアドバタイズメントを有効にします。
ステップ 6	**network 0.0.0.0/0**	IPv4 デフォルト ルート ネットワーク ステートメントを作成しています。
ステップ 7	**maximum-paths ibgp** *number*	iBGP プレフィックスの等コスト マルチパス（ECMP）の有効化。
ステップ 8	**maximum-paths** *number*	eBGP プレフィックスの等コスト マルチパス（ECMP）の有効化。

例：一元管理型 VRF ルート リークの設定：カスタム VRF を使用した VRF デフォルト

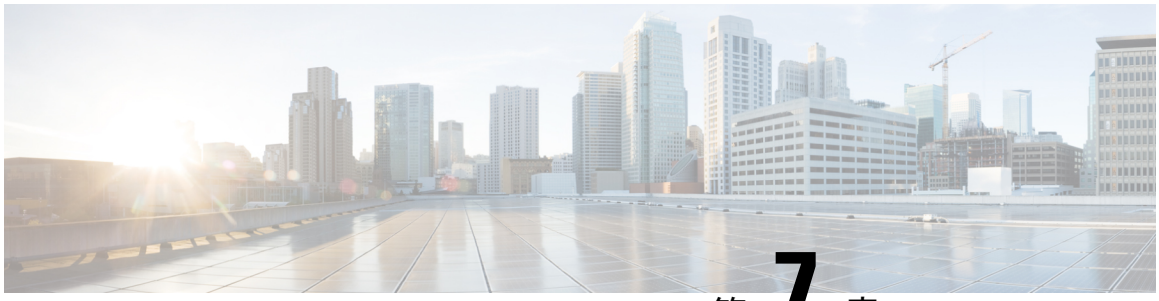
VRF デフォルトによる中央集中型 VRF ルート リークの例

VRF デフォルトの VXLAN BGP EVPN ボーダー ノードの設定

VXLAN BGP EVPN ボーダー ノードは、VRF デフォルトへの集中型アクセスを提供します。漏出設定は、コントロール プレーンの漏出とデータ パス転送が同じパスをたどるようにローカライズされます。最も重要な点は、ボーダー ノードの VRF 設定と、デフォルト ルートと特定性の低いプレフィックス（集約）をそれぞれの宛先 VRF にアドバタイズすることです。

```
ip route 0.0.0.0/0 10.9.9.1
!
ip prefix-list PL_DENY_EXPORT seq 5 permit 0.0.0.0/0
!
route-map permit 10
match ip address prefix-list PL_DENY_EXPORT
route-map RM_DENY_EXPORT permit 20
route-map RM_PERMIT_IMPORT permit 10
!
vrf context Blue
  vni 51010
  ip route 0.0.0.0/0 Null0
  rd auto
  address-family ipv4 unicast
    route-target both auto
    route-target both auto evpn
    import vrf default map RM_PERMIT_IMPORT
    export vrf default 100 map RM_DENY_EXPORT allow-vpn
!
vlan 2110
  vn-segment 51010
!
interface Vlan2110
  no shutdown
  mtu 9216
  vrf member Blue
  no ip redirects
  ip forward
!
vrf context Red
  vni 51020
  ip route 0.0.0.0/0 Null0
  rd auto
  address-family ipv4 unicast
    route-target both auto
    route-target both auto evpn
    import vrf default map RM_PERMIT_IMPORT
    export vrf default 100 map RM_DENY_EXPORT allow-vpn
!
vlan 2120
  vn-segment 51020
!
interface Vlan2120
  no shutdown
  mtu 9216
  vrf member Blue
  no ip redirects
  ip forward
!
interface nve1
  no shutdown
  host-reachability protocol bgp
  source-interface loopback1
  member vni 51010 associate-vrf
  member vni 51020 associate-vrf
!
router bgp 65002
  address-family ipv4 unicast
      aggregate-address 10.10.0.0/16
      aggregate-address 10.20.0.0/16
      maximum-paths 2
      maximum-paths ibgp 2
  vrf Blue
    address-family ipv4 unicast
```

```
    advertise l2vpn evpn
    network 0.0.0.0/0
    maximum-paths ibgp 2
    maximum-paths 2
vrf Red
  address-family ipv4 unicast
    advertise l2vpn evpn
    network 0.0.0.0/0
    maximum-paths ibgp 2
    maximum-paths 2
```



第 7 章

EVPN と L3VPN (MPLS LDP) のシームレスな統合の設定

この章は、次の内容で構成されています。

EVPN と L3VPN (MPLS LDP) のシームレスな統合の設定の詳細

データセンターの展開では、EVPN コントロール プレーン ラーニング、マルチテナンシー、シームレスなモビリティ、冗長性、POD の追加が容易になるなどの利点から、VXLAN EVPN を採用しています。同様に、コアは LDP ベースの MPLS L3VPN ネットワークであるか、従来の MPLS L3VPN LDP ベースのアンダーレイからセグメントルーティング（SR）のようなより高度なソリューション（SR）に移行するかのいずれかです。セグメント ルーティングは、ユニファイド IGP および MPLS コントロール プレーン、シンプルなトラフィック エンジニアリング方式、簡単な設定、SDN の採用などの利点のために採用されています。

データセンター内とコア内の 2 つの異なるテクノロジーにより、VXLAN から DCI ノードで MPLS ベースのコアにハンドオフするのは自然なことです。これらのノードは、DC ドメインのエッジにあり、コア エッジ ルータとインターフェイスします。

に関する注意事項と制限事項 EVPN と L3VPN (MPLS LDP) のシームレスな統合の設定

EVPN と L3VPN (MPLS LDP) のシームレスな統合の設定 の注意事項と制限事項は次のとおりです。

EVPN と L3VPN (MPLS LDP) のシームレスな統合の設定

サポートされる機能は次のとおりです。

- レイヤ 3 オーファン
- MPLS が拡張された ECMP（デフォルトで有効に設定されています）。
- Cisco NX-OS リリース 10.3(3)F 以降では、MPLS LDP ユーザー パスワードのタイプ 6 暗号化が Cisco NX-OS スイッチでサポートされています。

次の機能はサポートされていません。

- サブネットが DC ドメイン全体に拡大する
- vPC
- SVI/サブインターフェイス

EVPN と L3VPN (MPLS LDP) のシームレスな統合の設定

これらの構成手順は、XLAN ドメインから MPLS ドメインにルートをインポートして再発信し、VXLAN ドメインに戻すために DCI スイッチで必要です。

手順の概要

1. **configure terminal**
2. **feature mpls l3vpn**
3. **feature mpls ldp**
4. **nv overlay evpn**
5. **router bgp** *number*
6. **address-family ipv4 unicast**
7. **redistribute direct route-map** *route-map-name*
8. **exit**
9. **address-family l2vpn evpn**
10. **exit**
11. **neighbor** *address* **remote-as** *number*
12. **update-source** *type/id*
13. **ebgp-multihop** *ttl-value*
14. **address-family ipv4 unicast**
15. **send-community extended**
16. **exit**
17. **address-family vpnv4 unicast**
18. **send-community extended**
19. **import l2vpn evpn reoriginate**
20. **neighbor** *address* **remote-as** *number*
21. **address-family ipv4 unicast**
22. **send-community extended**
23. **address-family ipv6 unicast**

EVPN と L3VPN (MPLS LDP) のシームレスな統合の設定

24. **send-community extended**
25. **address-family l2vpn evpn**
26. **send-community extended**
27. **import vpn unicast reoriginate**

手順の詳細

手順

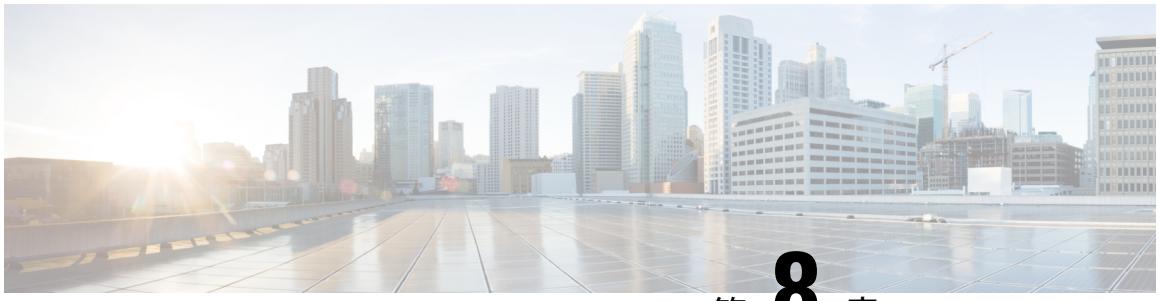
	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**feature mpls l3vpn** 例： `switch# feature mpls l3vpn`	MPLS レイヤ 3 VPN 機能をイネーブルにします。
ステップ 3	**feature mpls ldp** 例： `switch# feature mpls ldp`	MPLS ラベル配布プロトコル（LDP）をイネーブルにします。
ステップ 4	**nv overlay evpn** 例： `switch(config)# nv overlay evpn`	EVPN コントロール プレーンを VXLAN にイネーブルにします。
ステップ 5	**router bgp** *number* 例： `switch(config)# router bgp 100`	BGP を設定します。この引数の値の範囲は 1 ～ 4294967295 です。
ステップ 6	**address-family ipv4 unicast** 例： `switch(config-router)# address-family ipv4 unicast`	IPv4 のアドレス ファミリを設定します。
ステップ 7	**redistribute direct route-map** *route-map-name* 例： `switch(config-router-af)# redistribute direct route-map passall`	直接接続されたルート マップを設定します。
ステップ 8	**exit** 例： `switch(config-router-af)# exit`	コマンド モードを終了します。

EVPN と L3VPN (MPLS LDP) のシームレスな統合の設定

	コマンドまたはアクション	目的
ステップ 9	**address-family l2vpn evpn** 例： `switch(config-router)# address-family l2vpn evpn`	L2VPN アドレス ファミリを設定します。
ステップ 10	**exit** 例： `switch(config-router-af)# exit`	コマンド モードを終了します。
ステップ 11	**neighbor** *address* **remote-as** *number* 例： `switch(config-router)# neighbor 108.108.108.108 remote-as 22`	BGP ネイバーを設定します。引数 *number* の範囲は、1 ～ 65535 です。
ステップ 12	**update-source** *type/id* 例： `switch(config-router-neighbor)# update-source loopback100`	BGP セッションの送信元を指定し、更新します。
ステップ 13	**ebgp-multihop** *ttl-value* 例： `switch(config-router-neighbor)# ebgp-multihop 10`	リモート ピアにマルチホップ TTL を指定します *ttl-value* の範囲は 2 ～ 255 です。
ステップ 14	**address-family ipv4 unicast** 例： `switch(config-router-neighbor)# address-family ipv4 unicast`	ユニキャストサブアドレスファミリを設定します。
ステップ 15	**send-community extended** 例： `switch(config-router-neighbor-af)# send-community extended`	このネイバーのコミュニティ属性を設定します。
ステップ 16	**exit** 例： `switch(config-router-neighbor-af)# exit`	コマンド モードを終了します。
ステップ 17	**address-family vpnv4 unicast** 例： `switch(config-router-neighbor)# address-family vpnv4 unicast`	IPv4 のアドレス ファミリを設定します。
ステップ 18	**send-community extended** 例： `switch(config-router)# send-community extended`	拡張コミュニティ属性を送信します。

	コマンドまたはアクション	目的
ステップ 19	**import l2vpn evpn reoriginate** 例： `switch(config-router)# import l2vpn evpn reoriginate`	新しい RT でルートを再発信します。
ステップ 20	**neighbor** *address* **remote-as** *number* 例： `switch(config-router)# neighbor 175.175.175.2 remote-as 1`	ネイバーを定義します。
ステップ 21	**address-family ipv4 unicast** 例： `switch(config-router)# address-family ipv4 unicast`	IPv4 のアドレス ファミリを設定します。
ステップ 22	**send-community extended** 例： `switch(config-router)# send-community extended`	BGP ネイバーのコミュニティを設定します。
ステップ 23	**address-family ipv6 unicast** 例： `switch(config-router)# address-family ipv6 unicast`	IPv4 アンダーレイを使用した IPv6 over VXLAN に必要な IPv6 ユニキャスト アドレス ファミリを構成します。
ステップ 24	**send-community extended** 例： `switch(config-router)# send-community extended`	BGP ネイバーのコミュニティを設定します。
ステップ 25	**address-family l2vpn evpn** 例： `switch(config-router)# address-family l2vpn evpn`	L2VPN アドレス ファミリを設定します。
ステップ 26	**send-community extended** 例： `switch(config-router)# send-community extended`	BGP ネイバーのコミュニティを設定します。
ステップ 27	**import vpn unicast reoriginate** 例： `switch(config-router)# import vpn unicast reoriginate`	新しい RT でルートを再発信します。

EVPN と L3VPN (MPLS LDP) のシームレスな統合の設定



第 8 章

EVPN と L3VPN (MPLS SR) のシームレスな統合の設定

この章は、次の内容で構成されています。

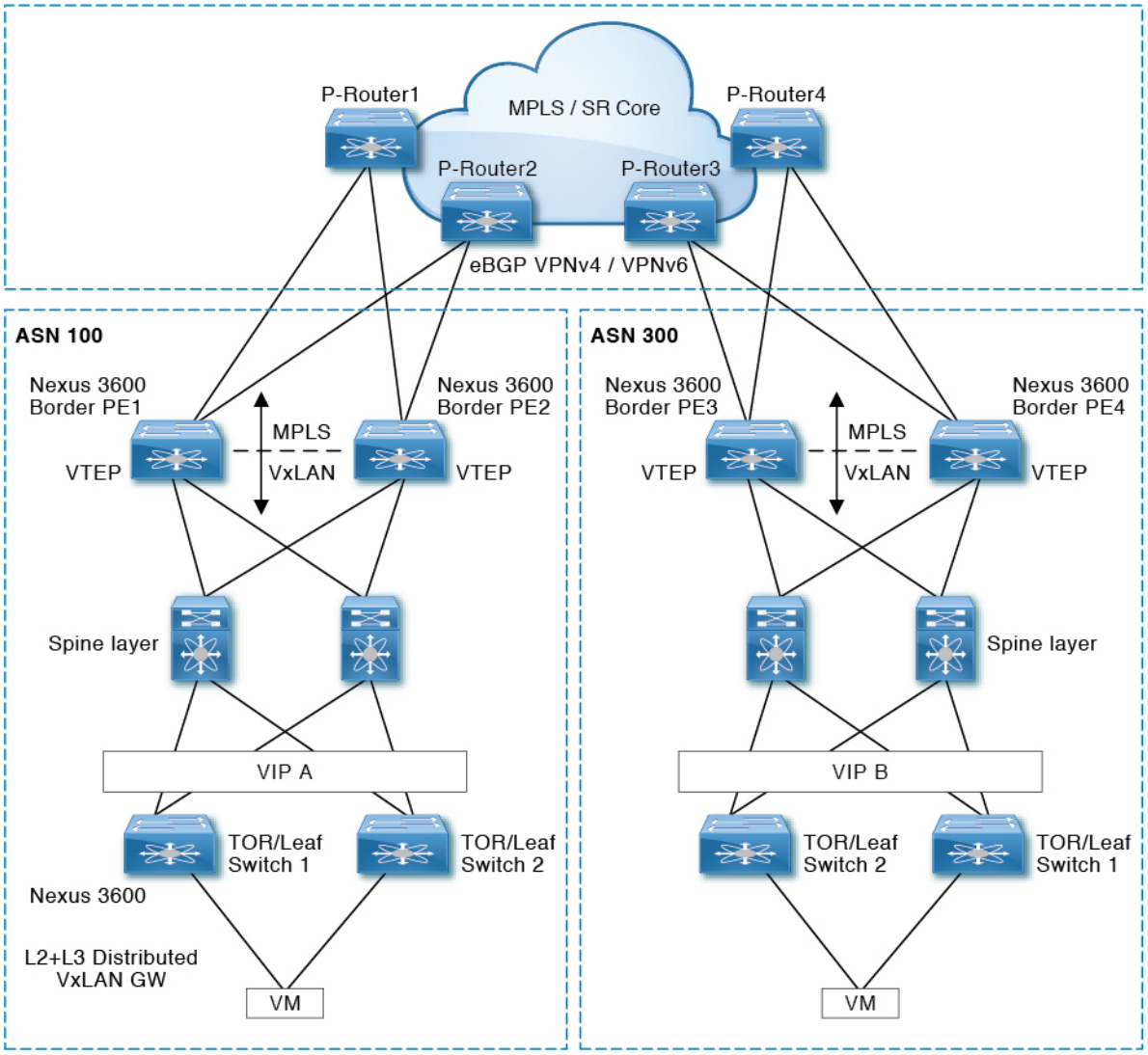
EVPN と L3VPN (MPLS SR) のシームレスな統合の設定の詳細

データセンター（DC）導入では、EVPN コントロール プレーン ラーニング、マルチテナンシー、シームレス モビリティ、冗長性、POD の追加が容易になるなどの利点から、VXLAN EVPN を採用しています。同様に、CORE は、ラベル配布プロトコル（LDP）ベースの MPLS L3VPN ネットワークであるか、または従来の MPLS L3VPN LDP ベースのアンダーレイからセグメント ルーティング（SR）のようなより高度なソリューションに移行します。セグメント ルーティングは、次のような利点のために採用されています。

- Unified IGP および MPLS コントロール プレーン
- よりシンプルなトラフィック エンジニアリング手法
- より簡単に行えるクライアント設定
- SDN の採用

データセンター（DC）内とCORE 内の 2 つの異なるテクノロジーでは、DCI ノードで VXLAN から MPLS ベースのコアにハンドオフする必要があります。コア エッジ ルータを使用します。

図 *8*: トポロジ概要



前の図では、それぞれ VXLAN を実行している 2 つの DC ポッドが、MPLS/SR を実行している WAN/コア上でレイヤ 3 拡張されています。もう 1 つの方法は、LDP を使用する従来の MPLS L3VPN です。DC ドメイン内のエッジデバイス（ボーダー PE1、PE2、PE3、および PE4）は、VXLAN と MPLS ベースのコア ネットワーク間のハンドオフを行う DCI ノードです。

に関する注意事項と制限事項 EVPN と L3VPN (MPLS SR) のシームレスな統合の設定

機能	Cisco Nexus 3600	注
VXLAN EVPN から SR-L3VPN へ	○	異なる DC ポッド間のレイヤ 3 接続を拡張します。SR 拡張を使用して IGP/BGP のアンダーレイを設定します。
VXLAN EVPN から SR-L3VPN へ	はい	VXLAN を実行する DC POD と SR を実行する任意のドメイン（DC または CORE）間のレイヤ 3 接続を拡張します。
VXLAN EVPN から MPLS L3VPN（LDP）	はい	アンダーレイは LDP です。

サポートされる機能は次のとおりです。

- レイヤ 3 オーファン
- レイヤ 3 ハンドオフ
- コアに向けたポートのレイヤ 3 物理インターフェイス タイプ
- VRF 単位のラベル
- LDP
- セグメント ルーティング

（注） セグメント ルーティングと LDP は共存できません。

次の機能はサポートされていません。

- 冗長性のための vPC
- サブネットが DC ドメイン全体に拡大する
- SVI/サブインターフェイスで設定された MAC アドレス
- 統計
- MPLS コアへの SVI

EVPN と L3VPN (MPLS SR) のシームレスな統合の設定

- エンドツーエンドの存続可能時間（TTL）のサポート（ハンドオフ シナリオのパイプ モードでのみ）
- ハンドオフ シナリオのエンドツーエンドの明示的輻輳通知（ECN）

EVPN と L3VPN (MPLS SR) のシームレスな統合の設定

次の手順では、VXLAN ドメインから MPLS ドメインへのルートをインポートし、他の方向に再送信します。

始める前に

手順の概要

1. **configure terminal**
2. **feature-set mpls**
3. **nv overlay evpn**
4. **feature bgp**
5. **feature mpls l3vpn**
6. **feature mpls segment-routing**
7. **feature interface-vlan**
8. **feature vn-segment-vlan-based**
9. **feature nv overlay**
10. **router bgp** *autonomous-system-number*
11. **address-family ipv4 unicast**
12. **redistribute direct route-map** *route-map-name*
13. **network** *address*
14. **exit**
15. **address-family l2vpn evpn**
16. **neighbor** *address* **remote-as** *number*
17. **update-source** *type/id*
18. **ebgp-multihop** *number*
19. **address-family ipv4 unicast**
20. **send-community extended**
21. **exit**
22. **address-family vpnv4 unicast**
23. **send-community extended**
24. **import l2vpn evpn reoriginate**
25. **neighbor** *address* **remote-as** *number*
26. **address-family ipv4 unicast**
27. **send-community extended**
28. **exit**
29. **address-family ipv6 unicast**
30. **send-community extended**

EVPN と L3VPN (MPLS SR) のシームレスな統合の設定

31. **exit**
32. **address-family l2vpn evpn**
33. **send-community extended**
34. **exit**
35. **import vpn unicast reoriginate**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**feature-set mpls** 例： `switch(config)# feature-set mpls`	MPLS フィーチャ セットを有効にします。
ステップ 3	**nv overlay evpn** 例： `switch(config)# nv overlay evpn`	VXLAN をイネーブル化します。
ステップ 4	**feature bgp** 例： `switch(config)# feature bgp`	BGP を有効にします。
ステップ 5	**feature mpls l3vpn** 例： `switch(config)# feature mpls l3vpn`	レイヤ 3 VPN を有効にします。
ステップ 6	**feature mpls segment-routing** 例： `switch(config)# feature mpls segment-routing`	セグメント ルーティングを有効化します。
ステップ 7	**feature interface-vlan** 例： `switch(config)# feature interface-vlan`	VLAN インターフェイスを有効にします。
ステップ 8	**feature vn-segment-vlan-based** 例： 例： `switch(config)# feature vn-segment-vlan-based`	VLAN ベースの VN セグメントを有効化します。

EVPN と L3VPN (MPLS SR) のシームレスな統合の設定

	コマンドまたはアクション	目的
ステップ 9	**feature nv overlay** 例： 例： `switch(config)# feature nv overlay`	VXLAN をイネーブル化します。
ステップ 10	**router bgp** *autonomous-system-number* 例： `switch(config)# router bgp 1`	BGP を設定します。*autonomous-system-number* の値は 1ー4294967295 です。
ステップ 11	**address-family ipv4 unicast** 例： `switch(config-router)# address-family ipv4 unicast`	IPv4 のアドレス ファミリを設定します。
ステップ 12	**redistribute direct route-map** *route-map-name* 例： `switch(config-router-af)# redistribute direct route-map passall`	再配布を構成します。
ステップ 13	**network** *address* 例： `switch(config-router-af)# network 0.0.0.0/0`	再配布とともにプレフィックスをハンドオフ BGP に注入します。
ステップ 14	**exit** 例： `switch(config-router-af)# exit`	コマンド モードを終了します。
ステップ 15	**address-family l2vpn evpn** 例： `switch(config-router)# address-family l2vpn evpn`	L2VPN アドレス ファミリを構成します。
ステップ 16	**neighbor** *address* **remote-as** *number* 例： `switch(config-router)# neighbor 108.108.108.108 remote-as 65535`	eBGP ネイバーの IPv4 アドレスおよびリモート自律システム（AS）番号を定義します。
ステップ 17	**update-source** *type/id* 例： `switch(config-router-af)# update-source loopback100`	eBGP ピアリングのインターフェイスを定義します。
ステップ 18	**ebgp-multihop** *number* 例： `switch(config-router)# ebgp-multihop 10`	リモート ピアにマルチホップ TTL を指定します。*number* の範囲は 2 ～ 255 です。

	コマンドまたはアクション	目的
ステップ 19	**address-family ipv4 unicast** 例： `switch(config-router)# address-family ipv4 unicast`	IPv4 のアドレス ファミリを設定します。
ステップ 20	**send-community extended** 例： `switch(config-router-af)# send-community extended`	BGP ネイバーのコミュニティを設定します。
ステップ 21	**exit** 例： `switch(config-router-af)# exit`	コマンド モードを終了します。
ステップ 22	**address-family vpnv4 unicast** 例： `switch(config-router)# address-family vpnv4 unicast`	IPv4 のアドレス ファミリを設定します。
ステップ 23	**send-community extended** 例： `switch(config-router-af)# send-community extended`	BGP ネイバーのコミュニティを設定します。
ステップ 24	**import l2vpn evpn reoriginate** 例： `switch(config-router)# import l2vpn evpn reoriginate`	新しいRTでルートを再発信します。オプションのルートマップを使用するように拡張できます。
ステップ 25	**neighbor** *address* **remote-as** *number* 例： `switch(config-router)# neighbor 175.175.175.2 remote-as 65535`	eBGP ネイバーの IPv4 アドレスおよびリモート自律システム（AS）番号を定義します。
ステップ 26	**address-family ipv4 unicast** 例： `switch(config-router)# address-family ipv4 unicast`	IPv4 のアドレス ファミリを設定します。
ステップ 27	**send-community extended** 例： `switch(config-router-af)# send-community extended`	BGP ネイバーのコミュニティを設定します。
ステップ 28	**exit** 例： `switch(config-router-af)# exit`	コマンド モードを終了します。

	コマンドまたはアクション	目的
ステップ 29	**address-family ipv6 unicast** 例： `switch(config-router)# address-family ipv6 unicast`	IPv6 ユニ キャスト アドレス ファミリを構成します。これは、IPv4 アンダーレイを使用した IPv6 over VXLAN に必要です。
ステップ 30	**send-community extended** 例： `switch(config-router-af)# send-community extended`	BGP ネイバーのコミュニティを設定します。
ステップ 31	**exit** 例： `switch(config-router-af)# exit`	コマンド モードを終了します。
ステップ 32	**address-family l2vpn evpn** 例： `switch(config-router)# address-family l2vpn evpn`	L2VPN アドレス ファミリを構成します。
ステップ 33	**send-community extended** 例： `switch(config-router-af)# send-community extended`	BGP ネイバーのコミュニティを設定します。
ステップ 34	**exit** 例： `switch(config-router-af)# exit`	コマンド モードを終了します。
ステップ 35	**import vpn unicast reoriginate** 例： `switch(config-router)# import vpn unicast reoriginate`	新しい RT でルートを再発信します。オプションのルートマップを使用するように拡張できます。

EVPN と L3VPN (MPLS SR) のシームレスな統合の設定 の設定例

次に示すのは、VXLAN ドメインから MPLS ドメインへ、および逆方向にルートをインポートおよび再発信するために必要な CLI 設定の例です。

```
switch# sh running-config

!Command: show running-config
!Running configuration last done at: Sat Mar 17 10:00:40 2001
!Time: Sat Mar 17 12:50:12 2001

version 9.2(2) Bios:version 05.22
hardware profile multicast max-limit lpm-entries 0
```

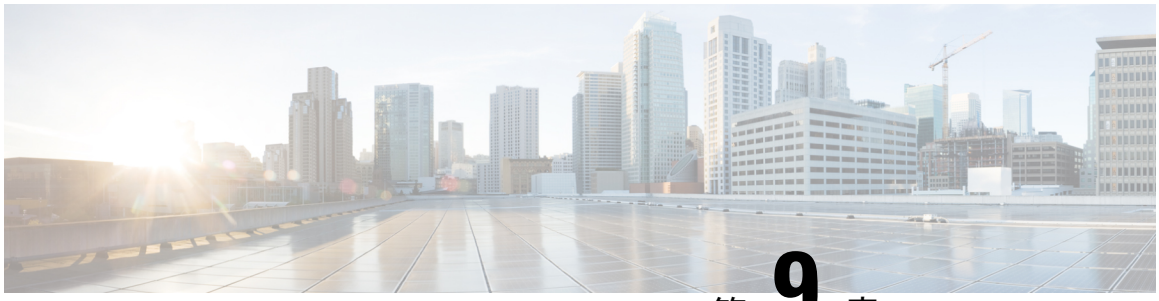
```
hostname switch
install feature-set mpls
vdc Scrimshaw id 1
  allow feature-set mpls
  limit-resource vlan minimum 16 maximum 4094
  limit-resource vrf minimum 2 maximum 4096
  limit-resource port-channel minimum 0 maximum 511
  limit-resource u4route-mem minimum 248 maximum 248
  limit-resource u6route-mem minimum 96 maximum 96
  limit-resource m4route-mem minimum 90 maximum 90
  limit-resource m6route-mem minimum 8 maximum 8
feature-set mpls

feature telnet
feature bash-shell
feature sftp-server
nv overlay evpn
feature ospf
feature bgp
feature mpls l3vpn
feature mpls segment-routing
feature interface-vlan
feature vn-segment-vlan-based
feature bfd
feature nv overlay

no password strength-check
username admin password 5
$5$eEI.wtRs$txfevWxMj/upb/1dJeXy5rNvFYKymzz3Zmc.fpuxTp
1  role network-admin
ip domain-lookup
copp profile strict
snmp-server user admin network-admin auth md5 0x116815e4934ab1f854dce5dd673f33d7
 priv 0x116815e4934ab1f854dce5dd673f33d7 localizedkey
rmon event 1 description FATAL(1) owner PMON@FATAL
rmon event 2 description CRITICAL(2) owner PMON@CRITICAL
rmon event 3 description ERROR(3) owner PMON@ERROR
rmon event 4 description WARNING(4) owner PMON@WARNING
rmon event 5 description INFORMATION(5) owner PMON@INFO

mpls label range 30000 40000 static 6000 8000
vlan 1-2,100,200,555
segment-routing mpls
  global-block 30000 40000
vlan 555
  vn-segment 55500

route-map ALL permit 10
route-map SRmap permit 10
  set label-index 666
route-map ULAY_NETWORK permit 10
  set label-index 600
route-map passall permit 10
vrf context ch5_swap
  ip route 199.1.1.0/24 16.1.1.2
  ip route 200.1.1.0/24 16.1.1.2
vrf context evpn
  vni 55500
  rd auto
  address-family ipv4 unicast
    route-target import 100:55500
    route-target import 100:55500 evpn
    route-target import 6:6000
```

```
    route-target export 100:55500
    route-target export 100:55500 evpn
    route-target export 6:6000
  address-family ipv6 unicast
    route-target import 6:6000
    route-target export 6:6000
vrf context management
  ip route 0.0.0.0/0 172.31.144.1
hardware forwarding unicast trace
vlan configuration 2
  ip igmp snooping static-group 225.1.1.1 interface Ethernet1/9

interface Vlan1

interface Vlan555
  no shutdown
  vrf member evpn

interface nve1
  no shutdown
  host-reachability protocol bgp
  source-interface loopback1
  member vni 55500 associate-vrf

interface Ethernet1/12
  mpls ip forwarding
  no shutdown

interface Ethernet1/13

interface Ethernet1/14
  no shutdown

interface Ethernet1/15
  no shutdown

interface Ethernet1/16
  no shutdown

interface Ethernet1/17
  no shutdown

interface Ethernet1/18

interface Ethernet1/19

interface Ethernet1/20
  no shutdown

interface Ethernet1/21
  ip address 6.2.0.1/24
  mpls ip forwarding
  no shutdown

interface Ethernet1/21.1
  encapsulation dot1q 1211
  vrf member evpn
  ip address 6.22.0.1/24
  no shutdown

interface Ethernet1/21.2
  encapsulation dot1q 1212
  ip address 6.222.0.1/24
  no shutdown
```

```
interface Ethernet1/21.3
  encapsulation dot1q 1213
  vrf member ch5_swap
  ip address 16.1.1.1/24
  no shutdown

interface Ethernet1/22
  no shutdown

interface Ethernet1/23
  description underlay
  ip address 6.1.0.1/24
  mpls ip forwarding
  no shutdown

interface Ethernet1/23.1
  encapsulation dot1q 1231
  vrf member evpn
  ip address 6.11.0.1/23
  no shutdown

interface Ethernet1/24
  no shutdown

interface Ethernet1/25
  no shutdown

interface Ethernet1/26
  description underlay
  ip address 6.0.0.1/24
  mpls ip forwarding
  no shutdown

interface Ethernet1/26.1
  encapsulation dot1q 1261
  ip address 7.0.0.1/24
  no shutdown

interface Ethernet1/27
  no shutdown

interface Ethernet1/28
  no shutdown

interface Ethernet1/29
  no shutdown

interface Ethernet1/30
  no shutdown

interface Ethernet1/31
  ip address 1.31.1.1/24
  no shutdown

interface Ethernet1/32
  no shutdown

interface Ethernet1/33
  ip address 87.87.87.1/24
  ip router ospf 100 area 0.0.0.0
  no shutdown

interface Ethernet1/34
```

```
  no shutdown

interface Ethernet1/35
  no shutdown

interface Ethernet1/36
  no shutdown

interface mgmt0
  vrf member management
  ip address 172.31.145.107/21

interface loopback1
  ip address 58.58.58.58/32

interface loopback6
  description used for SR underlay testing
  ip address 6.6.6.1/32
line console
line vty
monitor session 1
  source interface Ethernet1/21 rx
  source interface Ethernet1/23 both
  destination interface sup-eth0

mpls static configuration
  address-family ipv4 unicast
    lsp SL_AGG_BELL
      in-label 6001 allocate policy 88.1.1.0 255.255.255.0
        forward
          path 1 next-hop 6.0.0.2 out-label-stack implicit-null
router ospf 100
  redistribute direct route-map ALL
router bgp 600
  address-family ipv4 unicast
    network 6.6.6.1/32 route-map SRmap
    network 66.1.1.0/24 route-map ULAY_NETWORK
    redistribute direct route-map passall
    maximum-paths 32
    allocate-label all
  neighbor 6.0.0.2
    remote-as 50
    ebgp-multihop 255
    address-family ipv4 labeled-unicast
  neighbor 6.1.0.2
    remote-as 50
    ebgp-multihop 255
    address-family ipv4 labeled-unicast
  neighbor 6.6.6.3
    remote-as 300
    update-source loopback6
    ebgp-multihop 255
    address-family vpnv4 unicast
      send-community
      send-community extended
      next-hop-self
      import l2vpn evpn reoriginate
  neighbor 7.0.0.2
    remote-as 50
    ebgp-multihop 255
    address-family ipv4 labeled-unicast
  neighbor 21.21.21.21
    remote-as 600
    update-source loopback1
```

```
  address-family l2vpn evpn
    send-community
    send-community extended
    import vpn unicast reoriginate
vrf evpn
  address-family ipv4 unicast
    advertise l2vpn evpn
    redistribute direct route-map passall
    redistribute hmm route-map passall
  address-family ipv6 unicast
    redistribute direct route-map passall
```



第 9 章

EVPN (TRM) の MVPN とのシームレスな統合の設定

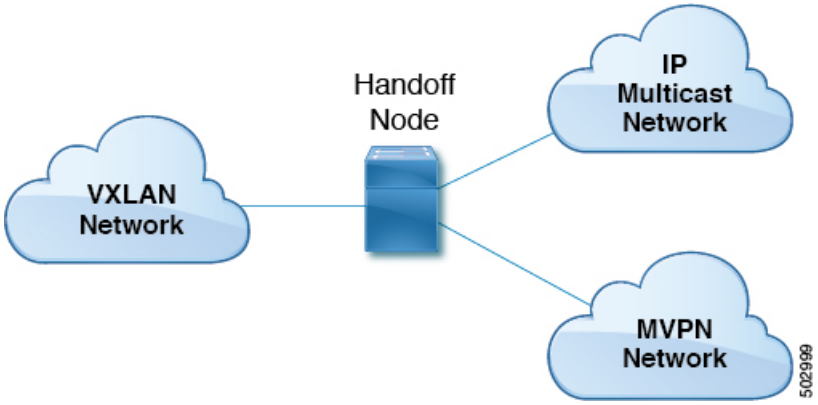
この章は、次の項で構成されています。

EVPN（TRM）の MVPN（Rosen ドラフト）とのシームレスな統合について

EVPN（TRM）と MVPN（ドラフトローゼン）のシームレスな統合により、VXLAN ネットワーク（TRM または TRM マルチサイト）と MVPN ネットワークの間でパケットをハンドオフできます。この機能をサポートするには、VXLAN TRM と MVPN が Cisco Nexus デバイス ノード（ハンドオフ ノード）でサポートされている必要があります。

ハンドオフ ノードは、MVPN ネットワークの PE および VXLAN ネットワークの VTEP です。次の図に示すように、VXLAN、MVPN、および IP マルチキャスト ネットワークに接続します。

図 *9*: *VXLAN* : *MVPN* ハンドオフ ネットワーク



送信元と受信者は、3 つのネットワーク（VXLAN、MVPN、または IP マルチキャスト）のいずれかに存在できます。

すべてのマルチキャスト トラフィック（つまり、VXLAN、MVPN、またはマルチキャスト ネットワークからのテナント トラフィック）は、あるドメインから別のドメインにルーティングされます。ハンドオフ ノードは中央ノードとして機能します。必要なパケット転送、カプセル化、およびカプセル化解除を実行して、それぞれの受信者にトラフィックを送信します。

サポートされる RP の位置

カスタマー（オーバーレイ）ネットワークのランデブー ポイント（RP）は、3 つのネットワーク（VXLAN、MVPN、または IP マルチキャスト）のいずれかに配置できます。

表 *2*: サポートされる *RP* の場所

RP の場所	説明
IP ネットワークの RP	• RP は MVPN PE にのみ接続でき、ハンドオフ ノードには接続できません。 • RPはVXLAN ハンドオフ ノードにのみ接続できます。 • RP は、MVPN PE と VXLAN の両方に接続できます。
VXLAN ファブリック内部の RP	すべての VTEP は、VXLAN ファブリック内の RP です。すべての MVPN PE は、VXLAN ファブリックに設定された RP を使用します。
VXLAN MVPN ハンドオフ ノード上の RP	RP は VXLAN MVPN ハンドオフ ノードです。

RP の場所	説明
MVPN ネットワークの RP	RP は VXLAN ネットワークの外部にあります。これは、ハンドオフ ノード以外の MPLS クラウド内のノードの 1 つで設定されます。
RP Everywhere（PIM エニーキャスト RP または MSDP ベースのエニーキャスト RP）	エニーキャスト RP は VXLAN リーフで設定できます。RP セットは、ハンドオフ ノードまたは任意の MVPN PE で設定できます。

EVPN（TRM）と MVPN とのシームレスな統合に関する注意事項と制約事項

この機能には、次の注意事項と制約事項があります。

- ハンドオフ ノードは、カスタマー ネットワークのローカル（直接接続）マルチキャスト送信元または受信者を持つことができます。
- MVPN 用の ASM/SSM や TRM 用の ASM などの既存のアンダーレイ プロパティは、ハンドオフ ノードでサポートされます。
- ハンドオフ ノードは、オーバーレイの PIM SSM および ASM をサポートします。
- Inter-AS オプション A は、IP マルチキャスト ネットワークへのハンドオフ ノードでサポートされます。
- サポートされている MDT 送信元ループバック IP アドレスと NVE ループバック IP アドレスの総数は16です。ループバック IP アドレスの数がこの制限を超えると、トラフィックがドロップされる可能性があります。
- 次の機能は、EVPN（TRM）と MVPN のシームレスな統合ではサポートされていません。
  - ハンドオフノードの vPC
  - VXLAN EVPN 入力複製
  - MVPN のコア方向インターフェイスとしての SVI およびサブインターフェイス
  - MVPN ノードの Inter-AS オプション B および C
  - VXLAN アンダーレイとしての PIM SSM
  - アンダーレイまたはオーバーレイとしての双方向 PIM
  - MPLS パスと IP パスが混在する ECMP
- VXLAN、TRM、および MVPN の既存の制限は、EVPN（TRM）と MVPN のシームレスな統合にも適用されます。

EVPN（TRM）と MVPN とのシームレスな統合のためのハンドオフ ノードの設定

このセクションでは、ハンドオフ ノードで必要な設定について説明します。他のノード（VXLAN リーフおよびスパイン、MVPN PE、RS/RR など）の設定は、以前のリリースと同じです。

ハンドオフ ノードの PIM/IGMP 設定

ハンドオフ ノードの PIM/IGMP を設定する場合は、次のガイドラインに従ってください。

- 次の例に示すように、ランデブー ポイント（RP）が TRM と MVPN アンダーレイで異なることを確認します。

```
ip pim rp-address 90.1.1.100 group-list 225.0.0.0/8 --- TRM Underlay
ip pim rp-address 91.1.1.100 group-list 233.0.0.0/8 --- MVPN Underlay
```

- オーバーレイ マルチキャスト トラフィックに共通の RP を使用します。
- RP は、静的、PIM エニーキャスト、または PIM MSDP モードにできます。次に、内部 VRF 設定モードを開始する例を示します。

```
vrf context vrfVxLAN5001
  vni 5001
  ip pim rp-address 111.1.1.1 group-list 226.0.0.0/8
  ip pim rp-address 112.2.1.1 group-list 227.0.0.0/8
```

- **ip igmp snooping vxlan** コマンドを使用して、VXLAN トラフィックの IGMP スヌーピングを有効にします。
- すべてのソース インターフェイスおよび PIM トラフィックの伝送に必要なインターフェイスで PIM スパース モードを有効にします。

ハンドオフ ノードの BGP 設定

ハンドオフ ノードの BGP の設定時には、次の注意事項に従ってください。

- すべての VXLAN リーフを L2EVPN および TRM ネイバーとして追加します。冗長ハンドオフ ノードを含めます。ルート リフレクタを使用する場合は、RR だけをネイバーとして追加します。
- すべての MVPN PE を VPN ネイバーとして追加します。MDT モードでは、MVPN PE を MDT ネイバーとして追加します。
- L2EVPN ネイバーから VPN ネイバーにユニキャスト ルートをアドバタイズするための設定をインポートします。
- BGP 送信元識別子は、VTEP 識別子（NVE インターフェイスで設定）/MVPN PE 識別子に使用される送信元インターフェイスとは異なる場合も、同じ場合もあります。

```
feature bgp
address-family ipv4 mdt
address-family ipv4 mvpn

neighbor 2.1.1.1
  address-family ipv4 mvpn
    send-community extended
  address-family l2vpn evpn
    send-community extended
    import vpn unicast reoriginate

neighbor 30.30.30.30
  address-family vpnv4 unicast
    send-community
    send-community extended
    next-hop-self
    import l2vpn evpn reoriginate
  address-family ipv4 mdt
    send-community extended
    no next-hop-third-party
```

- MVPN ピア間で Inter-AS オプション B を使用しないでください。代わりに、VPNv4 ユニキャスト アドレス ファミリで **no allocate-label option-b** コマンドを設定します。

```
address-family vpnv4 unicast
    no allocate-label option-b
```

- 最大パスの設定は EBGP モードで設定する必要があります。

```
address-family l2vpn evpn
    maximum-paths 8
vrf vrfVxLAN5001
    address-family ipv4 unicast
        maximum-paths 8
```

- ハンドオフ ノードがデュアル モードで展開されている場合は、**route-map** コマンドを使用して、VPN アドレス ファミリで孤立したホストに関連付けられているプレフィックスをアドバタイズします。

```
ip prefix-list ROUTES_CONNECTED_NON_LOCAL seq 2 premit 15.14.0.15/32

route-map ROUTES_CONNECTED_NON_LOCAL deny
    match ip address prefix-list ROUTES_CONNECTED_NON_LOCAL

neighbor 8.8.8.8
    remote-as 100
    update-source loopback1
    address-family vpnv4 unicast
      send-community
      send-community extended
      route-map ROUTES_CONNECTED_NON_LOCAL out
```

ハンドオフ ノードの VXLAN 設定

ハンドオフ ノードの VXLAN の設定時には、次の注意事項に従ってください。

- 次の機能をイネーブル化します。

```
feature nv overlay
feature ngmvpn
```

```
feature interface-vlan
feature vn-segment-vlan-based
```

- 必要な L3 VNI を設定します。

```
L3VNIs are mapped to tenant VRF.
vlan 2501
  vn-segment 5001 <-- Associate VNI to a VLAN.
```

- NVE インターフェイスを設定します。

```
interface nve1
  no shutdown
  host-reachability protocol bgp
  source-interface loopback1 <-- This interface should not be the same as the MVPN
source interface.
  global suppress-arp
member vni 5001 associate-vrf <-- L3VNI
  mcast-group 233.1.1.1 <-- The underlay multicast group for VXLAN should be different
 from the MVPN default/data MDT.
```

- テナント VRF を設定します。

```
vrf context vrfVxLAN5001
  vni 5001 <-- Associate VNI to VRF.
  rd auto
address-family ipv4 unicast
    route-target both auto
    route-target both auto mvpn
    route-target both auto evpn

interface Vlan2501 <-- SVI interface associated with the L3VNI
  no shutdown
  mtu 9216 <-- The overlay header requires 58 byes, so the max tenant traffic is
(Configured MTU - 58).
  vrf member vrfVxLAN5001
  no ip redirects
  ip forward
  ipv6 forward
  no ipv6 redirects
  ip pim sparse-mode <-- PIM is enabled.

interface Vlan2 <-- SVI interface associated with L2 VNI
  no shutdown
  vrf member vrfVxLAN5001
  no ip redirects
  ip address 100.1.1.1/16
  no ipv6 redirects
  ip pim sparse-mode <-- PIM enabled on L2VNI
 fabric forwarding mode anycast-gateway
```

ハンドオフ ノードの MVPN 設定

ハンドオフ ノードの MVPN の設定時には、次の注意事項に従ってください。

- 次の機能をイネーブル化します。

```
install feature-set mpls
allow feature-set mpls
feature-set mpls
feature mpls l3vpn
```

```
feature mvpn
feature mpls ldp
```

- MPLS LDP 設定
  - MPLS リンクであるすべてのインターフェイスで MPLS LDP（**mpls ip**）を有効にします。
  - VXLAN に使用されるループバック インターフェイスを MPLS プレフィックスとしてアドバタイズしないでください。
    - MVPN PE ノードを識別する IP アドレスを含むプレフィックス リストを設定します。

      ```
      ip prefix-list LDP-LOOPBACK seq 51 permit 9.1.1.10/32
      ip prefix-list LDP-LOOPBACK seq 52 permit 9.1.2.10/32
      ```

    - MVPN PE 識別子に対してのみラベル割り当てを設定します。

      ```
      mpls ldp configuration
        explicit-null
        advertise-labels for LDP-LOOPBACK
        label allocate global prefix-list LDP-LOOPBACK
      ```

- テナント VRF 設定：
  - デフォルトの MDT モードでは、VRF のすべてのテナント マルチキャスト トラフィックでアンダーレイ マルチキャスト グループを同じにします。

    ```
    vrf context vrfVxLAN5001
      vni 5001
      mdt default 225.1.100.1
      mdt source loopback100 <-- If the source interface is not configured, the BGP
     identifier is used as the source interface.
      mdt asm-use-shared-tree <-- If the underlay is configured in ASM mode
      no mdt enforce-bgp-mdt-safi <-- Enabled by default but should be negated if
    BGP MDT should not be used for discovery.
      mdt mtu <mtu-value> <-- Overlay ENCAP Max MTU value
    ```

  - データ MDT モードでは、テナント マルチキャスト トラフィックのサブセットまたはすべてに一意のマルチキャスト グループ セットを設定します。

    ```
    mdt data 229.1.100.2/32 immediate-switch
    mdt data 232.1.10.4/24 immediate-switch
    route-map DATA_MDT_MAP permit 10
      match ip multicast group 237.1.1.1/32
    mdt data 235.1.1.1/32 immediate-switch route-map DATA_MDT_MAP
    ```

- MVPN トンネル統計情報を有効にします。

  ```
  hardware profile mvpn-stats module all
  ```

ハンドオフノードの CoPP 設定

TRM と MVPN はどちらも、コントロール プレーンに大きく依存しています。トポロジに従って CoPP ポリシー帯域幅を設定してください。

次の CoPP クラスは、TRM および MVPN トラフィックに使用されます。

- **copp-system-p-class-multicast-router**（デフォルトの帯域幅は 3000 pps です）。
- **copp-system-p-class-l3mc-data**（デフォルトの帯域幅は 3000 pps です）。
- **copp-system-p-class-l2-default**（デフォルトの帯域幅は 50 pps です）。
- **copp-class-normal-igmp**（デフォルトの帯域幅は 6000 pps です）。

次の設定例は、マルチキャスト ルート スケールによる制御パケット ドロップを回避するように設定できる CoPP ポリシーを示しています。

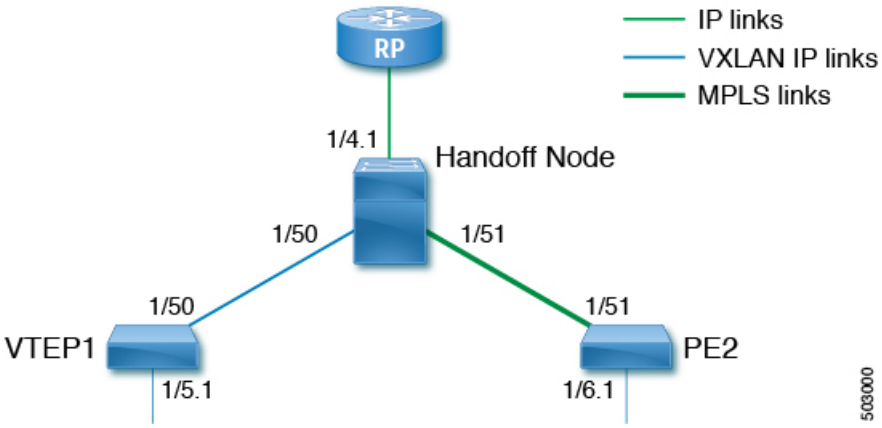
（注） この例のポリサー値は概算値であり、すべてのトポロジまたはトラフィック パターンに最適とは限りません。MVPN/TRM トラフィック パターンに従って CoPP ポリシーを設定します。

```
copp copy profile strict prefix custom
  policy-map type control-plane custom-copp-policy-strict
    class custom-copp-class-normal-igmp
      police cir 6000 pps bc 512 packets conform transmit violate drop
  control-plane
    service-policy input custom-copp-policy-strict

copp copy profile strict prefix custom
  policy-map type control-plane custom-copp-policy-strict
    class custom-copp-class-multicast-router
      police cir 6000 pps bc 512 packets conform transmit violate drop
  control-plane
    service-policy input custom-copp-policy-strict

copp copy profile strict prefix custom
  policy-map type control-plane custom-copp-policy-strict
    class copp-system-p-class-l3mc-data
      police cir 3000 pps bc 512 packets conform transmit violate drop
  control-plane
    service-policy input custom-copp-policy-strict

copp copy profile strict prefix custom
  policy-map type control-plane custom-copp-policy-strict
    class custom-copp-class-l2-default
      police cir 9000 pps bc 512 packets conform transmit violate drop
  control-plane
    service-policy input custom-copp-policy-strict
```

EVPN（TRM）と MVPN とのシームレスな統合の設定例

次の図は、左側に VXLAN ネットワーク、右側に MVPN ネットワーク、中央集中型ハンドオフノードを持つサンプル トポロジを示しています。

図 *10 : EVPN*（*TRM*）と *MVPN* のシームレスな統合のサンプル トポロジ



次に、このトポロジの VTEP、ハンドオフ ノード、および PE の設定例を示します。

VTEP1 の設定：

```
feature ngmvpn
feature interface-vlan
feature vn-segment-vlan-based
feature nv overlay
feature pim
nv overlay evpn
ip pim rp-address 90.1.1.100 group-list 225.0.0.0/8
ip pim ssm range 232.0.0.0/8

vlan 555
  vn-segment 55500

route-map ALL_ROUTES permit 10
interface nve1
  no shutdown
  host-reachability protocol bgp
  source-interface loopback2
  member vni 55500 associate-vrf
    mcast-group 225.3.3.3

interface loopack1
  ip address 196.196.196.196/32

interface loopback2
  ip address 197.197.197.197/32
  ip pim sparse-mode

feature bgp
router bgp 1
    address-family l2vpn evpn
        maximum-paths 8
        maximum-paths ibgp 8
    neighbor 2.1.1.2
        remote-as 1
        update-source loopback 1
        address-family ipv4 unicast
          send-community extended
        address-family ipv6 unicast
          send-community extended
        address-family ipv4 mvpn
```

```
          send-community extended
        address-family l2vpn evpn
          send-community extended
    vrf vrfVxLAN5023
        address-family ipv4 unicast
          advertise l2vpn evpn
          redistribute direct route-map ALL_ROUTES
          maximum-paths 8
          maximum-paths ibgp 8

vrf context vpn1
  vni 55500
  ip pim rp-address 27.27.27.27 group-list 224.0.0.0/4
  ip pim ssm range 232.0.0.0/8
  ip multicast multipath s-g-hash next-hop-based
rd auto
  address-family ipv4 unicast
    route-target both auto
    route-target both auto mvpn
    route-target both auto evpn

interface Vlan555
  no shutdown
  vrf member vpn1
  ip forward
  ip pim sparse-mode

interface Ethernet 1/50
  ip pim sparse-mode

interface Ethernet1/5.1
  encapsulation dot1q 90
  vrf member vpn1
  ip address 10.11.12.13/24
  ip pim sparse-mode
  no shutdown
```

ハンドオフ ノードの設定：

```
install feature-set mpls
  allow feature-set mpls
feature-set mpls
feature ngmvpn
feature bgp
feature pim
feature mpls l3vpn
feature mvpn
feature mpls ldp
feature interface-vlan
feature vn-segment-vlan-based
feature nv overlay
nv overlay evpn

ip pim rp-address 90.1.1.100 group-list 225.0.0.0/8
ip pim rp-address 91.1.1.100 group-list 232.0.0.0/8

interface loopback1
  ip address 90.1.1.100 /32
  ip pim sparse-mode

interface loopback2
  ip address 91.1.1.100 /32
  ip pim sparse-mode
```

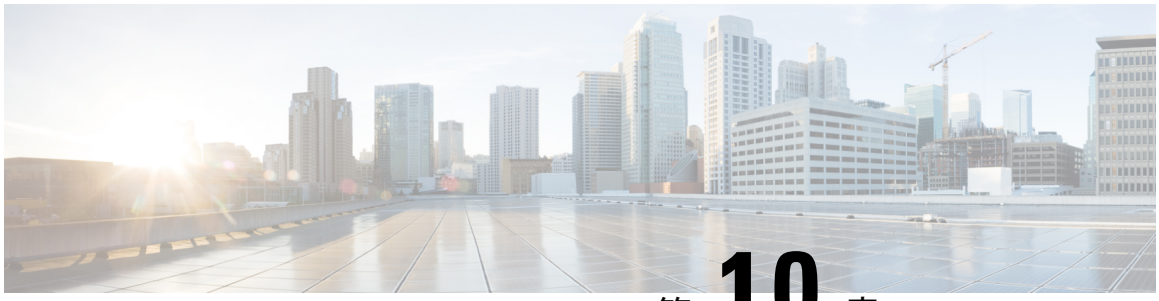
```
ip prefix-list LDP-LOOPBACK seq 2 permit 20.20.20.20/32
ip prefix-list LDP-LOOPBACK seq 3 permit 30.30.30.30/32
mpls ldp configuration
    advertise-labels for LDP-LOOPBACK
    label allocate label global prefix-list LDP-LOOPBACK

interface Ethernet 1/50
    ip pim sparse-mode

interface Ethernet 1/51
    ip pim sparse-mode
    mpls ip

interface Ethernet1/4.1
  encapsulation dot1q 50
  vrf member vpn1
  ip pim sparse-mode
  no shutdown

interface loopback0
  ip address 20.20.20.20/32
  ip pim sparse-mode

vlan 555
  vn-segment 55500

route-map ALL_ROUTES permit 10

interface nve1
  no shutdown
  host-reachability protocol bgp
  source-interface loopback3
  member vni 55500 associate-vrf
    mcast-group 225.3.3.3

interface loopback3
  ip address 198.198.198.198/32
  ip pim sparse-mode

vrf context vpn1
  vni 55500
  ip pim rp-address 27.27.27.27 group-list 224.0.0.0/4
  ip pim ssm range 232.0.0.0/8
  ip multicast multipath s-g-hash next-hop-based
  mdt default 232.1.1.1
  mdt source loopback 0
  rd auto
  address-family ipv4 unicast
    route-target both auto
    route-target both auto mvpn
    route-target both auto evpn

interface Vlan555
  no shutdown
  vrf member vpn1
  ip forward
  ip pim sparse-mode

router bgp 1
    address-family l2vpn evpn
        maximum-paths 8
        maximum-paths ibgp 8
    address-family vpnv4 unicast
        no allocate-label option-b
```

```
    address-family ipv4 mdt
    address-family ipv4 mvpn
        maximum-paths 8
        maximum-paths ibgp 8
    neighbor 196.196.196.196
        remote-as 1
        address-family ipv4 unicast
          send-community extended
        address-family ipv6 unicast
          send-community extended
        address-family ipv4 mvpn
          send-community extended
        address-family l2vpn evpn
          send-community extended
          import vpn unicast reoriginate

router bgp 1
    neighbor 30.30.30.30
        remote-as 100
        update-source loopback0
        ebgp-multihop 255
        address-family ipv4 unicast
          send-community extended
        address-family vpnv4 unicast
          send-community
          send-community extended
          next-hop-self
          import l2vpn evpn reoriginate
        address-family ipv4 mdt
          send-community extended
          no next-hop-third-party
```

PE2 の設定：

```
install feature-set mpls
  allow feature-set mpls
feature-set mpls
feature bgp
feature pim
feature mpls l3vpn
feature mpls ldp
feature interface-vlan

ip pim rp-address 91.1.1.100 group-list 232.0.0.0/8
ip prefix-list LDP-LOOPBACK seq 2 permit 20.20.20.20/32
ip prefix-list LDP-LOOPBACK seq 3 permit 30.30.30.30/32
mpls ldp configuration
    advertise-labels for LDP-LOOPBACK
    label allocate label global prefix-list LDP-LOOPBACK

interface Ethernet 1/51
    ip pim sparse-mode
    mpls ip

interface Ethernet1/6.1
  encapsulation dot1q 50
  vrf member vpn1
  ip pim sparse-mode
  no shutdown

interface loopback0
  ip address 30.30.30.30/32
  ip pim sparse-mode
```

```
vrf context vpn1
  ip pim rp-address 27.27.27.27 group-list 224.0.0.0/4
  ip pim ssm range 232.0.0.0/8
  ip multicast multipath s-g-hash next-hop-based
  mdt default 232.1.1.1
  mdt source loopback 0
  rd auto
  address-family ipv4 unicast
    route-target both auto
    route-target both auto mvpn
    route-target both auto evpn

router bgp 100
      router-id 30.30.30.30
      address-family vpnv4 unicast
            additional-paths send
            additional-paths receive
            no allocate-label option-b
      neighbor 20.20.20.20
            remote-as 1
            update-source loopback0
            address-family vpnv4 unicast
                send-community
                send-community extended
            address-family ipv4 mdt
                send-community extended
                no next-hop-third-party
```



第 10 章

vPC ファブリック ピアリングの設定

この章で説明する内容は、次のとおりです。

vPC ファブリック ピアリングの詳細

vPC ファブリック ピアリング は、vPC ピア リンクの物理ポートを無駄にすることなく、拡張デュアル ホーミング アクセス ソリューションを提供します。

vPC ファブリック ピアリング ソリューションを次に示します。

- 仮想メンバー（トンネル）を含む vPC ファブリック ピアリング ポートチャネル。
- vPC ファブリック ピアリング （トンネル）、物理ピアリンク要件の削除。
- vPC ファブリック ピアリング アップ/ダウン イベントは、ルートの更新とファブリックのアップ/ダウンに基づいてトリガーされます。
- 拡張障害カバレッジのアップリンク トラッキング。
- vPC ファブリック ピアリング ルーティングされたネットワーク（スパインなど）を介した到達可能性。
- vPC コントロール プレーン over TCP-IP（CFSoIP）の復元力の向上。
- VXLAN トンネル上のデータ プレーン トラフィック。
- vPC メンバー スイッチ間の通信では、VXLAN カプセル化が使用されます。
- ノード上のすべてのアップリンクに障害が発生すると、そのスイッチの vPC ポートがダウンします。このシナリオでは、vPC ピアがプライマリ ロールを引き受け、トラフィックを転送します。

- vPC のステート依存性とアップ/ダウンシグナリングによるアップリンク トラッキング。
- ポジティブ アップリンク ステート トラッキングにより、vPC プライマリ ロールの選択が促進されます。
- ボーダー リーフおよびスパインの場合、ネットワーク通信はファブリックを使用するため、VRF 単位のピアリングは必要ありません。
- VIP/PIP 機能をタイプ 2 ルートに拡張することにより、孤立したホストへの転送を強化します。
- インフラ VLAN は、vPC ファブリック ピアリングには必要ありません。

（注） 1 つの VTEP としてカウントされる通常の vPC とは異なり、vPC ファブリック ピアリング は 3 つの VTEP としてカウントされます。

vPC ファブリック ピアリングの注意事項と制約事項

次に、vPC ファブリック ピアリングの注意事項と制限事項を示します。

推奨構成

- vPC ファブリック ピアリングでは、リージョンの **ing-flow-redirect** の TCAM カービングが必要です。TCAM カービングでは、機能を使用する前に設定を保存し、スイッチをリロードする必要があります。

（注） この要件は、 Cisco Nexus 3600-R シリーズ プラットフォーム スイッチに適用されます。

- vPC ファブリック ピアリングを使用する場合、このような vPC ペアに対して SVI を介したルーティングを作成することはできません。
- vPC ファブリック ピアリングの送信元および宛先 IP を再設定する前に、vPC ドメインをシャットダウンする必要があります。vPC ファブリック ピアリングの送信元と宛先のIPを調整したら、vPC ドメインを有効にできます（**no shutdown**）。
- **virtual peer-link destination** コマンドでサポートされる送信元および接続先 IP は、クラス A、B、および C です。クラス D および E は、vPC ファブリック ピアリングではサポートされません。
- vPC 環境内の VLAN に不整合がある場合は、セカンダリ スイッチの vPC レッグ全体を停止するのではなく、影響を受ける（一致しない）VLAN のみが一時停止されます。

- ファブリック ピアリングから物理ピア リンクに変換した直後に、両方のピアで次の変更を行います。

  1. **hardware access-list tcam region ing-flow-redirect 0** コマンドを使用して、TCAM リージョンをグローバルに設定します。
  2. 必要に応じて、空き領域を他のクラスに割り当てます。詳細については、Nexus 9000 TCAM スペースの切り分け方法を理解するを参照してください。
  3. **copy running-config startup-config** コマンドを使用して、実行コンフィギュレーションを保存します。
  4. スイッチをリロードします。

- vPC ファブリック ピアリング ピアリンクは、トランスポート ネットワーク（ファブリックのスパイン層）を介して確立されます。vPC ピア間の通信がこのように行われると、ポート ステート情報、VLAN 情報、VLAN-to-VNI マッピング、ホスト MAC アドレスの同期に使用されるコントロール プレーン情報 CFS メッセージがファブリック経由で送信されます。CFS メッセージは、トランスポート ネットワークで保護する必要がある適切な DSCP 値でマーキングされます。次の例は、Cisco Nexus 9000 シリーズ スイッチのスパイン レイヤでの QoS 設定の例を示しています。

  DSCP 値を照合してトラフィックを分類します（DSCP 56 がデフォルト値です）。

```
class-map type qos match-all CFS
  match dscp 56
```

  適切なスパイン スイッチの完全プライオリティ キューに対応する qos-group にトラフィックを設定します。この例では、スイッチは完全プライオリティ キュー（キュー 7）に対応する qos-group 7にトラフィックを送信します。異なる Cisco Nexus プラットフォームでは、キューイング構造が異なる場合があることに注意してください。

```
policy-map type qos CFS
  class CFS
    Set qos-group 7
```

  VTEP（ネットワークのリーフ層）に向かうすべてのインターフェイスに分類サービス ポリシーを割り当てます。

```
interface Ethernet 1/1
  service-policy type qos input CFS
```

- レイヤ 3 テナント ルーテッド マルチキャスト（TRM）はサポートされていません。レイヤ 2/レイヤ 3 TRM（混合モード）はサポートされていません。
- この機能でタイプ 5 ルートを使用する場合、この **advertise-pip** コマンドは必須設定です。
- VIP/PIP 機能をタイプ 2 ルートに拡張して、孤立ホストへの転送を強化します。
- 孤立したタイプ 2 ホストは、PIP を使用してアドバタイズされます。vPC タイプ 2 ホストは、VIP を使用してアドバタイズされます。これはタイプ 2 ホストのデフォルトの動作です。

PIP を使用して孤立したタイプ 5 ルートをアドバタイズするには、BGP で PIP をアドバタイズする必要があります。

- 孤立ポートの場合、NVE 障害シナリオ中のトラフィックの中断を回避するために、両方の vPC ノードで **vpc orphan-port suspend** コマンドを設定することを強くお勧めします。
- リモート VTEP から孤立したホストへのトラフィックは、孤立した実際のノードに到達します。トラフィックのバウンスが回避されます。

（注） vPC レッグがダウンしている場合でも、vPC ホストは VIP IP でアドバタイズされます。

サポートされる機能、リリース、およびプラットフォーム

- Cisco NX-OS リリース 10.2(3)F 以降、vPC ファブリック ピアリングは Cisco Nexus C36180YC-R および N3K-C3636C-R プラットフォームでサポートされます。vPC ファブリック ピアリングを機能させるには、これらの R シリーズ モジュールで TCAM カービングを有効にする必要があります。
- 次の注意事項と制限事項は、Cisco Nexus C36180YC-R および N3K-C3636C-R プラットフォームにのみ適用されます。
  - vPC ファブリック ピアリングが有効になっている場合、入力 PACL MAC 機能はサポートされません。
  - vPC ファブリック ピアリングが有効な場合、MAC および CoS 値を使用するレイヤ 2 フィルタに基づくレイヤ 2 SPAN はサポートされません。レイヤ 2 SPAN の他のフィルタがサポートされています。
  - vPC ファブリック ピアリングを有効にすると、レイヤ 3 ホスト/隣接の 1 次元スケールが半分になります。
  - すべての vPC PO がアップしている定常状態では、コアからの BUM トラフィックが両方の vPC ピアで受信されます。すべてのフローに対して、vPC プライマリはトラフィックを vPC PO に転送します。
  - レイヤ 3 テナント ルーテッド マルチキャスト（TRM）はサポートされていません。
  - vPC PO の背後の BGP ピアリングはサポートされていません。
  - IGMP スヌーピングは vPC ファブリック ピアリングではサポートされていません
  - DHCP リレー エージェントはサポートされていません。
  - vPC ファブリック ピアリングは、ハンドオフ ノードではサポートされていません。

vPC ファブリック ピアリングの設定

サポートされない機能

- vPC ファブリック ピアリング ドメインは、マルチサイト vPC BGW のロールではサポートされません。
- IPv6 アンダーレイの vMCT は、FEX の接続をサポートしていません。
- vPC ポートの背後にある VTEP はサポートされません。これは、仮想ピアリンクピアが vPC ポートの背後にある VTEP の中継ノードとして機能できないことを意味します。
- SVI およびサブインターフェイス アップリンクはサポートされていません。

vPC ファブリック ピアリングの設定

両方の vPC メンバー スイッチで vPC ファブリック ピアリング DSCP 値が一致していることを確認します。対応する QoS ポリシーが vPC ファブリック ピアリング DSCP マーキングと一致することを確認します。

vPC ファブリック ピアリング を通過する通信を必要とするすべての VLAN は、VXLAN を有効にする必要があります（vn-segment）。これにはネイティブ VLAN が含まれます。

（注） MSTP では、ピアリンクと vPC レッグにデフォルトのネイティブ VLAN 設定がある場合、VLAN 1 は vPC ファブリック ピアリング全体に拡張する必要があります。この動作は、VLAN 1 を VXLAN（vn-segment）経由で拡張することで実現できます。ピアリンクおよび vPC レッグにデフォルト以外のネイティブ VLAN がある場合は、VLAN を VXLAN（vn-segment）に関連付けることによって、それらの VLAN を vPC ファブリック ピアリング全体に拡張する必要があります。

show vpc virtual-peerlink vlan consistency コマンドを使用して、vPC ファブリック ピアリングに使用する既存の VLAN-to-VXLAN マッピングを確認します。

vPC ファブリック ピアリング の **peer-keepalive** コマンドは、次のいずれかの設定でサポートされます。

- 管理インターフェイス
- デフォルトまたは非デフォルト VRF の専用レイヤ 3 リンク
- スパイン経由で到達可能なループバック インターフェイス。

機能の設定

例では、アンダーレイ ルーティング プロトコルとして OSPF を使用しています。

```
configure terminal
nv overlay evpn
feature ospf
feature bgp
feature pim
```

vPC ファブリック ピアリングの設定

```
feature interface-vlan
feature vn-segment-vlan-based
feature vpc

feature nv overlay
```

vPC の設定

（注） vPC ファブリック ピアリング 送信元または宛先 IP を変更するには、変更前に vPC ドメインをシャットダウンする必要があります。vPC ドメインは、**no shutdown** コマンドを使用して変更後に動作に戻すことができます。

TCAM カービングの設定

```
hardware access-list tcam region ing-racl 0
hardware access-list tcam region ing-sup 768
hardware access-list tcam region ing-flow-redirect 512
```

（注）
- ファブリック vPC ピアリングを設定する場合、Ingress-Flow-redirect TCAM リージョン サイズの最小サイズは 512 です。また、TCAM リージョン サイズが常に 512 の倍数で構成されていることを確認します。
- **ing-flow-redirect** リージョンの TCAM カービングは、 Cisco Nexus N3K-C36180YC-R および N3K-C3636C-R プラットフォーム スイッチでのみ必要です。
- TCAM カービングを有効にするには、スイッチのリロードが必要です。

vPC ドメインの設定

インターネット ユーザに商品やサービスを提供する IPv4

```
vpc domain 100
peer-keepalive destination 192.0.2.1
virtual peer-link destination 192.0.2.100 source 192.0.2.20/32 [dscp <dscp-value>]
Warning: Appropriate TCAM carving must be configured for virtual peer-link vPC
peer-switch
peer-gateway
ip arp synchronize
ipv6 nd synchronize
exit
```

IPv6 の場合

```
vpc domain 100
peer-keepalive destination 192:0:2::1
virtual peer-link destination 192:0:2::100 source 192:0:2::20/32 [dscp <dscp-value>]
Warning: Appropriate TCAM carving must be configured for virtual peer-link vPC
peer-switch
peer-gateway
ipv6 arp synchronize
ipv6 nd synchronize
exit
```

（注） オプションの **dscp** キーワード。範囲は 1 ～ 63 です。デフォルト値は 56 です。

vPC ファブリック ピアリング ポート チャネルの設定

次のポート チャネルのメンバーを設定する必要はありません。

```
interface port-channel 10
switchport
switchport mode trunk
vpc peer-link
```

interface loopback0

（注） このループバックは、NVE 送信元インターフェイス ループバック（VTEP IP アドレスに使用されるインターフェイス）ではありません。

インターネット ユーザに商品やサービスを提供する IPv4

```
interface loopback 0
ip address 192.0.2.20/32
ip router ospf 1 area 0.0.0.0
```

IPv6 の場合

```
interface loopback 0
ipv6 address 192:0:2::20/32
ipv6 router ospfv3 1 area 0.0.0.0
```

（注） BGP ピアリングまたは専用ループバックにループバックを使用できます。このルックバックは、ピアのキープ アライブとは異なる必要があります。

アンダーレイ インターフェイスの設定

L3 物理チャネルと L3 ポート チャネルの両方がサポートされます。SVI およびサブインターフェイスはサポートされていません。

インターネット ユーザに商品やサービスを提供する IPv4

```
router ospf 1
interface Ethernet1/16
port-type fabric
ip address 192.0.2.2/24
ip router ospf 1 area 0.0.0.0
no shutdown
interface Ethernet1/17
port-type fabric
ip address 192.0.2.3/24
ip router ospf 1 area 0.0.0.0
no shutdown
interface Ethernet1/40
port-type fabric
ip address 192.0.2.4/24
```

vPC ファブリック ピアリングの設定

```
ip router ospf 1 area 0.0.0.0
no shutdown
interface Ethernet1/41
port-type fabric
ip address 192.0.2.5/24
ip router ospf 1 area 0.0.0.0
no shutdown
```

IPv6 の場合

```
router ospfv3 1
interface Ethernet1/16
port-type fabric
ipv6 address 192:0:2::2/24
ipv6 router ospfv3 1 area 0.0.0.0
no shutdown
interface Ethernet1/17
port-type fabric
ipv6 address 192:0:2::3/24
ipv6 router ospfv3 1 area 0.0.0.0
no shutdown
interface Ethernet1/40
port-type fabric
ipv6 address 192:0:2::4/24
ipv6 router ospfv3 1 area 0.0.0.0
no shutdown
interface Ethernet1/41
port-type fabric
ipv6 address 192:0:2::5/24
ipv6 router ospfv3 1 area 0.0.0.0
no shutdown
```

（注） スパインに接続されるすべてのポートは、ポートタイプのファブリックである必要があります。

VXLAN 設定

（注） **advertise virtual-rmac**（NVE）と **advertise-pip**（BGP）の設定は必須の手順です。

SVI および VLAN の設定

```
vlan 10
vn-segment 10010
vlan 101
vn-segment 10101

interface Vlan101
no shutdown
mtu 9216
vrf member vxlan-10101
no ip redirects
ip forward
ipv6 address use-link-local-only
no ipv6 redirects
interface vlan10
no shutdown
```

```
mtu 9216
vrf member vxlan-10101
no ip redirects
ip address 192.0.2.102/24
ipv6 address 2001:DB8:0:1::1/64
no ipv6 redirects
fabric forwarding mode anycast-gateway
```

仮想ポート チャネルの設定

```
interface Ethernet1/3
switchport
switchport mode trunk
channel-group 100
no shutdown
exit
interface Ethernet1/39
switchport
switchport mode trunk
channel-group 101
no shutdown
interface Ethernet1/46
switchport
switchport mode trunk
channel-group 102
no shutdown
interface port-channel100
vpc 100
interface port-channel101
vpc 101
interface port-channel102
vpc 102
exit
```

vPCから vPC ファブリック ピアリング への移行

この手順には、通常の vPC から vPC ファブリック ピアリング への移行手順が含まれています。

vPC ピア間の直接レイヤ 3 リンクは、ピアキープアライブにのみ使用する必要があります。このリンクは、vPC ファブリック ピアリング ループバックのパスをアドバタイズするために使用しないでください。

（注） この移行は中断を伴います。

始める前に

移行前に、vPC ピア間のすべての物理レイヤ 2 リンクをシャットダウンすることを推奨します。また、移行前または移行後に VLAN を vn-segment にマッピングすることを推奨します。

手順の概要

1. **configure terminal**

2. **show vpc**
3. **show port-channel summary**
4. **interface ethernet** *slot/port*
5. **no channel-group**
6. インターフェイスごとにステップ 4 と 5 を繰り返します。
7. **show running-config vpc**
8. **vpc domain** *domain-id*
9. **virtual peer-link destination** *dest-ip* **source** *source-ip*
10. **interface {ethernet | port-channel}** *value*
11. **port-type fabric**
12. （任意） **show vpc fabric-ports**
13. **virtual peer-link destination** *dest-ip* | *dest_ipv6* **source** *source-ip* | *source_ipv6* **dhcp** *dhcp_val*
14. **hardware access-list tcam region ing-flow-redirect** *tcam-size*
15. **copy running-config startup-config**
16. **reload**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**show vpc** 例： `switch(config)# show vpc`	ポート チャネルのメンバー数を決定します。
ステップ 3	**show port-channel summary** 例： `switch(config)# show port-channel summary`	メンバーの数を決定します。
ステップ 4	**interface ethernet** *slot/port* 例： `switch(config)# interface ethernet 1/4`	設定するインターフェイスを指定します。 （注） これは、ピアリンク ポート チャネルです。
ステップ 5	**no channel-group** 例： `switch(config-if)# no channel-group`	vPC ピアリンク ポート チャネル メンバーを削除します。 （注） このステップの後に中断が発生します。

	コマンドまたはアクション	目的
ステップ 6	インターフェイスごとにステップ 4 と 5 を繰り返します。 例： 	
ステップ 7	**show running-config vpc** 例： `switch(config-if)# show running-config vpc`	vPC ドメインを決定します。
ステップ 8	**vpc domain** *domain-id* 例： `switch(config-if)# vpc domain 100`	vPC ドメイン コンフィギュレーション モードを入力します。
ステップ 9	**virtual peer-link destination** *dest-ip* **source** *source-ip* 例： `switch(config-vpc-domain)# virtual peer-link destination 192.0.2.1 source 192.0.2.100`	vPC ファブリック ピアリングの宛先および送信元 IP アドレスを指定します。
ステップ 10	**interface {ethernet | port-channel}** *value* 例： `switch(config-if)# interface Ethernet1/17`	構成する L3 アンダーレイ インターフェイスを指定します。
ステップ 11	**port-type fabric** 例： `switch(config-if)# port-type fabric`	アンダーレイ インターフェイスのポート タイプ ファブリックを設定します。 （注） スパインに接続されるすべてのポートは、ポート タイプのファブリックである必要があります。
ステップ 12	（任意） **show vpc fabric-ports** 例： `switch# show vpc fabric-ports`	スパインに接続されているファブリック ポートを表示します。
ステップ 13	**virtual peer-link destination** *dest-ip* | *dest_ipv6* **source** *source-ip* | *source_ipv6* **dhcp** *dhcp_val* 例： インターネット ユーザに商品やサービスを提供する IPv4 `switch(config-vpc-domain)# virtual peer-link destination 192.0.2.1 source 192.0.2.100 dhcp 56` 例： IPv6 の場合	vPC ファブリック ピアリングの宛先および送信元 IPv4/IPv6 アドレスを指定します。 （注） IPv4 vPC ファブリック ピアリング構成は IPv4 VXLAN アンダーレイでのみ機能し、IPv6 vPC ファブリック ピアリング構成は IPv6 VXLAN アンダーレイでのみ機能します。

	コマンドまたはアクション	目的
	`switch(config-vpc-domain)# virtual peer-link destination 6001:aaa::11 source 6001:aaa::22 dhcp 56`	
ステップ 14	**hardware access-list tcam region ing-flow-redirect** *tcam-size* 例： `switch(config-vpc-domain)# hardware access-list tcam region ing-flow-redirect 512`	TCAM カービングを実行します。 入力フローリダイレクト TCAM リージョン サイズの最小サイズは 512 です。また、512 の倍数で構成されていることを確認します。
ステップ 15	**copy running-config startup-config** 例： `switch(config-vpc-domain)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。
ステップ 16	**reload** 例： `switch(config-vpc-domain)# reload`	スイッチをリブートします。

vPC ファブリック ピアリング 設定の確認

vPC ファブリック ピアリング設定のステータスを表示するには、次のコマンドを入力します。

表 *3: vPC* ファブリック ピアリング 検証コマンド

コマンド	目的
show vpc fabric-ports	ファブリック ポートの状態を表示します。
show vpc	vPC ファブリック ピアリング モードに関する情報を表示します。
show vpc virtual-peerlink vlan consistency	vn-segment に関連付けられていない VLAN を表示します。

show vpc fabric-ports コマンドの例

```
switch# show vpc fabric-ports
Number of Fabric port : 9
Number of Fabric port active : 9

Fabric Ports State
-------------------------------------
Ethernet1/9 UP
Ethernet1/19/1 ( port-channel151 ) UP
Ethernet1/19/2 ( port-channel151 ) UP
Ethernet1/19/3 UP
Ethernet1/19/4 UP
```

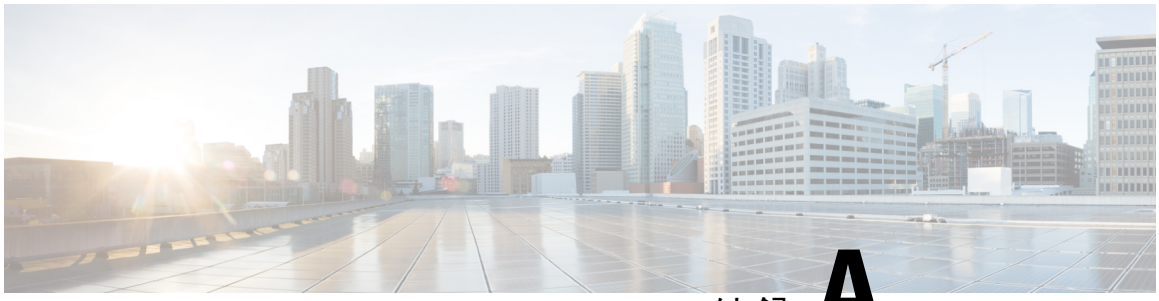
```
Ethernet1/20/1 UP
Ethernet1/20/2 ( port-channel152 ) UP
Ethernet1/20/3 ( port-channel152 ) UP
Ethernet1/20/4 ( port-channel152 ) UP
```

show vpc コマンドの例

```
switch# show vpc
Legend:
                (*) - local vPC is down, forwarding via vPC peer-link

vPC domain id                     : 3
Peer status                       : peer adjacency formed ok
vPC keep-alive status             : peer is alive
Configuration consistency status  : success
Per-vlan consistency status       : success
Type-2 consistency status         : success
vPC role                          : primary
Number of vPCs configured         : 1
Peer Gateway                      : Enabled
Dual-active excluded VLANs        : -
Graceful Consistency Check        : Enabled
Auto-recovery status              : Enabled, timer is off.(timeout = 240s)
Delay-restore status              : Timer is off.(timeout = 30s)
Delay-restore SVI status          : Timer is off.(timeout = 10s)
Operational Layer3 Peer-router    : Disabled
Virtual-peerlink mode             : Enabled

vPC Peer-link status
---------------------------------------------------------------------
id    Port   Status Active vlans
--    ----   ------ --------------------------------------------------
1     Po100  up     1,56,98-600,1001-3401,3500-3525

vPC status
----------------------------------------------------------------------------
Id    Port          Status Consistency Reason                Active vlans
--    ------------  ------ ----------- ------                ---------------
101   Po101         up     success     success               98-99,1001-280
                                                           0

Please check "show vpc consistency-parameters vpc <vpc-num>" for the
consistency reason of down vpc and for type-2 consistency reasons for
any vpc.

ToR_B1#
```

show vpc virtual-peerlink vlan 整合性コマンドの例

```
switch# show vpc virtual-peerlink vlan consistency
Following vlans are inconsistent
23
switch#
```



付録 A

VXLAN BGP EVPN 中の DHCP リレー

この付録の構成は、次のとおりです。

VXLAN BGP EVPN 中の DHCP リレーの概要

DHCP リレーは VXLAN BGP EVPN によってサポートされており、EVPN テナント クライアントに DHCP サービスをプロビジョニングするためのマルチテナント VXLAN EVPN デプロイメントで役立ちます。

マルチテナント EVPN 環境で DHCP リレーは、オプション 82 の次のサブオプションを使用します。

- サブオプション 151（0x97）：仮想サブネットの選択

  （RFC#6607 内に定義されています。)

  MPLS-VPN および VXLAN EVPN マルチテナント環境中の DHCP サーバへの VRF 関連情報の伝達に使用されます。

- サブオプション 11（0xb）：サーバー IDに のオーバーライド

  （RFC#5107 内に定義されています。)

  サーバ識別子（サーバ ID）のオーバーライド サブオプションは、DHCP リレー エージェントによるサーバ ID オプションへの新しい値の指定を可能にし、これは DHCP サーバにより応答パケットに挿入されます。このサブオプションによって DHCP リレー エージェントは実際の DHCP サーバとして機能するようになり、たとえば renew 要求は DHCP サーバではなくリレー エージェントに直接届くようになります。サーバ ID オーバーライド サブオプションには着信インターフェイスの IP アドレスが含まれており、これはクライアントからアクセス可能なリレー エージェント上の IP アドレスです。この情報を使用して、DHCP クライアントは renew および release 要求パケットをすべてリレー エージェントへ

送ります。リレー エージェントは適切なサブオプションをすべて付加した後、renew および release 要求パケットをオリジナルの DHCP サーバに転送します。この機能におけるシスコ独自の実装は、サブオプション 152（0x98）です。機能の制御には、**ip dhcp relay sub-option type cisco** コマンドを使用できます。

- サブオプション 5（0x5）：リンクの選択

  （RFC#3527 内に定義されています。）

  リンクの選択サブオプションが提供するのは、DHCP クライアントが存在するサブネット/リンクを、リレー エージェントとの通信に DHCP サーバが使用するゲートウェイ アドレス（giaddr）から分離するための機構です。リレー エージェントは正しいサブスクライバ サブネットにサブオプションを設定し、DHCP サーバはこの値を使用して giaddr 値ではなく IP アドレスを割り当てます。リレー エージェントは、giaddr を自身の IP アドレスに設定することで、DHCP メッセージがネットワーク上を転送できるようにします。この機能におけるシスコ独自の実装は、サブオプション 150（0x96）です。機能の制御には、**ip dhcp relay sub-option type cisco** コマンドを使用できます。

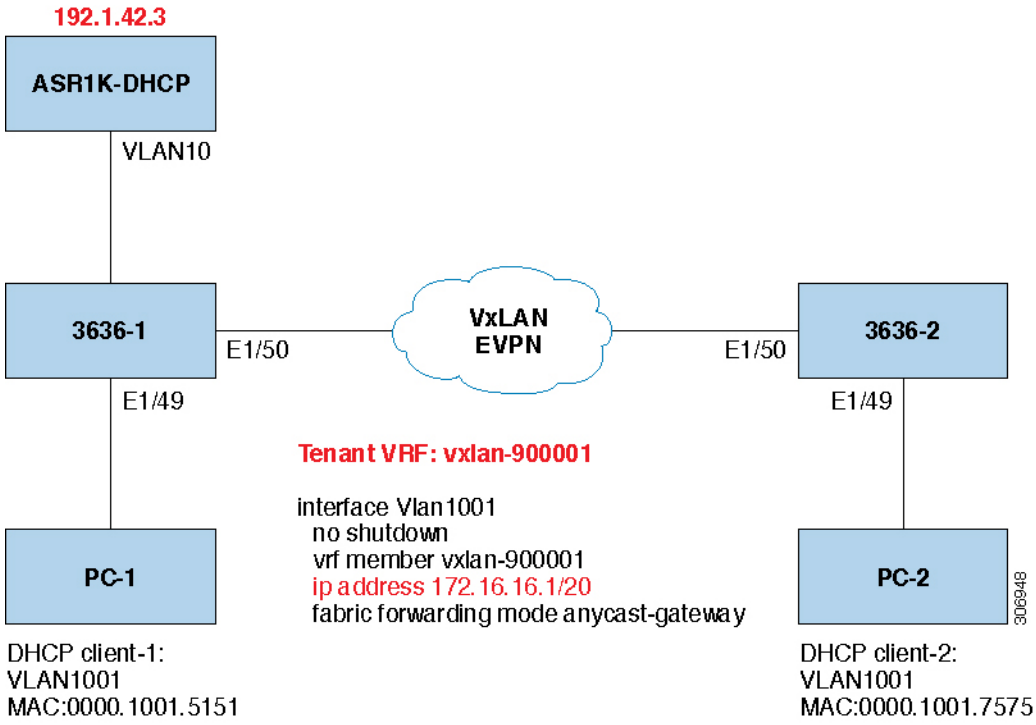
DHCP リレーの注意事項と制約事項

次には、VXLAN BGP EVPN 内の DHCP リレーのガイドラインと制限事項があります：

- Cisco NX-OSリリース 9.2（2）以降、 Cisco Nexus 3636C-R および 36180YC-R のサポートが追加されています。
- BFD マルチホップは、Cisco Nexus 36180YC-R および 3636C-R スイッチでのみサポートされます。

VXLAN BGP EVPN 中の DHCP リレーの例

図 *11* : トポロジの例



トポロジの特性：

- スイッチ 3636-1 と 3636-2 は、VXLAN ファブリックに接続された VTEP です。
- client1 と client2 は、vlan1001 中の DHCP クライアントです。これらはテナント VRF vxlan-900001 に属します。
- DHCP サーバは ASR1K であり、これは vlan10 に存在するルータです。
- DHCP サーバ設定

```
ip vrf vxlan900001
ip dhcp excluded-address vrf vxlan900001 172.16.16.1 172.16.16.9
ip dhcp pool one
 vrf vxlan900001
 network 172.16.16.0 255.255.240.0
 defaultrouter 172.16.16.1
```

基本 VXLAN BGP EVPN 構成

- 3636-1

VXLAN BGP EVPN 中の DHCP リレー

```
version 7.0(3)I1(3)
version 9.2(1)
hostname 3636C-R

nv overlay evpn
feature vn—segment—vlan—based
feature nv overlay

fabric forwarding anycast—gateway—mac 0000.1111.2222

vlan 101
  vn—segment 900001
vlan 1001
  vn—segment 2001001

vrf context vxlan—900001
  vni 900001
  rd auto
  address—family ipv4 unicast
    route—target both auto
    route—target both auto evpn

interface VlanlOl
  no shutdown
  vrf member vxlan—900001
  ip forward

interface VlanlOOl
  no shutdown
  vrf member vxlan—900001
  ip address 172.16.16.1/20
  fabric forwarding mode anycast—gateway
```

（注） NVEインターフェイスを作成するには、次の2つの手順のいずれかを選択できます。VNIの数が少ない場合は、最初のオプションを使用します。多数のVNIを構成するには、2番目のオプションを使用します。

オプション1

```
interface nve1
  no shutdown
  source-interface loopback1
  host-reachability protocol bgp
  member vni 10000 associate-vrf
  mcast-group 224.1.1.1
  member vni 10001 associate-vrf
  mcast-group 224.1.1.1
  member vni20000
  suppress-arp
  mcast-group 225.1.1.1
  member vni 20001
  suppress-arp
  mcast-group 225.1.1.1
```

VXLAN BGP EVPN 中の DHCP リレー

オプション 2

```
interface nve1
  no shutdown
  source-interface loopback 1
  host-reachibility protocol bgp
  global suppress-arp
  global mcast-group 224.1.1.1 L3
  global mcast-group 255.1.1.1 L2
  member vni 10000 associate-vrf
  member vni 10001 associate-vrf
  member vni 10002 associate-vrf
  member vni 10003 associate-vrf
  member vni 10004 associate-vrf
  member vni 10005 associate-vrf
  member vni 20000
  member vni 20001
  member vni 20002
  member vni 20003
  member vni 20004
  member vni 20005



interfaca Ethernetl/49
  switchport mode trunk
  switchport trunk allowed vlan 10,1001
  spanning—tree port type edge trunk

interface Ethernetl/50
  no switchport
  ip address 192.1.33.2/24
  ip router ospf 1 area 0.0.0.0
  ip pire sparse-mode
  no shutdown

interface loopback0
  ip address 1.1.1.1/32
  ip router ospf 1 area 0.0.0.0
  ip pim sparse—mode

interface loopbackl
  vrf member vxlan—900001
  ip address 11.11.11.11/32

router bgp 65535
  router—id 1.1.1.1
  log—neighbor-changes
  neighbor 2.2.2.2 remote—as 65535
    update—source loopback0
    address-family l2vpn evpn
      send-community both
  vrf vxlen—900001
    address—family ipv4 unicast
    network 11.11.11.11/32
    network 192.1.42.0/24
    advertise l2vpn evpn
evpn
  vni 2001001 12
```

VXLAN BGP EVPN 中の DHCP リレー

（注） **rd auto** および **route-target** コマンドは、**import** または **export** オプションを上書きするために使用しない限り、自動的に構成されます。

```
rd auto
    route-target import auto
    route-target export auto
```

- 3636-2

```
version 7.0(3)I1(3)
version 9.2(1)
hostname 3636-1

nv overlay evpn
feature vn-segment-vlan-based
feature nv overlay

fabric forwarding anycast-gateway-mac 0000.1111.2222

vlan 101
  vn-segment 900001
vlan 1001
  vn-segment 2001001

vrf context vxlan-900001
  vni 900001
  rd auto
  address-family ipv4 unicast
    route-target both auto
    route-target both auto evpn

interface Vlan101
no shutdown
vrf member vxlan-900001
ip forward

interface Vlan1001
  no shutdown
  vrf member vxlan-900001
  ip address 172.16.16.1/20
  fabric forwarding mode anycast-gateway
```

（注） **rd** および **route-target** コマンドは、**import** または **export** オプションを上書きするために入力しない限り、自動的に設定されます。

```
rd auto
  address-family ipv4 unicast
    route-target both auto
    route-target both auto evpn
```

VXLAN BGP EVPN 中の DHCP リレー

```
interface VianlOl
no shutdown
vrf member vxlan-900001
ip forward

interface Vlanl00l
  no shutdown
  vrf member vxlan—900001
  ip address 172.16.16.1/20
  fabric forwarding mcde anycast—gateway
```

（注） NVEインターフェイスを作成するには、次の2つの手順のいずれかを選択できます。VNIの数が少ない場合は、最初のオプションを使用します。多数のVNIを構成するには、2番目のオプションを使用します。

オプション1

```
interface nve1
  no shutdown
  source-interface loopback1
  host-reachability protocol bgp
  member vni 10000 associate-vrf
  mcast-group 224.1.1.1
  member vni 10001 associate-vrf
  mcast-group 224.1.1.1
  member vni20000
  suppress-arp
  mcast-group 225.1.1.1
  member vni 20001
  suppress-arp
  mcast-group 225.1.1.1
```

オプション2

```
interface nve1
  no shutdown
  source-interface loopback 1
  host-reachibility protocol bgp
  global suppress-arp
  global mcast-group 224.1.1.1 L3
  global mcast-group 255.1.1.1 L2
  member vni 10000 associate-vrf
  member vni 10001 associate-vrf
  member vni 10002 associate-vrf
  member vni 10003 associate-vrf
  member vni 10004 associate-vrf
  member vni 10005 associate-vrf
  member vni 20000
  member vni 20001
  member vni 20002
  member vni 20003
  member vni 20004
  member vni 20005


interface Ethernetl/49
```

```
  switchport mode trunk
  switchport trunk alluwed vlan 10,1001
  spanning—tree port type edge trunk

interface Ethernetl/50
  no switchport
  ip address 192.1.34.2/24
  ip router ospf 1 area 0.0.0.0
  ip pim sparse-mode
  no shutdown

interface loopback0
  ip address 2.2.2.2/32
  ip router ospf 1 area 0.0.0.0
  ip pim sparse—mode

interface loopbackl
  vrf member vxlan—900001
  ip address 22.22.22.22/32

router bgp 65535
  router—id 2.2.2.2
  log—neighbor-changes
  neighbor 1.1.1.1 remote—as 65535
    update—source loopback0
    address-family l2vpn evpn
      send-community both
  vrf vxlen—900001
    address—family ipv4 unicast
    network 22.22.22.22/32

    advertise l2vpn evpn
evpn
  vni 2001001 12
```

（注） **rd** および **route-target** コマンドは、**import** または **export** オプションを上書きするために入力しない限り、自動的に設定されます。

```
rd auto
    route—target import auto
    route—target export auto
```

VTEP の DHCP リレー

次に示したのは、一般的な展開シナリオです。

- テナント VRF にあるクライアントと異なるレイヤ 3 デフォルト VRF にあるサーバ。
- テナント VRF（SVI X）にあるクライアントと同じテナント VRF（SVI Y）にあるサーバ。
- テナント VRF（VRF X）にあるクライアントと異なるテナント VRF（VRF Y）にあるサーバ。

• テナント VRF にあるクライアントと非デフォルトの非 VXLAN VRF にあるサーバ。

次に示すのは、これとは異なるシナリオとして、vlan10 を別の VRF に移動させたものです。

テナント VRF にあるクライアントと異なるレイヤ 3 デフォルト VRF にあるサーバ

DHCP サーバー（192.1.42.3）をデフォルト VRF に設置して、3636-1 と 3636-2 の両方からデフォルト VRF を介してそこに到達可能であることを確認します。

```
3636-1# sh run int vl 10

!Command: show running-config interface Vlan10
!Time: Mon Aug 7 07:51:16 2018

version 9.2(1)

interface Vlan10
  no shutdown
  ip address 192.1.42.1/24
  ip router ospf 1 area 0.0.0.0

3636-1# ping 192.1.42.3 cou 1

PING 192.1.42.3 (192.1.42.3): 56 data bytes
64 bytes from 192.1.42.3: icmp_seq=0 ttl=254 time=0.593 ms
- 192.1.42.3 ping statistics -
1 packets transmitted, 1 packets received, 0.00% packet loss
roundtrip min/avg/max = 0.593/0.592/0.593 ms

3636-2# ping 192.1.42.3 cou 1
PING 192.1.42.3 (192.1.42.3): 56 data bytes
64 bytes from 192.1.42.3: icmp_seq=0 ttl=252 time=0.609 ms
- 192.1.42.3 ping statistics -
1 packets transmitted, 1 packets received, 0.00% packet loss
round-trip min/avg/max = 0.609/0.608/0.609 ms
```

DHCP リレー設定

• 3636-1

```
3636-1# sh run dhcp

!Command: show running-config dhcp
!Time: Mon Aug 6 08:26:00 2018

version 9.2(1)
feature dhcp

service dhcp
ip dhcp relay
ip dhcp relay information option
ip dhcp relay information option vpn
ipv6 dhcp relay

interface Vlan1001
  ip dhcp relay address 192.1.42.3 use-vrf default
```

VXLAN BGP EVPN 中の DHCP リレー

- 3636-2

```
3636-2# sh run dhcp

!Command: show running—config dhcp
!Time: Mon Aug 6 08:26:16 2018

version 9.2(1)
feature dhcp

service dhcp
ip dhcp relay
ip dhcp relay information option
ip dhcp relay information option vpn
ipv6 dhcp relay

interfaoe Vlanl001
  ip dhcp relay address 192.1.42.3 use—vrf default
```

debug コマンドの出力例

- 次に示すのは、DHCP のインタラクティブ シーケンスのパケット ダンプです。

```
3636-1# ethanalyzer local interface inband display-filter
"udp.srcport==67 or udp.dstport==67" limit-captured frames 0

Capturing on inband
20150824 08:35:25.066530 0.0.0.0 -> 255.255.255.255 DHCP DHCP Discover - Transaction
 ID 0x636a38fd
20150824 08:35:25.068141 192.1.42.1 -> 192.1.42.3 DHCP DHCP Discover - Transaction
ID 0x636a38fd
20150824 08:35:27.069494 192.1.42.3 -> 192.1.42.1 DHCP DHCP Offer Transaction - ID
0x636a38fd
20150824 08:35:27.071029 172.16.16.1 -> 172.16.16.11 DHCP DHCP Offer Transaction -
ID 0x636a38fd
20150824 08:35:27.071488 0.0.0.0 -> 255.255.255.255 DHCP DHCP Request Transaction -
 ID 0x636a38fd
20150824 08:35:27.072447 192.1.42.1 -> 192.1.42.3 DHCP DHCP Request Transaction -
ID 0x636a38fd
20150824 08:35:27.073008 192.1.42.3 -> 192.1.42.1 DHCP DHCP ACK Transaction - ID
0x636a38fd
20150824 08:35:27.073692 172.16.16.1 -> 172.16.16.11 DHCP DHCP ACK Transaction - ID
 0x636a38fd
```

（注） Ethanalyzer はすべての DHCP パケットをキャプチャできない可能性がありますが、これは、フィルタ使用時のインバンドの解釈に問題があるためです。これは SPAN を使用することで回避できます。

- DHCP Discover パケット 3636-1 は DHCP サーバーに送信されています。

VXLAN BGP EVPN 中の DHCP リレー

giaddr は 192.1.42.1（vlan10 の IP アドレス）に設定され、それに応じてサブオプション 5/11/151 を設定します。

```
Bootp flags: 0x0000 (unicast)
client IP address: 0.0.0.0 (0.0.0.0)
Your (client) IP address: 0.0.0.0 (0.0.0.0)
Next server IP address: 0.0.0.0 (0.0.0.0)
Relay agent IP address: 192.1.42.1 (192.1.42.1)
client MAC address Hughes_01:51:51 (00:00:10:01:51:51)
client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
Option: (53) DHCP Message Type
  Length: 1
  DHCP: Discover (1)
Option: (55) Parameter Request List
  Length: 4
  Parameter Request List Item: (1) Subnet Mask
  Parameter Request List Item: (3) Router
  Parameter Request List Item: (58) Renewal Time Value
  Parameter Request List Item: (59) Rebinding Time Value
Option: (61) client identifier
  Length: 7
  Hardware type: Ethernet (0x01)
  Client MAC address: Hughes_01:51:51 (00:00:10:01:51:51)
Option: (82) Agent Information Option
  Length: 47
Option 82 Suboption: (1) Agent Circuit ID
  Length: 10
  Agent Circuit ID: 01080006001e88690030
Option 82 Suboption: (2) Agent Remote ID
  Length: 6
  Agent Remote ID: f8c2882333a5
Option 82 Suboption: (151) VRF name/VPN ID
Option 82 Suboption: (11) Server ID Override
  Length: 4
  Server ID Override: 172.16.16.1 (172.16.16.1)
Option 82 Suboption: (5) Link selection
  Length: 4
  Link selection: 172.16.16.0 (172.16.16.0)
```

```
ASR1K-DHCP# sh ip dhcp bin
Bindings from all pools not associated with VRF:
IP address ClientID/ Lease expiration Type State Interface
         Hardware address/
         User name

Bindings from VRF pool vxlan900001:
IP address ClientID/ Lease expiration Type State Interface
         Hardware address/
         User name
172.16.16.10 0100.0010.0175.75 Aug 25 2015 09:21 AM Automatic Active
GigabitEthernet2/1/0
172.16.16.11 0100.0010.0151.51 Aug 25 2015 08:54 AM Automatic Active
GigabitEthernet2/1/0

3636-1# sh ip route vrf vxlan900001
IP Route Table for VRF "vxlan900001"
```

```
'*' denotes best ucast nexthop
'**' denotes best mcast nexthop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

11.11.11.11/32, ubest/mbest: 2/0, attached
  *via 11.11.11.11, Lo1, [0/0], 18:31:57, local
  *via 11.11.11.11, Lo1, [0/0], 18:31:57, direct
22.22.22.22/32, ubest/mbest: 1/0
  *via 2.2.2.2%default, [200/0], 18:31:57, bgp65535,internal, tag 65535 (evpn)segid:
 900001 tunnelid: 0x2020202
encap: VXLAN

172.16.16.0/20, ubest/mbest: 1/0, attached
 *via 172.16.16.1, Vlan1001, [0/0], 18:31:57, direct
172.16.16.1/32, ubest/mbest: 1/0, attached
 *via 172.16.16.1, Vlan1001, [0/0], 18:31:57, local
172.16.16.10/32, ubest/mbest: 1/0
 *via 2.2.2.2%default, [200/0], 00:00:47, bgp65535,internal, tag 65535 (evpn)segid:
 900001 tunnelid: 0x2020202
encap: VXLAN

172.16.16.11/32, ubest/mbest: 1/0, attached
 *via 172.16.16.11, Vlan1001, [190/0], 00:28:10, hmm

3636-1# ping 172.16.16.11 vrf vxlan900001 count 1
PING 172.16.16.11 (172.16.16.11): 56 data bytes
64 bytes from 172.16.16.11: icmp_seq=0 ttl=63 time=0.846 ms
- 172.16.16.11 ping statistics -
1 packets transmitted, 1 packets received, 0.00% packet loss
round-trip min/avg/max = 0.846/0.845/0.846 ms

3636-1# ping 172.16.16.10 vrf vxlan900001 count 1
PING 172.16.16.10 (172.16.16.10): 56 data bytes
64 bytes from 172.16.16.10: icmp_seq=0 ttl=62 time=0.874 ms
- 172.16.16.10 ping statistics -
1 packets transmitted, 1 packets received, 0.00% packet loss
round-trip min/avg/max = 0.874/0.873/0.874 ms
```

テナント VRF（SVI X）にあるクライアントと同じテナント VRF（SVI Y）にあるサーバ

DHCP サーバー（192.1.42.3）を vxlan-900001 の VRF に設置して、3636-1 と 3636-2 の両方から vxlan-900001 の VRF を介してそこに到達可能であることを確認します。

```
3636-1# sh run int vl 10

!Command: show running-config interface Vlan10
!Time: Mon Aug 6 09:10:26 2018

version 9.2(1)

interface Vlan10
  no shutdown
  vrf member vxlan-900001
  ip address 192.1.42.1/24
```

172.16.16.1 はすべての VTEP に設定された vlan1001 のエニーキャスト アドレスであるため、DHCP サーバからの応答をオリジナルの DHCP リレー エージェントへ確実に配送させるため

VXLAN BGP EVPN 中の DHCP リレー

には、DHCP リレー パケットの送信元アドレスとして一意のアドレスをピック アップする必要があります。このシナリオでは、loopback1 を使用しており、loopback1 には VRF vxlan-900001 のどこからでも到達可能であることを確認する必要があります。

```
3636-1# sh run int lo1

!Command: show running-config interface loopback1
!Time: Mon Aug 6 09:18:53 2018

version 9.2(1)

interface loopback1
  vrf member vxlan-900001
  ip address 11.11.11.11/32

3636-1# ping 192.1.42.3 vrf vxlan900001 source 11.11.11.11 cou 1
PING 192.1.42.3 (192.1.42.3) from 11.11.11.11: 56 data bytes
64 bytes from 192.1.42.3: icmp_seq=0 ttl=254 time=0.575 ms
- 192.1.42.3 ping statistics -
1 packets transmitted, 1 packets received, 0.00% packet loss
round-trip min/avg/max = 0.575/0.574/0.575 ms

3636-2# sh run int lo1

!Command: show running-config interface loopback1
!Time: Mon Aug 6 09:19:30 2018

version 9.2(1)

interface loopback1
  vrf member vxlan900001
  ip address 22.22.22.22/32

3636-2# ping 192.1.42.3 vrf vxlan-900001 source 22.22.22.22 cou 1
PING 192.1.42.3 (192.1.42.3) from 22.22.22.22: 56 data bytes
64 bytes from 192.1.42.3: icmp_seq=0 ttl=253 time=0.662 ms
- 192.1.42.3 ping statistics -
1 packets transmitted, 1 packets received, 0.00% packet loss
round-trip min/avg/max = 0.662/0.662/0.662 ms
```

DHCP リレー設定

- 3636-1

```
3636—1# sh run dhcp

!Command: show running-config dhcp
!Time: Mon Aug 6 08:26:00 2018

version 9.2(1)
feature dhcp

service dhcp
ip dhcp relay
ip dhcp relay information option
I4ip dhcp relay information option vpn
ipv6 dhcp relay

interface Vlanl001
```

VXLAN BGP EVPN 中の DHCP リレー

```
  ip dhcp relay address 192.1.42.3
  ip dhcp relay source—interface loopback1
```

- 3636-2

```
3636—2# sh run dhcp

!Command: show running-config dhcp
!Time: Mon Aug 6 08:26:16 2018

version 9.2(1)
feature dhcp

service dhcp
ip dhcp relay
ip dhcp relay information option
ip dhcp relay information option vpn
ipv6 dhcp relay

interface Vlan1001
  ip dhcp relay address 192.1.42.3
  ip dhcp relay source—interface loopback1
```

debug コマンドの出力例

- 次に示すのは、DHCP のインタラクティブ シーケンスのパケット ダンプです。

```
3636-1# ethanalyzer local interface inband display-filter
"udp.srcport==67 or udp.dstport==67" limit-captured frames 0

Capturing on inband
20150824 09:31:38.129393 0.0.0.0 -> 255.255.255.255 DHCP DHCP Discover - Transaction
 ID 0x860cd13
20150824 09:31:38.129952 11.11.11.11 -> 192.1.42.3 DHCP DHCP Discover - Transaction
 ID 0x860cd13
20150824 09:31:40.130134 192.1.42.3 -> 11.11.11.11 DHCP DHCP Offer - Transaction ID
 0x860cd13
20150824 09:31:40.130552 172.16.16.1 -> 172.16.16.11 DHCP DHCP Offer - Transaction
ID 0x860cd13
20150824 09:31:40.130990 0.0.0.0 -> 255.255.255.255 DHCP DHCP Request - Transaction
 ID 0x860cd13
20150824 09:31:40.131457 11.11.11.11 -> 192.1.42.3 DHCP DHCP Request - Transaction
ID 0x860cd13
20150824 09:31:40.132009 192.1.42.3 -> 11.11.11.11 DHCP DHCP ACK - Transaction ID
0x860cd13
20150824 09:31:40.132268 172.16.16.1 -> 172.16.16.11 DHCP DHCP ACK - TransactionID
0x860cd13
```

（注） Ethanalyzer はすべての DHCP パケットをキャプチャできない可能性がありますが、これは、フィルタ使用時のインバンドの解釈に問題があるためです。これは SPAN を使用することで回避できます。

VXLAN BGP EVPN 中の DHCP リレー

• DHCP Discover パケット 3636-1 は DHCP サーバーに送信されています。

giaddr は 11.11.11.11（loopback1）に設定され、それに応じてサブオプション 5/11/151 を設定します。

```
Bootstrap Protocol
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 1
  Transaction ID: 0x0860cd13
  Seconds elapsed: O
  Bootp flags: 0x0000 (unicast)
  Client IP address: 0.0.0.0 (0.0.0.0)
  Your (client) IP address: 0.0.0.0 (0.0.0.0)
  Next server IP address: 0.0.0.0 (0.0.0.0)
  Relay agent iP address: 11.11.11.11 (11.11.11.11)
  Client MAC address: Hughes_01:51:51 (00:00:10:01:51:51)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  Option: (53) DHCP Message Type
    Length: 1
    DHCP: Discover (1)
  Option: (55) Parameter Request List
  Option: (61) Client Identifier
  Option: (82) Agent Information Option
    Length: 47
  Option 82 suboption: (1) Aqent Circuit ID
  Option 82 suboption: (151) Agent Remote ID
  Option 82 suboption: (11) Server ID Override
    Length: 4
    Server ID override: 172.16.16.1 (172.16.16.1)
  Option 82 suboption: (5) Link selection
    Length: 4
    Link selection: 172.16.16.0 (172.16.16.0)
```

```
ASR1K-DHCP# sh ip dhcp bin
Bindings from all pools not associated with VRF:
IP address ClientID/Lease expiration Type State Interface
         Hardware address/
         User name

Bindings from VRF pool vxlan-900001:
IP address ClientID/Lease expiration Type State Interface
         Hardware address/
         User name

172.16.16.10 0100.0010.0175.75 Aug 25 2015 10:02 AM Automatic Active
GigabitEthernet2/1/0
172.16.16.11 0100.0010.0151.51 Aug 25 2015 09:50 AM Automatic Active
GigabitEthernet2/1/0
```

```
3636-1# sh ip route vrf vxlan-900001
IP Route Table for VRF "vxlan-900001"
'*' denotes best ucast nexthop
'**' denotes best mcast nexthop
'[x/y]' denotes [preference/metric]
```

```
'%<string>' in via output denotes VRF <string>

11.11.11.11/32, ubest/mbest: 2/0, attached
  *via 11.11.11.11, Lo1, [0/0], 19:13:56, local
  *via 11.11.11.11, Lo1, [0/0], 19:13:56, direct
22.22.22.22/32, ubest/mbest: 1/0
 *via 2.2.2.2%default, [200/0], 19:13:56, bgp65535,internal, tag 65535 (evpn)segid:
 900001 tunnelid: 0x2020202
encap: VXLAN
172.16.16.0/20, ubest/mbest: 1/0, attached
  *via 172.16.16.1, Vlan1001, [0/0], 19:13:56, direct
172.16.16.1/32, ubest/mbest: 1/0, attached
  *via 172.16.16.1, Vlan1001, [0/0], 19:13:56, local
172.16.16.10/32, ubest/mbest: 1/0
  *via 2.2.2.2%default, [200/0], 00:01:27, bgp65535,
internal, tag 65535 (evpn)segid: 900001 tunnelid: 0x2020202
encap: VXLAN
172.16.16.11/32, ubest/mbest: 1/0, attached
  *via 172.16.16.11, Vlan1001, [190/0], 00:13:56, hmm
192.1.42.0/24, ubest/mbest: 1/0, attached
  *via 192.1.42.1, Vlan10, [0/0], 00:36:08, direct
192.1.42.1/32, ubest/mbest: 1/0, attached
  *via 192.1.42.1, Vlan10, [0/0], 00:36:08, local
9372-1# ping 172.16.16.10 vrf vxlan-900001 cou 1
PING 172.16.16.10 (172.16.16.10): 56 data bytes
64 bytes from 172.16.16.10: icmp_seq=0 ttl=62 time=0.808 ms
- 172.16.16.10 ping statistics -
1 packets transmitted, 1 packets received, 0.00% packet loss
round-trip min/avg/max = 0.808/0.808/0.808 ms

3636-1# ping 172.16.16.11 vrf vxlan-900001 cou 1
PING 172.16.16.11 (172.16.16.11): 56 data bytes
64 bytes from 172.16.16.11: icmp_seq=0 ttl=63 time=0.872 ms
- 172.16.16.11 ping statistics -
1 packets transmitted, 1 packets received, 0.00% packet loss
round-trip min/avg/max = 0.872/0.871/0.872 ms
```

テナント VRF（VRF X）にあるクライアントと異なるテナント VRF（VRF Y）にあるサーバ

DHCP サーバは他のテナント VRF vxlan-900002 の中に置かれて、DHCP 応答パケットがオリジナルのリレー エージェントにアクセスできるようにされます。ここでは loopback2 を使用して、DHCP リレー パケットの送信元アドレスとされているエニーキャスト IP アドレスをすべて回避します。

```
3636-1# sh run int vl 10
!Command: show runningconfig interface Vlan10
!Time: Tue Aug 6 08:48:22 2018

version 9.2(1)
interface Vlan10
  no shutdown
  vrf member vxlan900002
  ip address 192.1.42.1/24

3636-1# sh run int lo2
!Command: show runningconfig interface loopback2
!Time: Tue Aug 7 08:48:57 2018
version 9.2(1)
interface loopback2
```

VXLAN BGP EVPN 中の DHCP リレー

```
  vrf member vxlan900002
  ip address 33.33.33.33/32

3636-2# sh run int lo2
!Command: show runningconfig interface loopback2
!Time: Tue Aug 7 08:48:44 2018
version 9.2(1)
interface loopback2
  vrf member vxlan900002
  ip address 44.44.44.44/32

9372-1# ping 192.1.42.3 vrf vxlan-900002 source 33.33.33.33 cou 1
PING 192.1.42.3 (192.1.42.3) from 33.33.33.33: 56 data bytes
64 bytes from 192.1.42.3: icmp_seq=0 ttl=254 time=0.544 ms
- 192.1.42.3 ping statistics -
1 packets transmitted, 1 packets received, 0.00% packet loss
round-trip min/avg/max = 0.544/0.544/0.544 ms

3636-2# ping 192.1.42.3 vrf vxlan-900002 source 44.44.44.44 count 1
PING 192.1.42.3 (192.1.42.3) from 44.44.44.44: 56 data bytes
64 bytes from 192.1.42.3: icmp_seq=0 ttl=253 time=0.678 ms
- 192.1.42.3 ping statistics -
1 packets transmitted, 1 packets received, 0.00% packet loss
round-trip min/avg/max = 0.678/0.678/0.678 ms
```

DHCP リレー設定

- 3636-1

```
3636—1# sh run dhcp

!Command: show running—config dhcp
!Time: Mon Aug 6 08:26:00 2018

version 9.2(1)
feature dhcp

service dhcp
ip dhcp relay
ip dhcp relay information option
ip dhcp relay information option vpn
ipv6 dhcp relay

interface VlanlOOl
  ip dhcp relay address 192.1.42.3 use—vrf vxlan—900002
  ip dhcp relay source—interface loopback2
```

- 3636-2

```
!Command: show running-config dhcp
!Time: Mon Aug 6 08:26:16 2018

version 9.2(1)
feature dhcp

service dhcp
ip dhcp relay
ip dhcp relay information option
ip dhcp relay information option vpn
```

VXLAN BGP EVPN 中の DHCP リレー

```
ipv6 dhcp relay

interface VlaniOOl
  ip dhcp relay address 192.1.42.3 use-vrf vxlan—900002
  ip dhcp relay source—interface loopback2
```

debug コマンドの出力例

- 次に示すのは、DHCP のインタラクティブ シーケンスのパケット ダンプです。

```
3636-1# ethanalyzer local interface inband display-filter "udp.srcport==67 or
udp.dstport==67" limit-captured-frames 0
Capturing on inband
20180806 08:59:35.758314 0.0.0.0 -> 255.255.255.255 DHCP DHCP Discover - Transaction
 ID 0x3eebccae
20180806 08:59:35.758878 33.33.33.33 -> 192.1.42.3 DHCP DHCP Discover - Transaction
 ID 0x3eebccae
20180806 08:59:37.759560 192.1.42.3 -> 33.33.33.33 DHCP DHCP Offer - Transaction ID
 0x3eebccae
20180806 08:59:37.759905 172.16.16.1 -> 172.16.16.11 DHCP DHCP Offer - Transaction
ID 0x3eebccae
20180806 08:59:37.760313 0.0.0.0 -> 255.255.255.255 DHCP DHCP Request - Transaction
 ID 0x3eebccae
20180806 08:59:37.760733 33.33.33.33 -> 192.1.42.3 DHCP DHCP Request - Transaction
ID 0x3eebccae
20180806 08:59:37.761297 192.1.42.3 -> 33.33.33.33 DHCP DHCP ACK - Transaction ID
0x3eebccae
20180806 08:59:37.761554 172.16.16.1 -> 172.16.16.11 DHCP DHCP ACK - Transaction ID
 0x3eebccae
```

- DHCP Discover パケット 3636-1 は DHCP サーバーに送信されています。

  giaddr は 33.33.33.33（loopback2）に設定され、それに応じてサブオプション 5/11/151 を設定します。

```
Bootstrap Protocol
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 1
  Transaction ID: Ox3eebccae
  Seconds elapsed: O
  Bootp flags: 0x0000 (unicast)
  Client IP address: 0.0.0.0 (0.0.0.0)
  Your (client) IP address: 0.0.0.0 (0.0.0.0)
  Next server IP address: 0.0.0.0 (0.0.0.0)
  Relay agent IP address: 33.33.33.33 (33.33.33.33)
  Client MAC address: i-iughes_01:51:51 (00:00:10:01:51:51)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  Option: (53) DHCP Message Type
    Length: 1
    DHCP: Discover (1)
  Option: (55) Parameter Request List
  Option: (61) client identifier
  Option: (82) Agent Information option
```

```
  Length: 47
Option 82 Suboption: (1) Agent circuit W
Option 82 suboption: (2) Agent Remote 10
Option 82 suboption: (151) VRF name/VPN ID
Option 82 Suboption: (11) Server ID Override
  Length: 4
  Server ID Override: 172.16.16.1 (172.16.16.1)
Option 82 Suboption: (5) Link selection
  Length: 4
  Link selection: 172.16.16.0 (172.16.16.0)
```

テナント VRF にあるクライアントと非デフォルトの非 VXLAN VRF にあるサーバ

DHCP サーバは管理 VRF に配置され、M0 インターフェイスを介して到達可能です。それに応じて IP アドレスは 10.122.164.147 に変更されます。

```
3636-1# sh run int m0
!Command: show running-config interface mgmt0
!Time: Tue Aug 7 09:17:04 2018
version 9.2(1)
interface mgmt0
  vrf member management
  ip address 10.122.165.134/25

3636-1# ping 10.122.164.147 vrf management cou 1
PING 10.122.164.147 (10.122.164.147): 56 data bytes
64 bytes from 10.122.164.147: icmp_seq=0 ttl=251 time=1.024 ms
- 10.122.164.147 ping statistics -
1 packets transmitted, 1 packets received, 0.00% packet loss
round-trip min/avg/max = 1.024/1.024/1.024 ms

3636-2# sh run int m0
!Command: show running-config interface mgmt0
!Time: Tue Aug 25 09:17:47 2015
version 7.0(3)I1(3)
interface mgmt0
  vrf member management
  ip address 10.122.165.148/25

3636-2# ping 10.122.164.147 vrf management cou 1
PING 10.122.164.147 (10.122.164.147): 56 data bytes
64 bytes from 10.122.164.147: icmp_seq=0 ttl=251 time=1.03 ms
- 10.122.164.147 ping statistics -
1 packets transmitted, 1 packets received, 0.00% packet loss
round-trip min/avg/max = 1.03/1.03/1.03 ms
```

DHCP リレー設定

- 3636-1

```
3636—1# sh run dhcp 3636—2# sh run dhcp

!Command: show running-config dhcp
!Time: Mon Aug 6 08:26:00 2018

version 9.2(1)
feature dhcp
```

VXLAN BGP EVPN 中の DHCP リレー

```
service dhcp
ip dhcp relay
ip dhcp relay information option
ip dhcp relay information option vpn
ipv6 dhcp relay

interface VlanlOOl
  ip dhcp relay address 10.122.164.147 use—vrf management
```

- 3636-2

```
3636-2# sh run dhcp
!Command: show running-config dhcp
!Time: Tue Aug 7 09:17:47 2018

version 9.2(1)
feature dhcp

service dhcp
ip dhcp relay
ip dhop relay information option
ip dhcp relay information option vpn
ipv6 dhcp relay

interface VlanlOOl
ip dhcp relay address 10.122.164.147 use—vrf management
```

debug コマンドの出力例

- 次に示すのは、DHCP のインタラクティブ シーケンスのパケット ダンプです。

```
3636-1# ethanalyzer local interface inband display-filter "udp.srcport==67 or
udp.dstport==67" limit-captured-frames 0
Capturing on inband
20180806 09:30:54.214998 0.0.0.0 -> 255.255.255.255 DHCP DHCP Discover - Transaction
 ID 0x28a8606d
20180806 09:30:56.216491 172.16.16.1 -> 172.16.16.11 DHCP DHCP Offer - Transaction
ID 0x28a8606d
20180806 09:30:56.216931 0.0.0.0 -> 255.255.255.255 DHCP DHCP Request - Transaction
 ID 0x28a8606d
20180806 09:30:56.218426 172.16.16.1 -> 172.16.16.11 DHCP DHCP ACK - Transaction ID
 0x28a8606d

3636-1# ethanalyzer local interface mgmt display-filter "ip.src==10.122.164.147 or
ip.dst==10.122.164.147" limit-captured-frames 0
Capturing on mgmt0
20180806 09:30:54.215499 10.122.165.134 -> 10.122.164.147 DHCP DHCP Discover -
Transaction ID 0x28a8606d
20180806 09:30:56.216137 10.122.164.147 -> 10.122.165.134 DHCP DHCP Offer - Transaction
 ID 0x28a8606d
20180806 09:30:56.217444 10.122.165.134 -> 10.122.164.147 DHCP DHCP Request -
Transaction ID 0x28a8606d
20180806 09:30:56.218207 10.122.164.147 -> 10.122.165.134 DHCP DHCP ACK - Transaction
 ID 0x28a8606d
```

- DHCP Discover パケット 3636-1 は DHCP サーバーに送信されています。

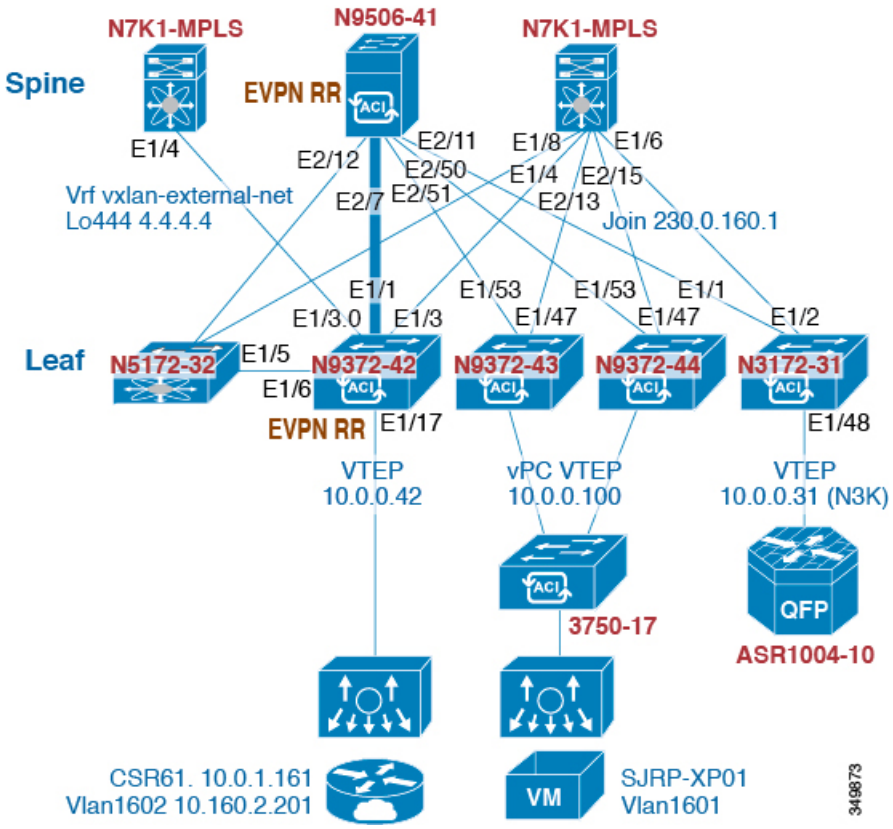
giaddr は 10.122.165.134（mgmt0）に設定され、それに応じてサブオプション 5/11/151 を設定します。

```
Bootstrap Protocol
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 1
  Transaction ID: 0x28a8606d
  Seconds elapsed: O
  Bootp flags: 0x0000 (Unicast)
  Client IP address: 0.0.0.0 (0.0.0.0)
  Your (client) IP address: 0.0.0.0 (0.0.0.0)
  Next server IP address: 0.0.0.0 (0.0.0.0)
  Relay agent IP address: 10.122.165.134 (10.122.165.134)
  Client MAC address: Hughes_01:51:51 (00:00:10:01:51:51)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  Option: (53) DHCP Message Type
    Length: 1
    DHCP: Discover (1)
  Option: (55) Parameter Request List
  Option: (61) Client identifier
  Option: (82) Agent Information Option
    Length: 47
    Option 82 Suboption: (1) Agent Circuit ID
    Option 82 Suboption: (2) Agent Remote ID
    Option 82 Suboption: (151) VRF name/VPN ID
    Option 82 Suboption: (11) Server ID Override
      Length: 4
      Server ID Override: 172.16.16.1 (172.16.16.1)
    Option 82 Suboption: (5) Link selection
      Length: 4
      Link selection: 172.16.16.0 (172.16.16.0)
```

VPC ピアの構成例

次の例では、DHCP リレー構成用のオーバーレイ VLAN にある VPC ピア間のルーティングを構成します。

VXLAN BGP EVPN 中の DHCP リレー



• DHCP サービスをイネーブルにします。

```
service dhcp
```

• DHCP リレーを設定します。

```
ip dhcp relay
ip dhcp relay information option
ip dhcp relay sub-option type cisco
ip dhcp relay information option vpn
```

• DHCP リレー サービスを必要とする VRF でループバックを作成します。

```
interface loopback601
  vrf member evpn-tenant-kk1
  ip address 160.1.0.43/32
  ip router ospf 1 area 0     /* Only required for VPC VTEP. */
```

• レイヤ 3 VRF BGP に LoX をアドバタイズします。

```
Router bgp 2
vrf X
   network 10.1.1.42/32
```

- VRF で SVI に DHCP リレーを設定します。

```
interface Vlan1601
  vrf member evpn-tenant-kk1
  ip address 10.160.1.254/24
  fabric forwarding mode anycast-gateway
  ip dhcp relay address 10.160.2.201
  ip dhcp relay source-interface loopback601
```

- レイヤ 3 VNI SVI を**ip forward** で構成します。

```
interface Vlan1600
  vrf member evpn-tenant-kk1
    ip forward
```

- VPC VRF のルーティング VLAN/SVI を作成します。

（注） VPC VTEP でのみ必要です。

```
Vlan 1605
interface Vlan1605
  vrf member evpn-tenant-kk1
  ip address 10.160.5.43/24
  ip router ospf 1 area 0.0.0.41
```

- VRF ルーティングを作成します。

（注） VPC VTEP でのみ必要です。

```
router ospf 1
vrf evpn-tenant-kk1
    router-id 10.160.5.43
```

vPC VTEP DHCP リレーの設定例

vPC VLAN など、MCT/ピア リンク全体で許可される VLAN を設定する必要性に応えるため、SVI は VLAN に関連付けることが可能であり、テナント VRF 内部で作成されます。これが OSPF など、アンダーレイ プロトコル付きのアンダーレイ ピアリングとなりますが、これはルーティング プロセスでインスタンス化されるテナント VRF を必要とします。

あるいは、ルーティング プロトコル中への SVI の配置およびルーティング プロセス下でのテナント VRF のインスタンス化の代わりに、MCT 全体の vPC ピア間でスタティック ルートを使用することが可能です。このアプローチにより、サーバからの応答が正しい場所に返され、

VXLAN BGP EVPN 中の DHCP リレー

各 VTEP が GiAddr について異なるループバック インターフェイスを使用することが保証されます。

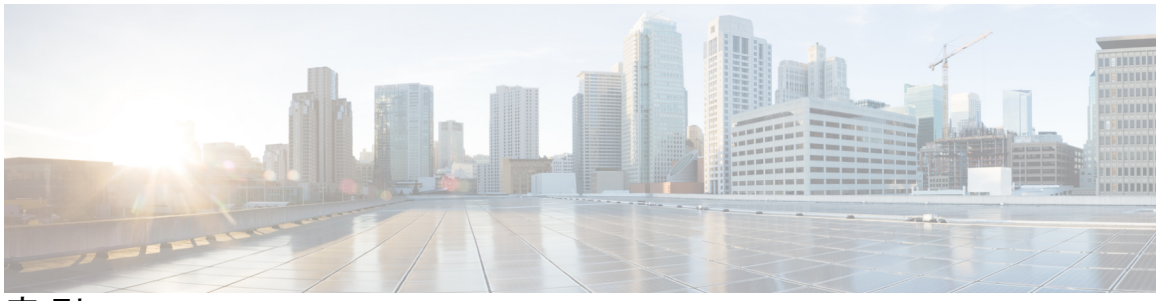
次に示すのは、これらの設定例です。

- アンダーレイ ルーティング内での SVI の設定：

```
/* vPC Peer-1 */

router ospf UNDERLAY
vrf tenant-vrf

interface Vlan2000
  no shutdown
  mtu 9216
  vrf member tenant-vrf
  ip address 192.168.1.1/30
  ip router ospf UNDERLAY area 0.0.0.0


/* vPC Peer-2 */

router ospf UNDERLAY
vrf tenant-vrf

interface Vlan2000
  no shutdown
  mtu 9216
  vrf member tenant-vrf
  ip address 192.168.1.2/30
  ip router ospf UNDERLAY area 0.0.0.0
```

- MCT 全体での vPC ピア間のスタティック ルートを使用した SVI 設定：

```
/* vPC Peer-1 */

interface Vlan2000
  no shutdown
  mtu 9216
  vrf member tenant-vrf
  ip address 192.168.1.1/30

vrf context tenant-vrf
ip route 192.168.1.2/30 192.168.1.1


/* vPC Peer-2 */

interface Vlan2000
  no shutdown
  mtu 9216
  vrf member tenant-vrf
  ip address 192.168.1.2/30

vrf context tenant-vrf
ip route 192.168.1.1/30 192.168.1.2
```



索 引

V

い

ゆ

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。