



# 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 について \(1 ページ\)](#)
- [VXLAN BGP EVPN の注意事項と制約事項 \(3 ページ\)](#)
- [ダウンストリーム VNI を使用した VXLAN EVPN に関する \(9 ページ\)](#)
- [ダウンストリーム VNI を使用する VXLAN EVPN の注意事項と制約事項 \(11 ページ\)](#)
- [VXLAN BGP EVPN の設定 \(13 ページ\)](#)
- [ND 抑制の構成 \(66 ページ\)](#)

## VXLAN BGP EVPN について

### RD Auto について

自動派生ルート識別子 (rd auto) は、IETF RFC 4364 セクション 4.2 で説明されているタイプ 1 エンコーディング形式に基づいています。<https://tools.ietf.org/html/rfc4364#section-4.2>タイプ 1 エンコーディングでは、4 バイトの管理フィールドと 2 バイトの番号フィールドを使用できます。Cisco NX-OS 内では、自動導出 RD は、4 バイトの管理フィールド (RID) としての BGP ルータ ID の IP アドレスと、2 バイトの番号フィールド (VRF ID) の内部 VRF ID を使用して構築されます。

2 バイトの番号付けフィールドは常に VRF から取得されますが、IP-VRF または MAC-VRF での使用に応じて異なる番号付け方式になります。

- IP-VRF の 2 バイトの番号付けフィールドは、1 から始まる内部 VRF ID を使用します。VRF ID 1 および 2 は、それぞれデフォルト VRF および管理 VRF 用に予約されています。最初のカスタム定義 IP VRF は VRF ID 3 を使用します。
- MAC-VRF の 2 バイトの番号付けフィールドは、VLAN ID + 32767 を使用します。その結果、VLAN ID 1 は 32768 になります。

例：自動取得ルート識別子 (RD)

- BGP ルータ ID 192.0.2.1 および VRF ID 6-RD 192.0.2.1:6 の IP-VRF

- BGP ルータ ID 192.0.2.1 および VLAN 20-RD 192.0.2.1:32787 の MAC-VRF

## Route-Target Auto について

自動派生Route-Target (route-target import/export/both auto) は、IETF RFC 4364 セクション 4.2 (<https://tools.ietf.org/html/rfc4364#section-4.2>) で説明されているタイプ 0 エンコーディング形式に基づいています。IETF RFC 4364 セクション 4.2 ではルート識別子形式について説明し、IETF RFC 4364 セクション 4.3.1では、Route-Target に同様の形式を使用することが望ましいとしています。タイプ 0 エンコーディングでは、2 バイトの管理フィールドと 4 バイトの番号フィールドを使用できます。Cisco NX-OS 内では、自動派生 Route-Target は、2 バイトの管理フィールドとして自律システム番号 (ASN) 、4 バイトの番号フィールドのサービス識別子 (VNI) で構成されます。

### 2 バイト ASN

タイプ 0 エンコーディングでは、2 バイトの管理フィールドと 4 バイトの番号フィールドを使用できます。Cisco NX-OS 内では、自動派生 Route-Target は、2 バイトの管理フィールドとしての自律システム番号 (ASN) と、4 バイトの番号フィールドのサービス識別子 (VNI) で構成されます。

自動派生 Route-Target (RT) の例 :

- ASN 65001 と L3VNI 50001 内の IP-VRF : Route-Target 65001:50001
- ASN 65001 と L2VNI 30001 内の MAC-VRF : Route-Target 65001:30001

Multi-AS 環境では、Route-Target を静的に定義するか、Route-Target の ASN 部分と一致するように書き換える必要があります。

[https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/7-x/command\\_references/configuration\\_commands/b\\_N9K\\_Config\\_Commands\\_703i7x/b\\_N9K\\_Config\\_Commands\\_703i7x\\_chapter\\_010010.html#wp4498893710](https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/7-x/command_references/configuration_commands/b_N9K_Config_Commands_703i7x/b_N9K_Config_Commands_703i7x_chapter_010010.html#wp4498893710)

### 4 バイト ASN

タイプ 0 エンコーディングでは、2 バイトの管理フィールドと 4 バイトの番号フィールドを使用できます。Cisco NX-OS 内では、自動派生 Route-Target は、2 バイトの管理フィールドとしての自律システム番号 (ASN) と、4 バイトの番号フィールドのサービス識別子 (VNI) で構成されます。4 バイト長の ASN 要求と 24 ビット (3 バイト) を必要とする VNI では、拡張コミュニティ内のサブフィールド長が使い果たされます (2 バイトタイプと 6 バイトサブフィールド)。長さ形式の制約、およびサービス識別子 (VNI) の一意性の重要性の結果、4 バイトの ASN は、IETF RFC 6793 セクション 9 (<https://tools.ietf.org/html/rfc6793#section-9>) で説明されているように、AS\_TRANS という名前の 2 バイトの ASN で表されます。2 バイトの ASN 23456 は、4 バイトの ASN をエイリアスする特別な目的の AS 番号である AS\_TRANS として IANA (<https://www.iana.org/assignments/iana-as-numbers-special-registry/iana-as-numbers-special-registry.xhtml>) によって登録されます。

4 バイトの ASN (AS\_TRANS) を使用した自動派生 Route-Target (RT) の例 :

- ASN 65656 と L3VNI 50001 内の IP-VR : Route-Target 23456:50001

- ASN 65656 と L2VNI 30001 内の MAC-VRF : Route-Target 23456:30001



(注) Cisco NX-OS リリース 9.2(1)以降、4バイト ASN の自動派生 Route-Target がサポートされます。

## 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。

- BGP EVPN を使用する VXLAN/VTEP には、次の注意事項と制約事項が適用されます。
  - SPAN 送信元または宛先は、任意のポートでサポートされます。

詳細については、『[Cisco Nexus 9000 シリーズ NX-OS システム管理設定ガイド、リリース 9.3\(x\)](#)』を参照してください。

- ARP 抑制に関係なく、VTEP（フラッドアンドラーニング、または EVPN）で SVI が有効になっている場合は、**hardware access-list tcam region arp-ether 256 double-wide** コマンドを使用して ARP-ETHER TCAM が切り分けられるようにします。この要件は、Cisco Nexus 9200、9300-EX、9300-FX/FX2/FX3 および 9300-GX プラットフォーム スイッチ、および 9700-EX/FX ラインカードを備えた Cisco Nexus 9500 プラットフォーム スイッチには適用されません。
- R シリーズ ライン カードを搭載した Cisco Nexus 9504 および 9508 では、VXLAN EVPN（レイヤ 2 およびレイヤ 3）は 9636C-RX および 96136YC-R ラインカードでのみサポートされます。
- VXLAN は N9K-C92348GC-X スイッチではサポートされていません。
- セグメントルーティングまたは MPLS を介して EVPN を設定できます。詳細については、『[Cisco Nexus 9000 Series NX-OS Label Switching Configuration Guide, Release 9.3\(x\)](#)』を参照してください。
- 新しい CLI `encapsulation mpls` コマンドを使用して MPLS トンネル カプセル化を使用できます。EVPN アドレス ファミリのラベル割り当てモードを設定できます。詳細については、『[Cisco Nexus 9000 Series NX-OS Label Switching Configuration Guide, Release 9.3\(x\)](#)』を参照してください。
- 2K VNI スケール設定を持つ VXLAN EVPN セットアップでは、コントロールプレーンのダウンタイムに 200 秒以上かかる場合があります。潜在的な BGP フラップを回避するには、グレースフル リスタート時間を 300 秒に延長します。
- 特定のインターフェイスでコマンド「`clear ip arp <interface> vrf <vrf-name> force-delete`」を実行すると、通常そのインターフェイスに属する ARP からエントリが削除され、トラフィックが再学習されます。ただし、同じ IP の ARP がすべての ECMP パスで解決されている場合、ECMP インターフェイスの 1 つに属する ARP エントリを強制的に削除すると、そのリンクがダウンしていない限り、そのエントリが自動的に再学習されます。

- EVPN アンダーレイの IP アドレスは ECMP をサポートします。複数の IP アドレスリンクが、同じスイッチ間で背中合わせに接続されています。ARP は接続されたすべてのインターフェイスで解決されるため、ECMP が提供されます。
- Cisco NX-OS リリース 10.2(2)F 以降、次のスケール制限が強化されています — レイヤ 2 VNI、拡張レイヤ 2 VNI、レイヤ 3 VNI、分散エニーキャスト ゲートウェイを使用する SVI、インターネット ピアリング モードの IPv4 および IPv6 ホスト ルート、および ECMP パス。VXLAN スケール制限情報については、『Cisco Nexus 9000 シリーズ NX-OS 検証済みスケラビリティガイド、リリース 10.2(2)F』を参照してください。
- Cisco NX-OS リリース 10.2(1q)F 以降、VXLAN EVPN は Cisco Nexus N9K-C9332D-GX2B プラットフォーム スイッチでサポートされます。
- Cisco NX-OS リリース 10.2(3)F 以降、VXLAN EVPN は Cisco Nexus 9364D-GX2A および 9348D-GX2A プラットフォーム スイッチでサポートされます。
- Cisco NX-OS リリース 9.3(5) 以降、新しい VXLAN アップリンク機能が導入されています。
  - デフォルト VRF の物理インターフェイスは、VXLAN アップリンクとしてサポートされます。
  - VRF および dot1q タグを持つサブインターフェイスを伝送するデフォルト VRF の親インターフェイスは、VXLAN アップリンクとしてサポートされます。
  - VRF 内および dot1q タグ付きのサブインターフェイスは、VXLAN アップリンクとしてサポートされません。
  - VRF の SVI は、VXLAN アップリンクとしてサポートされません。
  - 物理ピアリンクを使用する vPC では、SVI を vPC メンバー (infra-VLAN、system nve infra-vlan) 間でのみバックアップ アンダーレイ、デフォルト VRF として利用できません。
  - vPC ペアでは、vPC ノードの 1 つで NVE または NVE ループバックをシャットダウンする構成はサポートされていません。これは、片側 NVE シャットまたは片側ループバック シャットでのトラフィック フェイルオーバーがサポートされていないことを意味します。
  - FEX ホストインターフェイスは VXLAN アップリンクとしてサポートされないため、VTEP を接続できません (BUD ノード)。
- vPC ボーダー ゲートウェイの起動プロセス中に、NVE ソースループバック インターフェイスはホールドダウン タイマーを 1 回だけでなく 2 回実行します。これは day-1 であり予期された動作です。
- NVE インターフェイスの遅延タイマーの値は、マルチサイトの遅延復元タイマーよりも小さい値に設定する必要があります。
- VXLAN セットアップでパス最大伝送ユニット (MTU) 検出 (PMTUD) を有効にするには、VXLAN アップリンクを **ip unreachable** で構成する必要があります。PMTUD は、パケットの発信元から宛先へのパスに沿って最小 MTU を動的に決定することで、2 つのエ

ンドポイント間のパスのフラグメンテーションを防ぎます。12-04-2022  
12:35SYSTEM:USER-AUTO-STEP

- 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 ノードに一意のルート識別子を設定する必要があります。すべてのボーダーノードで一意のルート識別子を使用しないことはサポートされていません。ファブリックのすべてのVTEP に対して、一意のルート識別子を使用することを強く推奨します。
- 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。
- ローカルで発信されたタイプ2ルート (MAC/MAC-IP) のモビリティシーケンス番号は、1つのvTEP がシーケンス番号 K を持ち、同じコンプレックス内の他のvTEP はシーケンス番号 0 の同じルートを持つことができるため、vPC ピア間で不一致になる可能性があります。これは機能上の影響はなく、ホストが移動した後でもトラフィックには影響しません。
- 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。
- RAACL は、VXLAN アップリンク インターフェイスではサポートされません。VAACL は、出力方向の VXLAN カプセル化解除トラフィックではサポートされません。これは、ネットワーク (VXLAN) からアクセス (イーサネット) に向かう内部トラフィックに適用されます。

ベストプラクティスとして、ネットワーク ディレクションへのアクセスに対して、PAACL/VAACL を使用します。VXLAN ACL 機能のその他のガイドラインと制限事項については、『[Cisco Nexus 9000 Series NX-OS Security Configuration Guide, Release 9.3\(x\)](#)』を参照してください。

- Cisco Nexus 9000 QoS バッファ ブースト機能は、VXLAN トラフィックには適用できません。
- EBGp を使用した VXLAN BGP EVPN ファブリックには、次の推奨事項が適用されます。
  - EBGPEVPN ピアリングセッション (オーバーレイ コントロールプレーン) にはループバックを使用することをお勧めします。
  - EBGp IPv4/IPv6 ピアリングセッション (アンダーレイ) に物理インターフェイスを使用することをお勧めします。
- NVE ソースインターフェイスを専用ループバック インターフェイスにバインドし、このループバックをレイヤ3 プロトコルの機能またはピアリングと共有しないでください。VXLAN VTEP 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。

- 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。同じループバックを使用する NVE およびその他のレイヤ 3 プロトコルはサポートされません。
- NVE ソースインターフェイスループバックは、デフォルト VRF に存在する必要があります。
- VTEP と外部ノード（エッジルータ、コアルータ、または VNF）間の EBGp ピアリングのみがサポートされます。
  - 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 VTEP から外部ノードへの EBGp ピアリングが推奨されます。これはベスト プラクティスです（外部接続）。
  - VTEP から外部ノードへの EBGp ピアリングは、デフォルト VRF またはテナント VRF（外部接続）に存在できます。
  - VXLAN を介した VTEP から外部ノードへの EBGp ピアリングは、テナント VRF 内に存在し、ループバック インターフェイスの更新ソースを使用する必要があります（VXLAN を介したピアリング）。
  - VTEP から外部ノードへの EBGp ピアリングに SVI を使用するには、VLAN がローカルである必要があります（VXLAN 拡張ではありません）。
- VXLAN BGP EVPN を設定する場合、「システム ルーティング モード：デフォルト」のみが次のハードウェア プラットフォームに適用されます。
  - Cisco Nexus 9200 プラットフォーム スイッチ
  - Cisco Nexus 9300 プラットフォーム スイッチ
  - Cisco Nexus 9300-EX プラットフォーム スイッチ
  - Cisco Nexus 9300-FX/FX2/FX3 プラットフォーム スイッチ
  - Cisco Nexus 9300-GX プラットフォーム スイッチ
  - X9500 ラインカード搭載の Cisco Nexus 9500 プラットフォーム スイッチ
  - X9700-EX および X9700-FX ラインカードを搭載した Cisco Nexus 9500 プラットフォーム スイッチ
- Cisco NX-OS リリース 10.2(3)F 以降、VXLAN BGP EVPN を構成する場合、「システム ルーティング モード：デフォルト」のみが Cisco Nexus 9300-GX2 プラットフォーム スイッチに適用されます。
- 「システム ルーティング モード」を変更するには、スイッチをリロードする必要があります。
- Cisco Nexus 9516 プラットフォームは、VXLAN EVPN ではサポートされません。

- VXLAN は Cisco Nexus 9500 プラットフォーム スイッチで次のラインカードを使用してサポートされています。
  - 9500-R
  - 9564PX
  - 9564TX
  - 9536PQ
  - 9700-EX
  - 9700-FX
- 9700-EX または -FX ラインカードを搭載した Cisco Nexus 9500 プラットフォーム スイッチは、VXLAN アップリンクで 1G、10G、25G、40G、100G、および 400G をサポートします。
- Cisco Nexus 9200 および 9300-EX/FX/FX2/FX3 および -GX は、VXLAN アップリンクで 1G、10G、25G、40G、100G、および 400G をサポートします。
- Cisco NX-OS リリース 10.2(3)F 以降、Cisco Nexus 9300-GX2 プラットフォーム スイッチは、VXLAN アップリンクで 10G、25G、40G、100G、および 400G をサポートします。
- Cisco Nexus 9000 プラットフォーム スイッチは、VXLAN カプセル化に UDP ポート番号 4789 に準拠する標準を使用します。この値は設定可能です。
- Application Spine Engine (ASE2) を搭載した Cisco Nexus 9200 プラットフォーム スイッチでは、パケットサイズが 99–122 バイトに制限されています。パケットドロップが発生する可能性があります。
- VXLAN ネットワーク ID (VNID) 16777215 が予約済みであり、明示的に設定しないでください。
- Non-Disruptive In Service Software Upgrade (ND-ISSU) は、VXLAN が有効になっている Nexus 9300 でサポートされます。例外は、Cisco Nexus 9300-FX3 および 9300-GX プラットフォーム スイッチの ND-ISSU サポートです。
- VXLAN to MPLS (LDP)、VXLAN to MPLS-SR (セグメントルーティング)、および VXLAN to SRv6 のゲートウェイ機能は、同じ Cisco Nexus 9000 シリーズ プラットフォームで動作できます。
  - VXLAN to MPLS (LDP) ゲートウェイは、Cisco Nexus 3600-R および R シリーズ ラインカードを搭載した Cisco Nexus 9500 でサポートされます。
  - VXLAN to MPLS-SR Gateway は、CR-Series ラインカードを搭載した Cisco Nexus 9300-FX2/FX3/GX および Cisco Nexus 9500 でサポートされます。
  - Cisco NX-OS Release 10.2(3)F 以降、VXLAN から MPLS-SR へのゲートウェイは、Cisco Nexus 9300-GX2 プラットフォーム スイッチでサポートされます。
  - VXLAN は、Cisco Nexus 9300-GX プラットフォームのみでサポートされます。

- Cisco NX-OS Release 10.2(3)F 以降、VXLAN から SRv6 へは、Cisco Nexus 9300-GX2 プラットフォーム スイッチでサポートされます。
- Cisco NX-OS リリース 10.2(3)F 以降、VXLAN と GRE の共存は、Cisco Nexus 9300-EX/FX/FX2/FX3/GX/GX2 スイッチ、および N9K-C93108TC-FX3P、N9K-C93180YC-FX3、N9K-X9716D-GX スイッチでサポートされます。GRE RX パス (カプセル化解除) のみがサポートされます。GRE TX パス (カプセル化) はサポートされていません。
- 複数のトンネルカプセル化 (VXLAN、GRE および/または MPLS、静的ラベルまたはセグメントルーティング) は、同じ Cisco Nexus 9000 シリーズ スイッチ上でネットワーク フォワーディング エンジン (NFE) と共存できません。
- 復元力のあるハッシュは、VXLAN VTEP が設定された次のスイッチ プラットフォームでサポートされます。
  - Cisco Nexus 9300-EX/FX/FX2/FX3/GX は ECMP 復元力のあるハッシュをサポートしません。
  - ALE アップリンク ポートを備えた Cisco Nexus 9300 は、復元力のあるハッシュをサポートしていません。



(注) 復元力のあるハッシュはデフォルトではディセーブルになっています。

- Cisco NX-OS Release 10.2(3)F 移行、ECMP レジリエント ハッシュは Cisco Nexus 9300-GX2 プラットフォーム スイッチでサポートされます。
- vPC VTEP として動作する Cisco Nexus 9000 プラットフォーム スイッチ上の単一の接続デバイスまたはルーテッド デバイスに **vpc orphan-ports suspend** コマンドを使用することをお勧めします。
- Cisco NX-OS リリース 10.3(2)F 以降、BGP EVPN のスタティック MAC は Cisco Nexus 9300-EX/FX/FXP/FX2/FX3/GX/GX2 シリーズ スイッチでサポートされています。
- **mac address-table static mac-address vlan vlan-id [[drop | interface {type slot/port} | port-channel number]]** コマンドは、BGP EVPN でサポートされています。
- Cisco Nexus は、SMET フラグ フィールドがオプションとして設定されている以前のバージョンの **draft-ietf-bess-evpn-igmp-mld-proxy** ドラフトに基づいて、タイプ 6 EVPN ルート (IPv4 用) をサポートします。
- エニーキャスト ゲートウェイ SVI を使用したルーティング プロトコル隣接関係はサポートされていません。



- (注) VXLAN BGP EVPN のスケーラビリティについては、『[Cisco Nexus 9000 Series NX-OS Verified Scalability Guide](#)』を参照してください。

## ダウンストリーム VNI を使用した VXLAN EVPN に関する

Cisco NX-OS リリース 9.3(5) では、ダウンストリーム VNI を備えた VXLAN EVPN が導入されています。以前のリリースでは、VXLAN EVPN ネットワーク内のすべてのノード間で通信を有効にするには、VNI の設定が一貫している必要があります。

VXLAN EVPN とダウンストリーム VNI は、次のソリューションを提供します。

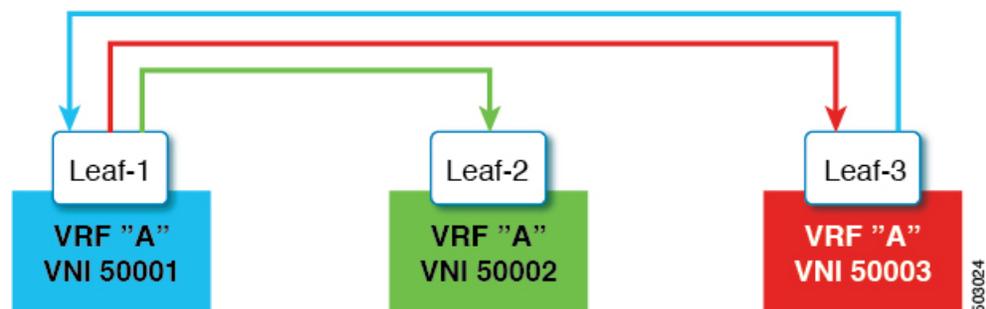
- VXLAN EVPN ネットワークのノード間での非対称 VNI 通信を有効にします。
- 顧客がドメイン外の共通の共有サービス（テナント VRF）にアクセスできるようにします。
- VNI の異なるセットを持つ分離された VXLAN EVPN サイト間の通信をサポートします。

### 非対称 VNI

ダウンストリーム VNI を使用する VXLAN EVPN は、非対称 VNI 割り当てをサポートします。

次の図に、非対称 VNI の例を示します。3 つの VTEP にはすべて、同じ IP VRF または MAC VRF に対して異なる VNI が設定されています。

図 1: 非対称 VNI



### 共有サービス VRF

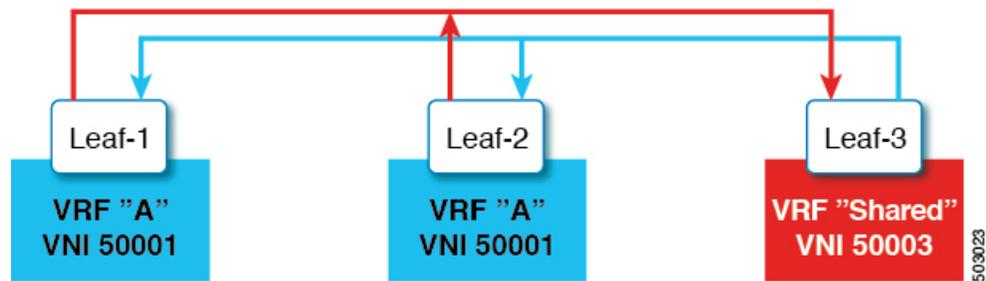
ダウンストリーム VNI を使用する VXLAN EVPN は、共有サービス VRF をサポートします。これは、複数の L3VRF を単一のローカル L3VRF にインポートし、ピア単位でダウンストリーム L3VNI の異なる値をサポートすることによって行われます。

たとえば、DNS サーバは、ホストが存在するテナント VRF に関係なく、データセンター内の複数のホストにサービスを提供する必要があります。DNS サーバは、L3VNI に接続されてい

る共有サービス VRF に接続されています。いずれかのテナント VRF からこのサーバにアクセスするには、共有サービス VRF に関連付けられた L3VNI がテナント VRF に関連付けられた L3VNI とは異なる場合でも、スイッチは共有サービス VRF からテナント VRF にルートをインポートする必要があります。

次の図では、リーフ 1 のテナント VRF A がリーフ 2 のテナント VRF A と通信できます。ただし、テナント VRF A は、リーフ 3 の背後にある共有サービスにアクセスする必要があります。

図 2: 共有サービス VRF

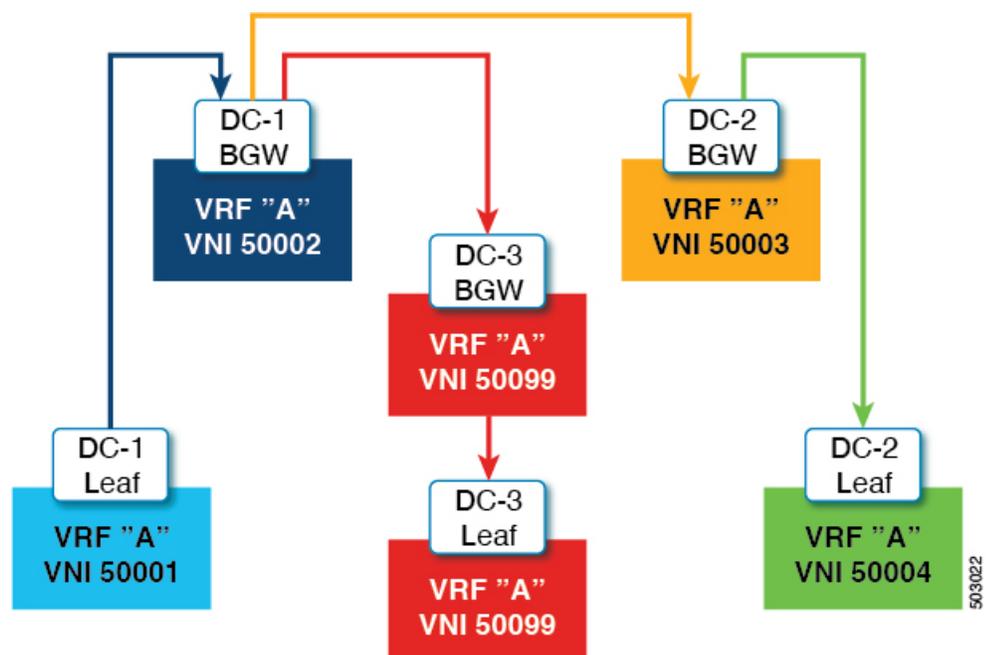


## 非対称 VNI を使用するマルチサイト

ダウンストリーム VNI を使用する VXLAN EVPN では、異なる VNI セットを持つサイト間の通信が可能です。これは、ボーダー ゲートウェイで非対称 VNI をステッチングすることによって行われます。

次の図では、DC-1 と DC-2 は非対称サイトであり、DC-3 は対称サイトです。各サイトは、サイト内の異なる VNI を使用して通信します。

図 3: 非対称 VNI を使用するマルチサイト



# ダウンストリーム VNI を使用する VXLAN EVPN の注意事項と制約事項

ダウンストリーム VNI をもつ VXLAN EVPN には、次の注意事項と制約事項があります。

- Cisco Nexus 9332C、9364C、9300-EX、および 9300-FX/FX2/FXP プラットフォーム スイッチと、-EX/FX ラインカードを備えた Cisco Nexus 9500 プラットフォーム スイッチは、ダウンストリーム VNI で VXLAN EVPN をサポートします。
- Cisco NX-OS リリース 9.3(7) 以降、Cisco Nexus 9300-GX プラットフォーム スイッチは、ダウンストリーム VNI で VXLAN EVPN をサポートします。
- Cisco NX-OS リリース 10.2(3)F 以降、ダウンストリーム VNI をもつ VXLAN EVPN は Cisco Nexus 9300-FX3/GX2 プラットフォーム スイッチでサポートされています。
- ダウンストリーム VNI を使用する VXLAN EVPN は、IPv4 アンダーレイでのみサポートされます。
- ダウンストリーム VNI は、ルート ターゲットのエクスポートおよびインポートに基づいて設定されます。ダウンストリーム VNI を活用するには、次の条件を満たす必要があります。
  - ダウンストリーム VNI では、異なる VRF (MAC-VRF または IP-VRF) を使用する必要があります。各 VRF には異なる VNI (非対称 VNI) が必要です。
  - 外部 VRF (MAC-VRF または IP-VRF) のルートをインポートするには、ローカル VRF へのインポートに適したルート ターゲットを設定する必要があります。
  - 自動派生ルート ターゲットのみを設定すると、ダウンストリーム VNI にはなりません。
  - VRF プレフィックスのエクスポートは、スタティックまたは自動派生ルート ターゲット設定によって実行できます。
  - 外部 VRF 自動導出ルート ターゲットのインポートがサポートされています。
  - 外部 VRF のスタティックに設定されたルート ターゲットのインポートがサポートされています。
- ダウンストリーム VNI は、次のアンダーレイ コンスタレーションでサポートされます。
  - レイヤ 3 VNI を使用するダウンストリーム VNI の場合、アンダーレイは入力レプリケーションまたはマルチキャスト ベースにすることができます。
  - レイヤ 2 VNI を使用するダウンストリーム VNI の場合、アンダーレイは入力複製内にある必要があります。マルチキャストベースのアンダーレイは、レイヤ 2 VNI のダウンストリーム VNI ではサポートされません。
- ダウンストリーム VNI には一貫した設定が必要です。

- サイト内のすべてのマルチサイト ボーダー ゲートウェイ (BGW) には、一貫した設定が必要です。
- vPC ドメイン内のすべての vPC メンバーに一貫した設定が必要です。
- マルチサイトでダウンストリーム VNI を使用するには、少なくとも Cisco NX-OS リリース 9.3(5) を実行するために、すべてのサイトですべての BGW が必要です。
- 既存の中央集中型 VRF ルートリーク展開では、Cisco NX-OS リリース 9.3(5) 以降への ISSU 中に短時間のトラフィック損失が発生する可能性があります。
- Cisco NX-OS リリース 9.3(5) から以前のリリースに正常にダウングレードするには、非対称 VNI 設定が削除されていることを確認します。ダウンストリーム VNI は Cisco NX-OS リリース 9.3(5) よりも前ではサポートされていないため、トラフィック転送に影響があります。
- レイヤ 3 VNI (IP-VRF) は、ピアごとに VNI 間で柔軟にマッピングできます。
  - VTEP1 上の VNI 50001 は、VNI 50001 との対称 VNI と、VTEP2 上の VNI 50002 との非対称 VNI を同時に実行できます。
  - VTEP1 の VNI 50001 は、VTEP2 の VNI 50002 および VTEP3 の VNI 50003 と非対称 VNI を実行できます。
  - VTEP1 上の VNI 50001 は、VTEP2 上の VNI 50002 および VNI 50003 と非対称 VNI を同時に実行できます。
- レイヤ 2 VNI (MAC-VRF) は、ピアごとに 1 つの VNI にのみマッピングできます。
  - VTEP1 の VNI 30001 は、VTEP2 の VNI 30002 および VTEP3 の VNI 30003 と非対称 VNI を実行できます。
  - VTEP1 上の VNI 30001 は、VTEP2 上の VNI 30002 および VNI 30003 と非対称 VNI を同時に実行できません。
- VRF 内の vPC ピア ノード間の iBGP セッションはサポートされていません。
- VXLAN およびダウンストリーム VNI での BGP ピアリングは、次のコンスタレーションをサポートします。
  - 対称 VNI 間の BGP ピアリングは、ループバックを使用してサポートされます。
  - 非対称 VNI 間の BGP ピアリングは、VNI が 1:1 の関係にある場合にサポートされません。VNI 50001 (VTEP1) からのループバックは、VNI 50002 (VTEP2) のループバックとピアリングできます。
  - 非対称 VNI 間の BGP ピアリングは、VNI が異なる VTEP 上にある 1:1 の関係にある場合にサポートされます。VNI 50001 (VTEP1) からのループバックは、VNI 50002 (VTEP2 および VTEP3) のループバックとピアリングできます。

- VNI が 1:N の関係にある場合、非対称 VNI 間の BGP ピアリングはサポートされません。VNI 50001 (VTEP1) のループバックは、VNI 50002 (VTEP2) および VNI 50003 (VTEP3) のループバックと同時にピアすることはできません。
- VXLAN 整合性チェッカは、ダウンストリーム VNI を使用する VXLAN EVPN ではサポートされません。
- ダウンストリーム VNI を使用する VXLAN EVPN は、現在、次の機能の組み合わせではサポートされていません。
  - VXLAN 静的トンネル
  - TRM およびマルチサイトでの TRM
  - CloudSec VXLAN EVPN トンネル暗号化
  - ESI ベースのマルチホーミング
  - L3VPN (MPLS SR) を備えた EVPN のシームレスな統合
  - ポリシーベース ルーティング (PBR)

## 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. **feature vn-segment-vlan-based**
4. **feature interface-vlan**
5. **nv overlay evpn**

#### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>feature vn-segment</b>	VLAN ベースの VXLAN をイネーブルにします。
ステップ 2	<b>feature nv overlay</b>	VXLAN をイネーブルにします。
ステップ 3	<b>feature vn-segment-vlan-based</b>	VLAN の VN-Segment を有効にします。
ステップ 4	<b>feature interface-vlan</b>	Switch Virtual Interface (SVI) を有効にします。

	コマンドまたはアクション	目的
ステップ 5	<b>nv overlay evpn</b>	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



(注) ステップ 3 からステップ 6 は、VXLAN VNI の VLAN を設定するためのオプションであり、カスタム ルート識別子またはルート ターゲット要件（自動派生を使用しない）の場合にのみ必要です。

### 手順の概要

1. **vlan number**
2. **vn-segment number**
3. **evpn**
4. **vni number l2**
5. **rd auto**
6. **route-target both {auto | rt}**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>vlan number</b>	VLAN を指定します。
ステップ 2	<b>vn-segment number</b>	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。
ステップ 3	<b>evpn</b>	EVI (EVPN 仮想インスタンス) 設定モードを開始します。
ステップ 4	<b>vni number l2</b>	EVI のサービスインスタンス (VNI) を指定します。
ステップ 5	<b>rd auto</b>	MAC-VRF のルート識別子 (RD) を指定します。
ステップ 6	<b>route-target both {auto   rt}</b>	MACプレフィックスのインポートおよびエクスポートのルートターゲット (RT) を設定します。RT は、MAC-VRF ごとの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。RT を入力する場合は、ASN2:NN、ASN4:NN、または IPV4:NN の形式がサポートされます。  (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 と非対称 VNI では手動で設定されたルートターゲットが必要です。

## 新しい L3VNI モードの構成

### 新しい L3VNI モードの注意事項と制限事項

新しい L3VNI の PBR/NAT 構成の注意事項と制限事項：

- Cisco NX-OS リリース 10.2(3)F 以降、新しい L3VNI モードが Cisco Nexus 9300-X クラウドスケール スイッチでサポートされます。
- **interface vni** 構成はオプションです（PBR/NAT 機能が必要ない場合は不要です）。
- VRF-VNI-L3 の新しい構成は、暗黙的に L3VNI インターフェイスを作成します。デフォルトでは、show running コマンドには表示されません。



(注) **interface vni** を構成する前に、VRF-VNI-L3 が構成されていることを確認します。

- 次の構成は、**interface vni** で許可されます。
  - PBR/NAT
  - no interface vni
  - デフォルトのインターフェイス vni（これが存在する場合は、PBR/NAT 構成は削除されます）
- **interface vni** では **shut/no shut** コマンドは許可されていません。VRF で **shut/no shut** コマンドを実行すると、L3VNI で shut/no shut が実行されます。
- 新しい L3VNI 構成で **no feature nv overlay** を実行すると、VRF の下のすべての vrf-vni-l3 設定が削除され、PBR/NAT 設定があればクリーンアップされます。既存の VRF 設定は削除されません。
- VBU 構成の注意事項および制約事項：
  - 古い L3VNI モード構成と新しい L3VNI モード構成の両方を同じスイッチに共存させることができます。
  - VPC/VMCT システムの場合、ピア間で同じ VNI 構成モードが一貫している必要があります。
  - アップグレード後も、古い L3VNI 設定が有効です。

- Cisco NX-OS リリース 10.3(1)F 以降、新しい L3VNI の TRM サポートが Cisco Nexus 9300-X クラウドスケールスイッチで提供されます。
- 構成置換とロールバックがサポートされています。
- ISSU (ND) は、新しい L3VNI でサポートされています。
- 新しい L3VNI の PBR/NAT 設定には、次の注意事項と制限事項があります。
  - NAT 構成は、新しい **interface vni** に適用できます。
  - PBR カプセル化サイドポリシーは、カプセル化ノードインターフェイス SVI で既存のものとして設定されたままです。
  - 新しい L3VNI の PBR デキャップサイドポリシーが、対応する L3VNI の **interface vni** に適用されるようになりました。
  - 新しい L3VNI の PBR 構成構文は、SVI インターフェイスに似ています。
  - **no interface vni** は、最初に PBR/NAT 構成を削除してから、**interface vni** を削除します。
  - **no interface vni** は、VRF-VNI-L3 設定がまだ存在している限り、設定から CLI を削除するだけで、**interface vni** はバックエンドにまだ存在します。
- 新しい L3VNI モードでは、次の機能がサポートされています。
  - L3VNI を使用するリーフ/VTEP 機能
    - VXLAN EVPN
      - IR とマルチキャスト。
      - IGMP スヌーピング
      - vPC
      - 分散型エニーキャスト ゲートウェイ
    - MCT のない vPC
    - VXLAN マルチサイト
      - ボーダー リーフ、ボーダー スパイン、マルチサイト ボーダー ゲートウェイに関連した既存のすべてのシナリオに対応
      - エニーキャスト BGW および vPC BGW
    - DSVNI
    - VxLAN NGOAM
  - VXLAN でサポートされる機能 : PBR、NAT、および QoS
  - VXLAN アクセス機能 (QinVNI、SQinVNI、NIA、BUD-Node など)

- VXLAN ポート VLAN マッピング VXLAN 機能の 4K スケール L2VNI。
- L3VNI 構成の移行の注意事項および制約事項：
  - L3VNI 構成を古いものから新しいものに移行するには、次の手順を実行します。
    1. VLAN および `vlan-vnsegment` 構成を削除します。
    2. インターフェイス `nve1 member-vni-associate` 構成は保持します。
    3. SVI インターフェイスも保持できますが、PBR/NAT 構成はクリーンアップする必要があります。
    4. 新しい VRF-VNI-L3 構成を追加します。詳細については、[新しい L3VNI モードの構成 \(18 ページ\)](#) を参照してください。
  - L3VNI 設定を新しいものから古いものに移行するには、次の手順を実行します。
    1. 新しい VRF-VNI-L3 構成を削除します。
    2. VLAN および `vlan-vnsegment` 構成を作成します。
    3. インターフェイス `nve1 member-vni-associate` 構成を保持します。
    4. L3VNI の SVI 構成を作成します。
    5. VRF 構成の下に `member-vni` を追加します。
- アップグレードとダウンロードの注意事項と制約事項：
  - アップグレード：
    - 既存の L3VNI 設定はそのまま、機能し続けます。
    - VLAN の関連付けなしで、新しいキーワード **L3** を使用して追加の L3VNI を設定できます。
    - VLAN の関連付けなしで、既存の L3VNI 設定を新しい L3VNI に 1 つずつ移行することを選択できます。
    - 必要に応じて、新しい L3VNI 構成から古い L3VNI 構成に戻すことができます (VLAN 関連付けあり)。
    - ND ISSU は、新しい L3VNI の将来のリリースでサポートされます。
  - ダウングレード：
    - 新しい L3 VNI が設定されている場合は、ダウングレードを実行する前に、新しい L3VNI 設定を確認して無効にします。
    - ダウングレードは、すべての新しい L3VNI 設定を削除した後のみ許可されません。

## 新しい L3VNI モードの構成

この手順により、スイッチで新しい L3VNI モードが有効になります：

### 手順の概要

1. **configure terminal**
2. **vrf context** *vrf-name*
3. **vni number** **L3**
4. **member vni** *vni id* **associate-vrf**
5. (任意) **{ip | ipv6} policy route-map** *map-name*
6. (任意) **ip nat outside**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： switch# configure terminal switch(config)#	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	<b>vrf context</b> <i>vrf-name</i> 例： switch(config)# <b>vrf context</b> <b>vxlan-501</b>	VRF を設定します。
ステップ 3	<b>vni number</b> <b>L3</b> 例： switch(config)# <b>vni</b> <b>500001</b> <b>L3</b>	VNI を指定します。 <b>L3</b> は、新しい L3VNI モードを示す新しいキーワードです。
ステップ 4	<b>member vni</b> <i>vni id</i> <b>associate-vrf</b> 例： switch(config)# <b>interface</b> <b>nve1</b> switch(config-intf)# no shutdown switch(config-intf)# member vni 500001 associate-vrf	L3VNI を VRF に関連付けます。
ステップ 5	(任意) <b>{ip   ipv6} policy route-map</b> <i>map-name</i> 例： switch(config)# <b>interface</b> <b>vni</b> <b>500001</b> 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-intf)# <b>ip policy route-map</b> <b>IPV4_PBR_Appgroup</b> 例：	IPv4 または IPv6 ポリシーベース ルーティング用のルートマップを L3VNI インターフェイスに割り当てます。

	コマンドまたはアクション	目的
	IPv6 の場合 switch(config-intf)# <b>ipv6 policy route-map IPV6_PBR_Appgroup</b>	
ステップ 6	(任意) <b>ip nat outside</b> 例 : switch(config)# <b>interface vni 500001</b> switch(config-intf)# <b>ip nat outside</b>	NAT のルート マップを L3VNI インターフェイスに割り当てます。

## 新しい L3VNI モードの構成の確認

新しい L3VNI モード構成情報を表示するには、次のタスクのいずれかを実行します。

コマンド	目的
<b>show system internal ofm vni-intf</b>	新しい L3VNI モードに関する情報を表示します。
<b>Show system internal ofm event-history interface vni</b>	インターフェイスごとの VNI イベント トランザクション履歴を表示します。
<b>show vlan internal info extended-vlans</b>	VNI-Vlan ダンプの詳細を表示します
<b>show vlan internal info extended-vlan-sdb</b>	VNI-Vlan 共有 DB ダンプの詳細を表示します
<b>show system int l3vm sdb vrf</b>	VRF の状態と L3VM SDB の VRF tp VNI ID マッピングを表示します。
<b>Show nve vni</b>	対応する新しい l3vni 状態を表示します
<b>show system internal eltm info vlan all</b>	ELTM の BD 詳細を表示します
<b>show system internal iftmc info vlan all</b>	IFTMC の BD 詳細を表示します
<b>show system internal eltm info interface all</b>	ELTM の VNI インターフェイスの詳細を表示します
<b>show system internal iftmc info interface all</b>	IFTMC の VNI インターフェイスを表示します

## VXLAN ルーティングの VRF の設定

テナント VRF を設定します。



(注) ステップ 3～ステップ 6 は、VXLAN ルーティング用の VRF を設定するためのオプションであり、カスタム ルート識別子またはルート ターゲット要件（自動導出を使用しない）の場合にのみ必要です。

## 手順の概要

1. **vrf context** *vrf-name*
2. **vni** *number*
3. **rd** *auto*
4. **address-family** {*ipv4* | *ipv6*} **unicast**
5. **route-target** *both* {*auto* | *rt*}
6. **route-target** *both* {*auto* | *rt*} **evpn**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>vrf context</b> <i>vrf-name</i>	VRF を設定します。
ステップ 2	<b>vni</b> <i>number</i>	VNI を指定します。
ステップ 3	<b>rd</b> <i>auto</i>	IP-VRF のルート識別子 (RD) を指定します。
ステップ 4	<b>address-family</b> { <i>ipv4</i>   <i>ipv6</i> } <b>unicast</b>	IPv4 または IPv6 ユニキャストアドレスファミリーを設定します。
ステップ 5	<b>route-target</b> <i>both</i> { <i>auto</i>   <i>rt</i> }	IPv4 または IPv6 プレフィックスのインポートおよびエクスポートのルートターゲット (RT) を設定します。RT は、IP-VRF プレフィックス単位のインポート/エクスポートポリシーに使用されます。RT を入力する場合は、ASN2:NN、ASN4:NN、または IPV4:NN の形式がサポートされます。  (注) <b>auto</b> オプションの指定は IBGP のみに適用されます。  EBGP と非対称 VNI では手動で設定されたルートターゲットが必要です。
ステップ 6	<b>route-target</b> <i>both</i> { <i>auto</i>   <i>rt</i> } <b>evpn</b>	IPv4 または IPv6 プレフィックスのインポートおよびエクスポートのルートターゲット (RT) を設定します。RT は、VRF 単位の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。RT を入力する場合は、ASN2:NN、ASN4:NN、または IPV4:NN の形式がサポートされます。

	コマンドまたはアクション	目的
		<p>(注) <b>auto</b> オプションの指定は IBGP のみに適用されます。</p> <p>EBGP と非対称 VNI では手動で設定されたルート ターゲットが必要です。</p>

## VXLAN UDP 送信元 ポートの設定

VXLAN UDP 送信元ポートを設定します。

### 手順の概要

1. `[no] vxlan udp src-port [high |rfc |low]`

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<code>[no] vxlan udp src-port [high  rfc  low]</code>	<p>VXLAN カプセル化パケットの VxLAN UDP 送信元ポート番号範囲を選択できます。</p> <p><b>high</b> : このオプションは、ポート番号の範囲を 0x8000 ~ 0xFFFF に設定します。</p> <p><b>rfc</b> : Cisco NX-OS リリース 10.4(1)F 以降では、ポート番号の範囲を 0xC000 ~ 0xFFFF に設定する <b>rfc</b> オプションが提供されています。</p> <p>(注) <b>rfc</b> オプションは、Cisco Nexus C93300-H2R プラットフォームスイッチでのみ使用できます。</p> <p><b>low</b> : Cisco NX-OS リリース 10.4(1)F 以降では、ポート番号の範囲をデフォルト値 (1024 ~ 32K-1) に設定する <b>low</b> オプションが提供されています。これがデフォルトのオプションです。 <b>high</b> および <b>rfc</b> コマンドの <b>no</b> フォームは、<b>low</b> コマンドと同等です。</p> <p>(注) <b>low</b> オプションは、すべての Cisco Nexus 9000 シリーズプラットフォームスイッチすべてで利用可能です。</p>

## コア向け VXLAN ルーティングの SVI の設定

コア側の SVI VRF を設定します。

## 手順の概要

1. `vlan number`
2. `vn-segment number`
3. `interface vlan-number`
4. `mtu vlan-number`
5. `vrf member vrf-name`
6. `no {ip |ipv6} redirects`
7. `ip forward`
8. `ipv6 address use-link-local-only`

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<code>vlan number</code>	VLAN を指定します。
ステップ 2	<code>vn-segment number</code>	VXLAN VLAN でのレイヤ 3 VNI を設定するために VLAN を VXLAN VNI にマッピングします。
ステップ 3	<code>interface vlan-number</code>	VLAN インターフェイスを指定します。
ステップ 4	<code>mtu vlan-number</code>	MTU サイズ (バイト単位) <68-9216>..
ステップ 5	<code>vrf member vrf-name</code>	VRF に割り当てます。
ステップ 6	<code>no {ip  ipv6} redirects</code>	IPv4 および IPv6 の IP リダイレクトメッセージの送信を無効にします。
ステップ 7	<code>ip forward</code>	これは、インターフェイス VLAN に定義された IP アドレスがない場合であっても、スイッチによる IPv4 ベースのルックアップを有効にします。
ステップ 8	<code>ipv6 address use-link-local-only</code>	IPv6 転送を有効にします。  (注) IPv6 アドレスの <code>use-link-local-only</code> は、IPv4 の <code>IP FORWARD</code> と同じ役割を果たします。これは、インターフェイス VLAN に定義された IP アドレスがない場合であっても、スイッチによる IP ベースのルックアップを可能にします。

## コア向け VXLAN ルーティングの SVI の設定

分散デフォルト ゲートウェイとして機能するホストの SVI を設定します。

手順の概要

1. **fabric forwarding anycast-gateway-mac** *address*
2. **vlan** *number*
3. **vn-segment** *number*
4. **interface** *vlan-number*
5. **vrf member** *vrf-name*
6. **ip address** *address*
7. **fabric forwarding mode anycast-gateway**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>fabric forwarding anycast-gateway-mac</b> <i>address</i>	分散ゲートウェイの仮想 MAC アドレスを設定します。  (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。
ステップ 2	<b>vlan</b> <i>number</i>	VLAN を指定します。
ステップ 3	<b>vn-segment</b> <i>number</i>	vn-segment を指定します。
ステップ 4	<b>interface</b> <i>vlan-number</i>	VLAN インターフェイスを指定します。
ステップ 5	<b>vrf member</b> <i>vrf-name</i>	VRF に割り当てます。
ステップ 6	<b>ip address</b> <i>address</i>	IP アドレスを指定します。
ステップ 7	<b>fabric forwarding mode anycast-gateway</b>	VLAN コンフィギュレーション モードで SVI をユニキャスト ゲートウェイと関連付けます。

## マルチキャストを使用する NVE インターフェイスと VNI の設定

手順の概要

1. **interface** *nve-interface*
2. **source-interface** *loopback1*
3. **host-reachability protocol** *bgp*
4. **global mcast-group** *ip-address* {L2 | L3}
5. **member vni** *vni*
6. **mcast-group** *ip address*
7. **member vni** *vni associate-vrf*
8. **mcast-group** *address*

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>interface</b> <i>nve-interface</i>	NVE インターフェイスを設定します。
ステップ 2	<b>source-interface</b> <i>loopback1</i>	NVE 送信元インターフェイスを専用のループバックインターフェイスにバインドします。
ステップ 3	<b>host-reachability protocol</b> <i>bgp</i>	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 4	<b>global mcast-group</b> <i>ip-address</i> {L2   L3}	NVE インターフェイスごとに <i>mcast</i> グループをグローバルに (すべての VNI に対して) 設定します。これは、すべてのレイヤ 2 またはレイヤ 3 VNI に適用され、継承されます。  (注) レイヤ 3 <i>mcast</i> グループは、テナントルーテッドマルチキャスト (TRM) にのみ使用されます。
ステップ 5	<b>member vni</b> <i>vni</i>	レイヤ 2 VNI をトンネルインターフェイスに追加します。
ステップ 6	<b>mcast-group</b> <i>ip address</i>	<i>mcast group</i> を VNI 単位で設定します。レイヤ 2 VNI 固有の <i>mcast</i> グループを追加し、グローバルセットの設定を上書きします。  (注) <i>mcast</i> グループの代わりに、入力レプリケーションを設定できます。
ステップ 7	<b>member vni vni associate-vrf</b>	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 8	<b>mcast-group address</b>	<i>mcast group</i> を VNI 単位で設定します。レイヤ 3 VNI 固有の <i>mcast</i> グループを追加し、グローバルセットの設定を上書きします。

## NVE インターフェイスでの遅延タイマーの設定

NVE インターフェイスで遅延タイマーを構成すると、BGP は VRF ピアへのファブリックルートアドバタイズメントおよびファブリックへの VRF ピアルートを遅延させることができるため、スイッチのリロード後にボーダー リーフ ノードが起動したときに一時的なトラフィックドロップが発生しません。NX-OS ボーダー リーフおよび AnyCast ボーダー ゲートウェイでこのタイマーを構成します。

NVE インターフェイスの遅延タイマーの値は、NVE ピア、VNI、ルートなどのスケール値に依存します。構成するタイマー値を把握するには、リロード後に最後の NVE ピアをプログラムするのにかかった時間を調べ、それに 100 秒のバッファ時間を追加します。このバッファ時間は、ルートアドバタイズメントの時間も提供します。コマンドを使用して、インストールされている各 NVE ピアのタイムスタンプを表示します。 **show forwarding internal trace nve-peer-history**

また、このタイマーが構成されている場合でも、NX-OS ボードリーフでのファブリック分離のコンバージェンスは改善されません。

## 手順の概要

1. **configure terminal**
2. **interface nve nve-interface**
3. **fabric-ready time seconds**
4. **show nve interface nve1 detail**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b>	グローバル設定モードを開始します。
ステップ 2	<b>interface nve nve-interface</b>	NVE インターフェイスを設定します。
ステップ 3	<b>fabric-ready time seconds</b>	NVE インターフェイスの遅延タイマー値を指定します。デフォルト値は 135 秒です。
ステップ 4	<b>show nve interface nve1 detail</b>	構成されたタイマー値を表示します。

## VXLAN EVPN 入力複製の設定

VXLAN EVPN 入力複製において、VXLAN VTEP はネットワークにある他の VTEP の IP アドレスのリストを使用して、BUM（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）トラフィックを送信します。これらの IP アドレスは、BGP EVPN コントロールプレーンを通じて VTEP 間で交換されます。



(注) VXLAN EVPN 入力複製は次のものでサポートされます。

- Cisco Nexus シリーズ 9300 シリーズ スイッチ (7.0(3)I1(2) 以降)。
- Cisco Nexus シリーズ 9500 シリーズ スイッチ (7.0(3)I2(1) 以降)。

**開始する前:** 次の要件は、VXLAN EVPN 入力複製の設定前に課されるものです (7.0(3)I1(2) 以降)。

- VXLAN をイネーブル化します。

- VLAN および VXLAN VNI を設定します。
- VTEP で BGP を設定します。
- VXLAN ブリッジングのルート ターゲットおよび RD を設定します。

## 手順の概要

1. **interface nve-interface**
2. **host-reachability protocol bgp**
3. **global ingress-replication protocol bgp**
4. **member vni vni associate-vrf**
5. **member vni vni**
6. **ingress-replication protocol bgp**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>interface nve-interface</b>	NVE インターフェイスを設定します。
ステップ 2	<b>host-reachability protocol bgp</b>	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	<b>global ingress-replication protocol bgp</b>	ローカルとリモート VTEP の IP アドレスを VNI で交換して入力複製リストを作成するため、VTEP をグローバルに（すべての VNI に）イネーブル化にします。これにより VNI の BUM トラフィックの送受信が行えるようになります。  (注) ingress-replication プロトコルを使用して、bgp はアンダーレイの設定に必要な可能性のあるマルチキャストのニーズがなくなります。
ステップ 4	<b>member vni vni associate-vrf</b>	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 5	<b>member vni vni</b>	レイヤ 2 VNI をトンネルインターフェイスに追加します。
ステップ 6	<b>ingress-replication protocol bgp</b>	ローカルとリモートの IP アドレスを VNI で交換して入力複製リストを作成するため、VTEP をイネーブルにします。これにより VNI の BUM トラフィックの送受信が行えるようになり、グローバル設定をオーバーライドします。

	コマンドまたはアクション	目的
		<p>(注) 入力複製の代わりに、mcast グループを設定できます。</p> <p>(注) 確認するために <b>ingress-replication protocol bgp</b> アンダーレイの設定に必要なとなる可能性のあるマルチキャストは、すべて設定不要になります。</p>

## 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** *l2vpn evpn*
5. (任意) **Allowas-in**
6. **send-community** *extended*
7. **vrf** *vrf-name*
8. **address-family** *ipv4 unicast*
9. **advertise** *l2vpn evpn*
10. **maximum-paths** *path {ibgp}*
11. **address-family** *ipv6 unicast*
12. **advertise** *l2vpn evpn*
13. **maximum-paths** *path {ibgp}*

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>router bgp</b> <i>number</i>	BGP を設定します。
ステップ 2	<b>router-id</b> <i>address</i>	ルータ アドレスを指定します。
ステップ 3	<b>neighbor</b> <i>address remote-as number</i>	MPBGP 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	<b>address-family</b> <i>l2vpn evpn</i>	<p>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。</p> <p>(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</p>

	コマンドまたはアクション	目的
ステップ 5	(任意) <b>Allowas-in</b>	EBGP 展開の場合のみ：AS パスで重複する自律システム (AS) 番号を許可します。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 6	<b>send-community extended</b>	BGP ネイバーのコミュニティを設定します。
ステップ 7	<b>vrf vrf-name</b>	VRF を指定します。
ステップ 8	<b>address-family ipv4 unicast</b>	IPv4 のアドレス ファミリを設定します。
ステップ 9	<b>advertise l2vpn evpn</b>	<p>EVPN ルートのアドバタイジングをイネーブルにします。</p> <p>(注) Cisco NX-OS リリース 9.2(1) 以降、<b>advertise l2vpn evpn</b> コマンドは有効になりません。EVPN に対する VRF のアドバタイズメントを無効にするには、インターフェイス <b>nve1</b> で <b>no member vni vni associate-vrf</b> コマンドを入力して、NVE で VNI を無効にします。<b>vni</b> は、その特定の VRF に関連付けられた VNI です。</p>
ステップ 10	<b>maximum-paths path {ibgp}</b>	それぞれの VRF の IPv6 アドレス ファミリ内の EVPN 転送 IP プレフィックスに対して ECMP を有効にします。
ステップ 11	<b>address-family ipv6 unicast</b>	IPv6 のアドレス ファミリを設定します。
ステップ 12	<b>advertise l2vpn evpn</b>	<p>EVPN ルートのアドバタイジングをイネーブルにします。</p> <p>(注) EVPN に対する VRF のアドバタイズメントを無効にするには、インターフェイス <b>nve1</b> で <b>no member vni vni associate-vrf</b> コマンドを入力して、NVE で VNI を無効にします。<b>vni</b> は、その特定の VRF に関連付けられた VNI です。</p>
ステップ 13	<b>maximum-paths path {ibgp}</b>	それぞれの VRF の IPv6 アドレス ファミリ内の EVPN 転送 IP プレフィックスに対して ECMP を有効にします。

## スパインでの EVPN の iBGP の設定

### 手順の概要

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

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<code>router bgp autonomous system number</code>	BGP を指定します。
ステップ 2	<code>neighbor address remote-as number</code>	ネイバーを定義します。
ステップ 3	<code>address-family l2vpn evpn</code>	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 4	<code>send-community extended</code>	BGP ネイバーのコミュニティを設定します。
ステップ 5	<code>route-reflector-client</code>	ルートルフレクタとしてスパインを有効にします。
ステップ 6	<code>retain route-target all</code>	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。
ステップ 7	<code>address-family l2vpn evpn</code>	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	<code>disable-peer-as-check</code>	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。

	コマンドまたはアクション	目的
ステップ 9	<b>route-map permitall out</b>	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。

## スパインでの EVPN の eBGP 設定

### 手順の概要

1. **route-map NEXT-HOP-UNCH 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 NEXT-HOP-UNCH out**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>route-map NEXT-HOP-UNCH permit 10</b>	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。
ステップ 2	<b>set ip next-hop unchanged</b>	ネクストホップアドレスを設定します。  (注) 2つのネクストホップがイネーブルの場合、ネクストホップの順序は維持されません。  ネクストホップの1つが VXLAN ネクストホップであり、他のネクストホップが FIB/AM/Hmm 経由でローカルに到達可能な場合、FIB/AM/Hmm 経由で到達可能なローカルネクストホップは、順序に関係なく常に取得されます。  直接/ローカル接続ネクストホップは、常にリモート接続ネクストホップよりも優先されます。
ステップ 3	<b>router bgp <i>autonomous system number</i></b>	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 4	<b>address-family l2vpn evpn</b>	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	<b>retain route-target all</b>	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。
ステップ 6	<b>neighbor address remote-as number</b>	ネイバーを定義します。
ステップ 7	<b>address-family l2vpn evpn</b>	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	<b>disable-peer-as-check</b>	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。
ステップ 9	<b>send-community extended</b>	BGP ネイバーのコミュニティを設定します。
ステップ 10	<b>route-map NEXT-HOP-UNCH out</b>	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。

## ARP の抑制

ARP 抑制には、ハードウェアの ACL Ternary Content Addressable Memory (TCAM) リージョンのサイズ変更も含まれます。



(注) ACL TCAM リージョン設定の詳細については、『[Cisco Nexus 9000 Series NX-OS Security Configuration Guide](#)』の「[Configuring IP ACLs](#)」の章を参照してください。

### 手順の概要

1. **hardware access-list tcam region arp-ether size double-wide**
2. **interface nve 1**
3. **global suppress-arp**

4. **member vni vni-id**
5. **suppress-arp**
6. **suppress-arp disable**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>hardware access-list tcam region arp-ether size double-wide</b>	<p>ARP を抑制するための TCAM リージョンを設定します。</p> <p><i>tcam-size</i>—TCAM サイズ。サイズは 256 の倍数にする必要があります。サイズが 256 より大きい場合は、512 の倍数でなければなりません。</p> <p>(注) TCAM 設定を有効にするには、リロードが必要です。</p> <p>(注) <b>hardware access-list tcam region arp-ether size double-wide</b> コマンドの設定は、Cisco Nexus 9200、9300-EX、および 9300-FX/FX2/FX3 および 9300-GX プラットフォームスイッチでは必要ありません。</p>
ステップ 2	<b>interface nve 1</b>	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。
ステップ 3	<b>global suppress-arp</b>	NVE インターフェイス内のすべてのレイヤ 2 VNI に対して ARP をグローバルに抑制するように設定します。
ステップ 4	<b>member vni vni-id</b>	VNI ID を指定します。
ステップ 5	<b>suppress-arp</b>	レイヤ 2 VNI で ARP を抑制するように設定し、グローバル設定のデフォルトを上書きします。
ステップ 6	<b>suppress-arp disable</b>	特定の VNI での ARP 抑制のグローバル設定を無効にします。

## 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

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b>	コンフィギュレーション モードに入ります。
ステップ 2	<b>no nv overlay evpn</b>	EVPN コントロールプレーンをディセーブルにします。
ステップ 3	<b>no feature vn-segment-vlan-based</b>	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	<b>no feature nv overlay</b>	VXLAN 機能をディセーブルにします。
ステップ 5	(任意) <b>copy running-config startup-config</b>	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

## IP アドレスの場合 :

Cisco NX-OS は、IP 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、2つの VTEP の下で同時にホストが表示される場合、特定の期間 (秒) 内での移動回数に基づいた、IP アドレスの重複検出が行えます。

2つの VTEP の下でのホストの同時可用性は、IPv4 ホストの場合は 600 ミリ秒のリフレッシュタイムアウトで、IPv6 アドレスの場合はデフォルトのリフレッシュタイムアウトロジック (デフォルトは 3 秒) のホスト モビリティ ロジックによって検出されます。

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)。

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 24 時間以内に最大 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。 (**show fabric forwarding ip local-host-db vrf abc**)。

ホスト IP アドレスが永続的に固定されている場合は常に、HMM によって書き込まれた syslog メッセージ。

```
2021 Aug 26 01:08:26 leaf hmm: (vrf-name) [IPv4] Freezing potential duplicate host
20.2.0.30/32, reached recover count (5) threshold
```

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
<pre>switch(config)# fabric forwarding ? anycast-gateway-mac dup-host-ip-addr-detection</pre>	<p>使用可能なサブコマンド：</p> <ul style="list-style-type: none"> <li>• スイッチのエニーキャストゲートウェイ MAC。</li> <li>• n 秒以内の重複するホストアドレスを検出。</li> </ul>
<pre>switch(config)# fabric forwarding dup-host-ip-addr-detection ? &lt;1-1000&gt;</pre>	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。
<pre>switch(config)# fabric forwarding dup-host-ip-addr-detection 100 ? &lt;2-36000&gt;</pre>	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。
<pre>switch(config)# fabric forwarding dup-host-ip-addr-detection 100 10</pre>	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）。

#### MAC アドレスの場合：

Cisco NX-OS は、MAC アドレスの重複データ検出をサポートしています。これによって、特定の時間間隔（秒）での移動回数に基づいて、重複した MAC アドレスを検出できます。

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）。

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。（**show l2rib internal permanently-frozen-list**）。

MAC アドレスが永続的に固定されている場合は常に、L2RIB によって書き込まれた syslog メッセージ。

```
2017 Jul  5 10:27:34 leaf %$ VDC-1 %$ %USER-2-SYSTEM_MSG: Unfreeze limit (3) hit, MAC
0000.0033.3333in topo: 200 is permanently frozen - l2rib
2017 Jul  5 10:27:34 leaf %$ VDC-1 %$ %USER-2-SYSTEM_MSG: Detected duplicate host
0000.0033.3333, topology 200, during Local update, with host located at remote VTEP
1.2.3.4, VNI 2 - l2rib
2017 Jul  5 10:27:34 leaf %$ VDC-1 %$ %USER-2-SYSTEM_MSG: Unfreeze limit (3) hit, MAC
0000.0033.3334in topo: 200 is permanently frozen - l2rib
2017 Jul  5 10:27:34 leaf %$ VDC-1 %$ %USER-2-SYSTEM_MSG: Detected duplicate host
0000.0033.3334, topology 200, during Local update, with host 1
```

MACアドレスは、ローカルエントリとリモートエントリの両方が存在するまで、永久に凍結されたリストに残ります。

以下のコマンドの設定を解除しても、永久に凍結された機能が無効になることはなく、パラメーターがデフォルト値に変更されます。

- **l2rib dup-host-mac-detection**
- **l2rib dup-host-recovery**

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
<pre>switch(config)# l2rib dup-host-mac-detection ? &lt;1-1000&gt; default</pre>	<p>L2RIB で利用可能なサブコマンド：</p> <ul style="list-style-type: none"> <li>• 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。</li> <li>• デフォルト設定（180秒以内に 5つの移動）。</li> </ul>
<pre>switch(config)# l2rib dup-host-mac-detection 100 ? &lt;2-36000&gt;</pre>	<p>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。</p>
<pre>switch(config)# l2rib dup-host-mac-detection 100 10</pre>	<p>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）。</p>

## VXLAN BGP EVPN 設定の確認

VXLAN BGP EVPN の設定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
<b>show nve vrf</b>	VRF および関連する VNI を表示します。
<b>show bgp l2vpn evpn</b>	ルーティング テーブルの情報を表示します。
<b>show ip arp suppression-cache [detail   summary   vlan vlan   statistics ]</b>	ARP 抑制情報を表示します。
<b>show vxlan interface</b>	VXLAN インターフェイス ステータスを表示します。

コマンド	目的
<b>show vxlan interface   count</b>	VXLAN VLAN 論理ポート VP カウントを表示します。  (注) VP はポート単位、VLAN 単位で割り当てられます。すべての VXLAN 対応レイヤ 2 ポートについての全 VP の合計が、論理ポート VP カウントの合計になります。たとえば、レイヤ 2 トランク インターフェイスが 10 個で、それぞれ 10 個の VXLAN VLAN がある場合、トータルの VXLAN VLAN 論理ポート VP カウントは $10 \times 10 = 100$ です。
<b>show l2route evpn mac [all   evi evi [bgp   local   static   vxlan   arp]]</b>	レイヤ 2 ルート情報を表示します。
<b>show l2route evpn fl all</b>	すべての fl ルートを表示します。
<b>show l2route evpn imet all</b>	すべての imet ルートを表示します。
<b>show l2route evpn mac-ip all</b> <b>show l2route evpn mac-ip all detail</b>	すべての MAC IP ルートを表示します。
<b>show l2route topology</b>	レイヤ 2 ルートのトポロジを表示します。



(注) BGP 設定の確認には **show ip bgp** コマンドが利用可能ですが、ベストプラクティスとして好ましいのは、その代わりに **show bgp** コマンドを使用することです。

## ダウンストリーム VNI 設定による VXLAN EVPN の確認

ダウンストリーム VNI 設定情報で VXLAN EVPN 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
<b>show bgp evi l2-evi</b>	L2VNI に関連付けられている VRF を表示します。
<b>show forwarding adjacency nve platform</b>	対称および非対称 NVE 隣接の両方を、対応する DestInfoIndex とともに表示します。

コマンド	目的
<b>show forwarding route vrf vrf</b>	各ネクストホップの出力 VNI またはダウンストリーム VNI を表示します。
<b>show ip route detail vrf vrf</b>	各ネクストホップの出力 VNI またはダウンストリーム VNI を表示します。
<b>show l2route evpn mac-ip all detail</b>	リモート MAC ルートに存在するラベル付きネクストホップを表示します。
<b>show l2route evpn imet all detail</b>	リモートピアに関連付けられた出力 VNI を表示します。
<b>show nve peers control-plane-vni peer-ip ip-address</b>	各 NVE 隣接の出力 VNI またはダウンストリーム VNI を表示します。

次の例は、**show bgp evi l2-evi** コマンドのサンプル出力を示しています。

```
switch# show bgp evi 100
-----
L2VNI ID           : 100 (L2-100)
RD                 : 3.3.3.3:32867
Secondary RD       : 1:100
Prefixes (local/total) : 1/6
Created            : Jun 23 22:35:13.368170
Last Oper Up/Down  : Jun 23 22:35:13.369005 / never
Enabled            : Yes
Associated IP-VRF : vni100
Active Export RT list :
    100:100
Active Import RT list :
    100:100
```

次の例は、**show forwarding adjacency nve platform** コマンドのサンプル出力を示しています。

```
switch# show forwarding adjacency nve platform
slot 1
=====
IPv4 NVE adjacency information

next_hop:12.12.12.12 interface:nve1 (0x49000001) table_id:1
Peer_id:0x49080002 dst_addr:12.12.12.12 src_addr:13.13.13.13 RefCt:1 PBRct:0
Flags:0x440800
cp : TRUE, DCI peer: FALSE is_anycast_ip FALSE dsvni peer: FALSE
HH:0x7a13f DstInfoIndex:0x3002
tunnel init: unit-0:0x3 unit-1:0x0

next_hop:12.12.12.12 interface:nve1 (0x49000001) table_id:1
Peer_id:0x49080002 dst_addr:12.12.12.12 src_addr:13.13.13.13 RefCt:1 PBRct:0
Flags:0x10440800
cp : TRUE, DCI peer: FALSE is_anycast_ip FALSE dsvni peer: TRUE
HH:0x7a142 DstInfoIndex:0x3ffd
tunnel init: unit-0:0x6 unit-1:0x0
...
```

次の例は、**show forwarding route vrf vrf** コマンドのサンプル出力を示します。

```
switch# show forwarding route vrf vrf1000

slot 1
=====

IPv4 routes for table vrf1000/base

-----+-----+-----+-----+-----
Prefix      | Next-hop      | Interface    | Labels        | Partial Install
-----+-----+-----+-----+-----
....
10.1.1.11/32  12.12.12.12    nve1         dsvni: 301000
10.1.1.20/32  123.123.123.123 nve1         dsvni: 301000
10.1.1.21/32  30.30.30.30    nve1         dsvni: 301000
10.1.1.30/32  10.1.1.30      Vlan10
```

次の例は、**show ip route detail vrf vrf** コマンドのサンプル出力を示します。

```
switch# show ip route detail vrf default
IP Route Table for VRF "default"
  '*' denotes best ucast next-hop
  '**' denotes best mcast next-hop
  '[x/y]' denotes [preference/metric]
  '%<string>' in via output denotes VRF <string>

193.0.1.0/24, ubest/mbest: 4/0
  *via 30.1.0.2, Eth1/1, [100/0], 00:00:05, urib_dt6-client1 segid: 6544, tunnelid:
  0x7b9 encaps: VXLAN

  *via 30.1.1.2, Eth1/1, [100/0], 00:00:05, urib_dt6-client1 segid: 6545, (Asymmetric)
  tunnelid: 0x7ba encaps: VXLAN

  *via 30.1.2.2, Eth1/1, [100/0], 00:00:05, urib_dt6-client1 segid: 6546, (Asymmetric)
  tunnelid: 0x7bb encaps: VXLAN
```

次の例は、**show l2route evpn mac-ip all detail** コマンドのサンプル出力を示しています。

```
switch# show l2route evpn mac-ip all
Flags -(Rmac):Router MAC (Stt):Static (L):Local (R):Remote (V):vPC link
(Dup):Duplicate (Spl):Split (Rcv):Recv(D):Del Pending (S):Stale (C):Clear
(Ps):Peer Sync (Ro):Re-Originated (Orp):Orphan
Topology Mac Address      Host IP   Prod   Flags Seq No  Next-Hops
-----
5          0000.0005.1301  1.3.13.1 BGP    --    0      102.1.13.1 (Label: 2000005)
5          0000.0005.1401  1.3.14.1 BGP    --    0      102.1.145.1 (Label: 2000005)
```

次の例は、**show l2route evpn imet all detail** コマンドのサンプル出力を示しています。

```
switch# show l2route evpn imet all

Flags- (F): Originated From Fabric, (W): Originated from WAN

Topology ID VNI          Prod IP Addr      Flags
-----
3          2000003    BGP  102.1.13.1    -
3          2000003    BGP  102.1.31.1    -
3          2000003    BGP  102.1.32.1    -
3          2000003    BGP  102.1.145.1   -
```

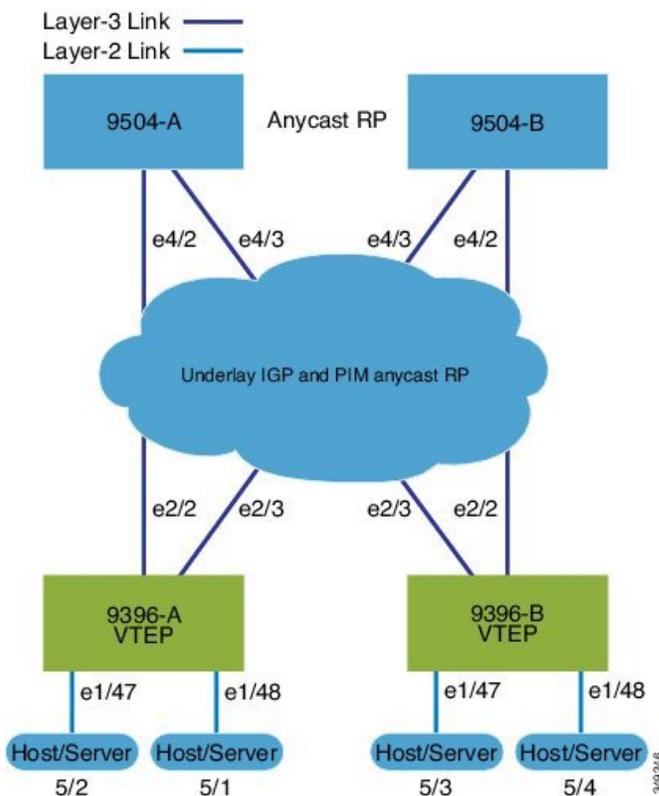
次の例は、**show nve peers control-plane-vni** コマンドのサンプル出力を示しています。この例では、3000003 がダウンストリーム VNI です。

```
switch# show nve peers control-plane-vni peer-ip 203.1.1.1
Peer      VNI      Learn-Source Gateway-MAC      Peer-type  Egress-VNI SW-BD  State
-----
203.1.1.1 2000003 BGP          f40f.1b6f.f8db   FAB        3000003  3005
peer-vni-add-complete
```

## VXLAN BGP EVPN の例 (IBGP)

VXLAN BGP EVPN の例 (IBGP)。

図 4: 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
feature pim
```

- ローカル ルータ ID、PIM、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
 ip pim sparse-mode
```

- 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
 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 router ospf 1 area 0.0.0.0
 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 224.0.0.0/4
ip pim anycast-rp 100.1.1.1 10.1.1.1
ip pim anycast-rp 100.1.1.1 20.1.1.1
```

- 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
 ip pim sparse-mode
 no shutdown
```

```
interface Ethernet4/3
 ip address 192.168.2.43/24
 ip router ospf 1 area 0.0.0.0
 ip pim sparse-mode
 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を有効にします。

```
nv overlay evpn
```

- 他のプロトコルを有効にします

```
feature ospf
feature bgp
feature pim
```

- ローカル ルータ ID、PIM、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
  ip pim sparse-mode
```

- 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
  ip pim sparse-mode
```

- AnycastRP 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
  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 224.0.0.0/4
ip pim anycast-rp 100.1.1.1 10.1.1.1
ip pim anycast-rp 100.1.1.1 20.1.1.1
```

- アンダーレイ ルーティングの 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 192.168.3.42/24
  ip router ospf 1 area 0.0.0.0
  ip pim sparse-mode
```

```

no shutdown

interface Ethernet4/3
ip address 192.168.4.43/24
ip router ospf 1 area 0.0.0.0
ip pim sparse-mode
no shutdown

```

- 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 pim
feature interface-vlan

```

- BGP EVPN を使用して分散型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

```

- 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 ルータ ID、PIM、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
ip pim sparse-mode

```

- 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
ip pim sparse-mode
```

- 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
ip pim sparse-mode
no shutdown
```

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

- ホスト SVI (サイレント ホスト) を再配布するためのルートマップを設定します

```
route-map HOST-SVI permit 10
match tag 54321
```

- PIM RP を設定します。

```
ip pim rp-address 100.1.1.1 group-list 224.0.0.0/4
```

- VLAN の作成

```
vlan 1001-1002
```

- 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
```

- 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
```

- VXLAN ルーティングのコア向け SVI を設定します

```
interface v1an101
no shutdown
vrf member vxlan-900001
ip forward
no ip redirects
ipv6 address use-link-local-only
no ipv6 redirects
```

- 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
rd auto

```



- (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設定されます。

```

\
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、分散型エニーキャスト 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 tag 54321
ipv6 address 4:1:0:1::1/64 tag 54321
fabric forwarding mode anycast-gateway

interface vlan1002
no shutdown
vrf member vxlan-900001
ip address 4.2.2.1/24 tag 54321
ipv6 address 4:2:0:1::1/64 tag 54321
fabric forwarding mode anycast-gateway

```

- ARP 抑制用の ACL TCAM リージョンを設定します。



- (注) **hardware access-list tcam region arp-ether 256 double-wide** コマンドは、Cisco Nexus 9300-EX および 9300-FX/FX2/FX3 および 9300-GX プラットフォーム スイッチでは必要ありません。

```

hardware access-list tcam region arp-ether 256 double-wide

```



- (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。簡易設定モードを活用するには、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 900001 associate-vrf
member vni 2001001
mcast-group 239.0.0.1
member vni 2001002
mcast-group 239.0.0.1
```

#### オプション2

```
interface nve1
source-interface loopback1
host-reachability protocol bgp
global mcast-group 239.0.0.1 L2
member vni 2001001
member vni 2001002
member vni 2001007-2001010
```

- 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
switchport access vlan 1002

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

- 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
    redistribute direct route-map HOST-SVI
  address-family ipv6 unicast
    redistribute direct route-map HOST-SVI
```



(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 12
  vni 2001002 12
```



(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設定されます。

```
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、自動的に設定されます。



(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 12
    rd auto
    route-target import auto
    route-target export auto
  vni 2001002 12
    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 pim
feature interface-vlan
```

- 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
```

- アンダーレイルーティングの OSPF の有効化

```
router ospf 1
```

- ローカル ルータ ID、PIM、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
 ip pim sparse-mode
```

- 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
 ip pim sparse-mode
```

- 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 192.168.3.22/24
 ip router ospf 1 area 0.0.0.0
 ip pim sparse-mode
 no shutdown
```

```
interface Ethernet2/3
 no switchport
 ip address 192.168.4.23/24
 ip router ospf 1 area 0.0.0.0
 ip pim sparse-mode
 shutdown
```

- ホスト SVI (サイレント ホスト) を再配布するためのルートマップを設定します

```
route-map HOST-SVI permit 10
 match tag 54321
```

- PIM RP を設定します。

```
ip pim rp-address 100.1.1.1 group-list 224.0.0.0/4
```

- VLAN の作成

```
vlan 1001-1002
```

- 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
```

- VXLAN ルーティングのコア向け SVI を設定します

```
interface vlan101
  no shutdown
  vrf member vxlan-900001
  ip forward
  no ip redirects
  ipv6 address use-link-local-only
  no ipv6 redirects
```

- 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
  rd auto
```



(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設定されます。

```
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
```

- ARP 抑制用の ACL TCAM リージョンを設定します。



- (注) **hardware access-list tcam region arp-ether 256 double-wide** コマンドは、Cisco Nexus 9300-EX および 9300-FX/FX2/FX3 および 9300-GX プラットフォーム スイッチでは必要ありません。

```
hardware access-list tcam region arp-ether 256 double-wide
```



- (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。簡易設定モードを活用するには、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 900001 associate-vrf
  member vni 2001001
    mcast-group 239.0.0.1
  member vni 2001002
    mcast-group 239.0.0.1
```

オプション 2

```
interface nve1
  interface nve1
  source-interface loopback1
  host-reachability protocol bgp
  global mcast-group 239.0.0.1 L2
  member vni 2001001
  member vni 2001002
  member vni 2001007-2001010
```

- 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
  switchport access vlan 1002
```

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

- BGP を設定します。

```
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
vrf vxlan-900001
  address-family ipv4 unicast
  redistribute direct route-map HOST-SVI
  address-family ipv6 unicast
  redistribute direct route-map HOST-SVI
```



- (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 12
  vni 2001002 12
```



- (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設定されます。

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



- (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 12
  rd auto
  route-target import auto
  route-target export auto
  vni 2001002 12
  rd auto
  route-target import auto
  route-target export auto
```

- ボーダーゲートウェイ (BGW) でインターフェイスVLANを設定します。

```
interface vlan101
  no shutdown
  vrf member evpn-tenant-3103101
  no ip redirects
  ip address 101.1.0.1/16
  ipv6 address cafe:101:1::1/48
  no ipv6 redirects
  fabric forwarding mode anycast-gateway
```



- (注) BGW間にIBGPセッションがあり、EBGPファブリックが使用されている場合は、ローカルVIPまたはVIP\_Rが（リロードまたはファブリックリンクフラップが原因で）ダウンしているときに、より高いAS-PATHでVIPまたはVIP\_Rルートアドバタイズメントを作成するようにルートマップを設定する必要があります。次に route-map 設定例を示します。この例では、192.0.2.1がVIPアドレスで、198.51.100.1が同じBGWサイトから学習したBGP VIPルートのネクストホップです。

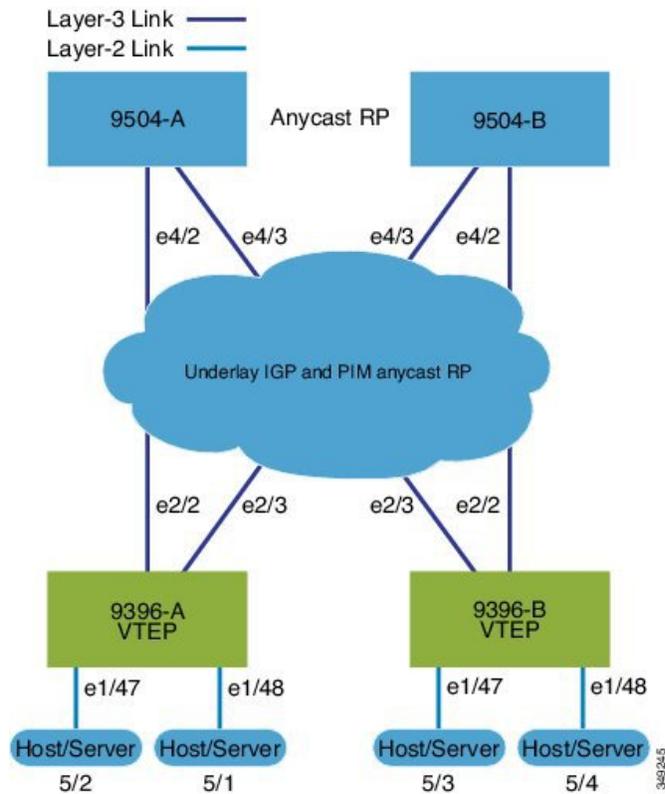
```
ip prefix-list vip_ip seq 5 permit 192.0.2.1/32
ip prefix-list vip_route_nh seq 5 permit 198.51.100.1/32

route-map vip_ip permit 5
  match ip address prefix-list vip_ip
  match ip next-hop prefix-list vip_route_nh
  set as-path prepend 5001 5001 5001
route-map vip_ip permit 10
```

## VXLAN BGP EVPN の例 (EBGP)

VXLAN BGP EVPN の例 (EBGP)。

図 5: 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 ルータ ID、PIM、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 tag 12345
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 tag 12345
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 224.0.0.0/4
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 NEXT-HOP-UNCH permit 10
  set ip next-hop unchanged
```

- ループバックを再配布するためのルートマップの設定

```
route-map LOOPBACK permit 10
  match tag 12345
```

- 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 NEXT-HOP-UNCH
    retain route-target all
  neighbor 30.1.1.1 remote-as 200
  update-source loopback0
  ebgp-multihop 3
  address-family l2vpn evpn
    send-community both
    disable-peer-as-check
    route-map NEXT-HOP-UNCH out
  neighbor 40.1.1.1 remote-as 200
  update-source loopback0
  ebgp-multihop 3
  address-family l2vpn evpn
    send-community both
    disable-peer-as-check
    route-map NEXT-HOP-UNCH out
```

- IPv4 ユニキャスト アドレス ファミリの BGP アンダーレイを設定します。

```
address-family ipv4 unicast
  redistribute direct route-map LOOPBACK
  neighbor 192.168.1.22 remote-as 200
  update-source ethernet4/2
  address-family ipv4 unicast
    allowas-in
```

```

    disable-peer-as-check
neighbor 192.168.2.23 remote-as 200
    update-source ethernet4/3
    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 ルータ ID、PIM、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 tag 12345
    ip pim sparse-mode
```

- AnycastRP のループバックを設定します

```
interface loopback1
    ip address 100.1.1.1/32 tag 12345
    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 224.0.0.0/4
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 NEXT-HOP-UNCH permit 10
    set ip next-hop unchanged
```

- ループバックを再配布するためのルートマップの設定

```
route-map LOOPBACK permit 10
    match tag 12345
```

- 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
    no switchport
    ip address 192.168.3.42/24
    ip router ospf 1 area 0.0.0.0
    ip pim sparse-mode
```

```

no shutdown

interface Ethernet4/3
no switchport
ip address 192.168.4.43/24
ip router ospf 1 area 0.0.0.0
ip pim sparse-mode
shutdown

```

- EVPN アドレス ファミリの 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
next-hop route-map NEXT-HOP-UNCH
retain route-target all
neighbor 30.1.1.1 remote-as 200
update-source loopback0
ebgp-multihop 3
address-family l2vpn evpn
send-community both
disable-peer-as-check
route-map NEXT-HOP-UNCH out
neighbor 40.1.1.1 remote-as 200
update-source loopback0
ebgp-multihop 3
address-family l2vpn evpn
send-community both
disable-peer-as-check
route-map NEXT-HOP-UNCH out

```

- IPv4 ユニキャスト アドレス ファミリの BGP アンダーレイを設定します。

```

address-family ipv4 unicast
redistribute direct route-map LOOPBACK
neighbor 192.168.3.22 remote-as 200
update-source ethernet4/2
address-family ipv4 unicast
allowas-in
disable-peer-as-check
neighbor 192.168.4.43 remote-as 200
update-source ethernet4/3
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
```

- 関連プロトコルを有効にします。

```
feature bgp
feature pim
```

```
feature interface-vlan
```

- BGP EVPN を使用して分散ユニキャスト 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
```

- 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 ルータ ID、PIM、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 pim sparse-mode
```

- VTEP のループバックを設定します。

```
interface loopback1
 ip address 33.1.1.1/32
 ip pim sparse-mode
```

- Spine-leaf interconnect 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 pim sparse-mode
 no shutdown
```

```
interface Ethernet2/3
 no switchport
 ip address 192.168.4.23/24
 ip pim sparse-mode
 shutdown
```

- Host-SVI (サイレントホスト) を再配布するようにルートマップを設定します。

```
route-map HOST-SVI permit 10
 match tag 54321
```

- PIM RP を有効にします。

```
ip pim rp-address 100.1.1.1 group-list 224.0.0.0/4
```

- VLAN を作成します。

```
vlan 1001-1002
```

- 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
```

- VXLAN ルーティングのコア向け SVI を設定します。

```
interface vlan101
no shutdown
vrf member vxlan-900001
ip forward
no ip redirects
ipv6 address use-link-local-only
no ipv6 redirects
```

- 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
rd auto
```



- (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設定されます。

```
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 tag 54321
ipv6 address 4:1:0:1::1/64 tag 54321
fabric forwarding mode anycast-gateway

interface vlan1002
no shutdown
vrf member vxlan-900001
ip address 4.2.2.1/24 tag 54321
ipv6 address 4:2:0:1::1/64 tag 54321
fabric forwarding mode anycast-gateway
```

- ARP 抑制用の ACL TCAM リージョンを設定します。



- (注) **hardware access-list tcam region arp-ether 256 double-wide** コマンドは、Cisco Nexus 9300-EX および 9300-FX/FX2/FX3 および 9300-GX プラットフォーム スイッチでは必要ありません。

```
hardware access-list tcam region arp-ether 256 double-wide
```



- (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。簡易設定モードを活用するには、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 900001 associate-vrf
  member vni 2001001
    mcast-group 239.0.0.1
  member vni 2001002
    mcast-group 239.0.0.1
```

オプション 2

```
interface nve1
  source-interface loopback1
  host-reachability protocol bgp
  global mcast-group 239.0.0.1 L2
  member vni 2001001
  member vni 2001002
  member vni 2001007-2001010
```

- 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
  switchport access vlan 1002
```

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

- IPv4 ユニキャスト アドレス ファミリの BGP アンダーレイを設定します。

```
router bgp 200
  router-id 30.1.1.1
  address-family ipv4 unicast
    redistribute direct route-map LOOPBACK
  neighbor 192.168.1.42 remote-as 100
  update-source ethernet2/2
  address-family ipv4 unicast
    allowas-in
    disable-peer-as-check
  neighbor 192.168.4.43 remote-as 100
  update-source ethernet2/3
  address-family ipv4 unicast
    allowas-in
    disable-peer-as-check
```

- EVPN アドレス ファミリ用の BGP オーバーレイを設定します。

```
address-family l2vpn evpn
  nexthop route-map NEXT-HOP-UNCH
  retain route-target all
neighbor 10.1.1.1 remote-as 100
update-source loopback0
ebgp-multihop 3
address-family l2vpn evpn
  send-community both
  disable-peer-as-check
  route-map NEXT-HOP-UNCH out
neighbor 20.1.1.1 remote-as 100
update-source loopback0
ebgp-multihop 3
address-family l2vpn evpn
  send-community both
  disable-peer-as-check
  route-map NEXT-HOP-UNCH out
vrf vxlan-900001
```



- (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 12
  vni 2001002 12
```



- (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設定されます。

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



(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 12
  rd auto
  route-target import auto
  route-target export auto
 vni 2001002 12
  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を有効にします。

```
nv overlay evpn
```

- 関連プロトコルを有効にします。

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

- 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
```

- 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
```

- ローカルルータ ID、PIM、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 pim sparse-mode
```

- VTEP のループバックを設定します。

```
interface loopback1
 ip address 44.1.1.1/32
 ip pim sparse-mode
```

- Spine-leaf interconnect のインターフェイスを設定します。

```
interface Ethernet2/2
 no switchport
 ip address 192.168.3.22/24
 ip pim sparse-mode
 no shutdown
```

```
interface Ethernet2/3
 no switchport
```

```
ip address 192.168.2.23/24
ip pim sparse-mode
shutdown
```

- Host-SVI (サイレントホスト) を再配布するようにルートマップを設定します。

```
route-map HOST-SVI permit 10
match tag 54321
```

- PIM RP をイネーブルにします。

```
ip pim rp-address 100.1.1.1 group-list 224.0.0.0/4
```

- VLAN の作成

```
vlan 1001-1002
```

- 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
```

- VXLAN ルーティングのコア向け SVI を設定します。

```
interface vxlan101
no shutdown
vrf member vxlan-900001
ip forward
no ip redirects
ipv6 address use-link-local-only
no ipv6 redirects
```

- 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
rd auto
```



(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。

```
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、分散型エニーキャスト 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 tag 54321
  ipv6 address 4:1:0:1::1/64 tag 54321
  fabric forwarding mode anycast-gateway
```

```
interface vlan1002
  no shutdown
  vrf member vxlan-900001
  ip address 4.2.2.1/24 tag 54321
  ipv6 address 4:2:0:1::1/64 tag 54321
  fabric forwarding mode anycast-gateway
```

- ARP 抑制用の ACL TCAM リージョンを設定します。



(注) **hardware access-list tcam region arp-ether 256 double-wide** コマンドは、Cisco Nexus 9300-EX および 9300-FX/FX2/FX3 および 9300-GX プラットフォーム スイッチでは必要ありません。

```
hardware access-list tcam region arp-ether 256 double-wide
```



(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。簡易設定モードを活用するには、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 900001 associate-vrf
  member vni 2001001
    mcast-group 239.0.0.1
  member vni 2001002
    mcast-group 239.0.0.1
```

オプション 2

```
interface nve1
  source-interface loopback1
  host-reachability protocol bgp
  global mcast-group 239.0.0.1 L2
  member vni 2001001
  member vni 2001002
  member vni 2001007-2001010
```

- 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
  switchport access vlan 1002

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

- IPv4 ユニキャスト アドレス ファミリの BGP アンダーレイを設定します。

```
router bgp 200
  router-id 40.1.1.1
  address-family ipv4 unicast
    redistribute direct route-map LOOPBACK
  neighbor 192.168.3.42 remote-as 100
  update-source ethernet2/2
  address-family ipv4 unicast
    allowas-in
    disable-peer-as-check
  neighbor 192.168.2.43 remote-as 100
  update-source ethernet2/3
  address-family ipv4 unicast
    allowas-in
    disable-peer-as-check
```

- EVPN アドレス ファミリ用の BGP オーバーレイを設定します。

```
address-family l2vpn evpn
  nexthop route-map NEXT-HOP-UNCH
  retain route-target all
neighbor 10.1.1.1 remote-as 100
update-source loopback0
ebgp-multihop 3
address-family l2vpn evpn
  send-community both
  disable-peer-as-check
  route-map NEXT-HOP-UNCH out
neighbor 20.1.1.1 remote-as 100
update-source loopback0
ebgp-multihop 3
address-family l2vpn evpn
  send-community both
  disable-peer-as-check
  route-map NEXT-HOP-UNCH out
vrf vxlan-900001
```



(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 12
vni 2001002 12
```



(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設定されます。

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



(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 12
rd auto
route-target import auto
route-target export auto
vni 2001002 12
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          State LearnType Uptime   Router-Mac
-----
nve1      30.1.1.1                Up      CP          00:00:38 6412.2574.9f27
```

### • show nve vni

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

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]
nve1      2001002          225.4.0.1       Up   CP   L2 [1002]
```

### • show ip arp suppression-cache detail

```

9396-B# show ip arp suppression-cache detail

Flags: + - Adjacencies synced via CFSOE
      L - Local Adjacency
      R - Remote Adjacency
      L2 - Learnt over L2 interface

Ip Address      Age      Mac Address      Vlan Physical-ifindex  Flags
-----
4.1.1.54        00:06:41 0054.0000.0000 1001 Ethernet1/48        L
4.1.1.51        00:20:33 0051.0000.0000 1001 (null)              R
4.2.2.53        00:06:41 0053.0000.0000 1002 Ethernet1/47        L
4.2.2.52        00:20:33 0052.0000.0000 1002 (null)              R

```



(注) **show vxlan interface** コマンドは、Cisco Nexus 99300-EX、9300-FX/FX2/FX3、および9300-GXプラットフォームスイッチではサポートされません。

#### • 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
leaf3#

```

#### • 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
```

## ND 抑制の構成

### オーバーレイの ND 抑制

ホストが2つの異なる VXLAN ピアの背後にある場合、ホストから別のホストへのマルチキャスト ネイバー要請パケットは、BGP/EVPN VXLAN コアを介してフラッディングされます。

ND 抑制キャッシュは、以下によって構築されます。

- ホストで NS 要求をスヌーピングし、要求のソース IP および MAC バインディングを ND 抑制キャッシュに取り込みます。
- BGP EVPN MAC ルート アドバタイズメントによる IPv6-Host または MAC アドレス情報の学習

ND 抑制を使用すると、2つの異なる VXLAN ピアの背後にあるホスト間通信の場合、リモートホストが抑制キャッシュで最初に学習されない場合、NS パケットは BGP/EVPN VXLAN コアを介してフラッディングされます。ただし、スイッチ S1 の ND 抑制キャッシュにリモートホストが読み込まれると、S1 の背後にあるホストのリモートホストに対する後続のすべての近隣要請要求パケットがスイッチ S1 によってプロキシされ、BGP-EVPN/VXLAN コア上の近隣要請パケットのフラッディングが防止されます。

ND 抑制キャッシュスケール値については、『Cisco Nexus 9000 シリーズ NX-OS 検証済みスケラビリティガイド』を参照してください。

### ND 抑制の注意事項および制限事項

ND 抑制には以下のような構成の注意事項および制限事項があります。

- Cisco NX-OS リリース 10.3 (1) F 以降、Cisco Nexus 9300-X クラウドスケール スイッチは、プレーン BGP EVPN でのみ ND 抑制機能をサポートします。
  - ND 抑制は、マルチサイト、仮想 MCT、IRB、集中型ゲートウェイ、ファイアウォールクラスタリング、vPC などの BGP-EVPN 機能バリエーションではサポートされていません。
  - ホストのリンク ローカルアドレスの場合、ND 抑制はサポートされておらず、代わりにホストのリンク ローカルアドレスのマルチキャスト NS が BGP EVPN VXLAN ネットワークのコアにフラッディングされます。
  - ND 抑制は、`suppress-arp` が有効になっているすべての VNI で有効になります。
  - ND Suppression CLI ノブは、次の条件下でのみ有効にする必要があります。
    - `suppress-arp` は VNI で有効にする必要があります、この VNI/VLAN に関連付けられた SVI が存在する必要があります。また、この SVI はアップ状態である必要があります、IPv4 と IPv6 の両方のアドレスが有効になっている必要があります。
    - ND 抑制は、次の条件では機能しません。
      - SVI が、`suppress-arp/suppress nd` が有効になっている VLAN/VNI に存在しない場合。
      - `suppress-arp/suppress-nd` が有効になっている VLAN VNI に関連付けられた SVI がダウンしている場合。
      - `suppress-arp/suppress-nd` が有効になっている VLAN/VNI に関連付けられた SVI に IPv4 アドレスのみがあり、IPv6 アドレスがない場合。
      - `suppress-arp/suppress-nd` が有効になっている VLAN/VNI に関連付けられた SVI に IPv6 アドレスのみがあり、IPv4 アドレスがない場合。
- 上記のすべての条件では、ホスト間のトラフィックがドロップされる可能性があります。
- ND 抑制 VACL を機能させるには、`hardware access-list tcam region sup-tcam 768` コマンドを使用して、SUP TCAM サイズを 768 以上に増やします。

## ND 抑制の構成

この手順では、NVE インターフェイスで ND 抑制機能を有効または無効にする方法について説明します。

### 始める前に

ARP 抑制が有効になっていることを確認します。

### 手順の概要

#### 1. configure terminal

2. **hardware access-list tcam region ing-sup 768**
3. **copy running-config startup-config**
4. **reload**
5. **configure terminal**
6. **interface nve 1**
7. **[no]suppress nd**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： switch# <b>configure terminal</b>	グローバル構成モードを開始します。
ステップ 2	<b>hardware access-list tcam region ing-sup 768</b> 例： switch# <b>hardware access-list tcam region ing-sup 768</b>	入力 SUP TCAM サイズを 768 に分割します。
ステップ 3	<b>copy running-config startup-config</b> 例： switch# <b>copy running-config startup-config</b>	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 4	<b>reload</b> 例： switch# <b>reload</b>	スイッチをリロードします。
ステップ 5	<b>configure terminal</b> 例： switch# <b>configure terminal</b>	グローバル構成モードを開始します。
ステップ 6	<b>interface nve 1</b> 例： switch(config)# <b>interface nve 1</b> switch(config-if-nve)#	interface nve 構成モードを開始します。
ステップ 7	<b>[no]suppress nd</b> 例： switch(config-if-nve)# <b>suppress nd</b>	すべての ARP 対応 VNI の ND 抑制を構成します。 オプション no は、すべての ARP 対応 VNI の ND 抑制を無効にします。



- (注)
- グローバル **suppress arp** コマンドを構成すると、すべての VNI で ND 抑制が有効になります。
  - グローバル **suppress arp** コマンドが構成されておらず、代わりに VNI ごとに **suppress arp** コマンドが構成されている場合、ARP 抑制が構成されているすべての VNI で ND 抑制が有効になります。
  - vPC ペアで **suppress arp** コマンドを有効にする場合は、機能を有効にする前に、両方のピアで手順 1 ~ 4 が完了していることを確認してください。

## ND 抑制構成の確認

ND 抑制構成情報を表示するには、次のコマンドのいずれかを入力します。

コマンド	目的
<b>show run nv overlay</b>	ND 抑制構成ステータスを表示します。
<b>show nve vni</b>	ARP が有効な VNI に対して ND 抑制構成が有効になっているかどうかを表示します。
<b>show nve internal export nve</b>	SDB で ND 抑制構成が有効になっているかどうかを表示します。
<b>show nve internal export vni</b>	SDB の VNI ごとの ND 抑制状態を表示します。
<b>show ipv6 nd suppression-cache detail</b> コマンド。	ローカルに存在する ICMPv6 キャッシュ エントリを表示します。
<b>show ipv6 nd suppression-cache remote</b>	リモートに存在する ICMPv6 キャッシュ エントリを表示します。
<b>show ipv6 nd suppression-cache summary</b>	ローカルとリモートの両方の IPv6 キャッシュ エントリの概要を表示します。
<b>show ipv6 nd suppression-cache statistics</b>	IPv6 ND 抑制キャッシュの統計情報を表示します。
<b>show ipv6 nd suppression-cache vlan "vlan_id"</b>	特定の VLAN の IPv6 ND 抑制キャッシュ エントリの詳細を表示します。

次の例は、**show run nv overlay** コマンドのサンプル出力を示しています。

```
switch(config-if-nve)# sh run nv overlay
!Command: show running-config nv overlay
!Running configuration last done at: Sat Mar 19 01:07:49 2022
!Time: Sat Mar 19 01:10:00 2022
```

```

version 10.2(3) Bios:version 07.68
feature nv overlay

vlan 101-110,200-203,500-501

interface nve1
  no shutdown
  host-reachability protocol bgp
  suppress nd
  global suppress-arp

```

次の例は、**show nve vni** コマンドのサンプル出力を示しています。

```

switch(config-if-nve-vni)# sh nve vni
Codes: CP - Control Plane      DP - Data Plane
       UC - Unconfigured      SA - Suppress ARP
       S-ND Suppress ND
       SU - Suppress Unknown Unicast
       Xconn - Crossconnect
       MS-IR - Multisite Ingress Replication
       HYB - Hybrid IRB mode

```

Interface	VNI	Multicast-group	State	Mode	Type [BD/VRF]	Flags
nve1	5000	239.2.0.2	Up	CP	L2 [500]	SA S-ND

次の例は、**show nve internal export nve** コマンドのサンプル出力を示しています。

```

switch(config-if-nve-vni)# sh nve internal export nve

NVE Interface information.
+-----+
Interface: nve1, Admin State: Up,
  State: nve-intf-add-complete, Encap: vxlan
  Source interface: loopback3, VRF: default,
  Anycast-interface: <none>
  Mcast-routing src intf <none>
  Primary IP: 4.4.4.4, Secondary IP: 0.0.0.0,
  VNI-VRF: default, Allow-Src-Lpbk-Down: No,
  Advertise MAC route: No,
  Virtual-rMAC: 0000.0000.0000,
  Mcast-routing Primary IP: 0.0.0.0
  Suppress ND: 1
  Host-reachability: CP
  unknown-peer-forwarding-mode: disable
  VNI assignment mode: n/a
  Multisite bgw-if: <none> (ip: 0.0.0.0, admin/oper state: Down/Down)
  src-node-last-notify: None
  anycast-node-last-notify: None
  mcast-src-node-last-notify: None
  multi-src-node-last-notify: None

```

次の例は、**show nve internal export vni** コマンドのサンプル出力を示しています。

```

switch(config-if-nve-vni)# sh nve internal export vni

NVE VNI Information.
+-----+
VNI: 5000 [500] Mgroup: 239.2.0.2 Provision-State: vni-add-complete
  Primary: 4.4.4.4 Secondary: 0.0.0.0 SRC-VRF: default
  Encap: vxlan Repl-mode: Mcast
  Suppress ARP: SP Suppress ND: Enabled Mode: CP, VNI-VRF: <FALSE> [vrf-id 0] [vrf flags]

```

```

0x0]
  Suppress Unknown-Unicast: FALSE
  X-connect : Disabled
  [VNI local configs] SA : TRUE, Mcast-group : TRUE, IR proto BGP: FALSE
  Config Src: CLI, VNI flags: 0x0
  Spine-AGW: Disabled, HYBRID: Disabled
  Multisite optimized IR: Disabled
  Multisite DCI Group Unknown Address

```

次の例は、**show ipv6 nd suppression-cache detail** コマンドのサンプル出力を示しています。

```
switch(config)# show ipv6 nd suppression-cache detail
```

```

Flags: + - Adjacencies synced via CFSOE
        L - Local Adjacency
        R - Remote Adjacency
        L2 - Learnt over L2 interface
        PS - Added via L2RIB, Peer Sync
        RO - Dervied from L2RIB Peer Sync Entry

```

IPv6 Address Addr	Age	Mac Address	Vlan	Physical-ifindex	Flags	Remote Vtep
172:11:1:1::51	00:00:18	acf2.c5f6.7641	11	Ethernet1/51	L	
172:11:1:1::201	00:06:14	0000.0011.1111	11	(null)	R	30.100.1.1
172:11:1:1::101	00:06:14	74a0.2f1d.d481	11	(null)	R	10.10.11.11

次の例は、**show ipv6 nd suppression-cache local** コマンドのサンプル出力を示しています。

```
switch(config)# show ipv6 nd suppression-cache local
```

```

Flags: + - Adjacencies synced via CFSOE
        L - Local Adjacency
        R - Remote Adjacency
        L2 - Learnt over L2 interface

```

Ip Address	Age	Mac Address	Vlan	Physical-ifindex	Flags
172:11:1:1::51	00:00:23	acf2.c5f6.7641	11	Ethernet1/51	L

次の例は、**show ipv6 nd suppression-cache remote** コマンドのサンプル出力を示しています。

```
switch(config)# show ipv6 nd suppression-cache remote
```

```

Flags: + - Adjacencies synced via CFSOE
        L - Local Adjacency
        R - Remote Adjacency
        L2 - Learnt over L2 interface
        PS - Added via L2RIB, Peer Sync
        RO - Dervied from L2RIB Peer Sync Entry

```

IPv6 Address Addr	Age	Mac Address	Vlan	Physical-ifindex	Flags	Remote Vtep
172:11:1:1::201	00:06:24	0000.0011.1111	11	(null)	R	30.100.1.1
172:11:1:1::101	00:06:24	74a0.2f1d.d481	11	(null)	R	10.10.11.11

次の例は、**show ipv6 nd suppression-cache statistics** コマンドのサンプル出力を示しています。

```
switch(config)# show ipv6 nd suppression-cache statistics
```

```
ND packet statistics for suppression-cache
```

```
Suppressed:
```

```

Total: 1
L3 mode :      Requests 1, Replies 1
                Flood ND Probe 0

Received:
Total: 1
L3 mode:      NS 1, Non-local NA 0
                Non-local NS 0

Mobility Requests:
Total: 0
L3 mode:      Remote-to-local 0, Local-to-remote 0
                Remote-to-remote 0

RARP Signal Refresh: 0

ND suppression-cache Local entry statistics
Adds 3, Deletes 0

```

次の例は、**show ipv6 nd suppression-cache summary** コマンドのサンプル出力を示しています。

```

switch(config)# show ipv6 nd suppression-cache summary

IPV6 ND suppression-cache Summary
Remote          :2
Local           :1
Total           :3

```

次の例は、**show ipv6 nd suppression-cache vlan "vlan\_id"** コマンドのサンプル出力を示しています。

```

switch(config)# show ipv6 nd suppression-cache vlan 11

Flags: + - Adjacencies synced via CFSOE
        L - Local Adjacency
        R - Remote Adjacency
        L2 - Learnt over L2 interface
        PS - Added via L2RIB, Peer Sync
        RO - Dervied from L2RIB Peer Sync Entry

IPv6 Address      Age      Mac Address      Vlan Physical-ifindex  Flags  Remote Vtep
Addr
172:11:1:1::51   00:00:40 acf2.c5f6.7641   11 Ethernet1/51       L
172:11:1:1::201 00:06:36 0000.0011.1111  11 (null)             R      30.100.1.1
172:11:1:1::101 00:06:36 74a0.2f1d.d481  11 (null)             R      10.10.11.11

```

## 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。