



## VXLAN の設定

この章は、次の内容で構成されています。

- [VXLAN の注意事項と制約事項 \(1 ページ\)](#)
- [VXLAN 展開の考慮事項 \(9 ページ\)](#)
- [VXLAN 展開に対する vPC の考慮事項 \(13 ページ\)](#)
- [VXLAN 展開に対するネットワークの考慮事項 \(18 ページ\)](#)
- [転送ネットワークの考慮事項 \(19 ページ\)](#)
- [VXLAN のトンネリングに関する考慮事項 \(20 ページ\)](#)
- [VXLAN の設定 \(22 ページ\)](#)
- [VXLAN および IP-in-IP トンネリング \(34 ページ\)](#)
- [VXLAN 静的トンネルの設定 \(37 ページ\)](#)

## 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。

表 1: Cisco Nexus 92300YC、92160YC-X、93120TX、9392PQ、および 9348GC-FXP スイッチの VXLAN トラフィックの ACL オプション

ACL の方向	ACL タイプ	VTEP タイプ	ポート タイプ	フローの方向	トラフィック タイプ	サポート対象
入力	PACL	入力 VTEP	L2 ポート	ネットワークにアクセス [GROUP : encap direction]	ネイティブ L2 トラフィック [GROUP : inner]	YES

ACL の方向	ACL タイプ	VTEP タイプ	ポート タイプ	フローの方向	トラフィック タイプ	サポート対象
	VACL	入力 VTEP	VLAN	ネットワークにアクセス [GROUP : encap direction]	ネイティブ L2 トラフィック [GROUP : inner]	YES
入力	RACL	入力 VTEP	テナント L3 SVI	ネットワークにアクセス [GROUP : encap direction]	ネイティブ L3 トラフィック [GROUP : inner]	YES
出力	RACL	入力 VTEP	アップリンク L3/L3-PO/SVI	ネットワークにアクセス [GROUP : encap direction]	VXLAN encap [GROUP : outer]	NO
入力	RACL	出力 VTEP	アップリンク L3/L3-PO/SVI	ネットワークにアクセス [GROUP : decap direction]	VXLAN encap [GROUP : outer]	NO
出力	PACL	出力 VTEP	L2 ポート	ネットワークにアクセス [GROUP : decap direction]	ネイティブ L2 トラフィック [GROUP : inner]	NO
	VACL	出力 VTEP	VLAN	ネットワークにアクセス [GROUP : decap direction]	ネイティブ L2 トラフィック [GROUP : inner]	NO

ACL の方向	ACL タイプ	VTEP タイプ	ポート タイプ	フローの方向	トラフィック タイプ	サポート対象
出力	RACL	出力 VTEP	テナント L3 SVI	ネットワークにアクセス [GROUP : decap direction]	Post-decap L3 トラフィック [GROUP : inner]	YES

- Cisco NX-OS リリース 10.3(1)F 以降、ノンブロッキング マルチキャスト (NBM) 機能と VXLAN は、同じボックスで 2 つの異なる VRF で共存できます。



(注) アンダーレイが実行されるデフォルトの VRF で NBM が有効になっていないことを確認してください。

- スケール環境では、VRF およびレイヤ 3 VNI (L3VNI) に関連する VLAN ID を **system vlan nve-overlay id** コマンドで予約する必要があります。
- ユニキャスト、マルチキャスト、および IGMP マルチキャスト モードの NLB は、Cisco Nexus 9000 スイッチ VXLAN VTEP ではサポートされていません。回避策は、(それぞれのモードで NLB をサポートする) 中間デバイスの背後に NLB クラスタを移動し、VXLAN ファブリックに外部プレフィックスとしてクラスタ IP アドレスを挿入することです。
- MultiAuth 認可変更 (CoA) のサポートが追加されました。詳細については、『[Cisco Nexus 9000 Series NX-OS Security Configuration Guide, Release 9.3\(x\)](#)』を参照してください。
- **lACP vpc-convergence** コマンドは、LACP をサポートするホストへの vPC ポート チャンネルがある VXLAN および非 VXLAN 環境で設定できます。
- vPC あり/なしの VXLAN アンダーレイの PIM BiDir がサポートされます。

VXLAN アンダーレイの PIM BiDir が設定されている場合、次の機能はサポートされません。

- VXLAN のフラッドイング アンド ラーニング
- テナント ルーテッド マルチキャスト (TRM)
- VXLAN EVPN マルチサイト
- VXLAN EVPN マルチホーミング
- vPC 接続 VTEP

冗長 RP の場合は、Phantom RP を使用します。

PIM ASM から PIM BiDir に、または PIM BiDir から PIM ASM アンダーレイに移行する場合は、次の手順例を使用することをお勧めします。

```
no ip pim rp-address 192.0.2.100 group-list 230.1.1.0/8
clear ip mroute *
clear ip mroute date-created *
clear ip pim route *
clear ip igmp groups *
clear ip igmp snooping groups * vlan all
```

すべてのテーブルがクリーンアップされるまで待ちます。

```
ip pim rp-address 192.0.2.100 group-list 230.1.1.0/8 bidir
```

- **no feature pim** コマンドを入力しても、ルートの NVE 所有権は削除されないため、ルートは維持され、トラフィックは流れ続けます。エーijingはPIMによって実行されます。PIM は VXLAN `encap` フラグを持つエントリをエーijingアウトしません。
- Fibre Channel over Ethernet (FCoE) N ポート仮想化 (NPV) は、異なるファブリック アップリンクで VXLAN と共存できますが、Cisco Nexus 93180YC-EX および 93180YC-FX スイッチの同じまたは異なる前面パネルポートにあります。  
ファイバチャネル N ポート仮想化 (NPV) は、異なるファブリック アップリンク上の VXLAN と共存できますが、Cisco Nexus 93180YC-FX スイッチの同じまたは異なる前面パネルポート上にあります。VXLAN は、イーサネット前面パネルポートにのみ存在し、FC 前面パネルポートには存在しません。
- VXLAN は Cisco Nexus 9348GC-FXP スイッチではサポートされています。
- VXLAN は Cisco Nexus 92348GC スイッチではサポートされません。
- SVI が VTEP (フラッドアンドラーニング、または EVPN) で有効になっている場合は、**hardware access-list tcam region arp-ether 256** コマンドを使用して ARP-ETHER TCAM が切り分けられていることを確認します。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 ラインカードを搭載した Cisco 9500 シリーズ スイッチには適用されません。
- VXLAN での PBR の **load-share** キーワードの使用方法については、『[Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide, Release 9.3\(x\)](#)』の「*Guidelines and Limitations for Policy-Based Routing*」セクションを参照してください。
- Cisco NX-OS リリース 9.3(3) 以降、ARP 抑制は Cisco Nexus 9300-GX 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、ARP 抑制は Cisco Nexus 9364C、9300-EX、9300-FX/FX2/FXP、および 9300-GX プラットフォーム スイッチのリフレクション リレーでサポートされます。リフレクティブリレーについては、『[Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide](#)』を参照してください。
- Cisco NX-OS リリース 9.3(5) 以降、Cisco Nexus 9332C、9364C、9300-EX、9300-FX/FX2/FXP、および 9300-GX 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 スイッチの非 VXLAN L3 IP トラフィックを伝送する VXLAN アップリンクのサブインターフェイスの機能があります。この機能は、VXLAN フラッドアンドラーニング、VXLAN EVPN、VXLAN EVPN マルチサイト、および DCI でサポートされます。

- Cisco NX-OS リリース 9.3(6)以降では、VXLAN フラッドアンドラーニングモードが Cisco Nexus 9300-GX 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 10.1(1)以降、VXLAN フラッドアンドラーニングモードは N9K-C9316D-GX、N9K-C93600CD-GX、および N9K-C9364C-GX TOR スイッチでサポートされます。
- -R ラインカードを備えた Cisco Nexus 9504 および 9508 スイッチの場合、VXLAN レイヤ 2 ゲートウェイは 9636C-RX ラインカードでサポートされます。Cisco Nexus 9508 スイッチで VXLAN と MPLS を同時に有効にすることはできません。
- -R ラインカードを備えた Cisco Nexus 9504 および 9508 スイッチでは、9636C-RX 以外のラインカードがある場合、レイヤ 2 ゲートウェイは有効にできません。
- -R ラインカードを搭載した Cisco Nexus 9504 および 9508 スイッチの場合、PIM/ASM はアンダーレイポートでサポートされます。PIM/Bidir はサポートされていません。詳細については、『Cisco Nexus 9000 Series NX-OS Multicast Routing Configuration Guide, Release 9.3(x)』を参照してください。
- -R ラインカードを使用する Cisco Nexus 9504 および 9508 スイッチでは、オーバーレイでの IPv6 ホストルーティングがサポートされます。
- -R ラインカードを搭載した Cisco Nexus 9504 および 9508 スイッチでは、ARP 抑制がサポートされています。
- Cisco NX-OS リリース 10.1(1)以降では、ITX および ePBR over VXLAN 機能が N9K-X9716D-GX TOR および N9K-C93180YC-FX3S プラットフォーム スイッチでサポートされています。
- Cisco NX-OS リリース 10.1(1)以降、PBR over VXLAN 機能は N9K-C9316D-GX、N9K-C93600CD-GX、および N9K-C9364C-GX TOR スイッチでサポートされます。
- PBR over VXLAN 機能のルートポリシーの設定手順に **load-share** キーワードが追加されました。

詳細については、『Cisco Nexus 9000 Series NX\_OS Unicast Routing Configuration Guide, Release 9.x』を参照してください。

- レイヤ 2 EVPN VXLAN のコンバージェンスを向上させるために、**lACP vpc-convergence** コマンドが追加されました。

```
interface port-channel10
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 1001-1200
  spanning-tree port type edge trunk
  spanning-tree bpdupfilter enable
  lACP vpc-convergence
  vpc 10
```

```
interface Ethernet1/34 <- The port-channel member-port is configured with LACP-active
mode (for example, no changes are done at the member-port level.)
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 1001-1200
```

```
channel-group 10 mode active
no shutdown
```

- VXLAN を使用したポート VLAN は、次の例外を除き、Cisco Nexus 9300-EX および 9500-EX ラインカードを搭載した 9500 シリーズ スイッチでサポートされます。
  - これらのスイッチでは、VXLAN を使用するポート VLAN でレイヤ 2（ルーティングなし）のみがサポートされます。
  - 内部 VLAN マッピングがサポートされていません。
- **system nve ipmc** CLI コマンドは、9700-EX ラインカードを搭載した Cisco 9200 および 9300-EX プラットフォーム スイッチには適用されません。
- NVE を、レイヤ 3 プロトコルに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。このベスト プラクティスは、vPC VXLAN 展開だけでなく、すべての VXLAN 展開にも適用できます。
- NVE インターフェイスから設定を削除するには、**default interface nve** コマンドを使用するのではなく、各設定を手動で削除することを推奨します。
- **show** コマンドは **internal** キーワード付きでサポートされていません。
- FEX ポートは、VXLAN VLAN で IGMP スヌーピングをサポートしません。
- VXLAN がサポートされるのは、Cisco Nexus 93108TC-EX と 93180YC-EX スイッチおよび Cisco Nexus 9500 シリーズ スイッチで X9732C-EX ラインカードを装備したものです。
- 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。
- 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。出力 VACL のサポートは、ネットワークのカプセル化解除されたパケットが内部ペイロードでディレクションにアクセスするためには使用できません。  
 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/VACL を使用します。
- 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。
- Cisco NX-OS リリース 9.3(5) よりも前のリリースには、次の制限事項が適用されます。
  - VTEP は、VRF 参加または IEEE 802.1Q カプセル化に関係なく、サブインターフェイスを介した VXLAN カプセル化トラフィックをサポートしません。
  - VRF の参加に関係なく、サブインターフェイスが設定されている場合、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。
  - VXLAN VLAN と非 VXLAN 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。

- Cisco NX-OS リリース 10.1(1)以降、サブインターフェイスを伝送する親インターフェイスを介した VXLAN カプセル化トラフィックは、Cisco Nexus 9300-FX3 プラットフォーム スイッチでサポートされます。
- Cisco NX-OS Release 9.3(5)以降では、サブインターフェイスが設定されている場合、VTEP は親インターフェイス上で VXLAN カプセル化トラフィックをサポートします。この機能は、VXLAN フラッドアンドラーニング、VXLAN EVPN、VXLAN EVPN マルチサイト、および DCI でサポートされます。次の設定例に示すように、VXLAN トラフィックはデフォルト VRF の親インターフェイス (eth1/1) で転送され、L3 IP (非 VXLAN) トラフィックはテナント VRF のサブインターフェイス (eth1/1.10) で転送されます。

```
interface ethernet 1/1
  description VXLAN carrying interface
  no switchport
  ip address 10.1.1.1/30
```

```
interface ethernet 1/1.10
  description NO VXLAN
  no switchport
  vrf member Tenant10
  encapsulation dot1q 10
  ip address 10.10.1.1/30
```

- テナント VRF (VNI を含む VRF) は、VNI がバインドされていない SVI (アンダーレイ VRF) では使用できません。
- ポイントツーマルチポイントのレイヤ 3 および SVI のアップリンクは、サポートされません。
- アップリンクとしての 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。
- FEX HIF (FEX ホスト インターフェイス ポート) は、VXLAN で拡張された VLAN ではサポートされています。
- 入力複製 VPC セットアップでは、vPC ピア デバイス間でレイヤ 3 接続が必要です。
- ポート VLAN マッピング機能が設定された VXLAN VLAN で、ロールバックはサポートされません。
- 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 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

- Cisco Nexus 9300 シリーズ スイッチで 100G アップリンクを備えたものは、VXLAN スイッチング/ブリッジングのみをサポートします

Cisco Nexus 9200、Cisco Nexus 9300-EX、および Cisco Nexus 9300-FX、および Cisco Nexus 9300-FX2 プラットフォーム スイッチには、この制限はありません。



(注) VXLAN ルーティングのサポートについては、40G アップリンクモジュールが必要です。

- MDP は VXLAN 設定ではサポートされません。
- 整合性チェッカは、VXLAN テーブルではサポートされません。
- 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 および 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 アドレスと、SVI の仮想 IP アドレスを持つエニーキャストゲートウェイ)。
- ARP 抑制は、VXLAN ファブリックでの L2VNI ごとのファブリック全体の設定です。ファブリック内のすべての VTEP で一貫してこの機能を有効または無効にします。VTEP 間での一貫性のない ARP 抑制設定はサポートされていません。
- 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。
- VXLAN はインサービス ソフトウェア アップグレード (ISSU) をサポートします。ただし、VXLAN ISSU は Cisco Nexus 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。
- VXLAN は、GRE トンネル機能または MPLS (静的またはセグメントルーティング) 機能との共存を、サポートしません。
- FEX ホストインターフェイスポートに接続されている VTEP はサポートされていません。
- 複数の VTEP がアンダーレイ マルチキャストに同じマルチキャストグループアドレスを使用しているが、VNI が異なる場合は、VTEP に少なくとも 1 つの共通の VNI が必要です。これにより、NVE ピアの検出が行われ、アンダーレイ マルチキャストトラフィックが正しく転送されます。たとえば、リーフ L1 と L4 は VNI 10 を持ち、リーフ L2 と L3 は VNI 20 を持つことができ、両方の VNI が同じグループアドレスを共有できます。リーフ L1 がリーフ L4 にトラフィックを送信すると、トラフィックはリーフ L2 または L3 を通過できます。NVE ピア L1 はリーフ L2 または L3 で学習されないため、トラフィックはドロップされます。したがって、グループアドレスを共有する VTEP には、ピアラーニングが発生し、トラフィックがドロップされないように、少なくとも 1 つの共通の VNI が必要です。この要件は、VXLAN バッドノードトポロジに適用されます。
- VXLAN は、-R ラインカードを使用した Cisco Nexus 9504 および 9508 の MVR および MPLS との共存をサポートしません。



- 復元力のあるハッシュ（ポートチャネルロードバランシング復元力）および VXLAN 設定は、ALE アップリンクポートを使用した VTEP と互換性がありません。



(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。

- -R ラインカードを使用する Cisco Nexus 9504 および 9508 スイッチの場合、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 のネイティブ VLAN はサポートされません。VXLAN のレイヤ 2 トランク上のすべてのトラフィックには、タグが設定される必要があります。この制限は、95xx ラインカードを搭載した Cisco Nexus 9300 および 9500 スイッチに適用されます。この制限は、-EX または -FX ラインカードを備えた Cisco Nexus 9200、9300-EX、9300-FX、および 9500 プラットフォーム スイッチには適用されません。
- ファブリック転送中に凍結された複製ホストを更新するには、「**fabric forwarding dup-host-recovery-timer**」コマンドのみを使用し、「**fabric forwarding dup-host-unfreeze-timer**」コマンドは非推奨であるため使用しないでください。
- L3VNI を使用する場合の VXLAN ファブリックを介した traceroute の場合、次のシナリオが想定される動作です。

L3VNI が VRF および SVI に関連付けられている場合、関連付けられた SVI には構成されている L3 アドレスがありませんが、代わりに「ip forward」構成コマンドがあります。このインターフェイスのセットアップにより、独自の SVI アドレスで traceroute に応答することはできません。代わりに、L3VNI を含む traceroute がファブリックを介して実行されると、報告される IP アドレスは、対応するテナント VRF に属する SVI の最小の IP アドレスになります。

- 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ません。
- Cisco NX-OS リリース 10.3(3)F 以降、新しい L3VNI モードの MHBFD は VXLAN ではサポートされません。
- Cisco NX-OS リリース 10.4(1)F 以降、VXLAN は Cisco Nexus 9332D-H2R プラットフォーム スイッチでサポートされます。

## VXLAN 展開の考慮事項

- スケール環境では、VRF およびレイヤ 3 VNI (L3VNI) に関連する VLAN ID を **system vlan nve-overlay id** コマンドで予約する必要があります。

これは、次のプラットフォームを拡張するために VXLAN リソース割り当てを最適化するために必要です。

- Cisco Nexus 9300 プラットフォーム スイッチ
- 9500 ライン カード搭載の Cisco Nexus 9500 プラットフォーム スイッチ

次に、VRF およびレイヤ 3 VNI に関連する VLAN ID を予約する例を示します。

```
system vlan nve-overlay id 2000

vlan 2000
  vn-segment 50000

interface Vlan2000
  vrf member MYVRF_50000
  ip forward
  ipv6 forward

vrf context MYVRF_50000
  vni 50000
```



(注) **system vlan nve-overlay id** コマンドは、VRF またはレイヤ 3 VNI (L3VNI) にのみ使用してください。通常の VLAN またはレイヤ 2 VNI (L2VNI) にはこのコマンドを使用しないでください。

- 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/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
- 「System Routing Mode: template-vxlan-scale」は適用されません。
- Cisco NX-OS リリース 7.0(3)I4(x) または NX-OS リリース 7.0(3)I5(1) と組み合わせて VXLAN BGP EVPN を使用する場合は、次のハードウェア プラットフォームでは「System Routing Mode: template-vxlan-scale」が必要です。
  - Cisco Nexus 9300-EX スイッチ
  - X9700-EX ラインカードを搭載したCisco Nexus 9500 スイッチ
- Cisco NX-OS リリース 10.3(1)F 以降、Cisco Nexus 9300-FX3/GX/GX2B ToR スイッチの ARP、ND、および MAC に対して、拡張された dual-stack-host-scale テンプレートのサポートが提供されます。

- ARP および ND をスケーリングするには、`system routing template-dual-stack-host-scale` コマンドを使用します。スケーリング制限については、*Cisco Nexus 9000 シリーズ NX-OS 検証済みスケーラビリティ ガイド*を参照してください。
- 「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。
- **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。
- スwitchの起動時に、**source-interface hold-down-time** ホールドダウン時間を使用できます。コマンドを使用すると、オーバーレイが収束し終わるまで、NVE ループバックアドレスのアドバタイズメントを抑制することができます。*hold-down-time* の範囲は 0 ~ 2147483647 秒です。デフォルトは 300 秒です。



(注) ループバックはまだダウンしていますが、トラフィックはカプセル化されてファブリックに送信されます。

- 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、いずれかの IGP プロトコルを介して設定できます。
- VXLAN のフラッドイングおよび学習モードでは、VXLAN VLAN のデフォルトゲートウェイを vPC デバイスのペアにある集中型ゲートウェイとして、両者の間で FHRP (First Hop Redundancy Protocol) を実行することを推奨します。

BGP EVPN では、すべての VTEP でエニーキャストゲートウェイ機能を使用することを推奨します。

- フラッドイングおよび学習モードでは、集中型レイヤ3ゲートウェイのみがサポートされています。エニーキャストゲートウェイはサポートされません。推奨されるレイヤ3ゲートウェイの設計は、vPC 中のスイッチペアをレイヤ3の集中型ゲートウェイにして、FHRP プロトコルを SVI で動作させることです。同じサブネットで使用されている異なる IP アドレスを使う場合であっても、同じ SVI のものを複数の VTEP でスパンさせることはできません。



(注) 一元化されたゲートウェイリーフでの SVI のフラッドイングおよび学習モードの設定時は、**hardware access-list tcam region arp-ether size double-wide**を設定することが必要ですがあります (このコマンドを使用する前に既存の TCAM リージョンのサイズを小さくする必要があります)。

次に例を示します。

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



(注) Cisco Nexus 9200シリーズスイッチでは、サイズの設定は不要です。 **hardware access-list tcam region arp-ether double-wide**

- BGP-EVPN で ARP 抑制を設定する場合は、 **hardware access-list tcam region arp-ether size double-wide** を使用します。 コマンドを使用して ARP をこのリージョンに対応させます（このコマンドを使用する前に既存の TCAM リージョンのサイズを小さくする必要があります）。



(注) この手順は、N9K-X9564PX、N9K-X9564TX、およびN9K-X9536PQ ラインカードを搭載した Cisco Nexus 9300 スイッチ (NFE/ALE) および Cisco Nexus 9500 スイッチに必要です。 Cisco Nexus 9200 スイッチ、Cisco Nexus 9300-EX スイッチ、または N9K-X9732C-EX ラインカードを搭載した Cisco Nexus 9500 スイッチでは、この手順は不要です。

- VXLAN トンネルでは、特定のアンダーレイ ポートで複数のアンダーレイ ネクスト ホップを持つことはできません。たとえば特定の出力アンダーレイ ポートでは、1つの宛先 MAC アドレスだけが、特定の出力ポートでの外部 MAC として利用できます。

これは、ポート単位の制限であり、トンネル単位の制限ではありません。このことは、同じアンダーレイ ポートを介して到達可能な2つのトンネルにおいて、2つの外部 MAC アドレスを利用できないことを意味します。

- VTEP デバイスの IP アドレスを変更する場合は、IP アドレスの変更前に NVE インターフェイスをシャットダウンしておきます。
- ベストプラクティスとして、VTEP のセットをマルチサイト BGW に移行する場合、この移行が実行されているすべての VTEP で NVE インターフェイスをシャットダウンする必要があります。移行が完了し、マルチサイトに必要なすべての設定が VTEP に適用されたら、NVE インターフェイスを再起動する必要があります。
- ベストプラクティスとして、マルチキャストグループの RP は、スパインレイヤ上でのみ設定する必要があります。RP のロードバランシングと冗長性のために、エニーキャスト RP を使用します。

次に、スパインでのエニーキャスト RP 設定の例を示します。

```
ip pim rp-address 1.1.1.10 group-list 224.0.0.0/4
ip pim anycast-rp 1.1.1.10 1.1.1.1
ip pim anycast-rp 1.1.1.10 1.1.1.2
```



- (注)
- 1.1.1.10 は、エニーキャスト RP セットに参加しているすべての RP で設定されたエニーキャスト RP の IP アドレスです。
  - 1.1.1.1 は、ローカル RP IP です。
  - 1.1.1.2 は、ピア RP IP です
- 
- 静的入力複製および BGP EVPN 入力複製は、アンダーレイでの IP マルチキャストルーティングを必要としません。

## VXLAN 展開に対する vPC の考慮事項

- ベストプラクティスとして、機能 vPC が VTEP に追加または VTEP から削除される場合、変更を行う前に、vPC プライマリと vPC セカンダリの両方の NVE インターフェイスをシャットダウンする必要があります。
- 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。
- VPC VXLAN の場合、SVI 数のスケールアップ時は、vPC 設定の **delay restore interface-vlan** タイマーの値を大きくすることを推奨します。たとえば、1000 VNI で 1000 SVI が存在する場合は、**delay restore interface-vlan** タイマーを 45 秒に増やすことを推奨します。
- vPC VTEP ノードから VXLAN VLAN 上の接続されたホストに対して ping が開始された場合、デフォルトで使用される送信元 IP アドレスは、SVI で設定されているエニーキャスト IP です。この ping は、応答が vPC ピア ノードにハッシュされる場合、ホストからの応答を取得できません。この問題は、一意の送信元 IP アドレスを使用せずに、VXLAN vPC ノードから接続されたホストに対して ping が開始された場合に発生する可能性があります。この状況の回避策として、VXLAN OAM を使用するか、各 vPC VTEP に一意のループバックを作成し、バックドアパスを介して一意のアドレスをルーティングします。
- NVE で使用されるループバック アドレスは、プライマリ IP アドレスとセカンダリ IP アドレスを持つように設定する必要があります。

セカンダリ IP アドレスは、VXLAN のすべてのトラフィック（マルチキャストおよびユニキャスト カプセル化トラフィックを含む）に使用されます。
- vPC ピアは同じ設定にする必要があります。
  - VLAN から vn-segment への一貫したマッピング。
  - 同じループバック インターフェイスへの一貫した NVE1 バインディング
    - 同じセカンダリ IP アドレスを使用する。
    - 異なるプライマリ IP アドレスを使用する。

- グループへの一貫した VNI マッピング。
- マルチキャストでは、RP (ランデブー ポイント) から (S, G) join を受け取る vPC ノードが DF (指定フォワーダ) になります。DF のノードでは、マルチキャストに対してカプセル化のルートがインストールされます。

カプセル化解除のルートは、vPC プライマリ ノードと vPC セカンダリ ノードの間でのカプセル化解除ノードの選択に基づいてインストールされます。カプセル化解除の選択で優先されるのは、RP へのコストが最小のノードです。ただし、RP へのコストが両方のノードで同じである場合は、vPC プライマリ ノードが選択されます。

カプセル化解除の選択で優先されるノードに、カプセル化解除マルチキャストルートがインストールされます。他のノードには、カプセル化解除のルートはインストールされません。

- vPC デバイスで、ホストからの BUM トラフィック (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) がピア リンクに複製されます。各ネイティブ パケットからコピーが作成され、各ネイティブ パケットは、ピア vPC スイッチに接続されたオーファンポートを提供するピア リンクを介して送信されます。

VXLAN ネットワークでのトラフィックループを防止するために、ピアリンクに入力されるネイティブ パケットは、アップリンクに送信できません。ただし、ピア スイッチがカプセル化ノードである場合は、コピーされたパケットがピアリンクを通過してアップリンクに送信されます。




---

(注) コピーされた各パケットは、特別な内部 VLAN (VLAN 4041 または VLAN 4046) に送信されます。

---

- ピア リンクが shut の場合、vPC セカンダリにある NVE で使用されるループバック インターフェイスは停止し、ステータスは **Admin Shut** になります。これは、アップストリーム上でループバックへのルートが取り消され、アップストリームがすべてのトラフィックを vPC プライマリへ転送できるようにするために行われます。




---

(注) vPC セカンダリに接続されているオーファンでは、ピアリンクが shut である間にトラフィックの損失が発生します。これは、従来の vPC セットアップのセカンダリ vPC におけるレイヤ 2 オーファンに類似しています。

---

- vPC ドメインがシャットダウンされる時、シャットダウンされる vPC のある VTEP 上の NVE で使用されているループバック インターフェイスは停止し、ステータスは **Admin Shut** になります。これは、アップストリーム上でループバックへのルートが取り消され、アップストリームがすべてのトラフィックを他の vPC VTEP へ転送できるようにするために行われます。

- ピアリンクが **no-shut** の場合、NVE ループバック アドレスが再度提示されます。ルートはアドバタイズされたアップストリームとなり、トラフィックを誘導します。
- vPC の場合、ループバック インターフェイスには、プライマリ IP アドレスとセカンダリ IP アドレスの 2 つの IP アドレスがあります。

プライマリ IP アドレスは一意で、レイヤ 3 プロトコルで使用されます。

インターフェイス NVE は VTEP IP アドレスにセカンダリ IP アドレスを使用するため、ループバック上のセカンダリ IP アドレスは必須です。セカンダリ IP アドレスは、vPC の両方のピアで同じにする必要があります。

- vPC ピアゲートウェイ機能は、両方のピアで NVE RMAC/VMAC プログラミングを容易にするために有効にする必要があります。ピアゲートウェイ機能のために、少なくとも 1 つのバックアップ ルーティング SVI がピアリンクで有効にされ、PIM によって設定される必要があります。これにより、VTEP がスパインへの接続を完全に失ったときに、バックアップ ルーティングパスが提供されます。この場合、リモートピアの到達可能性は、ピアリンクを介して再ルーティングされます。バドノードトポロジにおいて、バックアップ SVI は、個々のアンダーレイ マルチキャストグループに対してスタティック OIF として追加する必要があります。

```
switch# sh ru int vlan 2

interface Vlan2
  description backup1_svi_over_peer-link
  no shutdown
  ip address 30.2.1.1/30
  ip router ospf 1 area 0.0.0.0
  ip pim sparse-mode
  ip igmp static-oif route-map match-mcast-groups

route-map match-mcast-groups permit 1
match ip multicast group 225.1.1.1/32
```



- (注) バドノードトポロジにおいて、バックアップ SVI は、個々のアンダーレイ マルチキャストグループに対してスタティック OIF として追加する必要があります。

SVI は両方の vPC ピアで設定し、PIM を有効にする必要があります。

- NVE またはループバックが vPC 設定で **shut** の場合：
  - プライマリ vPC スイッチでのみ NVE またはループバックが **shut** の場合、グローバル VXLAN vPC 整合性チェッカはエラーになります。その後、NVE、ループバック、および vPC がセカンダリ vPC スイッチでダウンになります。
  - セカンダリ vPC スイッチでのみ NVE またはループバックが **shut** の場合、グローバル VXLAN vPC 整合性チェッカはエラーになります。その後、NVE、ループバック、およびセカンダリ vPC がセカンダリ vPC スイッチでダウンになります。トラフィックのフローは、プライマリ vPC スイッチを介して継続されます。

- ベストプラクティスとして、プライマリとセカンダリの両方の vPC スイッチで NVE とループバックの両方がアップの状態を維持する必要があります。
- マルチキャストロードバランシングおよび RP の冗長性のためにネットワークで設定される冗長エニーキャスト RP は、vPC VTEP トポロジでサポートされます。
- ベストプラクティスとして、エニーキャスト vPC VTEP のセカンダリ IP アドレスの変更時には、vPC プライマリと vPC セカンダリの両方にある NVE インターフェイスが、IP の変更前に shut である必要があります。
- 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、および 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 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。
- **internal** キーワードが付いている **show** 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。
- 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。出力 VACL のサポートは、ネットワークのカプセル化解除されたパケットが内部ペイロードでディレクションにアクセスするためには使用できません。  
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/VACL 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。
- QoS 分類は、レイヤ 3 アップリンク インターフェイス上でディレクションにアクセスするための、ネットワーク内の VXLAN トラフィックではサポートされません。  
VXLAN QoS 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 Quality of Service Configuration Guide, Release 9.3\(x\)](#)』を参照してください。
- 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。
- Cisco NX-OS Release 9.3(5) 以降では、サブインターフェイスが設定されている場合、VTEP は親インターフェイス上で VXLAN カプセル化トラフィックをサポートします。
- 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 IEEE802.1Q カプセル化に関係ありません。
- VXLAN VLAN と非 VXLAN 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。
- ポイントツーマルチポイントのレイヤ 3 および SVI のアップリンクは、サポートされません。



- **ip forward** コマンドを使用すると、VXLAN のカプセル化解除されたパケットでルータ IP 宛てのものを、VTEP が SUP/CPU に転送できるようになります。
- SVI として設定する前に、バックアップ VLAN は、**system nve infra-vlans** コマンドでインフラ VLAN として Cisco Nexus 9200、9300-EX、および 9300-FX/FX2/FX3 および 9300-GX プラットフォームで設定する必要があります。
- 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。
  - 9564PX
  - 9564TX
  - 9536PQ
  - 9732C-EX
- Cisco Nexus 9500 プラットフォーム スイッチを VTEP として使用する場合、100G ラインカードは Cisco Nexus 9500 プラットフォーム スイッチではサポートされません。この制限は、9700-EX または -FX ラインカードを搭載した Cisco Nexus 9500 スイッチには適用されません。
- Cisco Nexus 9300 プラットフォーム スイッチで 100G アップリンクを備えたものは、VXLAN スイッチング/ブリッジングのみをサポートします Cisco Nexus 9200 および Cisco Nexus 9300-EX/ FX/ FX2 プラットフォーム スイッチには、この制限はありません。



---

(注) VXLAN ルーティングのサポートについては、40G アップリンクモジュールが必要です。

---

- 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。
- Application Spine Engine (ASE2) を搭載した Cisco Nexus 9200 プラットフォーム スイッチの場合、レイヤ 3 VXLAN (SVI) スループットの問題が存在します。サイズ 99 ~ 122 のパケットではデータ損失が生じます
- 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。
- VRRP はインサービス ソフトウェア アップグレード (ISSU) をサポートします。
- VXLAN ISSU は、Cisco Nexus 9300-GX プラットフォーム スイッチ。
- VXLAN は、GRE トンネル機能または MPLS (静的またはセグメントルーティング) 機能との共存を、サポートしません。
- FEX ホストインターフェイスポートに接続されている VTEP はサポートされていません。

- 復元力のあるハッシュ（ポート チャンネル ロードバランシング復元力）および VXLAN 設定は、ALE アップリンク ポートを使用した VTEP と互換性がありません。



(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。

- ARP 抑制が vPC 設定で有効または無効になっている場合、グローバル VXLAN vPC 整合性チェックが失敗し、ARP 抑制が片側だけで無効または有効になっていると、VLAN が一時停止するため、ダウンタイムが必要です。



(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、Release 9.3(x)』を参照してください。

## 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 packets 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 9000 シリーズ 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 9000 シリーズ 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 が見つかった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：
  - /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。  
(vPC VTEP では、プライマリおよびセカンダリの /32 IP アドレスを設定する必要があります)
  - 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。
- 転送ネットワーク全体：

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の場合は、**system nve infra-vlans** コマンドを使用する必要があります。それ以外の場合、VXLAN トラフィック (IP/UDP 4789) はスイッチによってアクティブに処理されます。次のシナリオは、完全なリストではありませんが、**system nve infra-vlans** の定義が必要な場合に最もよく見られます。

VNI (vn-segment) に関連付けられていないすべての VLAN は、次の場合に **system nve infra-vlans** として設定する必要があります。

VXLAN フラッドアンドラーニングおよび VXLAN EVPN の場合、非 VXLAN VLAN の存在は次のことに関連する可能性があります。

- 非 VXLAN VLAN に関連する SVI は、vPC ピアリンクを介した vPC ピア間のバックアップアンダーレイルーティング（バックアップルーティング）に使用されます。
- ダウンストリーム ルータ（外部接続、vPC 経由のダイナミックルーティング）を接続するには、非 VXLAN VLAN に関連する SVI が必要です。
- 非 VXLAN VLAN に関連する SVI は、テナント VRF ピアリング（L3 ルート同期およびテナント VRF 内の vPC VTEP 間のトラフィック）に必要です。
- 非 VXLAN VLAN に関連する SVI は、エンドポイント（Bud-Node）へのファーストホップルーティングに使用されます。

VXLAN フラッドアンドラーニングの場合、非 VXLAN VLAN の存在は次のことに関連している可能性があります。

- 非 VXLAN VLAN に関連する SVI は、スパイン（コアポート）へのアンダーレイアップリンクに使用されます。

**system nve infra-vlans** として VLAN を定義するルールは、次のような特殊なケースでは緩和できません。

- VXLAN トラフィックを転送しない非 VXLAN VLAN に関連する SVI（IP/UDP 4789）。
- SVI に関連付けられていない、または VXLAN トラフィックを転送しない非 VXLAN VLAN（IP/UDP 4789）。



(注) インフラ VLAN の特定の組み合わせを設定しないでください。たとえば、2 と 514、10 と 522 は 512 離れています。これは、VXLAN フラッドアンドラーニングで説明されている「コアポート」シナリオに限定されません。

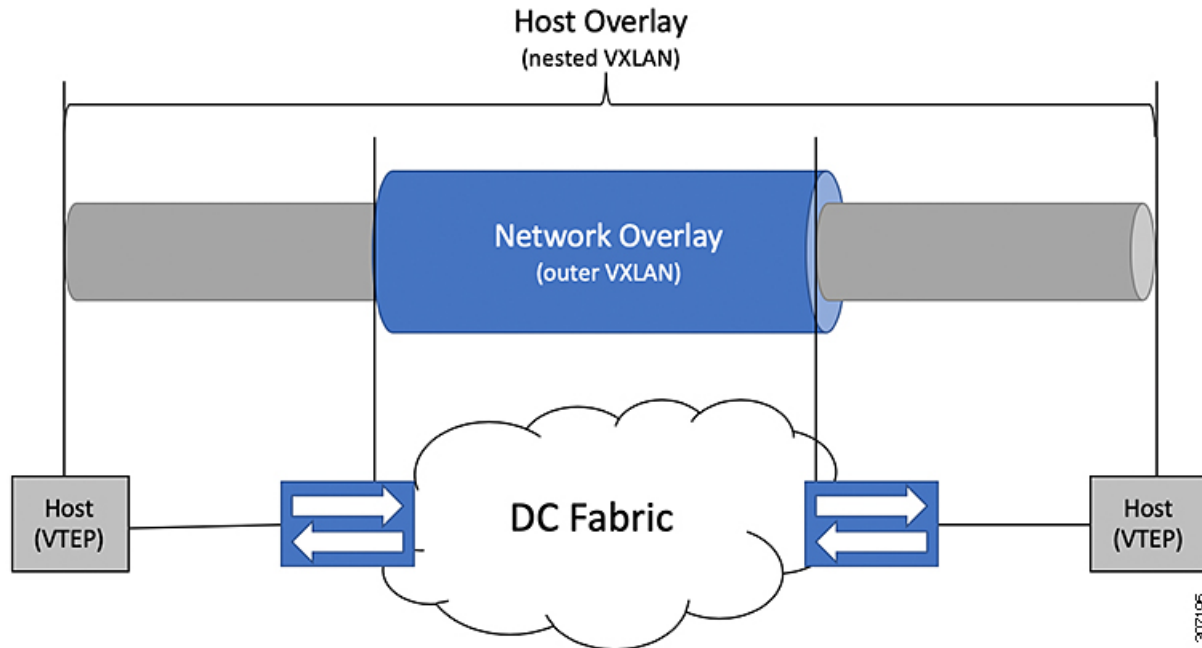
## VXLAN のトンネリングに関する考慮事項

VXLAN BGP EVPN を使用する DC ファブリックは、オーバーレイのトランスポートインフラストラクチャになりつつあります。これらのオーバーレイは、多くの場合、サーバ（ホストオーバーレイ）で生成され、既存のトランスポートインフラストラクチャ（ネットワークオーバーレイ）の上部での統合またはトランスポートが必要です。

Cisco Nexus 9200、9300-EX、9300-FX、9300-FX2、9500-EX、9500-FX プラットフォームスイッチ上の Cisco NX-OS リリース 7.0(3)I7(4) および Cisco NX-OS リリース 9.2(2) から、ネストされた VXLAN（Host Overlay over Network Overlay）のサポートが追加されました。また、Cisco NX-OS リリース 9.3(5) 以降の Cisco Nexus 9300-FX3 プラットフォームスイッチでもサポートされます。

ネストされた VXLAN は、Cisco NX-OS リリース 9.3 (4) 以前のリリースでは、レイヤ 3 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ではサポートされません。Cisco NX-OS リリース 9.3 (5) 以降のレイヤ 3 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でサポートされます。

図 1: ホストオーバーレイ



ネストされた VXLAN サポートを提供するには、スイッチのハードウェアとソフトウェアが 2 つの異なる VXLAN プロファイルを区別する必要があります。

- VXLAN は、VXLAN BGP EVPN (ネストされた VXLAN) を介した転送のために、ハードウェア VTEP の背後で発信されました。
- VXLAN は、ハードウェア VTEP の背後で発生し、VXLAN BGP EVPN (BUD ノード) と統合されました。

2 つの異なる VXLAN プロファイルの検出は自動的に行われ、ネストされた VXLAN に特定の設定は必要ありません。VXLAN でカプセル化されたトラフィックが VXLAN 対応の VLAN に到着するとすぐに、トラフィックは VXLAN BGP EVPN 対応の DC ファブリックを介して転送されます。

ネストされた VXLAN では、次の接続モードがサポートされています。

- タグなしトラフィック (トランクポートまたはアクセスポートのネイティブ VLAN)
- タグ付きトラフィック レイヤ 2 ポート (IEEE 802.1Q トランクポート上のタグ付き VLAN)
- vPC ドメインに接続されているタグなしおよびタグ付きトラフィック
- レイヤ 3 ポートチャネルインターフェイスまたはレイヤ 3 インターフェイス上のタグなしトラフィック

- レイヤ 3 ポート チャンネル インターフェイスまたはレイヤ 3 インターフェイス上のタグなしトラフィック

## VXLAN の設定

### VXLAN のイネーブル化

#### 手順の概要

1. **configure terminal**
2. **[no] feature nv overlay**
3. **[no] feature vn-segment-vlan-based**
4. (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>	グローバル設定モードを開始します。
ステップ 2	<b>[no] feature nv overlay</b>	VXLAN 機能をイネーブルにします。
ステップ 3	<b>[no] feature vn-segment-vlan-based</b>	すべての VXLAN ブリッジ ドメインにグローバルモードを設定します。
ステップ 4	(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。

### VLAN から VXLAN VNI へのマッピング

#### 手順の概要

1. **configure terminal**
2. **vlan *vlan-id***
3. **vn-segment *vnid***
4. **exit**

#### 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 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	<b>vlan</b> <i>vlan-id</i>	VLAN を指定します。
ステップ 3	<b>vn-segment</b> <i>vnid</i>	VXLAN VNID（仮想ネットワーク ID）を指定します
ステップ 4	<b>exit</b>	コンフィギュレーション モードを終了します。

## NVE インターフェイスと関連 VNI の作成および設定

NVE インターフェイスは、VXLAN トンネルの終端となるオーバーレイ インターフェイスです。

次のように、NVE（オーバーレイ）インターフェイスを作成および設定できます。

### 手順の概要

1. **configure terminal**
2. **interface nve** *x*
3. **source-interface** *src-if*
4. **member vni** *vni*
5. **mcast-group** *start-address* [*end-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>configure terminal</b>	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>interface nve</b> <i>x</i>	VXLAN トンネルの終端となる 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	<b>source-interface</b> <i>src-if</i>	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一時デバイスおよびリモート VTEP によって認識される必要があります。これは、転送ネットワークのダイナミックルーティングプロトコルを介してアドレスを通知することによって、実現されます。
ステップ 4	<b>member vni</b> <i>vni</i>	VXLAN VNI（仮想ネットワーク ID）を NVE インターフェイスに関連付けます。

	コマンドまたはアクション	目的
ステップ 5	<code>mcast-group start-address [end-address]</code>	VNI にマルチキャスト グループを割り当てます。 (注) BUM トラフィックだけに使用します。

## NVE インターフェイス ループバックの作成および構成

従来、単一のループバック インターフェイスは NVE 送信元 インターフェイスとして設定され、vPC コンプレックスの PIP と VIP の両方が構成されています。CloudSec 対応の vPC BGW に個別のループバックを構成できます。Cisco では、MLAG 展開でのコンバージェンスを向上させるために、NVE の下で送信元とエニーキャスト IP アドレスに個別のループバック インターフェイスを使用することをお勧めします。送信元インターフェイスに構成されている IP アドレスは vPC ノードの PIP であり、エニーキャスト インターフェイスに構成されている IP アドレスはその vPC コンプレックスの VIP です。NVE エニーキャスト インターフェイスも構成されている場合、NVE ソース インターフェイスで構成されたセカンダリ IP は効果がありません。

個別のループバックを使用すると、DCI 側を宛先とするデュアル接続 EVPN タイプ 2 およびタイプ 5 トラフィックのコンバージェンスが改善されます。

Cisco NX-OS リリース 10.4(1)F 以降、タイプ 2 ルートは、vMCT に固有のネクストホップとして PIP を使用してアドバタイズされます。ホールドダウン タイマーが期限切れになる前に、PIP が NVE インターフェイスでアップ状態になっています。したがって、PIP ネクストホップを持つすべてのルートは、ホールドダウン タイマーが期限切れになる前にアドバタイズします。ルートには、vMCT の孤立したタイプ 2 ルートと、redist HMM を介して学習したローカルタイプ 5 ルート、vPC/vMCT の直接ルートまたは接続ルートが含まれます。

孤立したルートまたはローカルに接続されたルートをアドバタイズできるタイミングを示すために、ファブリック対応タイマーが vPC に追加されます。タイマーは、孤立したルートまたはローカルに接続されたルートのコンバージェンスを強化するのに役立ちます。



(注) ファブリック コンバージェンス タイマーを設定します。デフォルトでは、タイマーは NVE ホールドダウン タイマーの 75% に設定されます。

### 手順の概要

1. `configure terminal`
2. `interface nve x`
3. `source-interface loopback-interface-identifier`
4. (任意) `source-interface [loopback-interface-identifier] anycast loopback[loopback-interface-identifier]`
5. `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> 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>interface nve x</b> 例： switch(config-if-nve)#	VXLAN トンネルの終端となる 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	<b>source-interface loopback-interface-identifier</b> 例： switch(config-if-nve)# <b>source-interface loopback 1</b>	ループバック インターフェイスを VTEP の送信元 インターフェイスとして設定します。
ステップ 4	(任意) <b>source-interface [loopback-interface-identifier] anycast loopback[loopback-interface-identifier]</b> 例： switch(config-if-nve)# source-interface loopback 1 <b>anycast loopback2</b>	エニーキャスト ループバック インターフェイスを構成します。  (注) この構成は、以前のリリースの IPv6 アンダーレイに存在します。このリリースから、IPv4 アンダーレイの構成が追加されました。
ステップ 5	<b>show nve interface nve1 detail</b>	構成されたエニーキャスト ループバック インターフェイスに関する情報を表示します。

## 例

次に、エニーキャスト ループバック インターフェイスの構成例を示します。

```
switch# configure terminal
switch(config)# interface nve 1
switch(config-if-nve)# source-interface loopback 1
switch (config-if-nve)# source-interface loopback 1 anycast loopback 4
```

次に、スイッチに構成されたループバック インターフェイスの show コマンドを表示する例を示します。この show コマンドは、エニーキャスト ループバック インターフェイス、エニーキャスト インターフェイスに関連付けられた IP、インターフェイスの状態、ファブリック コンバージェンス タイマーなどの詳細を表示します。



(注) ファブリック コンバージェンス タイマーのデフォルト値は 135 秒です。

```

switch(config-if-nve)# show nve interface nve1 detail
Interface: nve1, State: Up, encapsulation: VXLAN
VPC Capability: VPC-VIP-Only [notified]
Local Router MAC: e41f.7b2e.977f
Host Learning Mode: Control-Plane
Source-Interface: loopback1 (primary: 20.1.0.15)
Anycast-Interface: loopback4 (secondary: 20.1.0.145)
Source Interface State: Up
Anycast Interface State: Up
Virtual RMAC Advertisement: Yes
NVE Flags:
Interface Handle: 0x49000001
Source Interface hold-down-time: 120
Source Interface hold-up-time: 30
Remaining hold-down time: 0 seconds
Virtual Router MAC: 0200.1401.0091
Interface state: nve-intf-add-complete
Fabric convergence time: 90 seconds
Fabric convergence time left: 0 seconds

```



(注) スプリットループバック機能がサポートされていない下位バージョンにスイッチをダウングレードすることはできません。MLAG 構成からダウングレードが開始された場合にのみ、MLAG 展開でスプリットループバックをサポートするバージョンにスイッチをダウングレードできます。

## 単一の NVE 送信元ループバック インターフェイスから別の送信元ループバックへの移行

単一の NVE 送信元ループバック インターフェイスを持つ既存の vPC 展開を、VIP および PIP の別の送信元ループバックに移動できます。この移行は、トラフィック損失への影響が少なく、既存のループバック展開をスプリットループバック展開に移行するのに役立ちます。

単一の NVE をスプリットループバック展開に移行するには、次の手順を実行します。

1. vPC セカンダリを分離します。これは、トラフィックがプライマリのみを通過するようにするためです。

vPC セカンダリで、次の手順を実行します。

1. ip pim isolate
2. router bgp 2
3. 分離
4. router ospf underlay
5. 分離
6. sleep instance 2 20
7. vPC domain 100

8. shutdown
2. vPC セカンダリ上
  1. プライマリ インターフェイスのセカンダリ IP を削除します。
  2. 前のセカンダリと同じ IP アドレスを使用してエニーキャスト インターフェイスを構成します。この新しい動作により、vPC CC の障害は発生せず、NVE は稼働します。
3. vPC セカンダリを接続します。ホールドダウン タイマーの期限切れを許可します。
4. vPC ロールを変更します。
5. 新しい vPC セカンダリに対してステップ 1～3 を繰り返します。これにより、構成が変更され、新しい vPC セカンダリと vPC ボックスの両方の新しい構成で更新されます。

## vPC での VXLAN VTEP の設定

vPC で VXLAN VTEP を設定できます。

### 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 ルーテッド パスとして非 VXLAN 対応 VLAN を定義します。
9. インフラ VLAN として使用する VLAN を作成します。
10. 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。
11. プライマリおよびセカンダリ IP アドレスを作成します。
12. ループバック インターフェイスにプライマリ IP アドレスを作成します。
13. vPC ドメインを作成します。
14. 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。
15. vPC ドメインでピアゲートウェイを有効にします。
16. vPC ドメインでピアスイッチを有効にします。
17. 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。
18. (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。
19. 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。
20. STP hello-time、forward-time、および max-age time を変更します。

## 21. (任意) SVI の遅延復元タイマーを有効にします。

### 手順の詳細

**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 224.0.0/4
```

**ステップ 8** 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。

```
switch(config)# system nve infra-vlans 10
```

**ステップ 9** インフラ VLAN として使用する VLAN を作成します。

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

**ステップ 10** 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  
(Optional) switch(config-if)# ip igmp static-oif route-map match-mcast-groups  
switch(config-if)# no shutdown  
(Optional) switch(config)# route-map match-mcast-gropus permit 10  
(Optional) switch(config-route-map)# match ip multicast group 225.1.1.1/32
```

**ステップ 11** 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 12** ループバック インターフェイスにプライマリ IP アドレスを作成します。

```
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 13** vPC ドメインを作成します。

```
switch(config)# vpc domain 5
```

**ステップ 14** 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 172.28.230.85
```

(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 9000 Series NX-OS Unicast Routing Configuration Guide](#)』を参照してください。

**ステップ 15** 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 16** 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 17** 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 18** (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 19** 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 1,10,100-200
switch(config-if)# mtu 9216
switch(config-if)# vpc peer-link
switch(config-if)# no shutdown
switch(config-if)# interface Ethernet 1/1 , 1/21
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 20** 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 21** (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

```

## VXLAN VTEP でのスタティック MAC の設定

VXLAN VTEP のスタティック MAC は、フラッディングおよび学習を行う Cisco Nexus 9300 シリーズスイッチでサポートされます。この機能により、ピア VTEP でのスタティック MAC アドレス設定が可能になります。



(注) スタティック MAC は、BGP EVPN 対応 VNI のコントロールプレーンには設定できません。

### 手順の概要

1. **configure terminal**
2. **mac address-table static mac-address vni vni-id interface nve x peer-ip ip-address**
3. **exit**
4. (任意) **copy running-config startup-config**
5. (任意) **show mac address-table static interface nve x**

## 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 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>mac address-table static mac-address vni vni-id interface nve x peer-ip ip-address</b>	リモート VTEP をポイントする MAC アドレスを指定します。
ステップ 3	<b>exit</b>	グローバル コンフィギュレーション モードを終了します。
ステップ 4	(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。
ステップ 5	(任意) <b>show mac address-table static interface nve x</b>	リモート VTEP をポイントするスタティック MAC アドレスを表示します。

## 例

次に示すのは、VXLAN VTEP に設定されたスタティック MAC アドレスの出力例です。

```
switch# show mac address-table static interface nve 1

Legend:
      * - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
      age - seconds since last seen, + - primary entry using vPC Peer-Link,
      (T) - True, (F) - False
      VLAN      MAC Address      Type      age      Secure NTFY Ports
-----+-----+-----+-----+-----+-----+-----
* 501      0047.1200.0000  static   -        F        F        nve1(33.1.1.3)
* 601      0049.1200.0000  static   -        F        F        nve1(33.1.1.4)
```

## VXLAN のディセーブル化

## 手順の概要

1. **configure terminal**
2. **no feature vn-segment-vlan-based**
3. **no feature nv overlay**
4. (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>	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>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 3	<b>no feature nv overlay</b>	VXLAN 機能をディセーブルにします。
ステップ 4	(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。

## BGP EVPN 入力複製の設定

次の設定では、ピアの入力複製をする BGP EVPN をイネーブルにします。

## 手順の概要

1. **configure terminal**
2. **interface nve x**
3. **source-interface src-if**
4. **member vni vni**
5. **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>configure terminal</b>	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>interface nve x</b>	VXLAN トンネルの終端となる 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	<b>source-interface src-if</b>	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一時デバイスおよびリモート VTEP によって認識される必要があります。これは、転送ネットワークのダイナミックルー



	コマンドまたはアクション	目的
		テリングプロトコルを介してアドレスを通知することによって、実現されます。
ステップ 4	<b>member vni vni</b>	VXLAN VNI (仮想ネットワーク ID) を NVE インターフェイスに関連付けます。
ステップ 5	<b>ingress-replication protocol bgp</b>	VNI の入力複製をする BGP EVPN をイネーブルにします。

## 静的入力複製の設定

次の設定では、ピアの静的入力複製をイネーブルにします。

### 手順の概要

1. **configuration terminal**
2. **interface nve x**
3. **member vni [vni-id | vni-range]**
4. **ingress-replication protocol static**
5. **peer-ip n.n.n.n**

### 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>configuration terminal</b>	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>interface nve x</b>	VXLAN トンネルの終端となる 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	<b>member vni [vni-id   vni-range]</b>	VXLAN VNI を NVE インターフェイスにマッピングします。
ステップ 4	<b>ingress-replication protocol static</b>	VNI の静的入力複製を有効にします。
ステップ 5	<b>peer-ip n.n.n.n</b>	ピア IP を有効にします。

## VXLAN および IP-in-IP トンネリング

Cisco NX-OS リリース 9.3(6)以降のリリースでは、VXLAN と IP-in-IP トンネリングの共存がサポートされています。

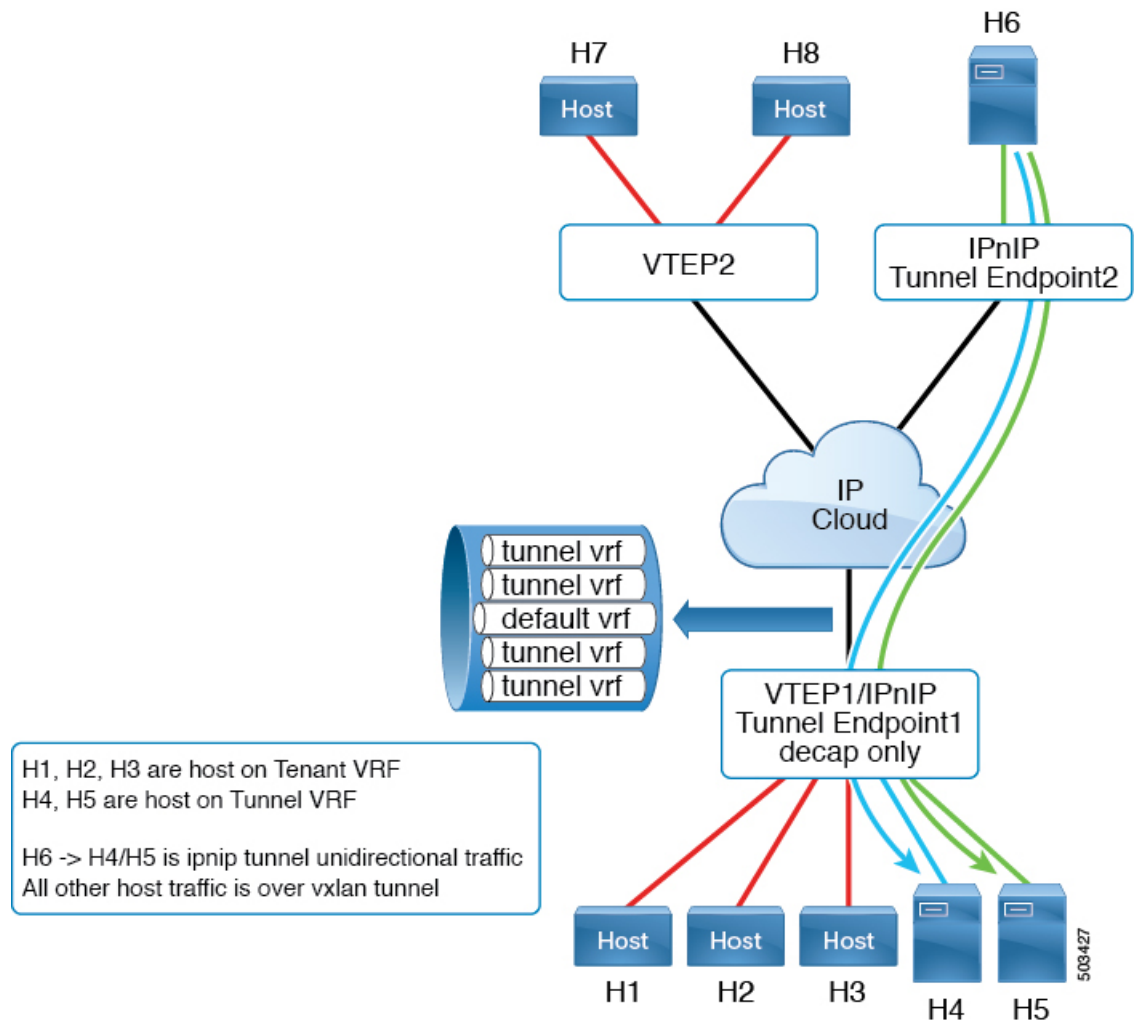
これらの機能を共存させるには、独自の VRF 内で IP-in-IP トンネルと VXLAN を分離する必要があります。VRF を分離することで、VXLAN とトンネルの両方が独立して動作します。VXLAN トンネル終端は、同じまたは異なる VRF 上で IP-in-IP トンネルとして（またはその逆に）再カプセル化されません。

インターフェイスの下にサブインターフェイスを設定して VRF を分離することで、同じアップリンクを使用して VXLAN と IP-in-IP トンネルトラフィックの両方を伝送できます。親ポートはデフォルト VRF に、サブインターフェイスはデフォルト以外の VRF に設定できます。

ポートチャネルサブインターフェイスで受信した IP-in-IP カプセル化パケットを終了するには、これらのサブインターフェイスをトンネルインターフェイスと同じ非デフォルト VRF で設定する必要があります、\* 1 \* 非デフォルト VRF のメンバーにのみなれます。。

異なる親 PC からの複数のポートチャネルサブインターフェイスは、IP-in-IP カプセル化を終了するために、同じデフォルト以外の VRF で引き続き設定できます。この制限は、1つのポートチャネルのサブインターフェイスにのみ適用されます。この制限は、L3 ポートには適用されません。

次の例に示すように、VXLAN トラフィックはデフォルト VRF の親インターフェイス (eth1/1) で転送され、IP-in-IP (非 VXLAN) トラフィックはトンネル VRF のサブインターフェイス (eth1/1.10) で転送されます。



Cisco Nexus 9300-FX2 プラットフォーム スイッチは、VXLAN と IP-in-IP トンネリングの共存をサポートしますが、次の制限があります。

- VXLAN はデフォルト VRF で設定する必要があります。
- 共存は、VXLAN と EVPN コントロールプレーンでサポートされます。
- IP-in-IP トンネリングは、デフォルト以外の VRF で設定する必要があります、decapsulate-any モードでのみサポートされます。



(注) デフォルト VRF でカプセル化解除トンネルが設定されているときに VXLAN を有効にしようとすると、エラーメッセージが表示されます。VXLAN と IP-in-IP トンネリングは、デフォルト以外の VRF 内の decapsulate-any トンネルに対してのみ共存でき、設定を削除できることが示されています。

- ポイントツーポイント GRE トンネルはサポートされません。ポイントツーポイント トンネルを設定しようとする、VXLAN と IP-in-IP トンネリングが decapsulate-any トンネルに対してのみ共存できることを示すエラー メッセージが表示されます。
- 通常、トンネルを設定するには、2つのエンドポイントを提供する必要があります。ただし、decapsulate-any は受信専用トンネルであるため、送信元 IP アドレスまたは送信元インターフェイス名のみを指定する必要があります。トンネルは、同じ VRF 内の任意の IP インターフェイスで終端します。
- トンネル統計情報は出力カウンタをサポートしていません。
- VXLAN トンネルと IP-in-IP トンネルは、同じ送信元ループバック インターフェイスを共有できません。各トンネルには、独自の送信元ループバック インターフェイスが必要です。

次の例は、設定サンプルを示しています。

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

interface ethernet 1/1
  description VXLAN carrying interface
  no switchport
  ip address 10.1.1.1/30

interface ethernet 1/1.10
  description IPinIP carrying interface
  no switchport
  vrf member tunnel
  encapsulation dot1q 100
  ip address 10.10.1.1/30

interface loopback 0
  description VXLAN-loopback
  ip address 125.125.125.125/32

interface loopback 100
  description Tunnel_loopback
  vrf member tunnel
  ip address 5.5.5.5/32

interface Tunnel1
  vrf member tunnel
  ip address 55.55.55.1/24
  tunnel mode ipip decapsulate-any ip
  tunnel source loopback100
  tunnel use-vrf tunnel
  no shutdown

interface nve1
  host-reachability protocol bgp
  source-interface loopback0
  global mcast-group 224.1.1.1 L2
  global mcast-group 225.3.3.3 L3
  member vni 10000
  suppress-arp
  ingress-replication protocol bgp
```

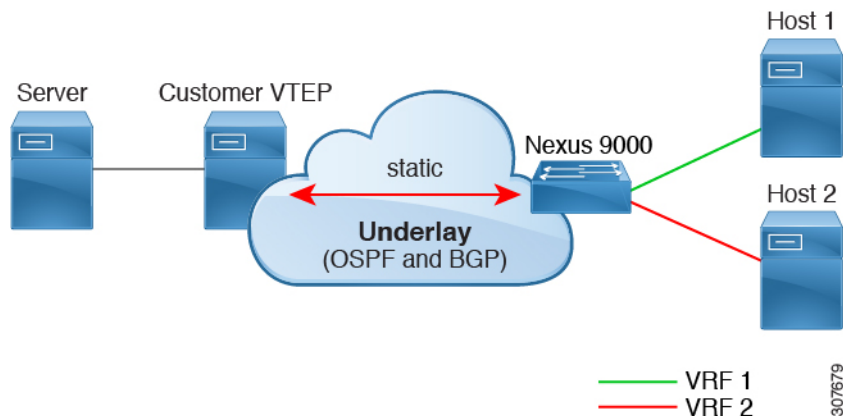
```
member vni 55500 associate-vrf
```

## VXLAN 静的トンネルの設定

### VXLAN 静的トンネルについて

Cisco NX-OS リリース9.3(3)以降では、一部の Cisco Nexus スイッチは、静的トンネルを介して顧客提供のソフトウェア VTEP に接続できます。静的トンネルはカスタマー定義であり、BGP EVPN などのコントロールプレーンプロトコルを必要とせずにホスト間の VXLAN カプセル化トラフィックをサポートします。静的トンネルは、Nexus スイッチから手動で設定することも、アンダーレイの NETCONF クライアントを介してプログラムで設定することもできます。

図 2: VXLAN 静的トンネル接続ソフトウェア VTEP



静的トンネルは VRF ごとにサポートされます。各 VRF は専用の L3VNI を持ち、スイッチとソフトウェア VTEP（静的ピア）で適切にカプセル化およびカプセル解除されたパケットを転送できます。通常、静的ピアは、1 つ以上の VNI を終端する 1 つ以上の VM を備えた Cisco Nexus 1000V またはベアメタルサーバです。ただし、静的ピアは、RFC 7348 の「Virtual eXtensible Local Area Network (VXLAN) : 仮想化レイヤ 2 ネットワークをレイヤ 3 ネットワーク上にオーバーレイするためのフレームワーク」に準拠した、お客様が開発したデバイスです。顧客が静的ピアを提供し、コントロールプレーンプロトコルが存在しないため、静的ピアが VXLAN 関連の設定を転送し、正しいホストにルーティングすることを確認する必要があります。

Cisco NX-OS Release 9.3(5) 以降では、この機能はトンネルを出入りするパケットの処理をサポートします。具体的には、Nexus スイッチがトンネルを介してホストまたは他のスイッチにパケットを送信できるようにします。Cisco NX-OS リリース 9.3(3) および 9.3(4) では、VXLAN スタティック トンネルは、ローカル ホストからリモート ホストへの通信のみをサポートしません。

## VXLAN 静的トンネルの注意事項と制約事項

VXLAN 静的トンネル機能には、次の注意事項と制約事項があります。

- Cisco Nexus 9332C、9334C、9300-EX、および9300-FX/FX2/FX3、9300-GX、および9300-FX3 プラットフォーム スイッチは、VXLAN 静的トンネルをサポートします。
- Cisco NX-OS リリース10.1 (1) 以降、VXLAN 静的トンネルは Cisco Nexus 9300-FX3 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 スタティック トンネルは 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。
- ソフトウェア VTEP には次のような注意事項が適用されます。
  - VNI からのトラフィックの転送方法を決定するために、必要に応じてソフトウェア VTEP を設定する必要があります。
  - ソフトウェア VTEP は RFC 7348 に準拠している必要があります。
- アンダーレイには、OSPFv2、BGP、IS-IS、または IPv4 を使用できます。
- オーバーレイは IPv4 のみです。
- 追加の VXLAN 機能 (TRM、マルチサイト、OAM、クロスコネクト、VXLAN QoS など)、IGMP スヌーピング、MPLS ハンドオフ、スタティック MPLS、SR、SRv6 はサポートされていません。
- ローカルテナント VRF ループバックからソフトウェア VTEP の背後にあるホストへのオーバーレイでの ping はサポートされていません。
- 静的トンネルは ECMP 設定をサポートしません。
- 静的トンネルは、従来のフラッドアンドラーニングまたは BGP EVPN ファブリックと同じファブリックでは設定できません。
- ローカル ホストは、VNI 対応 VLAN ではサポートされません。したがって、VNI を設定したのと同じ VLAN にホストを配置することはできません。
- ファブリックフォワーディングは、静的トンネルでサポートされます。ファブリック転送が有効になっている場合は、SVI と MAC アドレスの使用方法に影響することに注意してください。次の設定例を考えます。

```
feature fabric forwarding
fabric forwarding anycast-gateway-mac 0000.0a0a.0a0a
```

```
interface Vlan802
no shutdown
vrf member vrfvxlan5201
ip address 103.33.1.1/16
fabric forwarding mode anycast-gateway
```

ファブリック転送が有効の場合：

- **fabric forwarding mode anycast-gateway** が設定されているすべての SVI（たとえば、Vlan802）が使用されます。
- **fabric forwarding anycast-gateway-mac anycast-mac-address**（0000.0a0a.0a0a）で設定された MAC アドレスが使用されます。

## VXLAN 静的トンネルの有効化

VXLAN 静的トンネルを有効にするには、次の機能を有効にします。

### 手順の概要

1. **config terminal**
2. **feature vn-segment**
3. **feature ofm**

### 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>config terminal</b> 例： switch# <b>configure terminal</b> switch(config)#	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	<b>feature vn-segment</b> 例： switch(config)# <b>feature vn-segment</b> switch(config)#	VLAN ベースの VXLAN を有効にします。
ステップ 3	<b>feature ofm</b> 例： switch(config)# <b>feature ofm</b> switch(config)#	静的 VXLAN トンネルを有効にします。

### 次のタスク

静的トンネルを介した VXLAN ルーティング用の VRF オーバーレイ VLAN を設定します。

## 静的トンネルの VRF オーバーレイの設定

VXLAN 静的トンネル用に VRF オーバーレイを設定する必要があります。

### 手順の概要

1. **vlan number**

## 2. `vn-segment number`

### 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><code>vlan number</code></b> 例 : <pre>switch(config)# <b>vlan 2001</b> switch(config-vlan)#</pre>	VLAN を指定します。
ステップ 2	<b><code>vn-segment number</code></b> 例 : <pre>switch(config-vlan)# <b>vn-segment 20001</b> switch(config-vlan)#</pre>	VN セグメントを指定します。

### 次のタスク

静的トンネルを介した VXLAN ルーティングの VRF を設定します。

## 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 vrf-name`
2. `vni number`

### 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><code>vrf context vrf-name</code></b> 例 : <pre>switch(config-vlan)# <b>vrf context cust1</b> switch(config-vrf)#</pre>	テナント VRF を設定します。
ステップ 2	<b><code>vni number</code></b> 例 : <pre>switch(config-vrf)# <b>vni 20001</b> switch(config-vrf)#</pre>	テナント VRF の VNI を指定します。

### 次のタスク

ホストの L3 VNI を設定します。



## 静的トンネルの L3 VNI の設定

VTEP の L3 VNI を設定します。

### 始める前に

VLAN インターフェイス機能を有効にする必要があります。必要に応じて **feature interface-vlan** を使用します。

### 手順の概要

1. **vlan number**
2. **interface vlan-number**
3. **vrf member vrf-name**
4. **ip forward**
5. **no shutdown**

### 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> 例 : <pre>switch(config-vrf)# vlan 2001 switch(config-vlan)#</pre>	VLAN 番号を指定します
ステップ 2	<b>interface vlan-number</b> 例 : <pre>switch(config)# interface vlan2001 switch(config-if)#</pre>	VLAN インターフェイスを指定します。
ステップ 3	<b>vrf member vrf-name</b> 例 : <pre>switch(config-if)# vrf member cust1 Warning: Deleted all L3 config on interface Vlan2001 switch(config-if)#</pre>	テナント VRF に VLAN インターフェイスを接続します。
ステップ 4	<b>ip forward</b> 例 : <pre>switch(config-if)# ip forward switch(config-if)#</pre>	インターフェイスで IPv4 トラフィックを有効にします。
ステップ 5	<b>no shutdown</b> 例 : <pre>switch(config-if)# no shutdown switch(config-if)#</pre>	インターフェイスを有効にします。

## 次のタスク

トンネル プロファイルを設定します。

# トンネル プロファイルの設定

スタティック トンネルを設定するには、Nexus スイッチのインターフェイス、スタティックピアの MAC アドレス、およびスタティック ピアのインターフェイスを指定するトンネル プロファイルを作成します。

## 始める前に

VXLAN スタティック トンネルを設定するには、アンダーレイが完全に設定され、正しく動作している必要があります。

## 手順の概要

1. **tunnel-profile** *profile-name*
2. **encapsulation** {*VXLAN* / *VXLAN-GPE* / *SRv6*}
3. **source-interface loopback** *virtual-interface-number*
4. **route vrf** *tenant-vrf destination-host-prefix destination-vtep-ip-address next-hop-vrf destination-vtep-vrf vni vni-number dest-vtep-mac destination-vtep-mac-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>tunnel-profile</b> <i>profile-name</i> 例 : switch(config)# <b>tunnel-profile</b> test switch(config-tnl-profile)#	トンネル プロファイルを作成し、名前を指定します。
ステップ 2	<b>encapsulation</b> { <i>VXLAN</i> / <i>VXLAN-GPE</i> / <i>SRv6</i> }	トンネルプロファイルの適切なカプセル化タイプを設定します。  (注) NX-OSリリース9.3(3)では、カプセル化タイプ <b>vxlan</b> のみがサポートされます。
ステップ 3	<b>source-interface loopback</b> <i>virtual-interface-number</i> 例 : switch(config-tnl-profile)# <b>source-interface loopback 1</b> switch(config-tnl-profile)#	ループバック インターフェイスをトンネルプロファイルの送信元インターフェイスとして設定します。仮想インターフェイス番号は 0-1023 です。
ステップ 4	<b>route vrf</b> <i>tenant-vrf destination-host-prefix destination-vtep-ip-address next-hop-vrf destination-vtep-vrf vni vni-number dest-vtep-mac destination-vtep-mac-address</i>	宛先ソフトウェア VTEP を指定し、VNI および宛先 VTEP MAC アドレスのルート情報を入力して、トンネル ルートを作成します。

	コマンドまたはアクション	目的
	例 : <pre>switch(tunnel-profile)# route vrf cust1 101.1.1.2/32 7.7.7.1 next-hop-vrf default vni 20001 dest-vtep-mac f80f.6f43.036c switch(tunnel-profile)#</pre>	(注) <b>route vrf</b> コマンドは、すべてのルートで <i>destination-vtep-ip-address</i> ごとに1つの <i>destination-vtep-mac-address</i> を受け入れます。追加のルートを設定すると、それらのルートはエラー ルートとしてキャッシュされ、それぞれに対してエラー <b>syslog</b> が生成されます。

## VXLAN 静的トンネルの検証

トンネルの一端がダウンしても、VXLAN 静的トンネルは設定されたままになります。トンネルの一方の端がダウンしている間は、そのVTEPに到達できないため、パケットはドロップされます。ダウンしたVTEPがオンラインに戻ると、アンダーレイが接続を再学習した後、トラフィックはトンネルを介して再開できます。

**show** コマンドを使用して、トンネルプロファイルとトンネルルートの状態を確認できます。

始める前に

### 手順の概要

1. **show tunnel-profile**
2. **show ip route tenant-vrf-name**
3. **show running-config ofm**

### 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>show tunnel-profile</b>	ソフトウェアのトンネルプロファイルに関する情報を表示します。
ステップ 2	<b>show ip route tenant-vrf-name</b>	ソフトウェア VTEP に接続している VRF のルート情報を表示します。たとえば、VRF のトンネルにルートが存在することを確認するために、ルート到達不能エラーが発生した場合にこのコマンドを使用できます。
ステップ 3	<b>show running-config ofm</b>	OFM 機能および静的トンネルの実行設定を表示します。ルート到達不能エラーが発生したときにこのコマンドを使用すると、宛先 VTEP のルート情報が存在するかどうかを確認できます。

### 次のタスク

VXLAN の検証に加えて、SPAN を使用して、スイッチを通過するパケットのポートと送信元 VLAN を確認できます。

## VXLAN 静的トンネルの設定例

次の設定例は、サポートされる方式による VXLAN 静的トンネル設定を示しています。

### NX-OS CLI

```
vlan 2001
vlan 2001
  vn-segment 20001

interface Vlan2001
  no shutdown
  vrf member vrf1601
  ip forward

vrf context cust1
  vni 20001

feature ofm

tunnel-profile test
  encapsulation vxlan
  source-interface loopback1
  route vrf cust1 101.1.1.2/32 7.7.7.1 next-hop-vrf default vni 20001 dest-vtep-mac
  f80f.6f43.036c
```

## 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。