



# EVPN VXLAN レイヤ2 オーバーレイネットワークの設定

- [EVPN VXLAN レイヤ2 オーバーレイネットワークについて \(1 ページ\)](#)
- [EVPN VXLAN レイヤ2 オーバーレイネットワークの設定方法 \(4 ページ\)](#)
- [EVPN VXLAN レイヤ2 オーバーレイネットワークの設定例 \(15 ページ\)](#)
- [EVPN VXLAN レイヤ2 オーバーレイネットワークの確認 \(21 ページ\)](#)

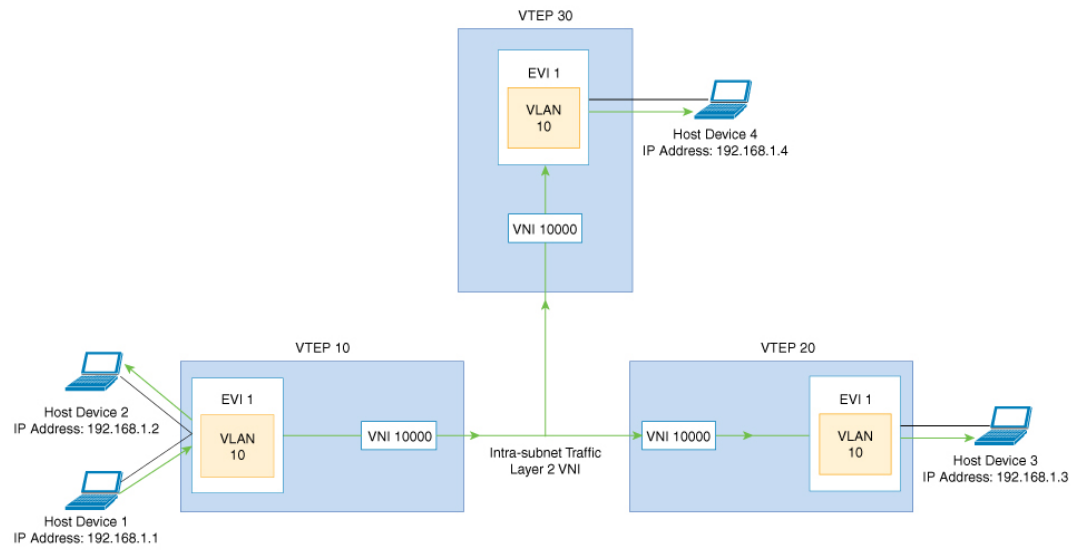
## EVPN VXLAN レイヤ2 オーバーレイネットワークについて

EVPN VXLAN レイヤ2 オーバーレイネットワークでは同じサブネット内のホストデバイスがブリッジドトラフィックまたはレイヤ2トラフィックを相互に送信できます。ネットワークはレイヤ2 仮想ネットワークインスタンス (VNI) を使用してブリッジドトラフィックを転送します。

## ブロードキャスト、不明ユニキャスト、およびマルチキャストのトラフィック

VXLAN ネットワークのマルチデスティネーションレイヤ2トラフィックは、通常、ブロードキャスト、不明ユニキャスト、およびマルチキャスト (BUM) トラフィックと呼ばれます。BGP EVPN VXLAN ファブリックでは、アンダーレイネットワークが VXLAN オーバーレイ内の共通のレイヤ2ブロードキャストドメインに接続されているすべてのエンドポイントに BUM トラフィックを転送します。

次の図に、レイヤ2 VNI を通過する BUM トラフィックのフローを示します。ネットワークは BUM トラフィックをホストデバイス 1 からすべての VTEP に転送し、VTEP は同じサブネット内のすべてのホストデバイスにトラフィックを送信します。



MP-BGP EVPN コントロールプレーンは VXLAN ネットワークで BUM トラフィックの転送に 2 つの異なる方法を使用します。

- アンダーレイマルチキャスト
- 入力のコピー

## アンダーレイマルチキャスト

アンダーレイマルチキャストでは、アンダーレイネットワークがマルチキャストグループを介してトラフィックを複製します。アンダーレイマルチキャストを使用して BUM トラフィックを転送するには、アンダーレイネットワークで IP マルチキャストを設定する必要があります。BUM トラフィックの 1 つのコピーが入力 VTEP または送信元 VTEP からアンダーレイ トランスポート ネットワークに移動します。ネットワークはこのコピーをマルチキャストツリーに沿って転送するため、このコピーは指定されたマルチキャストグループに参加しているすべての出力または宛先 VTEP に到達します。マルチキャストツリーに沿って移動している間、ネットワーク内のさまざまな分岐点でコピーが複製されます。これらの分岐点では、受信側が VNI に関連付けられたマルチキャストグループに含まれている場合のみコピーが複製されます。

アンダーレイマルチキャストによる BUM トラフィック転送は、レイヤ 2 VNI をマルチキャストグループにマッピングすることで実現します。このマッピングは、レイヤ 2 VNI に関連付けられているすべての VTEP で設定する必要があります。VTEP がマルチキャストグループに参加すると、そのグループで転送されるすべてのトラフィックを受信します。関連付けられていない VNI でトラフィックを受信すると、VTEP はそのトラフィックをドロップします。このアプローチは、ネットワーク内に 1 つのリンクを維持するため、BUM トラフィックを効率的に転送できます。

## 入力の複製

入力の複製（ヘッドエンドレプリケーション）はマルチデスティネーションレイヤ2オーバーレイ BUM トラフィックを処理するユニキャストアプローチです。入力の複製では、入力デバイスがすべての着信 BUM パケットを複製し、それらを個別のユニキャストとしてリモート出力デバイスに送信します。入力の複製はEVPNルートタイプ3を介して行われます。これは包括的マルチキャストイーサネットタグ（IMET）ルートとも呼ばれています。BGPEVPNの入力の複製では、VXLAN 経由で BUM トンネルを設定するためにリモートピアの自動検出に IMET ルートを使用します。入力の複製を使用して BUM トラフィックを処理すると、入力デバイスがレイヤ2 VNIに関連付けられた VTEP の数だけ BUM トラフィックを複製する必要があります。そのため、スケーリングの問題が発生する可能性があります。

### 入力の複製の操作

IMET ルートはリモートピアからアドバタイズされたリモート VNI または出力 VNI を伝送します。これはローカル VNI とは異なる場合があります。入力デバイスがリモート NVE ピアから IMET の入力の複製ルートを受信すると、ネットワークは VXLAN トンネルの隣接関係を作成します。トンネルの隣接関係は、VXLAN トンネルの IP または UDP のカプセル化を含む MID チェーンの隣接関係です。トンネルに複数の VNI がある場合、複数の VNI がトンネルを共有します。EVPN の入力の複製では、リモートピアごとに複数のユニキャストトンネル隣接関係とさまざまな出力 VNI を設定できます。

ネットワークは各 VTEP によってアドバタイズされたルートを使用してフラッドの複製リストを作成します。ダイナミック複製リストには、同じレイヤ2 VNI 内の BGP IMET ルートで検出されたすべてのリモートの宛先ピアが保存されます。複製リストはリモートピアでレイヤ2 VNI を設定するたびに更新されます。ネットワークはリモート NVE ピアが IMET の入力の複製ルートを取り消すたびに、トンネルの隣接関係と VXLAN のカプセル化を複製リストから削除します。NVE ピアを使用していない場合、ネットワークはトンネルの隣接関係を削除します。

入力デバイスに到達する BUM トラフィックは複製リストの作成後に複製されます。入力デバイスは複製されたトラフィックをネットワーク全体で同じ VNI 内のすべてのリモートピアに転送します。

## フラッドの抑制

EVPN では、ネットワークの VTEP 間での IPv4 または IPv6 アドレスと MAC アドレス間のバインディングを配布できます。MAC-IP ルートに関連付けられた EVPN インスタンスに参加するすべての VTEP 間に MAC-IP バインディングを配布します。IPv4 または IPv6 アドレスに関連付けられた MAC アドレスは、リモート VTEP から学習されてもローカルに認識されます。ローカルに接続されたエンドポイントは、リモートエンドポイントを検出するときに、Address Resolution Protocol (ARP) または IPv6 ネイバー検出要求を送信します。MAC-IP バインディングの配布により、VTEP は ARP または IPv6 ネイバー検出要求を受信すると、ローカルキャッシュ内でルックアップを実行できます。リモートエンドポイントの MAC-IP アドレス情報が使用可能な場合、VTEP はこの情報を使用して ARP 要求のフラッドを回避できます。リ

モートエンドポイントのMACまたはIPアドレス情報が使用できない場合、要求はファブリック全体にフラッディングします。

フラッディングを抑制することで、EVPN VXLAN ネットワーク上でのARPおよびIPv6ネイバー検出パケットのフラッディングを回避します。ローカルおよびリモートの両方のホストまたはアクセスデバイスへのフラッディングを抑制します。ネットワークは、ARPまたはネイバー検出リレーを実装することで、フラッディングを抑制します。これは、指定されたIPv4またはIPv6アドレスの既知のMACアドレスを使用し、ブロードキャストおよびマルチキャスト要求をユニキャスト要求に変換することによって実現されます。EVPN対応のVLANでは、フラッディングの抑制がデフォルトで有効になっています。EVPN VXLAN ネットワークは次のタイプのトラフィックのフラッディングを抑制します。

#### ARP フラッディングの抑制

VTEPはブロードキャストパケットとしてARP要求を送信します。ARP要求はレイヤ2ブロードキャストトラフィックの大部分を占めます。フラッディングの抑制では、それらをユニキャストパケットに変換し、ネットワークのフラッディングを軽減します。

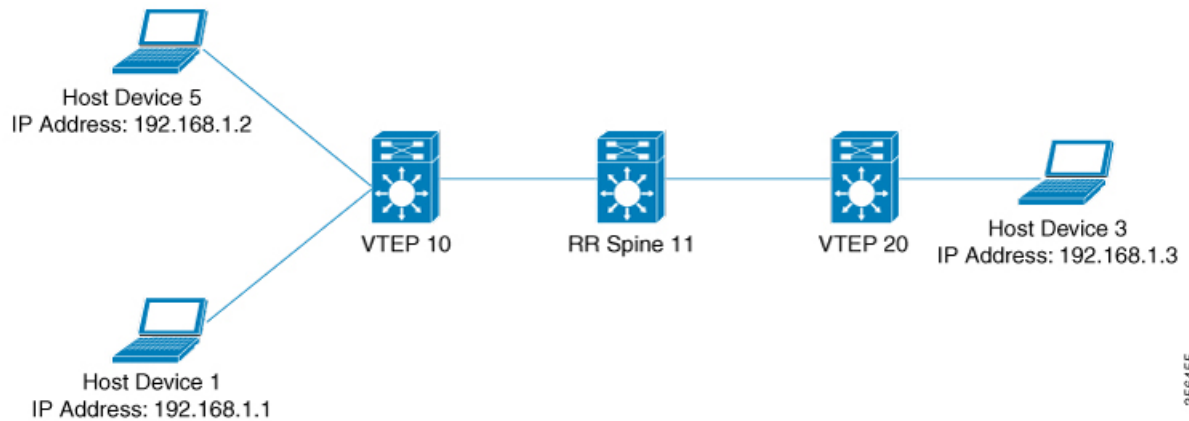
#### IPv6 ネイバー検出のフラッディングの抑制

IPv6ネイバー検出プロセスはネイバーの検出を可能にし、ピアが互いのリンク層アドレスを決定するのに役立ちます。また、ネイバーの到達可能性を確認し、ネイバールータを追跡します。IPv6ネイバー検出では、Internet Control Message Protocol (ICMP) のメッセージと要請ノードマルチキャストアドレスを使用して、これらの機能を実現します。

フラッディングの抑制はInternet Control Message Protocolバージョン6 (ICMPv6) パケット間のすべてのマルチキャストネイバー要請パケットを抑制します。

## EVPN VXLAN レイヤ2 オーバーレイネットワークの設定方法

次の図に、EVPN VXLAN ネットワークのトポロジ例を示します。ホストデバイス1とホストデバイス3は同じサブネットに含まれています。ネットワークはレイヤ2 VNIを使用して、アンダーレイマルチキャストまたは入力のコピー方式のいずれかでホストデバイス1からホストデバイス3にBUMトラフィックを転送します。



(注) 2-VTEP トポロジでは、スパインスイッチは必須ではありません。EVPN VXLAN ネットワークでのスパインスイッチの設定については、「*BGP EVPN VXLAN* ファブリック内でのスパインスイッチの設定」モジュールを参照してください。

EVPN VXLAN レイヤ2オーバーレイネットワークを設定し、BUMトラフィックを転送するには次の一連の手順を実行します。

- VTEP でレイヤ2 VPN EVPN を設定します。
- VTEP の VLAN に EVPN インスタンスを設定します。
- VTEP の VLAN にアクセス側インターフェイスを設定します。
- VTEP でループバック インターフェイスを設定します。
- VTEP でネットワーク仮想エンドポイント (NVE) インターフェイスを設定します。
- VTEP で EVPN アドレスファミリーを使用して BGP を設定します。
- 指定された複製タイプが静的の場合、アンダーレイマルチキャストを設定します。詳細については『*IP Multicast Routing Configuration Guide*』を参照してください。

## VTEP でのレイヤ2 VPN EVPN の設定

VTEP でレイヤ2 VPN EVPN パラメータを設定するには次の手順を実行します。

### 手順

	コマンドまたはアクション	目的
ステップ1	<b>enable</b> 例： Device> <b>enable</b>	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。

	コマンドまたはアクション	目的
ステップ 2	<b>configure terminal</b> 例： Device# <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 3	<b>l2vpn evpn</b> 例： Device(config)# <b>l2vpn evpn</b>	EVPN 設定モードを開始します。
ステップ 4	<b>replication-type {ingress   static}</b> 例： Device(config-evpn)# <b>replication-type static</b>	レイヤ 2 VPN EVPN 複製タイプを設定します。  (注) マルチキャストがEVPNBUM トラフィックのアンダーレイ ネットワークで有効になっている場合はレイヤ 2 VPN EVPN 複製タイプを静的に設定します。  レイヤ 2 VPN EVPN 複製タイプが静的として設定されている場合、IMET ルートはアドバタイズされず、BUM トラフィックの転送は各 VTEP で設定されるアンダーレイマルチキャストに依存します。
ステップ 5	<b>router-id loopback-interface-id</b> 例： Device(config-evpn)# <b>router-id loopback 0</b>	自動生成ルート識別子で使用する IP アドレスを提供するインターフェイスを指定します。
ステップ 6	<b>default-gateway advertise</b> 例： Device(config-evpn)# <b>default-gateway advertise</b>	(任意) スイッチでデフォルトゲートウェイアドバタイズメントを有効にします。MAC エイリアシングを使用して VXLAN ネットワークで分散型エニーキャストゲートウェイを設定するにはネットワーク内のすべてのリーフスイッチでデフォルトゲートウェイアドバタイズメントを有効にします。  このコマンドは、レイヤ 2 およびレイヤ 3 VNI が VRF に共存する Integrated Routing and Bridging (IRB) シナリオに適用できます。詳細については、「EVPN VXLAN Integrated Routing and

	コマンドまたはアクション	目的
		<p>Bridging の設定」モジュールを参照してください。</p> <p>このコマンドは、すべてのアクセスSVIで同じMACアドレスが手動で設定されていない場合にのみ必須です。</p> <p>(注) グローバルデフォルトゲートウェイアドバタイズメント設定を上書きし、それを特定のEVPNインスタンスに対して有効または無効にするには、EVPNインスタンスコンフィギュレーションモードで <b>default-gateway advertise {enable   disable}</b> コマンドを使用します。</p>
ステップ7	<b>logging peer state</b> 例： Device(config-evpn)# <b>logging peer state</b>	(任意) 最初のルートが受信されたとき、または最後のルートが特定のリモートVTEPから取り消されたときに、syslogメッセージを表示します。
ステップ8	<b>mac duplication limit limit-number time time-limit</b> 例： Device(config-evpn)# <b>mac duplication limit 20 time 5</b>	(任意) MACアドレスの重複を検出するためのパラメータを変更します。
ステップ9	<b>ip duplication limit limit-number time time-limit</b> 例： Device(config-evpn)# <b>ip duplication limit 20 time 5</b>	(任意) IPアドレスの重複を検出するためのパラメータを変更します。
ステップ10	<b>route-target auto vni</b> 例： Device(config-evpn)# <b>route-target auto vni</b>	(任意) EVPN インスタンス番号の代わりにVNIを使用してルートターゲットを自動生成するように指定します。
ステップ11	<b>exit</b> 例： Device(config-evpn)# <b>exit</b>	EVPN コンフィギュレーションモードを終了し、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 12	<b>l2vpn evpn instance evpn-instance-number vlan-based</b>  例 :  Device(config)# <b>l2vpn evpn instance 1 vlan-based</b>	レイヤ2 VPN コンフィギュレーション モードで VLAN ベースの EVPN インス タンスを設定します。  EVPN インスタンスを明示的に設定す る必要があるのは、ルートターゲット など、EVPN インスタンスごとに何か を設定する必要がある場合だけです。
ステップ 13	<b>encapsulation vxlan</b>  例 :  Device(config-evpn-evi) # <b>encapsulation vxlan</b>	(任意) カプセル化形式を VXLAN と して定義します。  デフォルトではカプセル化形式は VXLAN です。
ステップ 14	<b>replication-type {ingress   static}</b>  例 :  Device(config-evpn-evi) # <b>replication-type ingress</b>	(任意) EVPN インスタンスの複製タ イプを設定します。  グローバル複製タイプがすでに設定さ れている場合は、グローバル設定が上 書きされます。
ステップ 15	<b>default-gateway advertise {enable   disable}</b>  例 :  Device(config-evpn-evi) # <b>default-gateway advertise disable</b>	(任意) EVPN インスタンスのデフォ ルトゲートウェイアドバタイズメント を有効または無効にします。  デフォルトゲートウェイアドバタイズ メントがすでにグローバルに設定され ている場合は、これによってグローバル 設定が上書きされます。  このコマンドは、すべてのアクセスSVI で同じ MAC アドレスが手動で設定さ れていない場合にのみ必須です。  MAC エイリアシングを使用して VXLAN ネットワークで分散型エニー キャストゲートウェイを設定するには ネットワーク内のすべてのリーフス イッチでデフォルトゲートウェイアド バタイズメントを有効にします。
ステップ 16	<b>ip local-learning {enable   disable}</b>  例 :  Device(config-evpn-evi) # <b>ip local-learning disable</b>	(任意) 指定した EVPN インスタンス のローカル IP アドレスの学習を有効ま たは無効にします。



	コマンドまたはアクション	目的
		IP アドレスの学習がすでにグローバルに設定されている場合は、グローバル設定が上書きされます。
ステップ 17	<b>no auto-route-target</b> 例： Device (config-evpn-evi) # <b>no auto-route-target</b>	(任意) ルートターゲットの自動生成を無効にします。
ステップ 18	<b>rd rd-value</b> 例： Device (config-evpn-evi) # <b>rd 65000:100</b>	(任意) ルート識別子を手動で設定します。
ステップ 19	<b>route-target {import   export   both} rt-value</b> 例： Device (config-evpn-evi) # <b>route-target both 65000:100</b>	(任意) ルートターゲットを手動で設定します。  (注) 自動生成されたルートターゲット値 (ASN:EVI または ASN:VNI) が VTEP 間で異なる場合は、ルートターゲットを手動で設定します。
ステップ 20	<b>end</b> 例： Device (config-evpn-evi) # <b>end</b>	特権 EXEC モードに戻ります。

## VTEP の VLAN での EVPN インスタンスの設定

VTEP の VLAN に EVPN インスタンスを設定するには、次の手順を実行します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	特権 EXEC モードを有効にします。  プロンプトが表示されたらパスワードを入力します。
ステップ 2	<b>configure terminal</b> 例： Device# <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 3	<b>vlan configuration</b> <i>vlan-id</i> 例： Device(config)# <b>vlan configuration 11</b>	指定した VLAN インターフェイスの VLAN 機能コンフィギュレーションモードを開始します。
ステップ 4	<b>member evpn-instance</b> <i>evpn-instance-id vni l2-vni-number</i> 例： Device(config-vlan)# <b>member evpn-instance 1 vni 10000</b>	EVPN インスタンスを VLAN 設定のメンバーとして追加します。  ここでの VNI は、レイヤ 2 VNI として使用されます。
ステップ 5	<b>end</b> 例： Device(config-vlan)# <b>end</b>	特権 EXEC モードに戻ります。

## VTEP の VLAN でのアクセス側インターフェイスの設定

VTEP の VLAN にアクセス側インターフェイスを設定するには、次の手順を実行します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	特権 EXEC モードを有効にします。  プロンプトが表示されたらパスワードを入力します。
ステップ 2	<b>configure terminal</b> 例： Device# <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 3	<b>interface</b> <i>interface-name</i> 例： Device(config)# <b>interface GigabitEthernet1/0/1</b>	指定したインターフェイスに対してインターフェイス コンフィギュレーションモードを開始します。
ステップ 4	<b>switchport access vlan</b> <i>vlan-id</i> 例： Device(config-if)# <b>switchport access vlan 11</b>	指定した VLAN の静的アクセスポートとしてインターフェイスを設定します。  必要に応じて、インターフェイスをトランクインターフェイスとして設定することもできます。
ステップ 5	<b>end</b> 例：	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	Device(config-if) # <b>end</b>	

## VTEP でのループバック インターフェイスの設定

VTEP にループバック インターフェイスを設定するには、次の手順を実行します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	<b>configure terminal</b> 例： Device# <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 3	<b>interface loopback-interface-id</b> 例： Device(config)# <b>interface Loopback0</b>	指定したループバック インターフェイスのインターフェイスコンフィギュレーションモードを開始します。
ステップ 4	<b>ip address ipv4-address</b> 例： Device(config-if)# <b>ip address 10.12.11.11</b>	ループバック インターフェイスの IP アドレスを設定します。
ステップ 5	<b>ip pim sparse mode</b> 例： Device(config-if)# <b>ip pim sparse mode</b>	ループバック インターフェイスで Protocol Independent Multicast (PIM) スパースモードを有効にします。
ステップ 6	<b>end</b> 例： Device(config-vlan)# <b>end</b>	特権 EXEC モードに戻ります。

## VTEP での NVE インターフェイスの設定

VTEP の NVE インターフェイスに VNI メンバーを追加するには、次の手順を実行します。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	<b>configure terminal</b> 例： Device# <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 3	<b>interface nve-interface-id</b> 例： Device(config)# <b>interface nve1</b>	トランクとして設定するインターフェイスを定義し、インターフェイスコンフィギュレーション モードを開始します。
ステップ 4	<b>no ip address</b> 例： Device(config-if)# <b>no ip address</b>	対応する IP アドレスを削除することによって、インターフェイス上での IP 処理をディセーブルにします。
ステップ 5	<b>source-interface loopback-interface-id</b> 例： Device(config-if)# <b>source-interface loopback0</b>	指定したループバック インターフェイスの IP アドレスを送信元 IP アドレスとして設定します。
ステップ 6	<b>host-reachability protocol bgp</b> 例： Device(config-if)# <b>host-reachability protocol bgp</b>	インターフェイス上で BGP をホスト到達可能性プロトコルとして設定します。
ステップ 7	<b>member vni layer2-vni-id</b> { <b>ingress-replication</b>   <b>mcast-group</b> <i>multicast-group-address</i> 例： Device(config-if)# <b>member vni 10000 mcast-group 227.0.0.1</b>	レイヤ 2 VNI メンバーを NVE に関連付けます。 指定した複製タイプは、グローバルに設定するか、または特定の EVPN インスタンスに対して設定している複製タイプと一致する必要があります。静的複製には <b>mcast-group</b> キーワードを使用し、入力の複製には <b>ingress-replication</b> キーワードを使用します。
ステップ 8	<b>end</b> 例： Device(config-if)# <b>end</b>	特権 EXEC モードに戻ります。

## EVPN アドレスファミリーを使用した VTEP での BGP の設定

EVPN アドレスファミリーとスパインスイッチをネイバーとして使用して VTEP で BGP を設定するには、次の手順を実行します。

### 手順

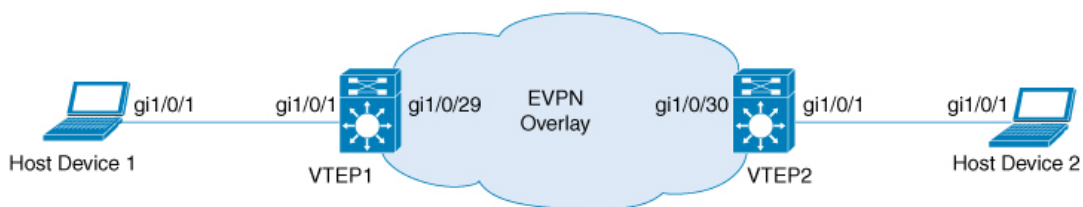
	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	<b>configure terminal</b> 例： Device# <b>configure terminal</b>	グローバル コンフィギュレーションモードを開始します。
ステップ 3	<b>router bgp autonomous-system-number</b> 例： Device(config)# <b>router bgp 1</b>	BGP ルーティングプロセスを有効にし、自律システム番号を割り当て、ルータ コンフィギュレーションモードを開始します。
ステップ 4	<b>bgp log-neighbor-changes</b> 例： Device(config-router)# <b>bgp log-neighbor-changes</b>	(任意) BGP ネイバーのステータスが変更された場合のロギングメッセージの生成を有効にします。 詳細については、『 <i>IP Routing Configuration Guide</i> 』の「 <i>Configuring BGP</i> 」モジュールを参照してください。
ステップ 5	<b>bgp update-delay time-period</b> 例： Device(config-router)# <b>bgp update-delay 1</b>	(任意) 最初の更新を送信するまでの最大初期遅延期間を設定します。 指定できる範囲は 1 ~ 3600 秒です。 詳細については、『 <i>IP Routing Configuration Guide</i> 』の「 <i>Configuring BGP</i> 」モジュールを参照してください。
ステップ 6	<b>bgp graceful-restart</b> 例： Device(config-router)# <b>bgp graceful-restart</b>	(任意) すべての BGP ネイバーで BGP グレースフルリスタート機能を有効にします。 詳細については、『 <i>IP Routing Configuration Guide</i> 』の「 <i>Configuring BGP</i> 」モジュールを参照してください。

	コマンドまたはアクション	目的
ステップ 7	<b>no bgp default ipv4-unicast</b> 例： Device(config-router)# <b>no bgp default ipv4-unicast</b>	(任意) デフォルトの IPv4 ユニキャストアドレスファミリーを無効にして BGP ピアリングセッションを確立します。 詳細については、『 <i>IP Routing Configuration Guide</i> 』の「 <i>Configuring BGP</i> 」モジュールを参照してください。
ステップ 8	<b>neighbor ip-address remote-as number</b> 例： Device(config-router)# <b>neighbor 10.11.11.11 remote-as 1</b>	マルチプロトコル BGP ネイバーを定義します。各ネイバーでレイヤ 2 仮想プライベートネットワーク (L2VPN) EVPN 設定を定義します。 スパインスイッチの IP アドレスをネイバー IP アドレスとして使用します。
ステップ 9	<b>neighbor {ip-address   group-name} update-source interface</b> 例： Device(config-router)# <b>neighbor 10.11.11.11 update-source Loopback0</b>	更新元を設定します。更新元は、ネイバーごとか、またはピアグループごとに設定できます。 スパインスイッチの IP アドレスをネイバー IP アドレスとして使用します。
ステップ 10	<b>address-family l2vpn evpn</b> 例： Device(config-router)# <b>address-family l2vpn evpn</b>	L2VPN アドレスファミリーを指定し、アドレスファミリー コンフィギュレーションモードを開始します。
ステップ 11	<b>neighbor ip-address activate</b> 例： Device(config-router-af)# <b>neighbor 10.11.11.11 activate</b>	BGP ネイバーからの情報交換を有効にします。 スパインスイッチの IP アドレスをネイバー IP アドレスとして使用します。
ステップ 12	<b>neighbor ip-address send-community [both   extended   standard]</b> 例： Device(config-router-af)# <b>neighbor 10.11.11.11 send-community both</b>	BGP ネイバーに送信したコミュニティ属性を指定します。 スパインスイッチの IP アドレスをネイバー IP アドレスとして使用します。
ステップ 13	<b>exit-address-family</b> 例： Device(config-router-af)# <b>exit-address-family</b>	アドレスファミリー コンフィギュレーションモードを終了し、ルータ コンフィギュレーションモードに戻ります。
ステップ 14	<b>end</b> 例：	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	Device (config-router) # <b>end</b>	

## EVPN VXLAN レイヤ2オーバーレイネットワークの設定例

この項では、EVPN VXLAN レイヤ2オーバーレイネットワークの設定例を示します。次に、2つのVTEP（VTEP1とVTEP2）が接続され、ブリッジングを実行するVXLANネットワークの設定例を示します。



356465



- (注) 2-VTEP トポロジでは、スパインスイッチは必須ではありません。EVPN VXLAN ネットワークでのスパインスイッチの設定については、「*BGP EVPN VXLAN* ファブリック内でのスパインスイッチの設定」モジュールを参照してください。

表 1: 2つの VTEP を接続してブリッジングを実行する VXLAN ネットワークの設定例

VTEP 1	VTEP 2
--------	--------



VTEP 1	VTEP 2
<pre> VTEP1# show running-config Building configuration... ! hostname VTEP1 ! ip routing ip multicast-routing ! l2vpn evpn   replication-type static   router-id Loopback0 ! l2vpn evpn instance 1 vlan-based   encapsulation vxlan   route-target export 103:1   route-target import 104:1 ! system mtu 9150 ! vlan configuration 201   member evpn-instance 1 vni 6000 ! ! interface Loopback0   ip address 10.1.1.10 255.255.255.255   ip pim sparse-mode ! ! interface GigabitEthernet1/0/1   description host1-interface   switchport access vlan 201   switchport mode access ! ! interface GigabitEthernet1/0/29   description core-underlay-interface   no switchport   ip address 172.16.1.29 255.255.255.0   ip pim sparse-mode ! ! interface nve10   no ip address   source-interface Loopback0   host-reachability protocol bgp   member vni 6000 mcast-group 232.1.1.1 ! router ospf 1   router-id 10.1.1.10   network 10.1.1.0 0.0.0.255 area 0   network 172.16.1.0 0.0.0.255 area 0 ! router bgp 10   bgp router-id interface Loopback0   bgp log-neighbor-changes   bgp update-delay 1   no bgp default ipv4-unicast   neighbor 10.2.2.20 remote-as 10   neighbor 10.2.2.20 update-source Loopback0 ! address-family ipv4 exit-address-family </pre>	<pre> VTEP2# show running-config Building configuration... ! hostname VTEP2 ! ip routing ip multicast-routing ! l2vpn evpn   replication-type static   router-id Loopback0 ! l2vpn evpn instance 1 vlan-based   encapsulation vxlan   route-target export 104:1   route-target import 103:1 ! system mtu 9150 ! vlan configuration 201   member evpn-instance 1 vni 6000 ! ! interface Loopback0   ip address 10.2.2.20 255.255.255.255   ip pim sparse-mode ! ! interface GigabitEthernet1/0/1   description host2-interface   switchport access vlan 201   switchport mode access ! ! interface GigabitEthernet1/0/30   description core-underlay-interface   no switchport   ip address 172.16.1.30 255.255.255.0   ip pim sparse-mode ! ! interface nve10   no ip address   source-interface Loopback0   host-reachability protocol bgp   member vni 6000 mcast-group 232.1.1.1 ! router ospf 1   router-id 10.2.2.20   network 10.2.2.0 0.0.0.255 area 0   network 172.16.1.0 0.0.0.255 area 0 ! router bgp 10   bgp router-id interface Loopback0   bgp log-neighbor-changes   bgp update-delay 1   no bgp default ipv4-unicast   neighbor 10.1.1.10 remote-as 10   neighbor 10.1.1.10 update-source Loopback0 ! address-family ipv4 exit-address-family </pre>

VTEP 1	VTEP 2
<pre> ! address-family l2vpn evpn   neighbor 10.2.2.20 activate   neighbor 10.2.2.20 send-community both exit-address-family ! ip pim rp-address 10.1.1.10 ! end </pre>	<pre> ! address-family l2vpn evpn   neighbor 10.1.1.10 activate   neighbor 10.1.1.10 send-community both exit-address-family ! ip pim rp-address 10.1.1.10 ! end </pre>

次に、上記で設定したトポロジの VTEP 1 と VTEP 2 での **show** コマンドの出力例を示します。

- [show l2vpn evpn peers vxlan](#) (18 ページ)
- [show nve peers](#) (18 ページ)
- [show l2vpn evpn mac](#) (19 ページ)
- [show bgp l2vpn evpn all](#) (19 ページ)
- [show platform software fed switch active matm macTable vlan](#) (20 ページ)

### show l2vpn evpn peers vxlan

#### VTEP 1

次に、VTEP 1 での **show l2vpn evpn peers vxlan** コマンドの出力例を示します。

```

VTEP1# show l2vpn evpn peers vxlan
Interface VNI      Peer-IP              Num routes eVNI      UP time
-----
nve10     6000      10.2.2.20           3          6000     00:12:44

```

#### VTEP 2

次に、VTEP 2 での **show l2vpn evpn peers vxlan** コマンドの出力例を示します。

```

VTEP2# show l2vpn evpn peers vxlan
Interface VNI      Peer-IP              Num routes eVNI      UP time
-----
nve10     6000      10.1.1.10           3          6000     00:01:41

```

### show nve peers

#### VTEP 1

次に、VTEP 1 での **show nve peers** コマンドの出力例を示します。

```

VTEP1# show nve peers
Interface VNI      Type Peer-IP              RMAC/Num_RTs  eVNI      state flags UP time
-----
nve10     6000      L2CP 10.2.2.20       3          6000     UP      N/A  00:12:48

```

## VTEP 2

次に、VTEP 2 での **show nve peers** コマンドの出力例を示します。

```
VTEP2# show nve peers
Interface VNI      Type Peer-IP          RMAC/Num_RTs  eVNI  state flags UP time
nve10     6000    L2CP 10.1.1.10      3           6000    UP   N/A  00:01:46
```

## show l2vpn evpn mac

## VTEP 1

次に、VTEP 1 での **show l2vpn evpn mac** コマンドの出力例を示します。

```
VTEP1# show l2vpn evpn mac
MAC Address      EVI  VLAN  ESI                      Ether Tag  Next Hop(s)
-----
0018.736c.5681  1    201   0000.0000.0000.0000.0000  0          10.2.2.20
0018.736c.56c3  1    201   0000.0000.0000.0000.0000  0          10.2.2.20
0059.dc50.ae01  1    201   0000.0000.0000.0000.0000  0          Gi1/0/1:201
0059.dc50.ae4c  1    201   0000.0000.0000.0000.0000  0          Gi1/0/1:201
```

## VTEP 2

次に、VTEP 2 での **show l2vpn evpn mac** コマンドの出力例を示します。

```
VTEP2# show l2vpn evpn mac
MAC Address      EVI  VLAN  ESI                      Ether Tag  Next Hop(s)
-----
0018.736c.5681  1    201   0000.0000.0000.0000.0000  0          Gi1/0/1:201
0018.736c.56c3  1    201   0000.0000.0000.0000.0000  0          Gi1/0/1:201
0059.dc50.ae01  1    201   0000.0000.0000.0000.0000  0          10.1.1.10
0059.dc50.ae4c  1    201   0000.0000.0000.0000.0000  0          10.1.1.10
```

## show bgp l2vpn evpn all

## VTEP 1

次に、VTEP 1 での **show bgp l2vpn evpn all** コマンドの出力例を示します。

```
VTEP1# show bgp l2vpn evpn all
BGP table version is 101, local router ID is 10.1.1.10
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
               x best-external, a additional-path, c RIB-compressed,
               t secondary path, L long-lived-stale,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

      Network          Next Hop          Metric LocPrf Weight Path
Route Distinguisher: 10.1.1.10:1
*>i  [2][10.1.1.10:1][0][48][0018736C5681][0][*]/20
      10.2.2.20          0      100      0 ?
*>i  [2][10.1.1.10:1][0][48][0018736C56C3][0][*]/20
      10.2.2.20          0      100      0 ?
```

```

*>i [2] [10.1.1.10:1] [0] [48] [0018736C56C3] [32] [192.168.1.89]/24
      10.2.2.20 0 100 0 ?
*> [2] [10.1.1.10:1] [0] [48] [0059DC50AE01] [0] [*]/20
      :: 32768 ?
*> [2] [10.1.1.10:1] [0] [48] [0059DC50AE4C] [0] [*]/20
      :: 32768 ?
*> [2] [10.1.1.10:1] [0] [48] [0059DC50AE4C] [32] [192.168.1.81]/24
      :: 32768 ?
Route Distinguisher: 10.2.2.20:1
*>i [2] [10.2.2.20:1] [0] [48] [0018736C5681] [0] [*]/20
      10.2.2.20 0 100 0 ?
*>i [2] [10.2.2.20:1] [0] [48] [0018736C56C3] [0] [*]/20
      10.2.2.20 0 100 0 ?
*>i [2] [10.2.2.20:1] [0] [48] [0018736C56C3] [32] [192.168.1.89]/24
      10.2.2.20 0 100 0 ?

```

## VTEP 2

次に、VTEP 2 での **show bgp l2vpn evpn all** コマンドの出力例を示します。

```

VTEP2# show bgp l2vpn evpn all
BGP table version is 99, local router ID is 10.2.2.20
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
               x best-external, a additional-path, c RIB-compressed,
               t secondary path, L long-lived-stale,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found
      Network          Next Hop          Metric LocPrf Weight Path
Route Distinguisher: 10.1.1.10:1
*>i [2] [10.1.1.10:1] [0] [48] [0059DC50AE01] [0] [*]/20
      10.1.1.10 0 100 0 ?
*>i [2] [10.1.1.10:1] [0] [48] [0059DC50AE4C] [0] [*]/20
      10.1.1.10 0 100 0 ?
*>i [2] [10.1.1.10:1] [0] [48] [0059DC50AE4C] [32] [192.168.1.81]/24
      10.1.1.10 0 100 0 ?
Route Distinguisher: 10.2.2.20:1
*> [2] [10.2.2.20:1] [0] [48] [0018736C5681] [0] [*]/20
      :: 32768 ?
*> [2] [10.2.2.20:1] [0] [48] [0018736C56C3] [0] [*]/20
      :: 32768 ?
*> [2] [10.2.2.20:1] [0] [48] [0018736C56C3] [32] [192.168.1.89]/24
      Network          Next Hop          Metric LocPrf Weight Path
      :: 32768 ?
*>i [2] [10.2.2.20:1] [0] [48] [0059DC50AE01] [0] [*]/20
      10.1.1.10 0 100 0 ?
*>i [2] [10.2.2.20:1] [0] [48] [0059DC50AE4C] [0] [*]/20
      10.1.1.10 0 100 0 ?
*>i [2] [10.2.2.20:1] [0] [48] [0059DC50AE4C] [32] [192.168.1.81]/24
      10.1.1.10 0 100 0 ?

```

## show platform software fed switch active matm macTable vlan

## VTEP 1

次に、VTEP 1 での **show platform software fed switch active matm mactable vlan** コマンドの出力例を示します。

```
VTEP1# show platform software fed switch active matm macTable vlan 201
VLAN  MAC                               Type Seq#  EC_Bi  Flags machandle          siHandle
      riHandle                            diHandle          *a_time *e_time  ports
-----
201   0018.736c.5681 0x1000001 0      0      64 0x7f5d852abaf8 0x7f5d850c1858
      0x7f5d8527def8 0x0          0      0      RLOC 10.2.2.20 adj_id
81
201   0018.736c.56c3 0x1000001 0      0      64 0x7f5d855be2b8 0x7f5d850c1858
      0x7f5d8527def8 0x0          0      0      RLOC 10.2.2.20 adj_id
81
201   0059.dc50.ae01 0x1      22     0      0      0x7f5d855c6388 0x7f5d85035248
      0x0          0x7f5d8517eae8 300    11    GigabitEthernet1/0/1
201   0059.dc50.ae4c 0x1      26     0      0      0x7f5d84fba3c8 0x7f5d85035248
      0x0          0x7f5d8517eae8 300    58    GigabitEthernet1/0/1

Total Mac number of addresses:: 4
```

## VTEP 2

次に、VTEP 2 での `show platform software fed switch active matm mactable vlan` コマンドの出力例を示します。

```
VTEP2# show platform software fed switch active matm macTable vlan 201
VLAN  MAC                               Type Seq#  EC_Bi  Flags machandle          siHandle
      riHandle                            diHandle          *a_time *e_time  ports
-----
201   0018.736c.5681 0x1      38     0      0      0x7f40e196cac8 0x7f40e196cf28
      0x0          0x7f40e0f6da38 300    12    GigabitEthernet1/0/1
201   0018.736c.56c3 0x1      39     0      0      0x7f40e19b6878 0x7f40e196cf28
      0x0          0x7f40e0f6da38 300    17    GigabitEthernet1/0/1
201   0059.dc50.ae01 0x1000001 0      0      64 0x7f40e19b88f8 0x7f40e1937b88
      0x7f40e193bd58 0x0          0      17    RLOC 10.1.1.10 adj_id
28
201   0059.dc50.ae4c 0x1000001 0      0      64 0x7f40e194d638 0x7f40e1937b88
      0x7f40e193bd58 0x0          0      17    RLOC 10.1.1.10 adj_id
28

Total Mac number of addresses:: 4
```

# EVPN VXLAN レイヤ2オーバーレイネットワークの確認

次の表に、レイヤ2 VXLAN オーバーレイネットワークの確認に使用する `show` コマンドを示します。

表 2: EVPN VXLAN レイヤ2オーバーレイネットワークを確認するコマンド

コマンド	目的
<code>show l2vpn evpn evi [detail]</code>	特定の EVPN インスタンスまたはすべての EVPN インスタンスの詳細情報を表示します。

コマンド	目的
<b>show l2vpn evpn mac [detail]</b>	レイヤ2 EVPN の MAC アドレスデータベースを表示します。
<b>show l2vpn evpn mac ip [detail]</b>	レイヤ2 EVPN の IP アドレスデータベースを表示します。
<b>show l2vpn evpn summary</b>	レイヤ2 EVPN 情報の要旨を表示します。
<b>show l2vpn evpn capabilities</b>	レイヤ2 EVPN のプラットフォーム機能情報を表示します。
<b>show l2vpn evpn peers</b>	レイヤ2 EVPN ピアルートカウントと稼働時間を表示します。
<b>show l2vpn evpn route-target</b>	レイヤ2 EVPN インポートルートのターゲットを表示します。
<b>show l2vpn evpn memory</b>	レイヤ2 EVPN メモリの使用量を表示します。
<b>show l2route evpn summary</b>	EVPN ルートの要旨を表示します。
<b>show l2route evpn mac [detail]</b>	EVPN コントロールプレーンでスイッチが学習した MAC アドレス情報を表示します。
<b>show l2route evpn mac ip [detail]</b>	EVPN コントロールプレーンでスイッチが学習した MAC アドレスと IP アドレス情報を表示します。
<b>show l2route evpn imet detail</b>	レイヤ2 EVPN アドレスファミリの IMET ルートの詳細を表示します。  このコマンドは、入力の複製を使用して転送されたトラフィックに関する詳細のみを表示します。
<b>show bgp l2vpn evpn</b>	レイヤ2 VPN EVPN アドレスファミリの BGP 情報を表示します。
<b>show bgp l2vpn evpn route-type 2</b>	L2VPN EVPN アドレスファミリのルートタイプ 2 の BGP 情報を表示します。
<b>show bgp l2vpn evpn evi context</b>	レイヤ2 EVPN インスタンスのコンテキスト情報を表示します。

コマンド	目的
<b>show bgp l2vpn evpn evi <i>evpn-instance-id</i> route-type 3</b>	指定したレイヤ2 EVPN インスタンスのルートタイプ3情報を表示します。  このコマンドは、入力の複製を使用して転送されたトラフィックに関する詳細のみを表示します。
<b>show l2fib bridge-domain <i>bridge-domain-number</i> detail</b>	レイヤ2 転送情報ベースのブリッジドメインの詳細情報を表示します。
<b>show l2fib bridge-domain <i>bridge-domain-number</i> address unicast</b>	レイヤ2 転送情報ベースのブリッジドメインのユニキャストMACアドレス情報を表示します。
<b>show nve vni</b>	NVE インターフェイスに関連付けられたVXLAN ネットワーク識別子のメンバーに関する情報を表示します。
<b>show nve vni <i>vni-id</i> detail</b>	VXLAN ネットワーク識別子のメンバーの詳細なNVEインターフェイスの状態の情報を表示します。
<b>show nve peers</b>	ピアリーフスイッチのNVEインターフェイスの状態の情報を表示します。
<b>show mac address-table vlan <i>vlan-id</i></b>	VLAN の MAC アドレスを表示します。
<b>show platform software fed switch active matm macTable vlan <i>vlan-id</i></b>	転送エンジンドライバ (FED) のMACアドレステーブル マネージャ データベースからVLAN の MAC アドレスを表示します。
<b>show device-tracking database</b>	デバイストラッキングデータベースを表示します。
<b>show device-tracking database mac</b>	デバイストラッキング MAC アドレスデータベースを表示します。
<b>show ip mroute</b>	マルチキャストルーティングテーブル情報を表示します。

