外部 VRF 接続とルート リークの設定

この章は、次の内容で構成されています。

外部 VRF 接続の設定

VXLAN BGP EVPN ファブリックの外部レイヤ 3 接続について

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

外部 VRF 接続とルート リークの注意事項と制約事項

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

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

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

ルート リークの設定

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

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

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

外部 VRF 接続とルート リークの注意事項と制約事項

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

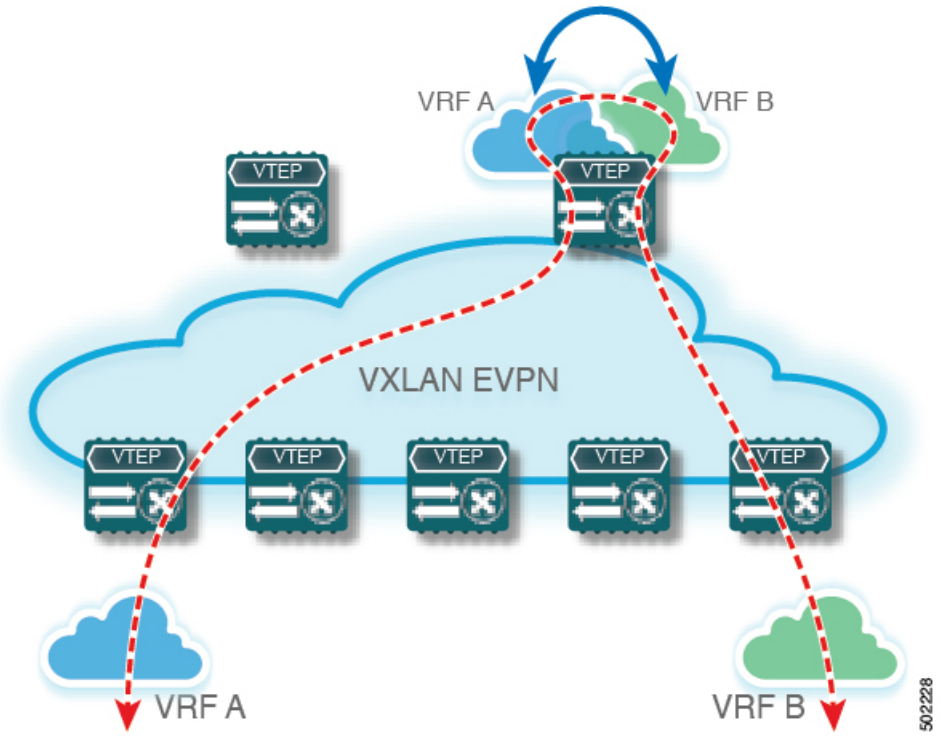
- Cisco Nexus 3600 プラットフォーム スイッチのサポートが追加されました。
- 物理レイヤ 3 インターフェイス（親インターフェイス）は、外部レイヤ 3 接続（つまり、VRF デフォルト）に使用できます。
- 複数のサブインターフェイスへの親インターフェイスは、外部レイヤ 3 接続（つまり、VRF デフォルトのイーサネット 1/1）には使用できません。代わりにサブインターフェイスを使用できます。
- サブインターフェイスが構成されている場合、VTEP は親インターフェイス上の VXLAN カプセル化トラフィックをサポートしません。これは、VRF 参加に関係ありません。
- VTEP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

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

次に、いくつかのポイントを示します。

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

図 *1* : 中央集中型 *VRF* ルートリーク：カスタム *VRF* による共有インターネット



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

ルーティング ブロック VTEP での VRF コンテキストの設定

この手順は、IPv6 にも同様に適用されます。

手順の概要

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

手順の詳細

手順

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

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

ルーティング ブロックでの BGP VRF インスタンスの設定

この手順は、IPv6 にも同様に適用されます。

手順の概要

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

手順の詳細

手順

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

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

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

VXLAN BGP EVPN ルーティング ブロックの設定

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

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

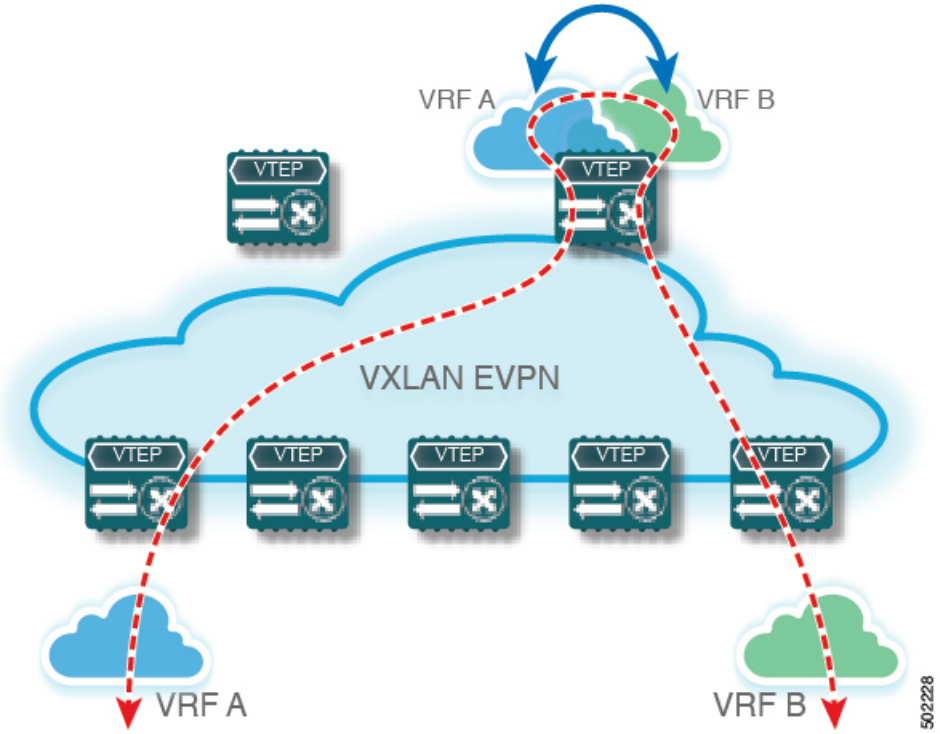
```
!
vlan 2120
  vn-segment 51020
!
interface Vlan2120
  no shutdown
  mtu 9216
  vrf member Blue
  no ip redirects
  ip forward
!
interface nve1
  no shutdown
  host-reachability protocol bgp
  source-interface loopback1
  member vni 51010 associate-vrf
  member vni 51020 associate-vrf
!
router bgp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

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

次に、いくつかのポイントを示します。

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

図 *2:* 中央集中型 *VRF* ルートリーク：カスタム *VRF* による共有インターネット



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

ボーダー ノードでのインターネット VRF の設定

この手順は、IPv6 にも同様に適用されます。

手順の概要

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

手順の詳細

手順

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

ボーダー ノードでの共有インターネット BGP インスタンスの設定

この手順は、IPv6 にも同様に適用されます。

手順の概要

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

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

手順の詳細

手順

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

ボーダーノードでのカスタム VRF コンテキストの設定 - 1

この手順は、IPv6 にも同様に適用されます。

手順の概要

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

手順の詳細

手順

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

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

ボーダー ノードでの BGP でのカスタム VRF インスタンスの設定

この手順は、IPv6 にも同様に適用されます。

手順の概要

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

手順の詳細

手順

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

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

共有インターネット VRF による中央集中型 VRF ルート リークの例

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

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

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

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

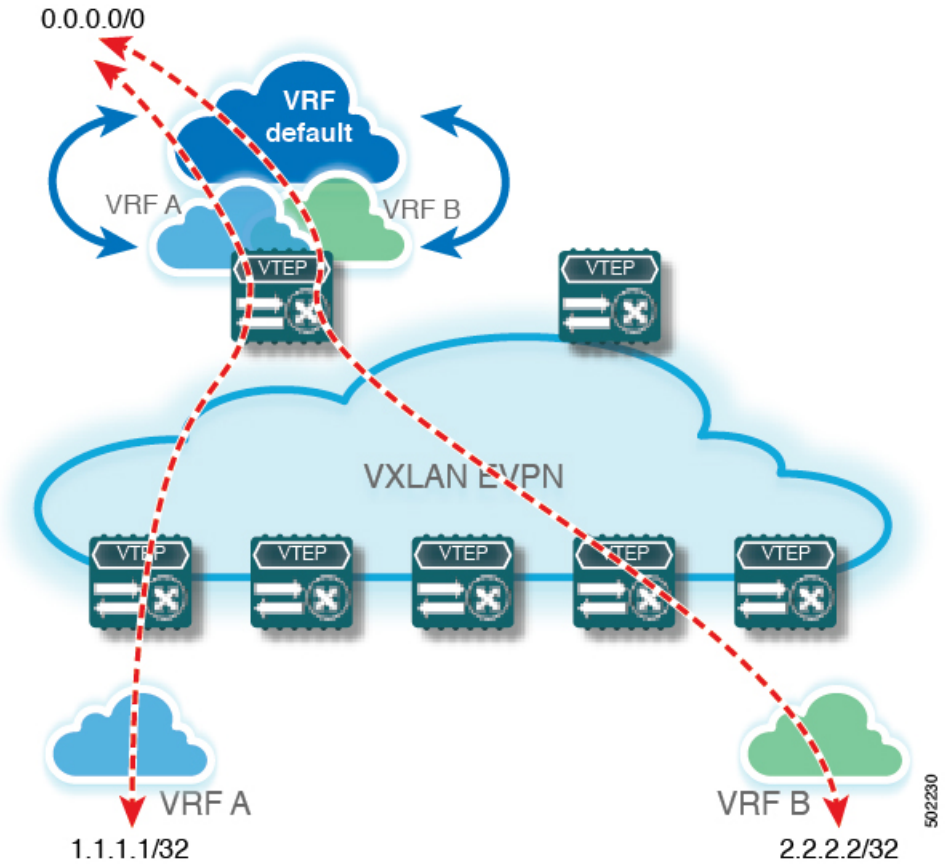
一元管理型 VRF ルート リーク ブリーフ：VRF デフォルトでの共有インターネット

いくつかのポインタを次に示します。

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

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

図 *3 :* 中央集中型 *VRF* ルートリーク：*VRF* デフォルトでの共有インターネット



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

ボーダー ノードでの VRF デフォルトの設定

この手順は、IPv6 にも同様に適用されます。

手順の概要

1. **configure terminal**

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

手順の詳細

手順

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

ボーダー ノードでの VRF デフォルトの BGP インスタンスの設定

この手順は、IPv6 にも同様に適用されます。

手順の概要

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

手順の詳細

手順

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

ボーダー ノードでのカスタム VRF の設定

この手順は、IPv6 にも同様に適用されます。

手順の概要

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

手順の詳細

手順

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

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

この手順は、IPv6 にも同様に適用されます。

手順の概要

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

手順の詳細

手順

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

ボーダーノードでのカスタム VRF コンテキストの設定 - 2

この手順は、IPv6 にも同様に適用されます。

手順の概要

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

手順の詳細

手順

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

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

ボーダー ノードでの BGP でのカスタム VRF インスタンスの設定

この手順は、IPv6 にも同様に適用されます。

手順の概要

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

手順の詳細

手順

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

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

VRF デフォルトによる中央集中型 VRF ルート リークの例

VRF デフォルトの VXLAN BGP EVPN ボーダー ノードの設定

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

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

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

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。