ACI ファブリックのレイヤ 3 Outside 接続

この章の内容は、次のとおりです。

BGP レイヤ 3 外部ネットワーク接続設定のガイドライン

BGP 外部ルーテッド ネットワークを設定するときは、以下のガイドラインに従ってください。

- リーフ スイッチにルータ ID を作成すると、必ず内部ループバック アドレスが作成されます。リーフ スイッチに BGP 接続をセットアップする場合、ルート ID をインターフェイスの IP アドレスと同じにすることはできません。これは、その設定が ACI リーフ スイッチではサポートされていないためです。ルータ ID は、別のサブネット内の別のアドレスである必要があります。外部レイヤ 3 デバイスでは、ルータ ID はループバック アドレスまたはインターフェイス アドレスです。スタティック ルートまたは OSPF 設定のいずれかを使用して、レイヤ 3 デバイスのルーティング テーブルにリーフ ルータ ID へのルートが存在することを確認してください。また、レイヤ 3 デバイスに BGP ネイバーをセットアップする場合、使用するピア IP アドレスはリーフ スイッチのルータ ID である必要があります。
- BGP を使用する 2 つの外部レイヤ 3 ネットワークを同じノードに設定する際、ループバック アドレスを明示的に定義する必要があります。このガイドラインに従わないと、BGP を確立できない可能性があります。

- 定義上、ルータ ID はループバック インターフェイスです。ルータ ID を変更してループバックに別のアドレスを割り当てるには、ループバック インターフェイス ポリシーを作成する必要があります（ループバック ポリシーは、アドレス ファミリ、IPv4、および IPv6 ごとに 1 つずつ設定できます）。ループバック ポリシーを作成しない場合は、ルータ ID ループバック（デフォルトで有効）を有効にすることができます。ルータ ID ループバックが無効である場合、導入先の特定のレイヤ 3 Outside に対するループバックは作成されません。
- この設定作業は iBGP および eBGP に適用されます。BGP 設定がループバック アドレスに対するものである場合、iBGP セッションまたはマルチホップ eBGP セッションです。ピア IP アドレスが BGP ピアが定義されている物理インターフェイスに対するものである場合、物理インターフェイスが使用されます。
- IPv6 を使用したループバックを介したピアリングを有効にするには、ユーザが IPv6 アドレスを設定する必要があります。
- 自律システム機能は eBGP ピアでしか使用できません。この機能では、ルータが実際の AS に加えて、2 番めの自律システム（AS）のメンバであるように見せることができます。ローカル AS を使用すると、ピアリングの調整を変更せずに 2 つの ISP をマージできます。マージされた ISP 内のルータは、新しい自律システムのメンバになりますが、使用者に対しては古い自律システム番号を使用し続けます。
- リリース 1.2（1x）以降、BGP `l3extOut` 接続のテナント ネットワーキング プロトコル ポリシーは、最大プレフィックス制限を使用して設定できます。これにより、ピアから受信されるルートプレフィックスの数をモニタし、制限することができます。最大プレフィックス制限を超えると、ログエントリの記録、それ以降のプレフィックスの拒否、固定期間中にカウントがしきい値未満になった場合の接続の再起動、または接続のシャットダウンを行うことができます。一度に 1 つのオプションだけを使用できます。デフォルト設定では 20,000 プレフィックスに制限され、その後は新しいプレフィックスは拒否されます。拒否オプションが導入されると、BGP は設定されている制限よりも 1 つ多くプレフィックスを受け入れ、APIC でエラーが発生します。

BGP 接続タイプおよびループバックのガイドライン

BGP 接続タイプおよびループバックの設定要件については、以下のガイドラインに従ってください。

- ノードのルータ ID が作成されると、ルータ ID と同じ IP アドレスでループバック インターフェイスも作成されます。これはデフォルトの動作ですが、ルータ ID を設定するときにオーバーライドできます。
- ルータ ID に対して設定される IP アドレスは、そのノードで設定されているその他すべての IP アドレスと異なるサブネットの異なるアドレスである必要があります。
- ノードあたりの外部 BGP ピアが 1 つのみである場合、ルータ ID IP アドレスを持つループバック インターフェイスを外部ルータとのピアリングに使用できます。同じノードにある複数の BGP ピアでピアリングする場合、ルート ID ループバック アドレスは使用できません。BGP ごとに明示的なループバック インターフェイス ポリシーを使用する必要があります。

- ループバック インターフェイス ポリシーは、直接接続されたネットワークの外部ルータとピアリングするときは必要ではありません。
- ループバック インターフェイス（iBGP または eBGP マルチホップ）を使用して外部ルータとピアリングする場合、リモート ピアのループバック アドレスに到達するためにスタティック ルートまたは OSPF ルートが必要です。
- BGP では、ループバックの作成がデフォルトで選択されています。これが選択されると、BGPセッションを確立するために、送信元インターフェイスとしてループバックが使用されます。ただし、物理インターフェイスを介してeBGPを確立するために、管理者がループバックを作成してはなりません。

表 *1* :

BGP 接続タイプ	ループバックが必要	ルータ ID と同じループバック	スタティック ルートまたは OSPF ルートが必要
直接 iBGP	いいえ	N/A	いいえ
iBGP ループバック ピアリング	はい（BGP ピアごとに個別のループバック）	いいえ（同じノードに複数のレイヤ 3 Out がある場合）	はい
直接 eBGP	いいえ	N/A	いいえ
eBGP ループバック ピアリング（マルチホップ）	はい（BGP ピアごとに個別のループバック）	いいえ（同じノードに複数のレイヤ 3 Out がある場合）	はい

GUI を使用した BGP 外部ルーテッド ネットワークの設定

はじめる前に

外部ルーテッドネットワークを設定するテナント、VRF、およびブリッジドメインがすでに作成されていること。

ステップ 1 [Navigation] ペインで、[Tenant_name] > [Networking] > [External Routed Networks] を展開します。

ステップ 2 右クリックし、[Create Routed Outside] をクリックします。

ステップ 3 [Create Routed Outside] ダイアログボックスで、次の操作を実行します。

a) [Name] フィールドに、外部ルーテッド ネットワーク ポリシーの名前を入力します。

b) [BGP] チェックボックスをクリックします。
（注） 次の 2 つの方法のいずれかで、BGP ピアの到達可能性を使用できるようになっている必要があります。スタティック ルートを設定するか、または OSPF を有効にする必要があります。

c) （任意） [Route Control Enforcement] フィールドで、[mport] チェックボックスをオンにします。
（注） BGP でインポート制御を適用する場合は、このチェックボックスをオンにします。

d) [VRF] フィールドのドロップダウン リストから、目的の VRF を選択します。

e) [Route Control for Dampening] フィールドを展開し、目的のアドレス ファミリ タイプとルート ダンプニング ポリシーを選択します。[Update] をクリックします。
このステップでは、ポリシーはステップ 4 で作成することができます。または、ポリシー名が選択されているドロップダウン リストでルート プロファイルを作成するオプションがあります。

f) [Nodes and Interfaces Protocol Policies] を展開します。

g) [Create Node Profile] ダイアログボックスに、ノード プロファイルの名前を入力します。

h) [Nodes] を展開します。

i) [Select Node] ダイアログボックスの [Node ID] フィールドのドロップダウン リストから、ノードを選択します。

j) [Router ID] フィールドに、ルータ ID を入力します。

k) [Loopback Address] を展開し、[IP] フィールドに IP アドレスを入力します。[Update] をクリックします。
（注） IPv6 アドレスを入力します。前のステップでルータ ID を追加しなかった場合は、[IP] フィールドに IPv4 アドレスを追加できます。

l) [OK] をクリックします。

ステップ 4 [Navigation] ペインで、[Tenant_name] > [Networking] > [Route Profiles] の順に展開します。[Route Profiles] を右クリックし、[Create Route Profile] をクリックします。[Create Route Profile] ダイアログボックスで、次の操作を実行します。

a) [Name] フィールドに、ルート制御 VRF の名前を入力します。

b) [Create Route Control Context] ダイアログボックスを展開します。

c) [Name] フィールドに、ルート制御 VRF の名前を入力します。

d) [Set Attribute] ドロップダウン リストから、[Create Action Rule Profile] を選択します。
アクション ルールを作成するときに、必要に応じてルート ダンプニング属性を設定します。

ステップ 5 [Create Interface Profiles] ダイアログボックスで、次の操作を実行します。

a) [Name] フィールドに、インターフェイス プロファイル名を入力します。

b) [Interfaces] 領域で、目的のインターフェイス タブを選択し、インターフェイスを展開します。

ステップ 6 [Select Routed Interface] ダイアログボックスで、次の操作を実行します。

a) [Path] ドロップダウン リストから、ノードおよびインターフェイスを選択します。

b) [IP Address] フィールドに、IP アドレスを入力します。
（注） 必要に応じて、IPv6 アドレスまたは IPv4 アドレスを追加できます。

c) （任意） 前のステップで IPv6 アドレスを入力した場合は、[Link-local Address] フィールドに IPv6 アドレスを入力します。

d) [BGP Peer Connectivity Profile] フィールドを展開します。

ステップ 7 [Create Peer Connectivity Profile] ダイアログボックスで、次の操作を実行します。

a) [Peer Address] フィールドでは、ダイナミック ネイバー機能を使用できます。必要に応じて、指定されたサブネット内のすべてのピアが BGP と通信またはルートを交換できます。
手順内の前のステップで入力した IPv4 または IPv6 のアドレスに対応する IPv4 または IPv6 のアドレスを入力します。

b) [BGP Controls] フィールドで、目的の制御をオンにします。

c) [Autonomous System Number] フィールドで、目的の値を選択します。

d) （任意） [Weight for routes from this neighbor] フィールドで、目的の値を選択します。

e) （任意） [Private AS Control] フィールドで、[Remove AS] のチェックボックスをオンにします。

f) （任意） [Local Autonomous System Number Config] フィールドで、目的の値を選択します。
eBGP ピアのローカル自律システム機能の場合にオプションで必要です。

g) （任意） [Local Autonomous System Number] フィールドで、目的の値を選択します。
eBGP ピアのローカル自律システム機能の場合にオプションで必要です。

（注） このフィールドの値は、[Autonomous System Number] フィールドの値と同じであってはなりません。

h) [OK] をクリックします。

ステップ 8 次のアクションを実行します。

a) [Select Routed Interface] ダイアログボックスで、[OK] をクリックします。

b) [Create Interface Profile] ダイアログボックスで、[OK] をクリックします。

c) [Create Node Profile] ダイアログボックスで、[OK] をクリックします。
[External EPG Networks] 領域が表示されます。

d) [Create Routed Outside] ダイアログボックスで、前に作成したノード プロファイルを選択し、[Next] をクリックします。

ステップ 9 [External EPG Networks] を展開し、[Create External Network] ダイアログボックスで、次の操作を実行します。

a) [Name] フィールドに、外部ネットワークの名前を入力します。

b) [Subnet] を展開します。

c) [Create Subnet] ダイアログボックスの [IP address] フィールドに、必要に応じてサブネット アドレスを入力します。

（注） 前のステップで入力した内容に応じて、IPv4 または IPv6 のアドレスを入力します。

外部サブネットを作成するときに、プレフィックス EPG の BGP ループバックの両方を設定するか、またはどちらも設定しない必要があります。BGP ループバックを 1 つのみ設定すると、BGP ネイバーシップは確立されません。

d) [Scope] フィールドで、[Export Route Control Subnet] 、[Import Route Control Subnet] 、および [Security Import Subnet] のチェックボックスをオンにします。[OK] をクリックします。

（注） BGP でインポート制御を適用する場合は、[Import Route Control Subnet] チェックボックスをオンにします。

ステップ 10 [Create External Network] ダイアログボックスで、[OK] をクリックします。

ステップ 11 [Create Routed Outside] ダイアログボックスで、[Finish] をクリックします。
eBGP は外部接続用に設定されています。

REST API を使用した BGP 外部ルーテッド ネットワークの設定

はじめる前に

外部ルーテッド ネットワークを設定するテナントがすでに作成されていること。

ここでは、REST API を使用して BGP 外部ルーテッド ネットワークを設定する方法を示します。

例：

```
<l3extOut descr="" dn="uni/tn-t1/out-l3out-bgp" enforceRtctrl="export" name="l3out-bgp" ownerKey=""
 ownerTag="" targetDscp="unspecified">
<l3extRsEctx tnFvCtxName="ctx3"/>
<l3extLNodeP configIssues="" descr="" name="l3extLNodeP_1" ownerKey="" ownerTag="" tag="yellow-green"
 targetDscp="unspecified">
<l3extRsNodeL3OutAtt rtrId="1.1.1.1" rtrIdLoopBack="no" tDn="topology/pod-1/node-101"/>
<l3extLIfP descr="" name="l3extLIfP_2" ownerKey="" ownerTag="" tag="yellow-green">
<l3extRsNdIfPol tnNdIfPolName=""/>
<l3extRsIngressQosDppPol tnQosDppPolName=""/>
<l3extRsEgressQosDppPol tnQosDppPolName=""/>
<l3extRsPathL3OutAtt addr="3001::31:0:1:2/120" descr="" encap="vlan-3001" encapScope="local"
ifInstT="sub-interface" llAddr="::" mac="00:22:BD:F8:19:FF" mode="regular" mtu="inherit"
tDn="topology/pod-1/paths-101/pathep-[eth1/8]" targetDscp="unspecified">
<bgpPeerP addr="3001::31:0:1:0/120" allowedSelfAsCnt="3" ctrl="send-com,send-ext-com" descr=""
name="" peerCtrl="bfd" privateASctrl="remove-all,remove-exclusive,replace-as" ttl="1" weight="1000">
<bgpRsPeerPfxPol tnBgpPeerPfxPolName=""/>
<bgpAsP asn="3001" descr="" name=""/>
</bgpPeerP>
</l3extRsPathL3OutAtt>
</l3extLIfP>
<l3extLIfP descr="" name="l3extLIfP_1" ownerKey="" ownerTag="" tag="yellow-green">
<l3extRsNdIfPol tnNdIfPolName=""/>
<l3extRsIngressQosDppPol tnQosDppPolName=""/>
<l3extRsEgressQosDppPol tnQosDppPolName=""/>
<l3extRsPathL3OutAtt addr="31.0.1.2/24" descr="" encap="vlan-3001" encapScope="local"
ifInstT="sub-interface" llAddr="::" mac="00:22:BD:F8:19:FF" mode="regular" mtu="inherit"
tDn="topology/pod-1/paths-101/pathep-[eth1/8]" targetDscp="unspecified">
<bgpPeerP addr="31.0.1.0/24" allowedSelfAsCnt="3" ctrl="send-com,send-ext-com" descr="" name=""
peerCtrl="" privateASctrl="remove-all,remove-exclusive,replace-as" ttl="1" weight="100">
<bgpRsPeerPfxPol tnBgpPeerPfxPolName=""/>
<bgpLocalAsnP asnPropagate="none" descr="" localAsn="200" name=""/>
<bgpAsP asn="3001" descr="" name=""/>
</bgpPeerP>
</l3extRsPathL3OutAtt>
</l3extLIfP>
</l3extLNodeP>
<l3extRsL3DomAtt tDn="uni/l3dom-l3-dom"/>
<l3extRsDampeningPol af="ipv6-ucast" tnRtctrlProfileName="damp_rp"/>
<l3extRsDampeningPol af="ipv4-ucast" tnRtctrlProfileName="damp_rp"/>
```

```
<l3extInstP descr="" matchT="AtleastOne" name="l3extInstP_1" prio="unspecified"
targetDscp="unspecified">
<l3extSubnet aggregate="" descr="" ip="130.130.130.0/24" name="" scope="import-rtctrl">
</l3extSubnet>
<l3extSubnet aggregate="" descr="" ip="130.130.131.0/24" name="" scope="import-rtctrl"/>
<l3extSubnet aggregate="" descr="" ip="120.120.120.120/32" name=""
scope="export-rtctrl,import-security"/>
<l3extSubnet aggregate="" descr="" ip="3001::130:130:130:100/120" name="" scope="import-rtctrl"/>
</l3extInstP>
<bgpExtP descr=""/>
</l3extOut>
<rtctrlProfile descr="" dn="uni/tn-t1/prof-damp_rp" name="damp_rp" ownerKey="" ownerTag=""
type="combinable">
 <rtctrlCtxP descr="" name="ipv4_rpc" order="0">
  <rtctrlScope descr="" name="">
   <rtctrlRsScopeToAttrP tnRtctrlAttrPName="act_rule"/>
  </rtctrlScope>
 </rtctrlCtxP>
</rtctrlProfile>
<rtctrlAttrP descr="" dn="uni/tn-t1/attr-act_rule" name="act_rule">
  <rtctrlSetDamp descr="" halfLife="15" maxSuppressTime="60" name="" reuse="750" suppress="2000"
type="dampening-pol"/>
</rtctrlAttrP>
```

オブジェクト モデル CLI を使用した BGP 外部ルーテッド ネットワークの設定

ステップ 1 CLI で、ディレクトリを /aci に変更します。

例：

```
admin@apic1:~> cd /aci
```

ステップ 2 テナントのスコープと外部ルーテッド ネットワークのスコープを入力します。

例：

```
admin@apic1:tenants> ls common infra  mgmt  tn1
admin@apic1:tenants> cd tn1/
admin@apic1:tn1> cd networking/external-routed-networks/
```

ステップ 3 レイヤ 3 Outside を作成します。

例：

```
admin@apic1:external-routed-networks> mocreate l3-outside bgp-ext-out
admin@apic1:external-routed-networks> moconfig commit
Committing mo 'tenants/tn1/networking/external-routed-networks/l3-outside-bgp-ext-out'
All mos committed successfully.
```

ステップ 4 レイヤ 3 Outside スコープで BGP を有効にします。論理ノード プロファイル、ノード プロファイルのノードを作成し、ルータ ID とルータ ループバックを設定します。

例：

```
admin@apic1:external-routed-networks> cd l3-outside-bgp-ext-out/
admin@apic1:l3-outside-bgp-ext-out> mocreate bgp-ext-profile
```

```
admin@apic1:l3-outside-bgp-ext-out> moconfig commit
Committing mo 'tenants/tn1/networking/external-routed-networks/l3-outside-bgp-ext-out/bgp-ext-profile'
All mos committed successfully.

admin@apic1:l3-outside-bgp-ext-out> moset private-network default
admin@apic1:l3-outside-bgp-ext-out> moconfig commit
Committing mo 'tenants/tn1/networking/external-routed-networks/l3-outside-bgp-ext-out'
All mos committed successfully.

admin@apic1:l3-outside-bgp-ext-out> cd logical-node-profiles
admin@apic1:logical-node-profiles> mocreate
 <name>  logical node profile name

admin@apic1:logical-node-profiles> mocreate np1
admin@apic1:logical-node-profiles> moconfig commit
Committing mo
'tenants/tn1/networking/external-routed-networks/l3-outside-bgp-ext-out/logical-node-profiles/np1'
All mos committed successfully.

admin@apic1:logical-node-profiles> cd np1/
admin@apic1:np1> cd nodes/
admin@apic1:nodes> mocreate fabric/inventory/pod-1/node-101
admin@apic1:nodes> ls
[fabric--inventory--pod-1--node-101]  summary
admin@apic1:nodes> cd \[fabric--inventory--pod-1--node-101\]/
admin@apic1:[fabric--inventory--pod-1--node-101]> moset router-id 1.1.1.2
admin@apic1:[fabric--inventory--pod-1--node-101]> moset rtridloopback yes
admin@apic1:[fabric--inventory--pod-1--node-101]> moconfig commit
Committing mo 'tenants/tn1/networking/external-routed-networks/l3-outside-bgp-ext-out
/logical-node-profiles/np1/nodes/[fabric/inventory/pod-1/node-101]'
All mos committed successfully.

admin@apic1:[fabric--inventory--pod-1--node-101]>
admin@apic1:[fabric--inventory--pod-1--node-101]> cd ..
admin@apic1:nodes> cd ..
```

ステップ 5 インターフェイス プロファイルを作成します。

例：

```
admin@apic1:np1> cd logical-interface-profiles/
admin@apic1:logical-interface-profiles> mocreate intfp1
admin@apic1:logical-interface-profiles> moconfig commit
Committing mo 'tenants/tn1/networking/external-routed-networks/l3-outside-bgp-ext-out
/logical-node-profiles/np1/logical-interface-profiles/intfp1'
All mos committed successfully.
```

ステップ 6 ルータ インターフェイスを設定します。

例：

```
admin@apic1:logical-interface-profiles> cd intfp1/
admin@apic1:intfp1> cd routed-interfaces/
admin@apic1:routed-interfaces> mocreate topology/pod-1/paths-102/pathep-[eth9/3] ip-address
100.1.1.2/24
admin@apic1:routed-interfaces> moconfig commit
Committing mo 'tenants/tn1/networking/external-routed-networks/l3-outside-bgp-ext-out
/logical-node-profiles/np1/logical-interface-profiles/intfp1/routed-interfaces
/[topology/pod-1/paths-102/pathep-[eth9/3]]'
All mos committed successfully.
```

ステップ 7 BGP ピア設定を作成します。

例：

```
admin@apic1:logical-interface-profiles> cd ../bgp-peer-connectivity/

admin@apic1:bgp-peer-connectivity>  mocreate 100.1.1.3/24 bgp-controls send-community add
autonomous-system-number 33
```

```
admin@apic1:bgp-peer-connectivity> moconfig commit
Committing mo 'tenants/tn1/networking/external-routed-networks/l3-outside-bgp-ext-out
/logical-node-profiles/np1/bgp-peer-connectivity/100.1.1.3/24'
All mos committed successfully.
```

ステップ 8 外部 EPG を作成します。

例：

```
admin@apic1:l3-outside-bgp-ext-out> cd networks/
admin@apic1:networks> mocreate extepg
admin@apic1:networks> moconfig commit
Committing mo 'tenants/tn1/networking/external-routed-networks/l3-outside-bgp-ext-out/networks/extepg'
All mos committed successfully.
```

ステップ 9 サブネットを作成し、サブネットのスコープを設定します。

例：

```
admin@apic1:networks> cd extepg/
admin@apic1:extepg> cd subnets/
admin@apic1:subnets> mocreate 1.1.1.2
admin@apic1:subnets> moconfig commit
Committing mo
'tenants/tn1/networking/external-routed-networks/l3-outside-bgp-ext-out/networks/extepg/subnets/1.1.1.2'
All mos committed successfully.

admin@apic1:subnets> cd 1.1.1.2/

admin@apic1:1.1.1.2> moset scope-of-the-external-subnet import-route-control-subnet
admin@apic1:1.1.1.2> moconfig commit
Committing mo
'tenants/tn1/networking/external-routed-networks/l3-outside-bgp-ext-out/networks/extepg/subnets/1.1.1.2'

All mos committed successfully.
admin@apic1:1.1.1.2>

The external BGP Outside is now configured successfully.
```

テナントのレイヤ 3 Outside ネットワーク接続の設定の概要

このトピックでは、APIC 使用時にテナント ネットワークに対してレイヤ 3 Outside を設定する方法の典型的な例を示します。

GUI を使用したテナント ネットワークのレイヤ 3 Outside の設定

この例で設定されている外部ルーテッド ネットワークを、IPv4 をサポートするように拡張することもできます。IPv4 と IPv6 両方のルートを外部ルーテッド ネットワークにアドバタイズし、外部ルーテッド ネットワークから学習することができます。

はじめる前に

- テナント、VRF、およびブリッジ ドメインが作成されていること。

- 外部ルーテッド ドメインが作成されていること。

ステップ 1 メニュー バーで、[TENANTS] をクリックします。

ステップ 2 [Navigation] ペインで、*[Tenant_name]* > [Networking] > [External Routed Networks] の順に展開し、次の操作を実行します。

a) [External Routed Networks] を右クリックし、[Create Routed Outside] をクリックします。
b) [Create Routed Outside] ダイアログボックスの [Name] フィールドに、ルーテッド Outside の名前を入力します。
c) ルーテッド プロトコルのチェックボックスがある領域で、目的のプロトコルをオンにします。
使用可能なオプションは、BGP、OSPF、EIGRP です。これにより、後のステップで [Create External Network] ダイアログボックスのルート集約ポリシーが有効になります。
d) [VRF] フィールドのドロップダウン リストから、適切な VRF を選択します。
e) [External Routed Domain] ドロップダウン リストから、適切な外部ルーテッド ドメインを選択します。
f) 目的のプロトコルのチェックボックスをオンにします。
選択するプロトコルに応じて、プロパティを設定する必要があります。
g) [Nodes and Interfaces Protocol Profile] を展開します。
h) [Create Node Profile] ダイアログボックスで、[Name] フィールドに、名前を入力します。
i) [Nodes] を展開します。
j) [Select Node] ダイアログボックスで、[Node ID] ドロップダウン メニューから適切なノード ID を選択します。
k) [Router ID] フィールドに、ルータ ID を入力します。
l) [Loopback Addresses] を展開し、[IP] フィールドに IP アドレスを入力します。[Update] をクリックします。
（注） [Loopback Addresses] フィールドで、必要に応じて IPv4 または IPv6 のループバックを作成します。
m) [OK] をクリックします。

ステップ 3 [Interface Profiles] を展開し、次の操作を実行します。

a) [Create Interface Profile] ダイアログボックスの [Name] フィールドに、プロファイルの名前を入力します。
b) [Routed Interfaces] を展開します。
c) [Select Routed Interface] ダイアログボックスの [Path] ドロップダウン リストから、インターフェイス パスを選択します。
d) [IP Address] フィールドに、IP アドレスを入力します。
（注） IPv6 を設定するには、ダイアログボックスの [Link-local Address] フィールドにリンクローカル アドレスを入力する必要があります。
e) [OK] をクリックします。
[Create Interface Profile] ダイアログボックスに、ルーテッド インターフェイスの詳細が表示されます。

f) [OK] をクリックします。

ステップ 4 [Create Node Profile] ダイアログボックスで、[OK] をクリックします。

ステップ 5 [Create Routed Outside] ダイアログボックスで、[Next] をクリックします。

ステップ 6 [External EPG Networks] 領域で、[External EPG Networks] を展開します。

ステップ 7 [Create External Networks] ダイアログボックスの [Name] フィールドに、外部ネットワークの名前を入力します。

ステップ 8 [Subnet] を展開します。

ステップ 9 [Create Subnet] ダイアログボックスで、次の操作を実行します。

a) [IP Address] フィールドに、IP アドレスを入力します。

b) [Scope] フィールドで、適切なチェックボックスをオンにします。[OK] をクリックします。

ステップ 10 [Create External Network] ダイアログボックスで、次の操作を実行します。

a) 別のサブネットを追加するために、[Subnet] を展開します。

b) [Create Subnet] ダイアログボックスの [IP Address] フィールドに、IP アドレスを入力します。

c) [Scope] フィールドで、適切なチェックボックスをオンにします。[OK] をクリックします。

（注）
- インポート制御ポリシーはデフォルトで有効になっていませんが、ユーザが有効にすることができます。インポート制御ポリシーは BGP ではサポートされますが、EIGRP および OSPF ではサポートされません。ユーザがサポートされていないプロトコルのインポート制御ポリシーを有効にしても、自動的に無視されます。
- エクスポート制御ポリシーは、BGP、EIGRP、および OSPF でサポートされます。
- ルート集約もサポートされ、ユーザは希望するエクスポートまたはインポートの方向でルート集約を任意で選択できます。この機能は、0.0.0.0/0 およびセキュリティ オプションの場合に使用できます。インポート制御ポリシーが有効になっていない場合、オンにすべきチェックボックスの例は、[Export Subnet]、[Security Import Subnet]、および [Aggregate Export] です。ユーザは、ルート マップおよびセキュリティ オプションを選択する必要があります。
- レイヤ 3 Outside に対して明示的なルート制御ポリシーが設定されている場合、特定のレイヤ 3 Outside ポリシーのみがサポートされます。集約ルートでは、明示的なルート制御ポリシーはサポートされません。

d) （任意） [Route Summarization Policy] フィールドで、必要に応じてドロップダウン リストから既存のルート集約ポリシーを選択するか、または新しいルート集約ポリシーを作成します。また、チェックボックス [Export Route Control Subnet] をオンにする必要があります。

e) [Create External Network] ダイアログボックスで、[OK] をクリックします。

ステップ 11 [Create Routed Outside] ダイアログボックスで、[Finish] をクリックします。

ステップ 12 [Navigation] ペインの *[Tenant_name]* > [Networking] > [Bridge Domains] で、[Bridge_Domain_name] を選択します。

ステップ 13 [Work] ペインの [Properties] の下の [L3 Out for Route Profile] のドロップダウン リストで、目的のレイヤ 3 Outside を関連付けます。[Submit] をクリックします。

これにより、テナント ネットワークに対してレイヤ 3 Outside が設定されます。

ステップ 14 （注） 受信するすべてのルートについて BGP、OSPF、または EIGRP の通信の属性を設定するには、default-import ルート制御プロファイルを作成し、適切な set アクションおよび no match アクションを作成します。

[Navigation] ペインで、[Route Profiles] をクリックし、[Create Route Profiles] を右クリックし、[Create Route Profiles] ダイアログボックスで次の操作を実行します。

a) [Name] フィールドに、名前を入力します。

b) [Type] フィールドで、[Use Routing Policy Only] をクリックする必要があります。[Submit] をクリックします。

REST API を使用したテナント ネットワークのレイヤ 3 Outside の設定

この例で設定されている外部ルーテッド ネットワークを、IPv4 をサポートするように拡張することもできます。IPv4 と IPv6 両方のルートを外部ルーテッド ネットワークにアドバタイズし、外部ルーテッド ネットワークから学習することができます。

はじめる前に

- テナント、プライベート ネットワーク、およびブリッジ ドメインが作成されていること。
- 外部ルーテッド ドメインが作成されていること。

テナント ネットワークの L3 Outside を設定し、ブリッジ ドメインを Layer3 Outside に関連付けます。

例：

```
<l3extOut name="L3Out1" enforceRtctrl="import,export">
            <l3extRsL3DomAtt tDn="uni/l3dom-l3DomP"/>
        <l3extLNodeP name="LNodeP1" >
            <l3extRsNodeL3OutAtt rtrId="1.2.3.4" tDn="topology/pod-1/node-101">
                <l3extLoopBackIfP addr="10.10.11.1" />
                <l3extLoopBackIfP addr="2000::3" />
            </l3extRsNodeL3OutAtt>
            <l3extLIfP  name="IFP1" >
                <l3extRsPathL3OutAtt addr="10.11.12.10/24"  ifInstT="l3-port"
tDn="topology/pod-1/paths-103/pathep-[eth1/17]" />
            </l3extLIfP>
            <l3extLIfP  name="IFP2" >
                <l3extRsPathL3OutAtt addr="2001::3/64"  ifInstT="l3-port"
tDn="topology/pod-1/paths-103/pathep-[eth1/17]" />
            </l3extLIfP>
        </l3extLNodeP>
        <l3extRsEctx tnFvCtxName="VRF1"/>
        <l3extInstP name="InstP1" >
            <l3extSubnet ip="192.168.1.0/24" scope="import-security" aggregate=""/>
            <l3extSubnet ip="0.0.0.0/0" scope="export-rtctrl,import-rtctrl,import-security"
aggregate="export-rtctrl,import-rtctrl"/>
            <l3extSubnet ip="192.168.2.0/24" scope="export-rtctrl" aggregate=""/>
          <l3extSubnet ip="::/0" scope="import-rtctrl,import-security" aggregate="import-rtctrl"/>
```

```
        <l3extSubnet ip="2001:17a::/64" scope="export-rtctrl" aggregate=""/>
    </l3extInstP>
</l3extOut>
```

（注） OSPF および EIGRP では、"enforceRtctrl=import" は適用できません。

オブジェクト モデル CLI を使用したテナント ネットワークのレイヤ 3 Outside の設定

この例で設定されている外部ルーテッド ネットワークを、IPv4 をサポートするように拡張することもできます。IPv4 と IPv6 両方のルートを外部ルーテッド ネットワークにアドバタイズし、外部ルーテッド ネットワークから学習することができます。

はじめる前に

- テナント、プライベート ネットワーク、およびブリッジ ドメインが作成されていること。
- 外部ルーテッド ドメインが設定されていること。

ステップ 1 CLI で、ディレクトリを /aci に変更します。

例：

```
admin@apic1:~> cd /aci
```

ステップ 2 テナントと外部ルータ ネットワークのスコープを入力します。

例：

```
admin@apic1:tenants> ls common infra  mgmt  tn1
admin@apic1:tenants> cd tn1/
admin@apic1:tn1> cd networking/external-routed-networks/
```

ステップ 3 レイヤ 3 Outside スコープで目的のプロトコルを有効にします。論理ノード プロファイル、ノード プロファイルのノードを作成し、ルータ ID とルータ ループバックを設定します。

例：

```
admin@apic1:external-routed-networks> mocreate l3-outside tenant-ext-out
admin@apic1:external-routed-networks> moconfig commit
Committing mo 'tenants/tn1/networking/external-routed-networks/l3-outside-tenant-ext-out'
All mos committed successfully.

admin@apic1:external-routed-networks> cd l3-outside-tenant-ext-out/
admin@apic1:l3-outside-tenant-ext-out> mocreate bgp-ext-profile
admin@apic1:l3-outside-tenant-ext-out> moconfig commit
Committing mo
'tenants/tn1/networking/external-routed-networks/l3-outside-tenant-ext-out/bgp-ext-profile'
All mos committed successfully.
```

```
admin@apic1:l3-outside-tenant-ext-out> moset private-network default
admin@apic1:l3-outside-tenant-ext-out> moconfig commit
Committing mo 'tenants/tn1/networking/external-routed-networks/l3-outside-tenant-ext-out'
All mos committed successfully.

admin@apic1:l3-outside-tenant-ext-out> moset  external-routed-domain fabric
/access-policies/physical-and-external-domains/external-routed-domains/dom1
admin@apic1:l3-outside-tenant-ext-out> moconfig commit
Committing mo 'tenants/tn1/networking/external-routed-networks/l3-outside-tenant-ext-out'

admin@apic1:l3-outside-tenant-ext-out> cd logical-node-profiles
admin@apic1:logical-node-profiles> mocreate np1
admin@apic1:logical-node-profiles> moconfig commit
Committing mo 'tenants/tn1/networking/external-routed-networks/l3-outside-tenant-ext-out
/logical-node-profiles/np1'
All mos committed successfully.

admin@apic1:logical-node-profiles> cd np1/
admin@apic1:np1> cd nodes/
admin@apic1:nodes> mocreate fabric/inventory/pod-1/node-101
admin@apic1:nodes> ls [fabric--inventory--pod-1--node-101]  summary
admin@apic1:nodes> cd \[fabric--inventory--pod-1--node-101\]/
admin@apic1:[fabric--inventory--pod-1--node-101]> moset router-id 1.1.1.1

admin@apic1:[fabric--inventory--pod-1--node-101]> moset rtridloopback yes
admin@apic1:[fabric--inventory--pod-1--node-101]> moconfig commit
Committing mo 'tenants/tn1/networking/external-routed-networks/l3-outside-tenant-ext-out
/logical-node-profiles/np1/nodes/[fabric/inventory/pod-1/node-101]'
All mos committed successfully.

admin@apic1:[fabric--inventory--pod-1--node-101]>
admin@apic1:[fabric--inventory--pod-1--node-101]> cd ..
admin@apic1:nodes> cd ..
```

ステップ 4 インターフェイス プロファイルを作成します。

例：

```
admin@apic1:np1> cd logical-interface-profiles/
admin@apic1:logical-interface-profiles> mocreate intfp1
admin@apic1:logical-interface-profiles> moconfig commit
Committing mo 'tenants/tn1/networking/external-routed-networks/l3-outside-tenant-ext-out
/logical-node-profiles/np1/logical-interface-profiles/intfp1'
All mos committed successfully.
```

ステップ 5 ルータ インターフェイスを設定します。

例：

```
admin@apic1:logical-interface-profiles> cd intfp1/
admin@apic1:intfp1> cd routed-interfaces/
admin@apic1:routed-interfaces> mocreate topology/pod-1/paths-102/pathep-[eth9/3] ip-address
100.1.1.2/24
admin@apic1:routed-interfaces> moconfig commit
Committing mo 'tenants/tn1/networking/external-routed-networks/l3-outside-tenant-ext-out
/logical-node-profiles/np1/logical-interface-profiles/intfp1/routed-interfaces/[topology/pod-1
/paths-102/pathep-[eth9/3]]'
All mos committed successfully.
```

ステップ 6 外部 EPG を作成します。

例：

```
admin@apic1:l3-outside-tenant-ext-out> cd networks/
admin@apic1:networks> mocreate extepg
admin@apic1:networks> moconfig commit
Committing mo 'tenants/tn1/networking/external-routed-networks/l3-outside-tenant-ext-out
```

```
/networks/extepg'
All mos committed successfully.
```

ステップ 7 サブネットを作成します。

例：

```
admin@apic1:networks> cd extepg/
admin@apic1:extepg> cd subnets/
admin@apic1:subnets> mocreate 0.0.0.0
admin@apic1:subnets> moconfig commit
Committing mo 'tenants/tn1/networking/external-routed-networks/l3-outside-tenant-ext-out
/networks/extepg/subnets/0.0.0.0'
All mos committed successfully.

admin@apic1:subnets> cd 0.0.0.0/

admin@apic1:1.1.1.1> moset scope-of-the-external-subnet import-route-control-subnet
admin@apic1:1.1.1.1> moconfig commit
Committing mo 'tenants/tn1/networking/external-routed-networks/l3-outside-tenant-ext-out
/networks/extepg/subnets/0.0.0.0'

All mos committed successfully.
admin@apic1:0.0.0.0>
```

ステップ 8 レイヤ 3 Out をブリッジ ドメインに関連付けます。

例：

```
admin@apic1:1.1.1.1> cd /aci/tenants/tn1/networking/bridge-domains
admin@apic1:bridge-domains> mocreate bd1
admin@apic1:bridge-domains> moconfig commit
All mos committed successfully.
admin@apic1:1.1.1.1>

admin@apic1:bridge-domains> cd bd1/
admin@apic1:bd1> ls associated-l3-outs  dhcp-relay-labels l4-l7-service-parameters mo rasubnets
subnets summary tags
admin@apic1:bd1> cd associated-l3-outs/
admin@apic1:associated-l3-outs> mocreate tenant-ext-out
admin@apic1:1.1.1.1> moconfig commit
```

これで、レイヤ 3 テナント Outside が正常に設定されました。

共有サービス コントラクトの使用

共有サービスを使用すると、テナントの分離とセキュリティ ポリシーを維持したままテナント間で通信できます。外部ネットワークへのルーテッド接続は、複数のテナントが使用する共有サービスの例です。

共有サービス コントラクトの設定時は、次のガイドラインに従ってください。

- さまざまなコンテキスト（VRF）にサブネットをエクスポートする共有サービスでは、EPG にサブネットを定義し、スコープを *advertised externally* および *shared between VRFs* に設定する必要があります。

- プライベート ネットワークを適用しない場合、ブリッジ間ドメインのトラフィックにコントラクトは不要です。
- コンテキスト（VRF）が適用されていない場合でも、共有サービスのコンテキスト（VRF）間トラフィックにはコントラクトが必要です。
- 共有サービスを提供している間は、プロバイダー EPG のコンテキスト（VRF）は非強制モードにできません。
- 共有サービスは、重複しないサブネットのみでサポートされます。共有サービスのサブネットを設定するときは、以下のガイドラインに従ってください。
  - 共有サービス プロバイダーのサブネットは、ブリッジ ドメイン下ではなく EPG 下で設定します。
  - 同じコンテキストを共有する EPG で設定されたサブネットは、統合および重複してはなりません。
  - あるコンテキストから他のコンテキストへ漏れたサブネットは統合および重複してはなりません。
  - 複数のコンシューマ ネットワークからあるコンテキストへ漏れたサブネットまたはその逆で漏れたサブネットは統合および重複してはなりません。

（注） 2 人のコンシューマが誤って同じサブネットに設定されている場合は、両方のサブネットの設定を削除してこの状態からリカバリし、その後サブネットを正しく再設定します。

- プロバイダー コンテキストで共有サービスを `AnyToProv` に設定しないでください。APIC はこの設定を拒否し、エラーが発生します。
- インバンド EPG とアウトオブバンド EPG の間でコントラクトが設定される場合、以下の制限が適用されます。
  - 両方の EPG は同じコンテキスト（VRF）にする必要があります。
  - フィルタは、着信方向のみに適用されます。
  - レイヤ 2 フィルタはサポートされません。
  - QoS は、インバンド レイヤ 4 ～ レイヤ 7 のサービスには適用されません。
  - 管理統計情報は利用できません。
  - CPU 宛てトラフィックの共有サービスはサポートされません。

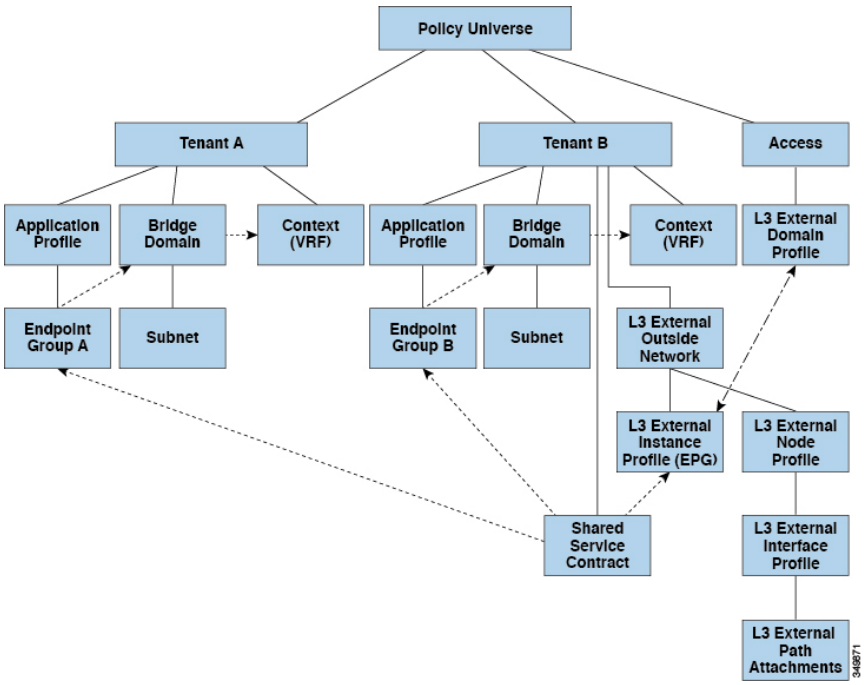
共有レイヤ 3 Out

共有レイヤ 3 Out 設定は、外部ネットワークへのルーテッド接続を共有サービスとして提供します。`l3extInstP` EPG は、外部ネットワークへのルーテッド接続を提供します。これは、任意のテナント（user、common、infra、または mgmt.）の共有サービスとしてプロビジョニングできます。リリース 1.2(1x) より前では、この設定は user テナントと common テナントでのみサポートされていました。任意のテナントの EPG が、`l3extInstP` EPG がファブリック内のどこにプロビジョニングされているかには関係なく、共有サービス コントラクトを使用してその `l3extInstP` EPG に接続できます。これにより、外部ネットワークへのルーテッド接続のプロビジョニングが簡単になります。複数のテナントが、外部ネットワークへのルーテッド接続用に単一の `l3extInstP` EPG を共有できます。`l3extInstP` EPG を共有すると、単一の共有 `l3extInstP` EPG を使用する EPG の数には関係なくスイッチ上で使用されるセッションは 1 つのみであるため、より効率的になります。

（注） l3extInstP EPG 共有サービス コントラクトを使用するすべてのスイッチは、APIC 1.2（1x）およびスイッチ 11.2（1x）の各リリース以降で使用可能なハードウェアおよびソフトウェアのサポートを必要とします。詳細については、『Firmware Management Guide and Release Notes』というマニュアルを参照してください。

次の図は、共有 `l3extInstP` EPG 用に設定された主なポリシー モデル オブジェクトを示しています。

図 *1*：共有レイヤ *3 Out* ポリシー モデル



共有レイヤ 3 Out 設定について、以下のガイドラインと制限事項に注意してください。

- テナント制限なし：テナント A と B は、任意の種類のテナント（user、common、infra、mgmt.）です。共有 l3extInstP EPG がテナント common にある必要はありません。
- EPG の柔軟な配置：上の図の EPG A と EPG B は異なるテナントにあります。EPG A と EPG B で同じブリッジ ドメインとコンテキストを使用することはできますが、それは必須ではありません。EPG A と EPG B は異なるブリッジ ドメインおよび異なるコンテキストにありますが、同じ `l3extInstP` EPG を共有しています。
- サブネットは、*private*、*public*、または *shared* です。レイヤ 3 Outside 外部ネットワークのコンシューマ EPG またはプロバイダー EPG は *shared* に設定されている必要があります。レイヤ 3 Outside 外部ネットワークにエクスポートされるサブネットは、*public* に設定されている必要があります。
- 共有サービス コントラクトは、共有レイヤ 3 Out サービスを提供する `l3extInstP` EPG が含まれているテナントからエクスポートされます。共有サービス コントラクトは、共有サービスを使用する EPG が含まれているテナントにインポートされます。
- 共有 L3 Out では禁止コントラクトを使用しないでください。この設定はサポートされません。
- vzAny およびレイヤ 3 Out EPG プロバイダの背後にある `l3extInstP` EPG は、共有サービスの場合はサポートされません。また、コンシューマ `l3extInstP` EPG が vzAny の背後にあり、レイヤ 3 Out EPG がダイレクト コントラクトのプロバイダーである場合、共有レイヤ 3 Out ではトランジット ルーティングはサポートされません。
- トラフィック フラップ：`l3instP` EPG が、`l3instP` サブセットのスコープ プロパティを共有ルート制御（*shared-rctrl*）または共有セキュリティ（*shared-security*）に設定して外部サブネット 0.0.0.0/0 を使用して設定されると、コンテキスト（VRF）はグローバル `pcTag` を使用して再配置されます。これにより、その VRF 内のすべての外部トラフィックがフラップされます（VRF がグローバル `pcTag` を使用して再配置されるため）。
- 共有レイヤ 3 Out のプレフィックスは一意である必要があります。同じコンテキスト（VRF）の同じプレフィックスを使用した、複数の共有レイヤ 3 Out 設定は動作しません。VRF にリークする外部サブネット（外部プレフィックス）が一意であることを確認してください（同じ外部サブネットが複数の `l3instP` に属することはできません）。プレフィックス prefix1 を使用したレイヤ 3 Outside 設定（たとえば、L3Out1）と、同様にプレフィックス prefix1 を使用した 2 番目のレイヤ 3 Outside 設定（たとえば、L3Out2）が同じコンテキスト（VRF）に属すると、動作しません（導入される pcTag は 1 つのみであるため）。
- 許可されないトラフィック：無効な設定で、共有ルート制御（shared-rtctrl）に対する外部サブネットのスコープが、共有セキュリティ（shared-security）に設定されているサブネットのサブセットとして設定されている場合、トラフィックは許可されません。たとえば、以下の設定は許可されません。
  - *shared rtctrl*：10.1.1.0/24, 10.1.2.0/24
  - *shared security*：10.1.0.0/16

この場合、10.1.1.0/24 および 10.1.2.0/24 の各プレフィックスがドロップ ルールを使用してインストールされているため、宛先 IP 10.1.1.1 を使用して非境界リーフに到達するトラフィックはドロップされます。トラフィックは許可されません。そのようなトラフィックは、shared-rtctrl プレフィックスを shared-security プレフィックスとしても使用するように設定を修正することで、有効にすることができます。

- 不注意によるトラフィック フロー：次の設定シナリオを避けることで、不注意によるトラフィック フローを予防します。
  - **ケース 1** 設定の詳細：
    - コンテキスト（VRF）1 を使用したレイヤ 3 Outside 設定（たとえば L3Out1）は provider1 と呼ばれます。
    - コンテキスト（VRF）2 を使用した 2 番目のレイヤ 3 Outside 設定（たとえば L3Out2）は provider2 と呼ばれます。
    - L3Out1 VRF1 はデフォルト ルートをインターネットにアドバタイズします = 0.0.0.0/0 = *shared-rtctrl*、*shared-security*。
    - L3Out2 VRF2 は特定のサブネットを DNS および NTP にアドバタイズします = 192.0.0.0/8 = *shared-rtctrl*。
    - L3Out2 VRF2 には特定のサブネット 192.1.0.0/16 があります = *shared-security*。
    - **バリエーション A**：EPG トラフィックが複数のコンテキスト（VRF）に向かいます。
      - EPG1 と L3Out1 の間の通信は *allow_all* コントラクトによって制御されます。
      - EPG1 と L3Out2 の間の通信は *allow_all* コントラクトによって制御されます。

        結果：EPG1 から L3Out2 へのトラフィックも 192.2.x.x に向かいます。
    - **バリエーション B**：EPG は 2 番目の共有レイヤ 3 Out の *allow_all* コントラクトに従います。
      - EPG1 と L3Out1 の間の通信は *allow_all* コントラクトによって制御されます。
      - EPG1 と L3Out2 の間の通信は *allow_icmp* コントラクトによって制御されます。

        結果：EPG1 -> L3Out2 -> 192.2.x.x のトラフィックは *allow_all* コントラクトに従います。
  - **ケース 2** 設定の詳細：
    - レイヤ 3 Out インスタンス プロファイル（l3instP）は、1 つの共有プレフィックスとその他の非共有プレフィックスを持っています。
    - `src = non-shared` で到達するトラフィックは、EPG に向かうことが許可されます。
      - **バリエーション A**：意図しないトラフィックが EPG を通過します。

- レイヤ 3 Out（l3instP）EPG トラフィックは、以下のプレフィックスを持っているレイヤ 3 Out を通過します。
  - `192.0.0.0/8 = import-security、shared-rtctrl`
  - `192.1.0.0/16 = shared-security`
  - EPG は `1.1.0.0/16 = shared` となっています。

    結果：192.2.x.x からのトラフィックも EPG に向かいます。

- **バリエーション B**：意図しないトラフィックが EPG を通過します。共有レイヤ 3 Out に到達するトラフィックは、コンテキスト（VRF）に応じて通過できます。
  - 共有レイヤ 3 Out のコンテキスト（VRF）は、`pcTag = prov vrf` の EPG と *allow_all* のコントラクトを持っています。
  - EPG は `<subnet> = shared` となっています。

    結果：レイヤ 3 Out に到達するトラフィックは EPG を通過することができます。

ネイバー探索

IPv6 ネイバー探索（ND）は、ノードのアドレスの自動設定、リンク上の他のノードの探索、他のノードのリンク層アドレスの判別、重複アドレスの検出、使用可能なルータと DNS サーバの検出、アドレスプレフィックスの探索、および他のアクティブなネイバーノードへのパスに関する到達可能性情報の維持を担当します。

ND 固有のネイバー要求/ネイバー アドバタイズメント（NS/NA）およびルータ要求/ルータ アドバタイズメント（RS/RA）パケット タイプは、物理、L3 Sub-if、および SVI（外部およびパーベイシブ）を含むすべての ACI ファブリックのレイヤ 3 インターフェイスでサポートされます。RS/RA パケットはすべての L3 インターフェイスの自動設定に使用されますが、パーベイシブ SVI の場合にのみ設定できます。ACI のブリッジ ドメイン ND は常にフラッド モードで動作します。ユニキャスト モードはサポートされません。

ACI ファブリック ND サポートに含まれるもの：

- インターフェイス ポリシー（`nd:IfPol`）は、NS/NA メッセージに関する ND タイマーと動作を制御します。
- ND プレフィックス ポリシー（`nd:PfxPol`）は、RA メッセージを制御します。
- ND の IPv6 サブネット（fv:Subnet）の設定。
- 外部ネットワークの ND インターフェイス ポリシー。

- 外部ネットワークの設定可能NDサブネットおよびパーベイシブブリッジドメインの任意サブネット設定はサポートされません。

設定可能なオプションは次のとおりです。

- 隣接関係
  - 設定可能な静的隣接関係：（<vrf、L3Iface、ipv6 アドレス> --> MAC アドレス）
  - 動的隣接関係：NS/NA パケットの交換によって学習
- インターフェイス単位
  - ND パケットの制御（NS/NA）
    - ネイバー要求間隔
    - ネイバー要求再試行回数
  - RA パケットの制御
    - RA の抑制
    - RA MTU の抑制
    - RA 間隔、RA 最小間隔、再送信時間
- プレフィックス単位（RA でアドバタイズ）の制御
  - ライフタイム、優先ライフタイム
  - プレフィックス制御（自動設定、リンク対象）

拡張 GUI を使用した IPv6 ネイバー探索対応のテナント、VRF、およびブリッジ ドメインの作成

このタスクでは、テナント、VRF、およびブリッジドメイン（BD）を作成し、それらの中に2つの異なるタイプのネイバー探索（ND）ポリシーを作成する方法を示します。これらは ND インターフェイス ポリシーと ND プレフィックス ポリシーです。ND インターフェイス ポリシーは BD に導入されますが、ND プレフィックス ポリシーは個々のサブネットに導入されます。各 BD に独自の ND インターフェイス ポリシーを適用することができます。ND インターフェイス ポリシーは、デフォルトですべての IPv6 インターフェイスに導入されます。Cisco APIC には、使用可能なデフォルトの ND インターフェイス ポリシーがすでに存在します。必要に応じて、代わりに使用するカスタム ND インターフェイス ポリシーを作成できます。ND プレフィックス ポリシー

はサブネット レベルにあります。すべての BD が複数のサブネットを持つことができ、各サブネットが異なる ND プレフィックスを持つことができます。

ステップ 1 メニュー バーで、[TENANT] > [Add Tenant] の順にクリックします。

ステップ 2 [Create Tenant] ダイアログボックスで、次のタスクを実行します。

a) [Name] フィールドに、名前を入力します。
b) [Security Domains +] アイコンをクリックして [Create Security Domain] ダイアログボックスを開きます。
c) [Name] フィールドに、セキュリティ ドメインの名前を入力します。[Submit] をクリックします。
d) [Create Tenant] ダイアログボックスで、作成したセキュリティ ドメインのチェックボックスをオンにし、[Submit] をクリックします。

ステップ 3 [Navigation] ペインで、[Tenant-name] > [Networking] の順に展開します。[Work] ペインで、[VRF] アイコンをキャンバスにドラッグして [Create VRF] ダイアログボックスを開き、次の操作を実行します。

a) [Name] フィールドに、名前を入力します。
b) [Submit] をクリックして VRF の設定を完了します。

ステップ 4 [Networking] 領域で、[BD] アイコンを [VRF] アイコンにつなげながらキャンバスにドラッグします。[Create Bridge Domain] ダイアログボックスが表示されたら、次の操作を実行します。

a) [Name] フィールドに、名前を入力します。
b) [L3 Configurations] タブをクリックし、[Subnets] を展開して [Create Subnet] ダイアログボックスを開き、[Gateway IP] フィールドにサブネット マスクを入力します。

ステップ 5 [Subnet Control] フィールドで、[ND RA Prefix] チェックボックスがオンになっていることを確認します。

ステップ 6 [ND Prefix policy] フィールドのドロップダウン リストで、[Create ND RA Prefix Policy] をクリックします。

（注） すべての IPv6 インターフェイスに導入される使用可能なデフォルト ポリシーがすでに存在しています。または、この例で示されているように、使用する ND プレフィックス ポリシーを作成できます。デフォルトでは、IPv6 ゲートウェイのサブネットは ND RA メッセージの ND プレフィックスとしてアドバタイズされます。ユーザは、[ND RA prefix] チェックボックスをオフにして、ND RA メッセージでサブネットをアドバタイズしないことを選択できます。

ステップ 7 [Create ND RA Prefix Policy] ダイアログボックスで、次の操作を実行します。

a) [Name] フィールドにプレフィックス ポリシーの名前を入力します。
（注） 特定のサブネットに対して存在できるプレフィックス ポリシーは 1 つのみです。サブネットは共通プレフィックス ポリシーを使用できますが、各サブネットに異なるプレフィックス ポリシーを適用することが可能です。
b) [Controller State] フィールドで、目的のチェックボックスをオンにします。
c) [Valid Prefix Lifetime] フィールドで、プレフィックスを有効にする期間について目的の値を選択します。
d) [Preferred Prefix Lifetime] フィールドで、目的の値を選択します。[OK] をクリックします。
（注） ND プレフィックス ポリシーが作成され、特定のサブネットに接続されます。

ステップ 8 [ND policy] フィールドのドロップダウン リストで、[Create ND Interface Policy] をクリックし、次のタスクを実行します。

a) [Name] フィールドにポリシーの名前を入力します。
b) [Submit] をクリックします。

ステップ 9 [OK] をクリックしてブリッジ ドメインの設定を完了します。
同様に、さまざまなプレフィックス ポリシーが適用された追加のサブネットを必要に応じて作成できます。

IPv6 アドレスのサブネットが BD に作成され、ND プレフィックス ポリシーが関連付けられています。

REST API を使用した IPv6 ネイバー探索対応のテナント、VRF、およびブリッジ ドメインの作成

ネイバー探索インターフェイス ポリシーとネイバー探索プレフィックス ポリシーが適用された、テナント、VRF、ブリッジ ドメインを作成します。

例：

```
<fvTenant descr="" dn="uni/tn-ExampleCorp" name="ExampleCorp" ownerKey="" ownerTag="">
    <ndIfPol name="NDPol001" ctrl="managed-cfg”  descr="" hopLimit="64" mtu="1500" nsIntvl="1000"
 nsRetries="3" ownerKey="" ownerTag="" raIntvl="600" raLifetime="1800" reachableTime="0"
retransTimer="0"/>
    <fvCtx descr="" knwMcastAct="permit" name="pvn1" ownerKey="" ownerTag="" pcEnfPref="enforced">

    </fvCtx>
    <fvBD arpFlood="no" descr="" mac="00:22:BD:F8:19:FF" multiDstPktAct="bd-flood" name="bd1"
ownerKey="" ownerTag="" unicastRoute="yes" unkMacUcastAct="proxy" unkMcastAct="flood">
        <fvRsBDToNdP tnNdIfPolName="NDPol001"/>
        <fvRsCtx tnFvCtxName="pvn1"/>
        <fvSubnet ctrl="nd" descr="" ip="34::1/64" name="" preferred="no" scope="private">
            <fvRsNdPfxPol tnNdPfxPolName="NDPfxPol001"/>
        </fvSubnet>
        <fvSubnet ctrl="nd" descr="" ip="33::1/64" name="" preferred="no" scope="private">
            <fvRsNdPfxPol tnNdPfxPolName="NDPfxPol002"/>
        </fvSubnet>
    </fvBD>
    <ndPfxPol ctrl="auto-cfg,on-link" descr="" lifetime="1000" name="NDPfxPol001" ownerKey=""
ownerTag="" prefLifetime="1000"/>
   <ndPfxPol ctrl="auto-cfg,on-link" descr="" lifetime="4294967295" name="NDPfxPol002" ownerKey=""
 ownerTag="" prefLifetime="4294967295"/>
</fvTenant>
```

（注） 外部ルーテッドを設定するときにパブリック サブネットがある場合は、ブリッジ ドメインを外部設定と関連付ける必要があります。

CLIを使用したIPv6ネイバー探索対応のテナント、VRF、およびブリッジ ドメインの設定

ステップ 1 CLI で、ディレクトリを /aci に変更します。

例：

```
admin@apic1:~> cd /aci
```

ステップ 2 ネイバー探索インターフェイス ポリシーを設定します。

例：

```
admin@apic1:aci> cd tenants/
admin@apic1:tenants> mocreate ExampleCorp
admin@apic1:tenants> moconfig commit
admin@apic1:tenants> cd ExampleCorp/
admin@apic1:ExampleCorp> cd networking/protocol-policies/nd/
admin@apic1:nd> mocreate interface-policy NDPol001
admin@apic1:nd> moconfig commit
admin@apic1:nd> cd interface-policy-NDPol001/
admin@apic1:interface-policy-NDPol001> moset mtu 1500
admin@apic1:interface-policy-NDPol001> moconfig commit
admin@apic1:interface-policy-NDPol001>
admin@apic1:interface-policy-NDPol001> cd ../../../private-networks/
admin@apic1:private-networks> mocreate pvn1
admin@apic1:private-networks> moconfig commit
admin@apic1:pvn1> cd ../../bridge-domains/
admin@apic1:bridge-domains> mocreate bd1
admin@apic1:bridge-domains> cd bd1
admin@apic1:bd1> moset custom-mac-address 00:22:BD:F8:19:FF
admin@apic1:bd1> moset nd-interface-policy NDPol001
admin@apic1:bd1> moconfig commit
```

ステップ 3 ネイバー探索プレフィックス ポリシーを設定します。

例：

```
admin@apic1:bd1> cd ../../protocol-policies/nd/
admin@apic1:nd> mocreate prefix-policy NDPfxPol001
admin@apic1:nd> cd prefix-policy-NDPfxPol001/
admin@apic1:prefix-policy-NDPfxPol001> moset valid-lifetime 1000
admin@apic1:prefix-policy-NDPfxPol001> moset preferred-lifetime 1000
admin@apic1:prefix-policy-NDPfxPol001> moconfig commit
admin@apic1:prefix-policy-NDPfxPol001> cd ../
admin@apic1:nd> mocreate prefix-policy NDPfxPol002
admin@apic1:nd> cd prefix-policy-NDPfxPol002/
admin@apic1:prefix-policy-NDPfxPol002> moset valid-lifetime 4294967295
admin@apic1:prefix-policy-NDPfxPol002> moset preferred-lifetime 4294967295
admin@apic1:prefix-policy-NDPfxPol002> moconfig commit
admin@apic1:prefix-policy-NDPfxPol002> cd ../../../bridge-domains/bd1/subnets/
admin@apic1:subnets> mocreate 34::1/64
admin@apic1:subnets> cd 34::1_64/
admin@apic1:34::1_64> moset nd-prefix-policy NDPfxPol001
admin@apic1:34::1_64> moconfig commit
admin@apic1:34::1_64> cd ../
admin@apic1:subnets> mocreate 33::1/64
admin@apic1:subnets> cd 33::1_64/
```

```
admin@apic1:33::1_64> moset nd-prefix-policy NDPfxPol002
admin@apic1:33::1_64> moconfig commit
```

インポート制御とエクスポート制御を使用するルーティング制御プロトコルの設定

このトピックでは、Cisco APIC 使用時にインポート制御とエクスポート制御を使用するルーティング制御プロトコルを設定する方法の典型的な例を示します。

GUI を使用した、インポート制御とエクスポート制御を使用するルート制御プロトコルの設定

このタスクでは、インポートポリシーとエクスポートポリシーの作成手順を示します。デフォルトでは、インポート制御は適用されていないため、インポート制御を手動で割り当てる必要があります。

はじめる前に

- テナント、プライベート ネットワーク、およびブリッジ ドメインが作成されていること。
- テナント ネットワークのレイヤ 3 Outside が作成されていること。

ステップ 1 メニュー バーで、[TENANTS] > *[Tenant_name]* > [Networking] > [External Routed Networks] > *[Layer3_Outside_name]* の順にクリックします。

ステップ 2 [Layer3_Outside_name] を右クリックし、[Create Route Profile] をクリックします。

ステップ 3 [Create Route Profile] ダイアログボックスで、次の操作を実行します。

a) [Name] フィールドのドロップダウン リストから、適切なルート プロファイルを選択します。
選択内容に応じて、特定の Outside でアドバタイズされている内容が自動的に使用されます。

b) [Type] フィールドで、[Combining Subnets with Routing Policy] を選択します。

c) [Order] を展開します。

ステップ 4 [Create Route Control Context] ダイアログボックスで、次の操作を実行します。

a) [Order] フィールドで、目的の順序の番号を選択します。

b) [Name] フィールドに、ルート制御プライベート ネットワークの名前を入力します。

c) [Match Rule] フィールドのドロップダウン リストで、[Create Match Rule] をクリックします。

d) [Create Match Rule] ダイアログボックスで、[Name] フィールドに、ルート一致ルール名を入力します。
[Submit] をクリックします。

必要に応じて、正規表現による一致コミュニティ条件および一致コミュニティ条件を指定します。一致コミュニティファクタでは、名前、コミュニティ、およびスコープを指定する必要があります。

e) [Set Attribute] ドロップダウン リストから、[Create Action Rule Profile] を選択します。
f) [Create Action Rule Profile] ダイアログボックスの [Name] フィールドに、ルールの名前を入力します。
g) 設定するルールのチェックボックスをオンにし、選択肢として表示されている適切な値を選択します。[Submit] をクリックします。
ポリシーが作成され、アクション ルールに関連付けられました。
h) [OK] をクリックします。
i) [Create Route Profile] ダイアログボックスで、[Submit] をクリックします。

ステップ 5 [Navigation] ペインで、[Route Profile] > *[route_profile_name]* > *[route_control_private_network_name]* の順に選択します。
[Work] ペインの [Properties] に、ルート プロファイル ポリシーと関連アクション ルール名が表示されます。

ステップ 6 [Navigation] ペインで、[Layer3_Outside_name] をクリックします。
[Work] ペインに、プロパティが表示されます。

ステップ 7 （任意） [Route Control Enforcement] フィールドをクリックし、「Import Control」と入力してインポート ポリシーを有効にします。
インポート制御ポリシーはデフォルトで有効になっていませんが、ユーザが有効にすることができます。インポート制御ポリシーはBGP ではサポートされますが、EIGRP およびOSPF ではサポートされません。ユーザがサポートされていないプロトコルのインポート制御ポリシーを有効にしても、自動的に無視されます。エクスポート制御ポリシーは、BGP、EIGRP、および OSPF でサポートされます。

ステップ 8 カスタマイズされたエクスポート ポリシーを作成するには、[Route Profiles] を右クリックし、[Create Route Profiles] をクリックし、次の操作を実行します。

a) [Create Route Profile] ダイアログボックスで、[Name] フィールドのドロップダウン リストから、エクスポート ポリシーの名前を選択します。
b) ダイアログ ボックスの [+] 記号を展開します。
c) [Create Route Control Context] ダイアログボックスの [Order] フィールドで、値を選択します。
d) [Name] フィールドに、ルート制御プライベート ネットワークの名前を入力します。
e) （任意） [Match Rule] フィールドのドロップダウン リストから、[Create Route Control Context] を選択し、必要に応じて一致ルール ポリシーを作成して付加します。
f) [Set Attribute] フィールドのドロップダウン リストから、[Create Action Rule Profile] を選択します。
または、必要に応じて既存の set アクションを選択し、[Submit] をクリックすることもできます。
g) [Create Action Rule Profile] ダイアログボックスで、[Name] フィールドに、名前を入力します。
h) 設定するルールのチェックボックスをオンにし、選択肢として表示されている適切な値を選択します。[Submit] をクリックします。
[Create Route Control Context] ダイアログ ボックスでは、ポリシーが作成されてアクション ルールに関連付けられています。
i) [OK] をクリックします。
j) [Create Route Profile] ダイアログボックスで、[Submit] をクリックします。

[Work] ペインに、エクスポート ポリシーが表示されます。

（注） エクスポート ポリシーを有効にするには、最初に適用する必要があります。この例では、このポリシーはネットワークのすべてのサブネットに適用されます。

ステップ 9 [Navigation] ペインで、[External Routed Networks] > *[External_Routed_Network_name]* > [Networks] > *[Network_name]* の順に展開し、次の操作を実行します。

a) [Name] フィールドのドロップダウン リストから、前に作成したポリシーを選択します。

b) [Direction] フィールドのドロップダウン リストから、[Route Control Profile] を選択します。[Update] をクリックします。

ステップ 10 [Submit] をクリックします。

REST API を使用した、インポート制御とエクスポート制御を使用するルート制御プロトコルの設定

はじめる前に

- テナント、プライベート ネットワーク、およびブリッジ ドメインが作成されていること。
- レイヤ 3 Outside テナント ネットワークが設定されていること。

インポート制御とエクスポート制御を使用するルート制御プロトコルを設定します。

例：

```
<l3extOut descr="" dn="uni/tn-Ten_ND/out-L3Out1" enforceRtctrl="export" name="L3Out1" ownerKey=""
 ownerTag="" targetDscp="unspecified">
        <l3extLNodeP descr="" name="LNodeP1" ownerKey="" ownerTag="" tag="yellow-green"
targetDscp="unspecified">
           <l3extRsNodeL3OutAtt rtrId="1.2.3.4" rtrIdLoopBack="yes" tDn="topology/pod-1/node-101">

               <l3extLoopBackIfP addr="2000::3" descr="" name=""/>
            </l3extRsNodeL3OutAtt>
            <l3extLIfP descr="" name="IFP1" ownerKey="" ownerTag="" tag="yellow-green">
                <ospfIfP authKeyId="1" authType="none" descr="" name="">
                    <ospfRsIfPol tnOspfIfPolName=""/>
                </ospfIfP>
                <l3extRsNdIfPol tnNdIfPolName=""/>
              <l3extRsPathL3OutAtt addr="10.11.12.10/24" descr="" encap="unknown" ifInstT="l3-port"

llAddr="::" mac="00:22:BD:F8:19:FF" mtu="1500" tDn="topology/pod-1/paths-101/pathep-[eth1/17]"
targetDscp="unspecified"/>
            </l3extLIfP>
        </l3extLNodeP>
        <l3extRsEctx tnFvCtxName="PVN1"/>
        <l3extInstP descr="" matchT="AtleastOne" name="InstP1" prio="unspecified"
targetDscp="unspecified">
            <fvRsCustQosPol tnQosCustomPolName=""/>
            <l3extSubnet aggregate="" descr="" ip="192.168.1.0/24" name="" scope=""/>
        </l3extInstP>
        <ospfExtP areaCost="1" areaCtrl="redistribute,summary" areaId="0.0.0.1" areaType="nssa"
descr=""/>
        <rtctrlProfile descr="" name="default-export" ownerKey="" ownerTag="">
```

```
            <rtctrlCtxP descr="" name="routecontrolpvtnw" order="3">
                <rtctrlScope descr="" name="">
                    <rtctrlRsScopeToAttrP tnRtctrlAttrPName="actionruleprofile2"/>
                </rtctrlScope>
            </rtctrlCtxP>
        </rtctrlProfile>
    </l3extOut>
```

オブジェクト モデル CLI を使用した、インポート制御とエクスポート制御を使用するルート制御プロトコルの設定

はじめる前に

- テナント、プライベート ネットワーク、およびブリッジ ドメインが作成されていること。
- レイヤ 3 Outside テナント ネットワークが設定されていること。

ステップ 1 CLI で、ディレクトリを /aci に変更します。

例：

```
admin@apic1:~> cd /aci
```

ステップ 2 ルート プロファイル スコープを入力します。

例：

```
admin@apic1:l3-outside-bgp-ext-out> cd route-profiles/
```

ステップ 3 ルート プロファイルを作成します。

例：

```
admin@apic1:route-profiles> mocreate test-rp
admin@apic1:route-profiles> moconfig commit
Committing mo
'tenants/tn1/networking/external-routed-networks/l3-outside-bgp-ext-out/route-profiles/test-rp'
All mos committed successfully.
```

ステップ 4 ルート制御プロファイルのコンテキストを作成し、順序とアクション ルール プロファイルを設定します。

例：

```
admin@apic1:route-profiles> cd test-rp/
admin@apic1:test-rp> cd contexts/
admin@apic1:contexts> mocreate rcctx
admin@apic1:contexts> cd rcctx/
admin@apic1:rcctx> moset order 1

admin@apic1:rcctx> moset action a1
admin@apic1:rcctx> moconfig commit
Committing mo
'tenants/tn1/networking/external-routed-networks/l3-outside-bgp-ext-out/route-profiles/test-rp/contexts/rcctx'
```

```
All mos committed successfully.
```

ステップ 5 ルート制御適用をエクスポートに設定します。
インポートのルート制御適用は BGP の場合にのみ使用できます。

例：

```
admin@apic1:rcctx> cd ../../../../
admin@apic1:l3-outside-bgp-ext-out> moset enforce-route-control export-control
```

ステップ 6 エクスポート ルート プロファイルを作成し、アクションを設定します。

例：

```
admin@apic1:l3-outside-bgp-ext-out> cd route-profiles
admin@apic1:route-profiles> mocreate export-rp
admin@apic1:route-profiles> moconfig commit
Committing mo
'tenants/tn1/networking/external-routed-networks/l3-outside-bgp-ext-out/route-profiles/export-rp'
All mos committed successfully.
admin@apic1:route-profiles> cd export-rp/
admin@apic1:export-rp> cd contexts/
admin@apic1:contexts> mocreate exp-ctx
admin@apic1:contexts> cd exp-ctx/
admin@apic1:exp-ctx> moset action a3
admin@apic1:exp-ctx> moconfig commit

Committing mo
'tenants/tn1/networking/external-routed-networks/l3-outside-bgp-ext-out/route-profiles/export-rp/contexts/exp-ctx'
All mos committed successfully.
```

ステップ 7 外部 EPG を作成し、目的のルート制御プロファイルを選択します。

例：

```
admin@apic1:networks> mocreate extepg
admin@apic1:networks> cd extepg/
admin@apic1:extepg> ls consumed-contracts  mo provided-contracts  route-control-profiles  subnets
  summary  tags
admin@apic1:extepg> cd route-control-profiles/

admin@apic1:route-control-profiles> mocreate export-rp route-export-policy
admin@apic1:route-control-profiles> moconfig commit
Committing mo
'tenants/tn1/networking/external-routed-networks/l3-outside-bgp-ext-out/networks/extepg/route-control-profiles/rp1-route-export-policy'

All mos committed successfully.
```

ACI トランジット ルーティング

ACI ファブリックは、境界ルータが他のドメインとの双方向再配布を実行できるようにする、トランジット ルーティングをサポートします。トランジット再配布をブロックする ACI ファブリックの以前のリリースのスタブ ルーティング ドメインとは異なり、双方向再配布では、1 つのルーティング ドメインから別のルーティング ドメインにルーティング情報を渡します。そのような再配布により、ACI ファブリックはさまざまなルーティング ドメイン間の完全な IP 接続を提供しま

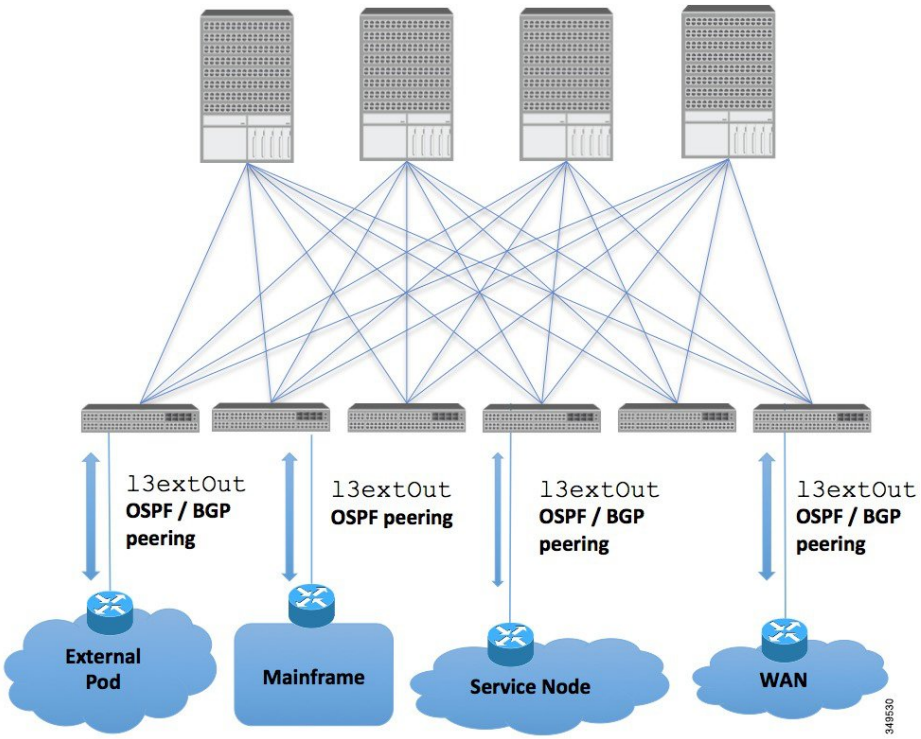
す。これにより、ルーティング ドメイン間のバックアップパスを有効にすることで冗長接続を提供することもできます。

最適でないルーティングや、ルーティング ループというさらに重大な問題を回避するように、トランジット再配布ポリシーを設計してください。通常、トランジット再配布は、元のトポロジとリンク状態情報を維持せず、ディスタンス ベクター方式で外部ルートを再配布します（リンクステートプロトコルの場合でもルートはベクタープレフィックスと関連距離としてアドバタイズされます）。このような状況では、ルータが想定外のルーティング ループを形成して、パケットを宛先に配信できなくなる可能性があります。

トランジット ルーティングの使用例

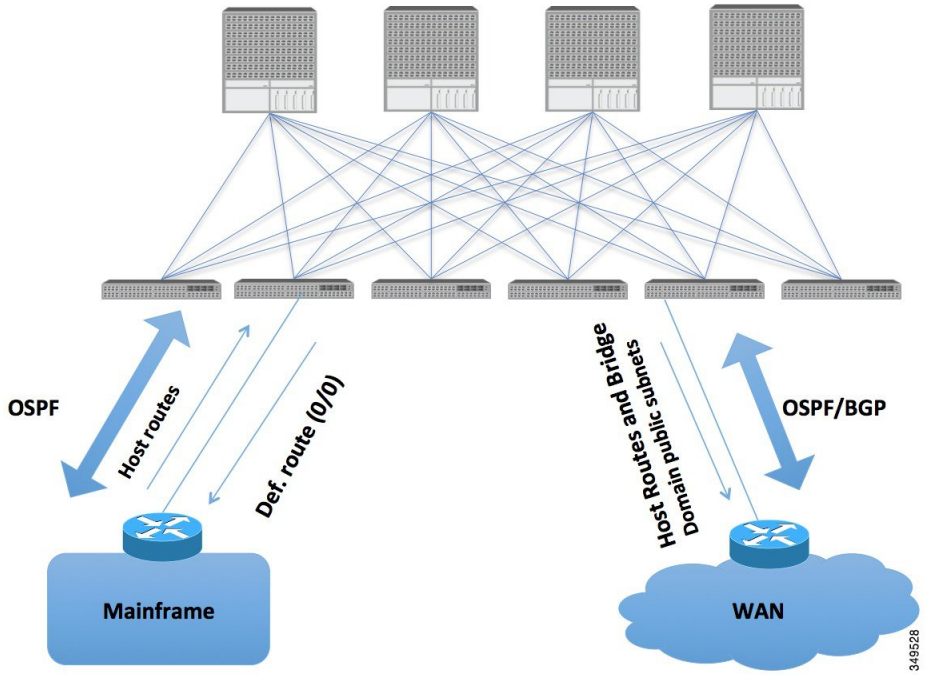
外部ポッド、メインフレーム、サービス ノード、WAN ルータなどの複数のレイヤ 3 ドメインがACIファブリックとピアリングして、それらの間のトランジット機能を提供することができます。

図 *2*：レイヤ *3* ドメイン間のトランジット ルーティング



メインフレームは、論理パーティション（LPAR）および仮想 IP アドレッシング（VIPA）の要件に対応する標準 IP ルーティング プロトコルを実行する IP サーバとして機能します。

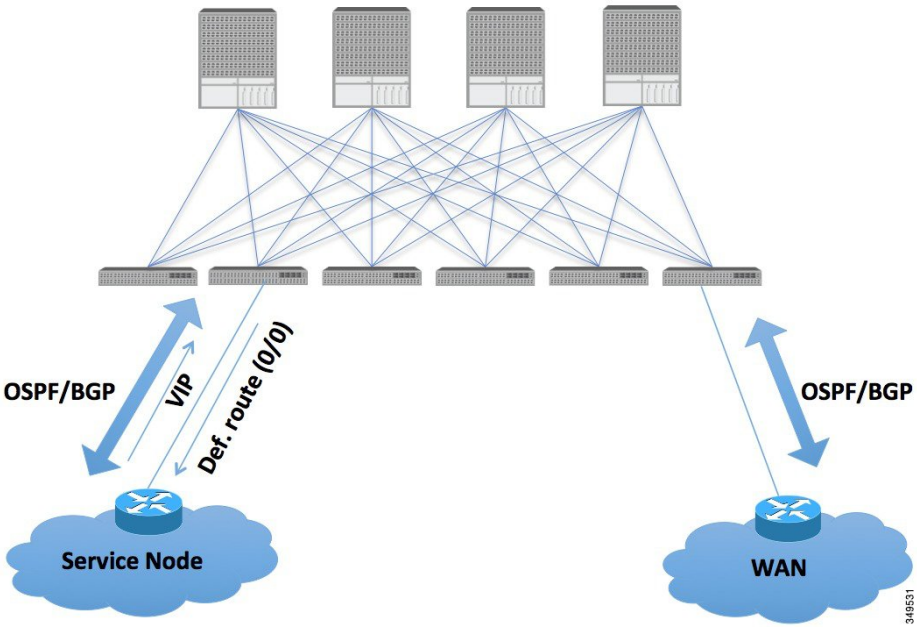
図 *3*：メインフレームのトランジット接続



メインフレームでは、ACI ファブリックが WAN ルータを介した外部ドメインおよびファブリック内の East-West トラフィックのトランジット ドメインである必要がありますが、ホスト ルートがファブリックにプッシュされ、それらのルートがファブリック内および外部インターフェイスに配布されます。

サービス ノードは ACI ファブリックとピアリングし、外部 WAN インターフェイスに再配布される仮想 IP（VIP）ルートをアドバタイズすることができます。

図 *4*：サービス ノードのトランジット接続

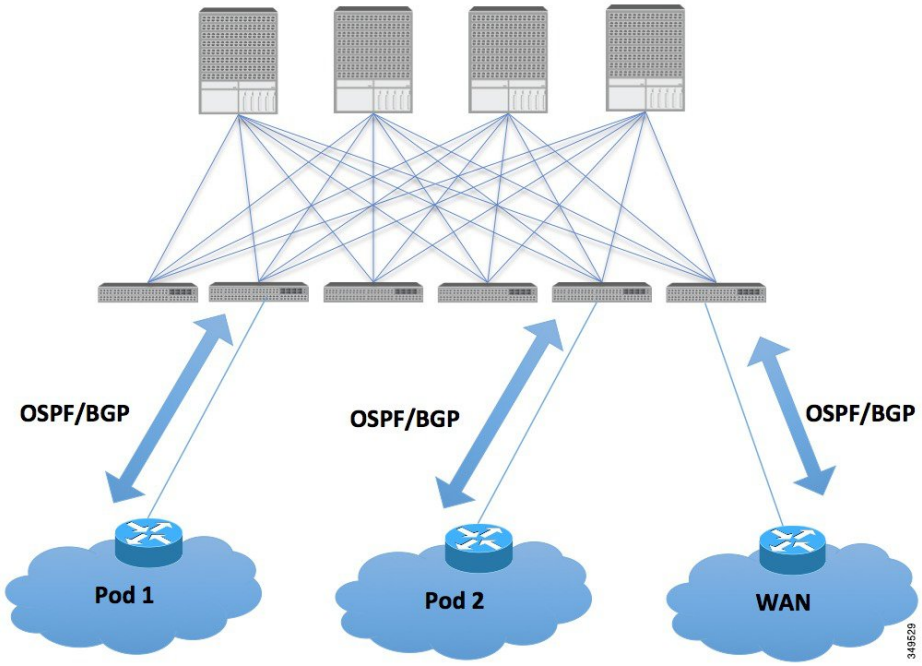


VIP は、特定のサイトやサービスの外部向けの IP アドレスです。VIP は、サービス ノードの背後にある 1 つ以上のサーバまたはノードに関連付けられています。

ACI ファブリックは、外部接続および POD（ポッド）間の相互接続のトランジットとして機能します。クラウドのプロバイダーは、顧客データ センター内に管理対象リソース POD を導入でき

ます。責任分界点は、OSPF および BGP とファブリックとのピアリングが行われている L3Out にすることができます。

図 *5*：複数ポッドのトランジット接続



このようなシナリオでは、ポリシーは責任分界点で管理され、ACI ポリシーを設定する必要はありません。

L4-L7 ルート ピアリングは、ファブリックをトランジットとして使用する特殊なケースであり、ACI ファブリックは他の POD（ポッド）に対する OSPF および BGP のトランジット ドメインの役目を果たします。ルート ピアリングは、L4-L7 サービス デバイスで OSPF および BGP のピアリングを設定し、接続先の ACI リーフ ノードとルートを交換できるようにするために使用されます。ルート ピアリングの一般的な使用例として、SLB VIP が OSPF および iBGP を介して ACI ファブリック外のクライアントにアドバタイズされるルート ヘルス インジェクションがあります。このシナリオの設定のウォークスルーについては、付録 H を参照してください。

トランジット ルーティングの概要

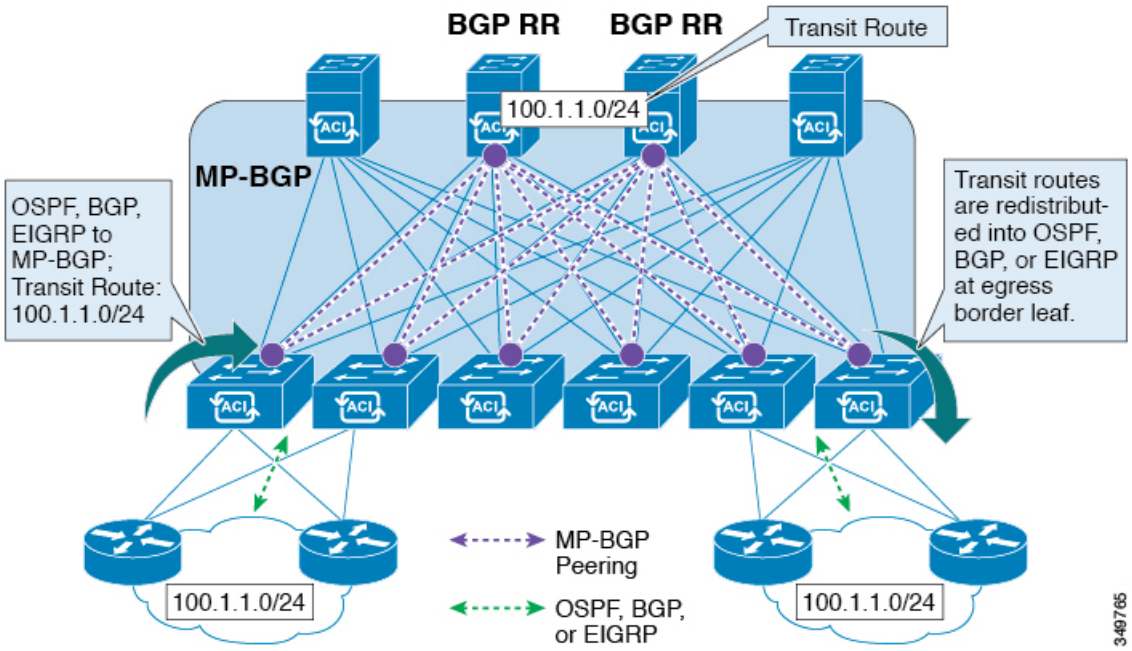
この記事では、Cisco APIC を使用したレイヤ 3 中継ルーティングの概要を示します。

ACI ソフトウェアは、OSPF（NSSA）および iBGP を使用した外部レイヤ 3 接続をサポートします。ACI ファブリックは、外部レイヤ 3 Outside 接続の外部ルータにテナント ブリッジ ドメインのサブネットをアドバタイズします。外部ルータから学習されたルートは、他の外部ルータにアドバタイズされません。ACI ファブリックはスタブ ネットワークと同じように動作し、外部レイヤ 3 ドメイン間のトラフィックの伝送に使用できます。

ACI ソフトウェアでは、トランジット ルーティングのサポートが追加されています。1 つのテナント/コンテキスト（VRF）内で複数の外部レイヤ 3 Outside 接続がサポートされ、ACI ファブリックは 1 つの外部レイヤ 3 Outside 接続から学習されたルートを別の外部レイヤ 3 Outside 接続にアドバタイズすることができます。外部レイヤ 3 ドメインは、リーフ スイッチ（境界リーフ）の ACI ファブリックとピアリングします。ファブリックはピア間の Multiprotocol-Border Gateway Protocol（MP-BGP）中継ドメインです。

外部レイヤ 3 Outside 接続用の ACI ファブリック設定は、テナントおよび VRF レベルで行われます。外部ピアから学習したルートは、VRF ごとに入力リーフの MP-BGP にインポートされます。外部レイヤ 3 Outside 接続から学習したプレフィックスは、テナント VRF が存在するリーフ スイッチにのみエクスポートされます。

図 *6*：トランジット ルーティングの概要を示す図



ACI ファブリック内のルート配布

ACI は以下のルーティング メカニズムをサポートします。

- スタティック ルート
- OSPFv2（IPv4）
- OSPFv3（IPv6）
- iBGP
- eBGP（IPv4 および IPv6）
- EIGRP（IPv4）プロトコル

ACI は、外部ルータに接続する際に VRF-Lite の実装をサポートします。サブインターフェイスを使用して、境界リーフは 1 つの物理インターフェイスを持つ複数のテナントへのレイヤ 3 Outside 接続を提供できます。VRF-Lite の実装では、テナントごとに 1 つのプロトコル セッションが必要です。

ACI ファブリック内の外部ルートを伝播するために、ACI ファブリック内のリーフ スイッチとスパイン スイッチの間に Multiprotocol BGP（MP-BGP）が実装されています。単一ファブリック内で多数のリーフ スイッチをサポートするために、BGP ルート リフレクタ テクノロジーが導入されています。リーフ スイッチとスパイン スイッチはすべて 1 つの BGP 自律システム（AS）内にあります。境界リーフが外部ルートを学習すると、MP-BGP アドレス ファミリ VPN バージョン 4 または VPN バージョン 6 に特定の VRF の外部ルートを再配布できます。アドレス ファミリ VPN バージョン 4 を使用して、MP-BGP は VRF ごとに別の BGP ルーティング テーブルを維持します。MP-BGP 内で、境界リーフは BGP ルート リフレクタであるスパイン スイッチにルートをアドバタイズします。その後、ルートは VRF（APIC GUI の用語ではプライベート ネットワーク）がインスタンス化されているすべてのリーフに伝播されます。

外部レイヤ 3 Outside 接続タイプ

ACI は、以下の外部レイヤ 3 Outside 接続オプションをサポートします。

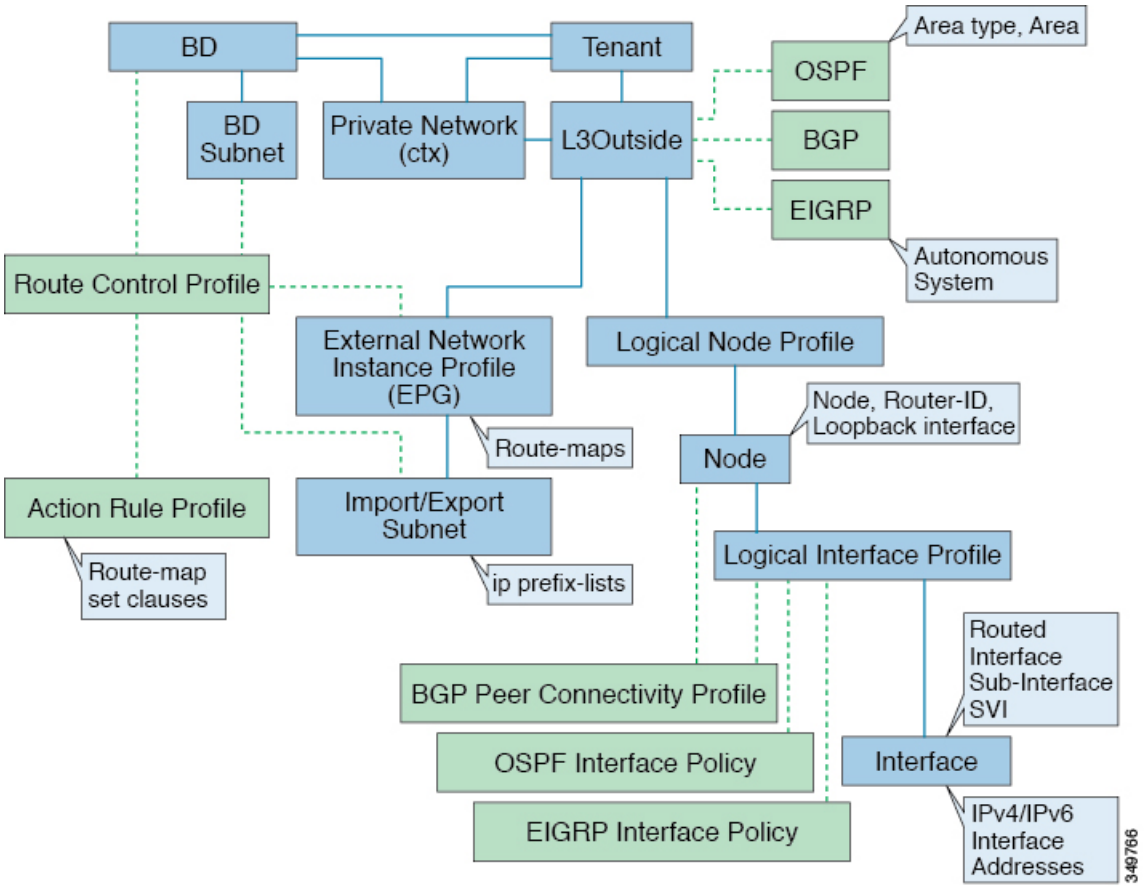
- スタティック ルーティング（IPv4 および IPv6 でサポート）
- 標準および NSSA エリアの OSPFv2（IPv4）
- 標準および NSSA エリアの OSPFv3（IPv6）
- iBGP（IPv4 および IPv6）
- eBGP（IPv4 および IPv6）
- EIGRP（IPv4 のみ）

外部レイヤ 3 Outside 接続は、以下のインターフェイスでサポートされます。

- レイヤ 3 ルーテッド インターフェイス
- 802.1Q タギング対応のサブインターフェイス：サブインターフェイスを使用すると、複数のプライベート ネットワークに対するレイヤ 2 外部接続を提供できます。

- スイッチ仮想インターフェイス（SVI）：SVIインターフェイスを使用すると、レイヤ2とレイヤ 3 をサポートする同じ物理インターフェイスをレイヤ 2 外部接続とレイヤ 3 外部接続に使用できます。

図 *7*：*ACI* レイヤ *3* 管理対象オブジェクト



L3Outside 接続に使用される管理対象オブジェクトは、次のとおりです。

- 外部レイヤ 3 Outside（L3ext）：ルーティング プロトコル オプション（OSPF エリア タイプ、エリア、EIGRP AS、BGP）、プライベート ネットワーク、外部物理ドメイン。
- 論理ノード プロファイル：外部レイヤ 3 Outside 接続に対して 1 つ以上のノードが定義されたプロファイル。ルータ ID とループバック インターフェイス設定はプロファイルで定義されます。

（注） 複数の外部レイヤ 3 Outside 接続間の同じノードには同じルータ ID を使用してください。

- 論理インターフェイス プロファイル：IPv4 および IPv6 インターフェイスの IP インターフェイス設定。これは、ルート インターフェイス、ルーテッド サブインターフェイス、および

SVI でサポートされます。SVI は、物理ポート、ポート チャネルまたは VPC で設定できます。

- OSPF インターフェイス ポリシー：OSPF ネットワーク タイプ、優先度など。
- EIGRP インターフェイス ポリシー：タイマー、スプリット ホライズン設定など。
- BGP ピア接続プロファイル：ほとんどの BGP ピア設定、リモート AS、ローカル AS、および BGP ピア接続オプションが設定されるプロファイル。BGP ピア接続プロファイルは、ノードプロファイルの下の論理インターフェイスプロファイルまたはループバック インターフェイスに関連付けることができます。これは、BGP ピアリング セッションの update-source 設定を決定します。
- 外部ネットワーク インスタンス プロファイル（EPG）（l3extInstP）：外部 EPG はプレフィックス ベースの EPG または InstP とも呼ばれます。インポートおよびエクスポートのルート制御ポリシー、セキュリティ インポート ポリシー、およびコントラクトの関連付けは、このプロファイルで定義されます。単一 L3Out に複数の外部 EPG を設定できます。単一外部レイヤ 3 Outside 接続で別のルートまたはセキュリティ ポリシーが定義されている場合、複数の外部 EPG を使用できます。1 つの外部 EPG または複数の外部 EGP がルート マップにまとめられます。外部 EPG で定義されるインポート/エクスポート サブネットは、ルート マップの IP プレフィックス リストの match 句と関連しています。外部 EPG は、インポート セキュリティ サブネットとコントラクトが関連付けられる場所でもあります。これは、この L3out のトラフィックの許可またはドロップに使用されます。
- アクション ルール プロファイル：アクション ルール プロファイルは、L3Out のルート マップの set 句を定義するために使用されます。サポートされる set 句は、BGP communities（standard および extended）、Tags、Preference、Metric、および Metric type です。
- ルート制御プロファイル：ルート制御プロファイルは、アクション ルール プロファイルを参照するために使用されます。これは、アクションルールプロファイルの順序付きプロファイルにすることができます。ルート制御プロファイルは、テナント BD、BD サブネット、外部 EPG、または外部 EPG サブネットで参照できます。

BGP、OSPF、および EIGRP L3Out 用の追加のプロトコル設定が存在します。これらの設定は、GUI の [ACI Protocol Policies] セクションでテナントごとに設定されます。

サポートされるトランジットの組み合わせのマトリックス

レイヤ 3 Outside 接続タイプ	OSPF	iBGP			eBGP		EIGRP	スタティック ルート
		OSPF 上の iBGP	スタティック ルート上の iBGP	直接接続上の iBGP	OSPF 上の eBGP	直接接続上の eBGP		
OSPF	○	○*	○	×	○	○	○	○

レイヤ 3 Outside 接続タイプ		OSPF	iBGP			eBGP		EIGRP	スタティック ルート
			OSPF 上の iBGP	スタティック ルート上の iBGP	直接接続上の iBGP	OSPF 上の eBGP	直接接続上の eBGP		
iBGP	OSPF 上の iBGP	○*	×	×	×	×	○	×	○
	スタティック ルート上の iBGP	○	×	×	×	×	○	×	○
	直接接続上の iBGP	○	×	×	×	×	○	×	○
eBGP	OSPF 上の eBGP	○	×	×	○	○	×	×	×
	直接接続上の eBGP	○	○	×	○	×	○	×	○
EIGRP		○	×	×	×	×	×	×	
スタティック ルート		○	○	○	○	×	○		○

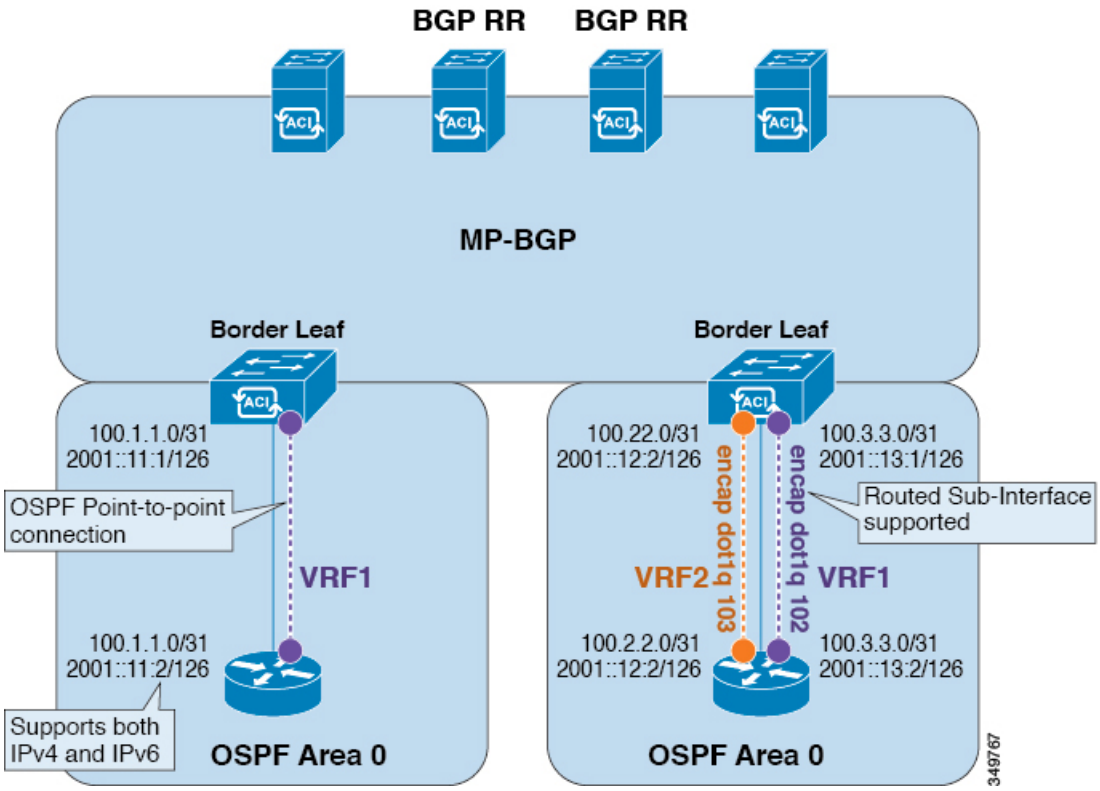
- * = 同じリーフ スイッチではサポートされません
- × = サポートされていないかテストされていない組み合わせ
- **太字 = このリリースでサポートされます**

OSPF レイヤ 3 Outside 接続

OSPF レイヤ 3 Outside 接続は、標準または NSSA エリアです。バックボーン（エリア 0）エリアも、OSPF レイヤ 3 Outside 接続エリアとしてサポートされます。ACI は、IPv4 の OSPFv2 と IPv6 の OSPFv3 の両方をサポートします。OSPF レイヤ 3 Outside を作成するときに、OSPF バージョンを設定する必要はありません。インターフェイス プロファイル設定（IPv4 または IPv6 アドレッシング）に基づいて、正しい OSPF プロセスが自動的に作成されます。IPv4 と IPv6 の両方のプロトコルが同じインターフェイス（デュアル スタック）でサポートされますが、2 つの個別インターフェイス プロファイルを作成する必要があります。

レイヤ 3 Outside 接続は、ルーテッド インターフェイス、ルーテッド サブインターフェイス、および SVI でサポートされます。SVI は、L2 と L3 両方のトラフィックで物理接続を共有する必要がある場合に使用されます。SVI は、ポート、ポート チャネル、VPC ポート チャネルでサポートされます。

図 *8*：*OSPF* レイヤ *3 Out* 接続



SVI がレイヤ 3 Outside 接続に使用されると、外部ブリッジ ドメインが境界リーフ スイッチに作成されます。外部ブリッジ ドメインは、ACI ファブリック上の 2 つの VPC スイッチ間の接続を可能にします。これにより、両方の VPC スイッチが、相互の、および外部 OSPF デバイスとの OSPF 隣接関係を確立できます。

ブロードキャスト ネットワークで OSPF を実行する場合、障害が発生したネイバーを検出する時間は dead 間隔（デフォルトは 40 秒）です。障害が発生した後でネイバー隣接関係を再確立する場合にも、代表ルータ（DR）の選定が原因で時間がかかる可能性があります。

（注） 1 つの VPC ノードへのリンクまたはポート チャネルに障害が発生しても、OSPF 隣接関係がダウンすることはありません。OSPF 隣接関係は、その他の VPC ノードを介してアクセスできる外部 BD によりアップ状態を維持することができます。

EIGRP レイヤ 3 Outside 接続

EIGRP レイヤ 3 Outside 接続は、OSPF と同じインターフェイス タイプでサポートされますが、EIGRP では IPv6 はサポートされません。

（注） EIGRP の VPC/SVI 設定は OSPF と同じです。

外部 BGP スピーカーに対する BGP プロトコル ピアリング

ACI は、iBGP と eBGP を使用して境界リーフと外部 BGP スピーカーの間のピアリングをサポートします。ACI は、BGP ピアリングで以下の接続をサポートします。

- OSPF 上の iBGP ピアリング
- OSPF 上の eBGP ピアリング
- 直接接続上の iBGP ピアリング
- 直接接続上の eBGP ピアリング
- スタティック ルート上の iBGP ピアリング

（注） BGP ピアリングで OSPF が使用される場合、OSPF は BGP ピアリング アドレスへのルートの学習とアドバタイズのみに使用されます。レイヤ 3 Outside ネットワーク（EPG）に適用されるすべてのルート制御が BGP プロトコル レベルで適用されます。

ACI は、外部ピアへの iBGP および eBGP 接続用に多数の機能をサポートします。BGP 機能は、[BGP Peer Connectivity Profile] で設定されます。

BGP ピアの接続プロファイル機能について、次の表で説明します。

表 *2*：*BGP* ピアの接続プロファイル機能

BGP 機能	機能の説明	NX-OS での同等のコマンド
Allow Self-AS	Allowed AS Number Count 設定と併用されます。	**allowas-in**
Disable peer AS check	アドバタイズ時のピア AS 番号のチェックを無効にします。	**disable-peer-as-check**
Next-hop self	常にローカル ピア アドレスにネクスト ホップ属性を設定します。	**next-hop-self**

BGP 機能	機能の説明	NX-OS での同等のコマンド
Send community	ネイバーにコミュニティ属性を送信します。	**send-community**
Send community extended	ネイバーに拡張コミュニティ属性を送信します。	**send-community extended**
Password	BGP MD5 認証。	**password**
Allowed AS Number Count	Allow Self-AS 機能と併用されます。	**allowas-in**
Disable connected check	直接接続されたEBGPネイバーの接続チェックを無効にします（EBGPネイバーがループバックからピアリングすることを許可）。	
TTL	EBGPマルチホップ接続のTTL値を設定します。これはEBGPでのみ有効です。	**ebgp-multihop <TTL>**
Autonomous System Number	ピアのリモート自律システム番号。	**neighbor <x.x.x.x> remote-as**
Local Autonomous System Number Configuration	ローカルAS機能を使用するときのオプション（No Prepend+replace-AS+dual-ASなど）。	
Local Autonomous System Number	ファブリック MP-BGP ルート リフレクタ プロファイルに割り当てられている AS とは異なる AS 番号をアドバタイズするために使用されるローカル AS 機能。これは EBGP ネイバーの場合にのみサポートされ、ローカル AS 番号がルート リフレクタ ポリシー AS と異なっている必要があります。	**local-as xxx <no-prepend> <replace-as> <dual-as>**

中継ルート制御

ACI ファブリックは、ダイナミック ルーティング プロトコル（OSPF、EIGRP、および BGP）を実行しているテナントおよび VRF ごとに複数の外部レイヤ 3 接続を持つことができます。外部レイヤ 3 Outside 接続から学習したルートまたはスタティック ルートとして設定したルートの配布を制御するために、ACI ファブリックにはルート制御ポリシーが実装されています。ACI はインポート ルート制御とエクスポート ルート制御をサポートします。インポート ルート制御とエクスポート ルート制御は、ルート マップと IP プレフィックス リストを使用して、ACI ファブリックに入ることを許可するプレフィックスおよび ACI ファブリックから外部にアドバタイズされるプレフィックスのインポートとエクスポートを制御します。

インポート ルート制御のデフォルト設定では、すべてのプレフィックスが許可されます。ACI ファブリック内のすべてのリーフ スイッチが、その VRF が導入されているすべての外部プレフィックスを学習します。エクスポート ルート制御のデフォルト設定では、すべてのプレフィックスが拒否されます。インポート ルート制御を有効にすることはできますが、BGP の場合にのみサポートされます。OSPF および EIGRP で学習されたすべてのルートは、レイヤ 3 Outside 接続が導入されている境界リーフ上のそれぞれのプロトコルで許可されます。これらのプレフィックスは、テナントおよび VRF ごとに、入力境界リーフで MP-BGP に再配布（インポート）されます。

インポート ルート制御

- 入力リーフのルーティング テーブルへのプレフィックスのインポートを制御します。
- デフォルトでは、ディセーブルです。
- BGP でのみサポートされます。
- 外部 BGP ネイバーに関連付けられている入力ルート マップを使用して実装されます。

エクスポート ルート制御

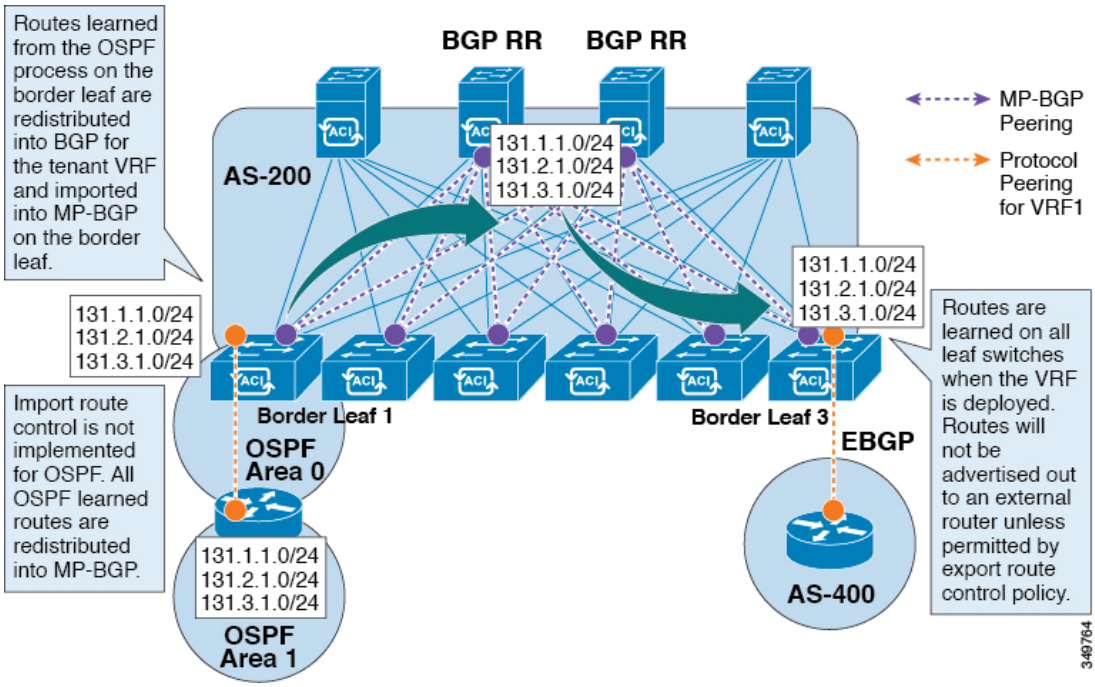
- ACI ファブリックの外部にアドバタイズされる中継プレフィックスのエクスポートを制御します（レイヤ 3 Outside 接続を使用）。
- すべてのレイヤ 3 Outside 接続タイプでサポートされます。
- 常にイネーブルです。
- デフォルト設定ではすべてのプレフィックスが拒否されます。
- 再配布ルート マップ（OSPF および EIGRP）およびネイバー ルート マップ（BGP）を使用して実装されます。
- テナント サブネットまたは元のデフォルト ルートのエクスポートの制御には使用されません。

インポートとエクスポートのルート制御は外部ネットワーク インスタンス プロファイル（l3extInstP）で設定されます。

（注） インポートとエクスポートのルート制御は、中継ルート プレフィックス（外部レイヤ 3 デバイスから学習したルート）およびスタティック ルートのインポートとエクスポートを制御するために使用されます。インポートとエクスポートのルート制御は、テナント サブネット（テナント ブリッジ ドメインに設定されているサブネット）の場合、および発生元がデフォルト ルートである場合は使用されません。

ACI のルート再配布

図 *9* : *ACI* のルート再配布



- 境界リーフの OSPF プロセスで学習されたルートは、テナント VRF 用に BGP に再配布され、それらは境界リーフの MP-BGP にインポートされます。
- インポート ルート制御は OSPF では実装されていません。OSPF で学習されたすべてのルートが MP-BGP に再配布されます。
- ルートは、VRF が導入されている境界リーフで学習されます。ルートは、エクスポート ルート制御で許可されていない限り、外部レイヤ 3 Outside 接続にアドバタイズされません。

レイヤ3Outsideネットワークインスタンスプロファイルで設定されているサブネットで有効な制御

レイヤ 3 Outside ネットワーク インスタンス プロファイルで設定されているサブネットに対して以下の制御を有効にすることができます。

表 *3*：ルート制御オプション

ルート制御設定	使用目的	オプション
エクスポート ルート制御	外部ピアにアドバタイズされるプレフィックスを許可します。IP プレフィックス リストで実装されます。	特定の一致（プレフィックスとプレフィックス長）。
インポート ルート制御	外部 BGP ピアから受信するプレフィックスを許可します。IP プレフィックス リストで実装されます。	特定の一致（プレフィックスとプレフィックス長）。
セキュリティ インポート サブネット	2 つのプレフィックス ベースの EPG 間のパケットを許可します。ACL で実装されます。	ACL のプレフィックスおよびワイルドカードによる一致ルールを使用します。
集約エクスポート	すべてのプレフィックスが外部ピアにアドバタイズされるようにします。0.0.0.0/ le 32 IP プレフィックス リストで実装されます。	0.0.0.0/0 サブネット（すべてのプレフィックス）の場合にのみサポートされます。
集約インポート	外部 BGP ピアから受信するすべてのプレフィックスを許可します。0.0.0.0/0 le 32 IP プレフィックス リストで実装されます。	0.0.0.0/0 サブネット（すべてのプレフィックス）の場合にのみサポートされます。

多くの場合、レイヤ 3 Outside 接続にすべての中継ルートをアドバタイズすることが優先されます。この場合、集約エクスポート オプションがプレフィックス 0.0.0.0/0 で使用されます。これにより、エクスポート ルート マップの match 句として設定された IP プレフィックス リスト エントリ（permit 0.0.0.0/0 le 30）が作成されます。出力を表示するには、**show route-map <outbound route-map>** コマンドと **show ip prefix-list <match-clause>** を使用します。

ファブリック外へのテナント BD サブネットのアドバタイズ

インポートおよびエクスポートのルート制御ポリシーは、中継ルート（他の外部ピアから学習したルート）およびスタティック ルートのみに適用されます。テナント BD サブネット上に設定されているファブリック内部のサブネットは、エクスポートポリシーサブネットを使用して外部にアドバタイズされません。IP プレフィックス リストおよびルート マップを使用すると IP テナントサブネットは許可されますが、これらは別の設定手順を使用して実装されます。テナントサブネットをファブリックの外部にアドバタイズする場合は、次の設定手順を参照してください。

ステップ 1 [subnet properties] ウィンドウで、テナント サブネットのスコープを [Public Subnet] として設定します。

ステップ 2 （任意） [subnet properties] ウィンドウで、[Subnet Control] を [ND RA Prefix] として設定します。

ステップ 3 テナント ブリッジ ドメイン（BD）を外部レイヤ 3 Outside に関連付けます。

ステップ 4 テナント EPG と外部 EPG 間のコントラクト（プロバイダー/コンシューマ）の関連付けを作成します。BD サブネットをスコープ [Public] に設定し、BD をレイヤ 3 Outside に関連付けると、BD サブネット プレフィックスの境界リーフに IP プレフィックスおよびルート マップの連続エントリが作成されます。

テナント EPG からレイヤ 3 Outside へのコントラクト

テナント EPG では、コントラクトのプロバイダーおよびコンシューマをレイヤ 3 Outside 接続に関連付ける必要があります。この関連付けにより、境界リーフにサブネットのルート エントリが作成され（テナント BD がまだリーフに導入されていない場合）、データ プレーンでのトラフィックを許可するためにも使用されます。

状況によっては、コントラクトを設定していなくてもテナント サブネットを外部ピアにアドバタイズできます。テナント サブネットは、次のいずれかの条件に該当すると外部にアドバタイズされます。

- テナント EPG および BD がすでに境界リーフに導入されている。
- テナント EPG および BD に、境界リーフに導入されているテナントおよび EPG とのコントラクトがある。

これら 2 つの条件に該当するとテナント サブネットのルーティング テーブルにエントリが作成され、パブリック スコープとレイヤ 3 Outside の関連付けによりサブネットを外部にアドバタイズできますが、コントラクトがないとデータ プレーン トラフィックは許可されません。

（注） このエントリは、Policy Control Enforcement を enforced に設定してテナント プライベート ネットワーク（コンテキスト）が設定されている場合にのみ有効です。Policy Control Enforcement が unenforced に設定されている場合、テナント プレフィックスはコントラクトなしで境界リーフに存在します。

デフォルト ルートのアドバタイズ

デフォルト ルートのみを必要とするファブリックへの外部接続の場合、OSPF、EIGRP、および BGP のレイヤ 3 Outside 接続をデフォルト ルートの起点とすることがサポートされます。外部ピアからデフォルトルートが受信されると、この文書で説明されている中継エクスポートルート制御に従って、このルートを別のピアに再配布できます。

デフォルト ルートは、デフォルト ルート リーク ポリシーを使用してアドバタイズすることもできます。このポリシーは、デフォルトルートがルーティングテーブル内にあるか、または常にデフォルトルートをアドバタイズすることがサポートされている場合、デフォルトルートのアドバタイズをサポートします。デフォルト ルート リーク ポリシーは、レイヤ 3 Outside 接続で設定されます。

デフォルト ルート リーク ポリシーを作成するときは、以下のガイドラインに従います。

- BGP の場合、[Always] プロパティは適用されません。
- BGP の場合、[Scope] プロパティを選択するときに [Outside] を選択する必要があります。
- OSPF の場合、[Scope] 値 [Context] はタイプ 5 LSA を作成しますが、[Scope] 値 [Outside] はタイプ 7 LSA を作成します。この選択は、そのレイヤ 3 Outside で使用されているエリア タイプによって異なります。したがって、エリア タイプが [regular] である場合はスコープを [Context] に設定し、エリア タイプが [NSSA] である場合はスコープを [Outside] に設定します。

ルート制御プロファイル ポリシー

ACI ファブリックは、ファブリックの内部と外部にアドバタイズされるルート用に、ルート マップの set 句もサポートします。ルート マップの set ルールは、ルート制御プロファイル ポリシーとアクション ルール プロファイルで設定されます。

ACI は以下の set オプションをサポートします。

表 *4* : アクション ルール プロファイルのプロパティ（ルートマップの *set* 句）

プロパティ	OSPF	EIGRP	BGP	注
Set Community			○	標準コミュニティと拡張コミュニティをサポートします。
Route Tag	○	○		BD のサブネットのみでサポートされます。中継プレフィックスには、常にタグ 4294967295 が割り当てられます。
Preference			○	BGP ローカル プリファレンスを設定します。
メトリック	○		○	BGP の MED を設定します。EIGRP のメトリックを変更しますが、EIGRP 複合メトリックは指定できません。
Metric Type	○			OSPF タイプ 1 と OSPF タイプ 2。

ルートプロファイルポリシーは、レイヤ 3 Outside 接続の下に作成されます。ルート制御ポリシーは、以下のオブジェクトで参照できます。

- テナント BD サブネット
- テナント BD
- 外部 EPG
- 外部 EPG のインポート/エクスポート サブネット

以下に、BGP のインポート ルート制御を使用し、2 つの異なるレイヤ 2 Outside から学習した外部ルートのローカル プリファレンスを設定する例を示します。AS300 への外部接続用のレイヤ 3 Outside 接続は、インポート ルート制御を適用して設定されています。アクション ルール プロファ

イルの設定では、[Local Preference] ウィンドウの [Action Rule Profile] でローカル プリファレンスが 200 に設定されています。

レイヤ 3 Outside 接続の外部 EPG は、0.0.0.0/0 インポート集約ポリシーを使用してすべてのルートを許可するように設定されています。これは、インポート ルート制御が適用されていますが、どのプレフィックスもブロックされてはならないためです。ローカル プリファレンスの設定を許可するために、インポート ルート制御が適用されています。また、[Route Control Profile] ウィンドウの [External EPG] で [Action Rule Profile] を参照するルート プロファイルを使用して、別のインポート サブネット 151.0.1.0/24 が追加されています。

MP-BGP テーブルを表示するには、**show ip bgp vrf overlay-1** コマンドを使用します。スパインの MP-BGP テーブルには、プレフィックス 151.0.1.0/24 とローカル プリファレンス 200、および BGP 300 レイヤ 3 Outside 接続の境界リーフの次のホップが表示されます。

default-import と default-export という、2 つの特殊なルート制御プロファイルがあります。名前 default-import および default-export を使用して設定すると、ルート制御プロファイルはインポートとエクスポート両方のレイヤ 3 Outside レベルで自動的に適用されます。default-import および default-export のルート制御プロファイルは、0.0.0.0/0 集約を使用して設定することはできません。

ルート制御プロファイルは、次の順序でファブリック ルートに適用されます。

1. テナント BD サブネット
2. テナント BD
3. レイヤ 3 Outside

ルート制御プロファイルは、次の順序で中継ルートに適用されます。

1. 外部 EPG プレフィックス
2. 外部 EPG
3. レイヤ 3 Outside

セキュリティ インポート ポリシー

本書で説明されているポリシーでは、ACI ファブリックの内外へのルーティング情報の交換、およびルートの制御とタグ付けに使用する方法を取り扱ってきました。ACI ファブリックはホワイトリスト モデルで動作します。この場合のデフォルトの動作では、ポリシーで明示的に許可されない限り、エンドポイント グループ間のすべてのデータ プレーン トラフィックがドロップされます。このホワイトリスト モデルは外部 EPG とテナント EPG に適用されます。

中継トラフィックの場合、テナント トラフィックと比較すると、セキュリティ ポリシーの設定方法と実装方法が少し異なります。

中継セキュリティ ポリシー

- プレフィックス フィルタリングを使用します。
- Ethertype、プロトコル、L4 ポート、および TCP フラグ フィルタはサポートしません。
- セキュリティ インポート サブネット（プレフィックス）と外部 EPG で設定されたコントラクトを使用して実装されます。

テナント EPG セキュリティ ポリシー

- プレフィックス フィルタリングを使用しません。
- Ethertype、プロトコル、L4 ポート、および TCP フラグ フィルタをサポートします。
- テナント EPG←→EPG およびテナント EPG←→外部 EPG でサポートされます。

外部プレフィックスベースのEPG間にコントラクトがなければ、トラフィックはドロップされます。2 つの外部 EPG 間のトラフィックを許可するには、コントラクトとセキュリティ プレフィックスを設定する必要があります。プレフィックス フィルタリングのみがサポートされるため、デフォルト フィルタを使用できます。

外部レイヤ 3 Outside 接続のコントラクト

レイヤ 3 Outside 接続が導入されているすべてのリーフ ノードで、各レイヤ 3 Outside 接続のプレフィックスの結合がプログラムされます。3 つ以上のレイヤ 3 Outside 接続が導入されている場合、キャッチオール ルール 0.0.0.0/0 を使用すると、コントラクトを持たないレイヤ 3 Outside 接続間のトラフィックが許可されます。

プロバイダー/コンシューマのコントラクト関連付けとセキュリティ インポート サブネットの設定は、外部レイヤ 3 Outside 接続のインスタンス プロファイル（instP）で行われます。

セキュリティ インポート サブネットが設定されており、キャッチオール ルール 0.0.0.0/0 がサポートされている場合、セキュリティ インポート サブネットは ACL タイプのルールに従います。セキュリティ インポート サブネットのルール 10.0.0.0/8 は 10.0.0.0～10.255.255.255 の範囲のすべてのアドレスに一致します。ルート制御サブネットで許可されているプレフィックスに対して正確なプレフィックス照合を設定する必要はありません。

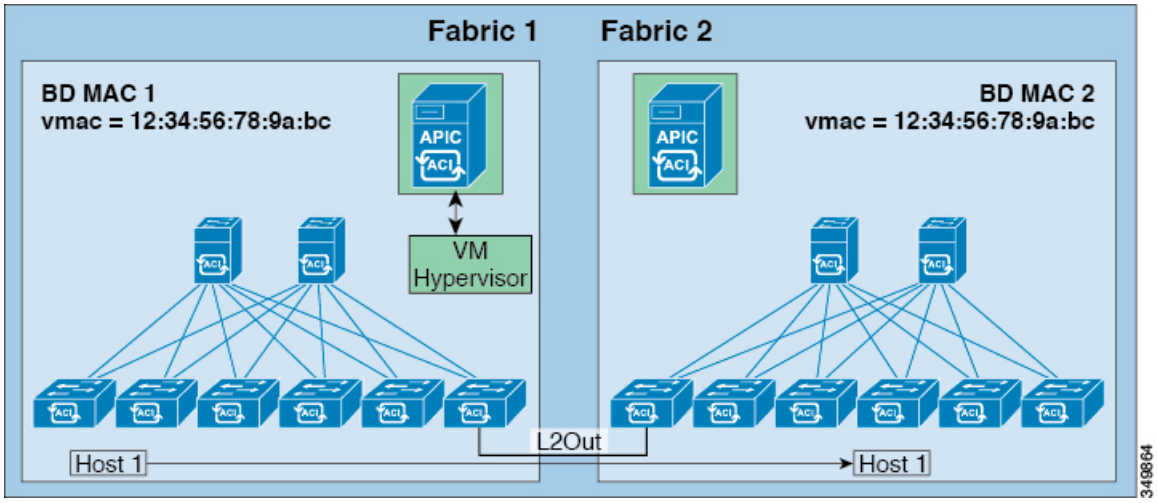
3 つ以上のレイヤ 3 Outside 接続が同じ VRF 内に設定されている場合は、ルールの結合を理由として、セキュリティ インポート サブネットを設定するときに注意する必要があります。

共通パーベイシブ ゲートウェイ

ブリッジ ドメインごとに IPv4 共通ゲートウェイを使用して複数の ACI ファブリックを設定できます。これにより、1 つ以上の仮想マシン（VM）または従来のホストを、ホストがその IP アドレスを保持したままファブリック間で移動できます。ファブリック間の VM ホストの移動は、VM ハイパーバイザによって自動的に行うことができます。ACI ファブリックは、同じ場所に配置することも、複数のサイト間でプロビジョニングすることもできます。ACI ファブリック間のレイ

ヤ 2 接続は、ローカル リンクか、ルーテッド WAN リンクになります。次の図は、基本的な共通パーベイシブ ゲートウェイ トポロジを示しています。

図 *10* : *ACI* 複数ファブリック共通パーベイシブ ゲートウェイ



ブリッジ ドメインごとの共通パーベイシブ ゲートウェイの設定要件は、次のとおりです。

- 各ファブリックのブリッジ ドメイン MAC（*mac*）値は一意である必要があります。

（注） デフォルトのブリッジ ドメイン MAC（*MAC*）アドレス値はすべての ACI ファブリックで同じです。共通パーベイシブ ゲートウェイでは、管理者は、ブリッジ ドメイン MAC（*mac*）値が各 ACI ファブリックで一意になるように設定する必要があります。

- ブリッジ ドメインの仮想 MAC（*vmac*）アドレスとサブネットの仮想 IP アドレスは、ブリッジ ドメインのすべての ACI ファブリックで同じにする必要があります。複数のブリッジ ドメインを、接続されている ACI ファブリック間で通信するように設定できます。仮想 MAC アドレスと仮想 IP アドレスは、ブリッジ ドメイン間で共有できます。

GUI を使用した共通パーベイシブ ゲートウェイの設定

はじめる前に

- テナントおよび VRF が作成されていること。
- ブリッジ ドメインの仮想 MAC アドレスとサブネットの仮想 IP アドレスは、ブリッジ ドメインのすべての ACI ファブリックで同じにする必要があります。複数のブリッジ ドメインを、接続されている ACI ファブリック間で通信するように設定できます。仮想 MAC アドレスと仮想 IP アドレスは、ブリッジ ドメイン間で共有できます。

- ACI ファブリック間で通信するように設定されているブリッジ ドメインは、フラッド モードである必要があります。
- ブリッジ ドメインの 1 つの EPG のみを（BD に複数の EPG がある場合）、2 つ目のファブリックに接続されているポートの境界リーフ上に設定する必要があります。
- 2 つの ACI ファブリック間のパーベイシブ共通ゲートウェイを有効にする相互接続されたレイヤ 2 ネットワークには、ホストを直接接続しないでください。

ステップ 1 メニュー バーで、[TENANTS] をクリックします。

ステップ 2 [Navigation] ペインで、*[Tenant_name]* > [Networking] > [Bridge Domains] の順に展開します。

ステップ 3 [Bridge Domains] を右クリックし、[Create Bridge Domain] をクリックします。

ステップ 4 [Create Bridge Domain] ダイアログボックスで、次の操作を実行し、適切な属性を選択します。

a) [Name] フィールドに、ブリッジ ドメインの名前を入力します。

b) [Subnets] を展開し、[Create Subnets] ダイアログボックスの [Gateway IP] フィールドに IP アドレスを入力します。[Treat as virtual IP address] フィールドで、チェックボックスをオンにします。[Ok] をクリックし、[Finish] をクリックします。

c) もう一度 [Subnets] を展開し、仮想 IP アドレスとして設定されているものと同じサブネットを使用して、[Create Subnets] ダイアログボックスの [Gateway IP] フィールドで物理 IP アドレスを作成します。

（注） 物理 IP アドレスは ACI ファブリック全体で一意である必要があります

ステップ 5 [Work] ペインで作成した物理ドメインをダブルクリックし、次の操作を実行します。

a) [Virtual MAC Address] フィールドをクリックし、[not-applicable] を適切な値に変更します。[Submit] をクリックします。

（注） デフォルト BD の MAC アドレス値はすべての ACI ファブリックで同じです。この設定では、ブリッジ ドメイン MAC 値が各 ACI ファブリックで一意である必要があります。

各ファブリックのブリッジ ドメイン MAC（pmac）値が一意であることを確認してください。

ステップ 6 BD をその他のファブリックに拡張するために、L2out EPG を作成します。これを行うには、[External Bridged Networks] を右クリックして [Create Bridged Outside] ダイアログを開き、次の操作を実行します。

a) [Name] フィールドに、ブリッジされる Outside の名前を入力します。

b) [Bridge Domain] フィールドで、すでに作成されているブリッジ ドメインを選択します。

c) [Encap] フィールドに、その他のファブリック l2out カプセル化に一致する VLAN カプセル化を入力します。

d) [Path Type] フィールドで、[Port]、[PC]、または [VPC] を選択して EPG を導入し、[Next] をクリックします。

e) 外部 EPG ネットワークを作成するには、[Name] フィールドをクリックしてネットワークの名前を入力し（QoS クラスの指定も可能）、[Finish] をクリックして共通パーベイシブ設定を完了します。

REST API を使用した共通パーベイシブ ゲートウェイの設定

はじめる前に

- テナント、VRF、およびブリッジ ドメインが作成されていること。

共通パーベイシブ ゲートウェイを設定します。

例：

```
<!-Things that are bolded only matters-->
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/policymgr/mo/.xml -->
<polUni>
  <fvTenant name="test">
    <fvCtx name="test"/>

    <fvBD name="test" vmac="12:34:56:78:9a:bc">
      <fvRsCtx tnFvCtxName="test"/>
      <!-- Primary address -->
      <fvSubnet ip="192.168.15.254/24" preferred="yes"/>
      <!-- Virtual address -->
      <fvSubnet ip="192.168.15.1/24" virtual="yes"/>
    </fvBD>

    <fvAp name="test">
      <fvAEPg name="web">
        <fvRsBd tnFvBDName="test"/>
        <fvRsPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1/3]" encap="vlan-1002"/>
      </fvAEPg>
    </fvAp>
  </fvTenant>
</polUni>
```

CLI を使用した共通パーベイシブ ゲートウェイの設定

はじめる前に

- テナント、VRF、およびブリッジ ドメインが作成されていること。

ステップ 1 CLI で、ディレクトリを /aci に変更します。

例：

```
admin@apic1:~> cd /aci
```

ステップ 2 共通パーベイシブ ゲートウェイを設定します。

例：

```
apic1#configure
apic1(config)#tenant demo
apic1(config-tenant)#bridge-domain test
apic1(config-tenant-bd)#l2-unknown-unicast flood
apic1(config-tenant-bd)#arp flooding
apic1(config-tenant-bd)#exit

apic1(config-tenant)#interface bridge-domain test
apic1(config-tenant-interface)#multi-site-mac-address 12:34:56:78:9a:bc
apic1(config-tenant-interface)#mac-address 00:CC:CC:CC:C1:01 (Should be unique for each ACI fabric)
apic1(config-tenant-interface)#ip address 192.168.10.1/24 multi-site
apic1(config-tenant-interface)#ip address 192.168.10.254/24 (Should be unique for each ACI fabric)
```