ルート ピアリングの設定

- ルート ピアリングについて （1 ページ）
- Open Shortest Path First ポリシー （2 ページ）
- Border Gateway Protocol ポリシー （6 ページ）
- クラスタ用の L3extOut ポリシーの選択 （9 ページ）
- ルート ピアリングのエンドツーエンド フロー （10 ページ）
- Cisco Application Centric Infrastructure トランジット ルーティング ドメインとして機能するファブリック （12 ページ）
- GUI を使用したルート ピアリングの設定 （13 ページ）
- NX-OS スタイルの CLI を使用したルート ピアリングの設定 （19 ページ）
- ルート ピアリングのトラブルシューティング （21 ページ）

ルート ピアリングについて

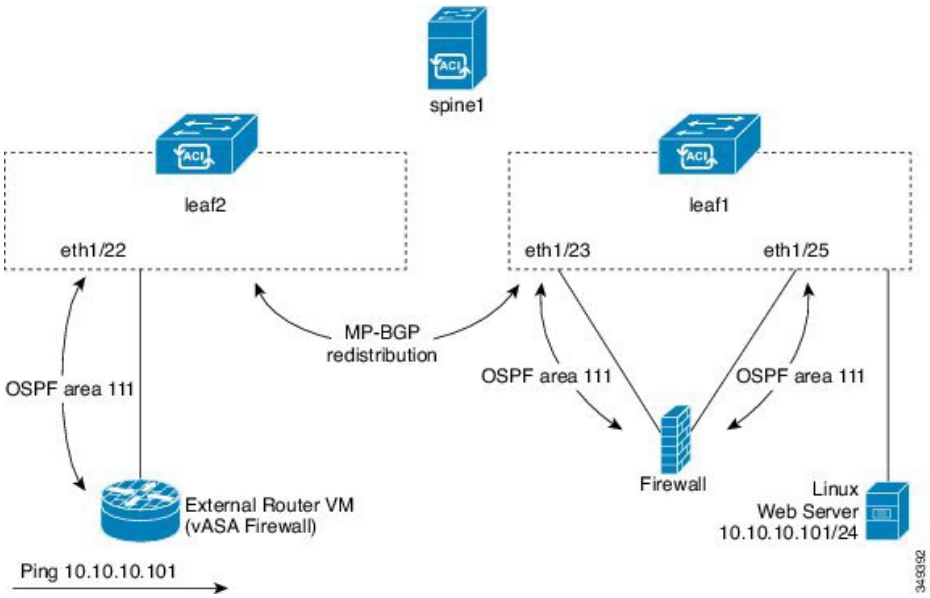
ルート ピアリングは、トランジットの使用例としてより一般的なCisco Application Centric Infrastructure（ACI）ファブリックの特殊ケースで、ルート ピアリングによってACI ファブリックが Open Shortest Path First（OSPF）プロトコルまたは Border Gateway Protocol（BGP）プロトコルのトランジット ドメインとして機能できるようになります。ルート ピアリングの一般的な使用例はルート ヘルス インジェクションであり、サーバのロード バランシング仮想 IP が OSPF または内部 BGP（iBGP）を使用して、ACI ファブリック外にあるクライアントにアドバタイズされます。デバイスが接続されている ACI リーフ スイッチとピアリングしたり、ルートを交換したりできるように、ルート ピアリングを使用して OSPF ピアリングや BGP ピアリングをサーバ デバイス上に設定したりすることができます。

次のプロトコルは、ルート ピアリングをサポートしています。

- OSPF
- OSPFv3
- iBGPv4
- iBGPv6
- スタティック ルート

次の図に、ルート ピアリングの一般的な導入方法を示します。

図 *1*:一般的なルート ピアリング トポロジ



図に示すように、ルート ピアリングを設定してサービス グラフを導入することによって、Web サーバのパブリック IP アドレスがファイアウォールを介して外部ルータにアドバタイズされます。ファイアウォールの各レッグに OSPF ルーティング ポリシーを導入する必要があります。通常、これを行うには、`l3extOut` ポリシーを導入します。これにより、Web サーバの到達可能性情報がファイアウォールを介してボーダー リーフ スイッチと外部ルータに OSPF でアドバタイズされるようになります。

ファブリック内のリーフ スイッチ間のルート配布は Multi-Protocol Border Gateway Protocol（MP-BGP）により内部的に実行されます。

ルート ピアリング トポロジのより詳しい例については、ルート ピアリングのエンドツーエンド フロー （10 ページ） を参照してください。

`l3extOut` ポリシーの設定の詳細については、『*Cisco Application Centric Infrastructure Fundamentals Guide*』を参照してください。

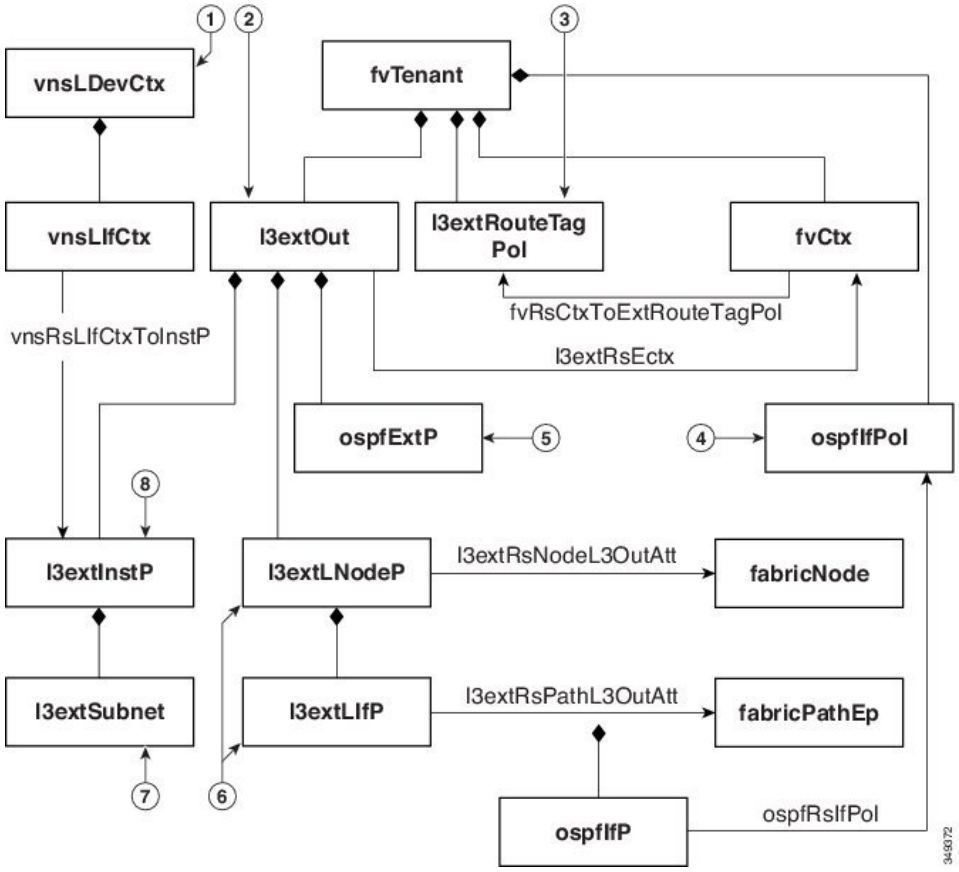
（注） ポイントツーポイントの非ブロードキャスト モードは、Adaptive Security Appliance （ASA）ではサポートされていません。Application Policy Infrastructure Controller（APIC）からポイントツーポイントの非ブロードキャスト モード設定を削除する必要があります（存在する場合）。

Open Shortest Path First ポリシー

ルート ピアリングを設定するには、最初に 1 つ以上の `l3extOut` ポリシーを作成し、サービス デバイスを接続するファブリック リーフ ノードに導入します。これらの `l3extOut` ポリシー

で、ファブリック リーフで有効にする必要がある Open Shortest Path First（OSPF）のパラメータを指定します。これらのポリシーは外部通信に使用される `l3extOut` ポリシーとよく似ています。次の図に、ルート ピアリング オブジェクトの関係を示します。

図 *2 : OSPF* ルート ピアリング オブジェクトの関係



1. `vnsLDevCtx`：デバイス選択ポリシー。
2. `l3extOut`：1 つのエリアのすべての OSPF ポリシーが含まれます。
3. `l3extRouteTagPol`：ルート ピアリングで必要な各コンテキストには OSPF ループを回避するための一意のルート タグが必要です。1 つのレッグから取得される OSPF ルートは、ルート タグが異なっていない限り、他のレッグでは取得されません。
4. `ospfIfPol`：インターフェイスごとの OSPF ポリシー。
5. `ospfExtP`：エリア ポリシーごとの OSPF。
6. `l3extLNodeP/l3extLIfP`：この `l3extOut` を導入するノードまたはポート。
7. `l3extSubnet`：ファブリックに対してエクスポートまたはインポートするサブネット。
8. `l3extInstP`：プレフィックス ベースの EPG。

次に、l3extOut の 2 つの 例（OspfExternal と OspfInternal）を示します。これらのポリシーは、図 1 : 一般的なルート ピアリング トポロジ （2 ページ） のファイアウォール デバイスの外部レッグと内部レッグに導入されます。l3extOut ポリシーは、ファブリック リーフがトラフィックを分類する方法と、サービスデバイスに対してルートをインポートまたはエクスポートする方法も制御する 1 つ以上のプレフィックス ベースの EPG（l3extInstP）を指定します。l3extOut ポリシーには、そのポリシーの下で指定される OSPF のエリアごとのポリシー（ospfExtP）と 1 つ以上の OSPF インターフェイス ポリシー（ospfIfPol）が含まれています。

次に、値「100」で設定される area-Id を持つ OSPF エリアの例を示します。

```
<ospfExtP areaId="100" areaType="regular" areaCtrl="redistribute"/>
```

エリア タイプは「regular」に設定し、エリア制御属性は「redistribute」に設定します。

OSPF インターフェイス ポリシーで、1 つ以上の OSPF インターフェイス タイマーを指定します。

```
<ospfIfPol name="ospfIfPol" ctrl="mtu-ignore" nwT="bcast" xmitDelay="1" helloIntvl="10"
  deadIntvl="40" status="created,modified"/>
```

デフォルト タイマーが正常であれば、このポリシーを指定する必要はありません。このポリシーでは、特定のタイマーをデフォルト値から変更し、次の関係を使用することによって、1 つ以上のインターフェイスに関連付けることができます。

```
<l3extRsPathL3OutAtt tDn="topology/pod-1/paths-101/pathep-[eth1/25]" ifInstT="ext-svi"
  encap="vlan-3844" addr="30.30.30.100/28" mtu="1500"/>
```

l3extRsPathL3OutAtt の関係の属性は次のとおりです。

- ifInstT：論理インターフェイス タイプ。通常は「ext-svi」。
- encap：このインターフェイスを作成するときは VLAN カプセル化を指定する必要があります。カプセル化はサービス デバイスにプッシュされます。
- addr：この l3extOut を導入するファブリック リーフで作成された SVI インターフェイスの IP アドレス。

次のポリシーで、l3extOut ポリシーをどこに導入するかを制御します。

```
<l3extNodeP name="bLeaf-101">
  <l3extRsNodeL30utAtt tDn="topology/pod-1/node-101" rtrId="180.0.0.11"/>
  <l3extLIfP name="portIf">
    <l3extRsPathL30utAtt tDn="topology/pod-1/paths-101/pathep-teth1/251"
      ifInstT="ext-svi" encap="vlan-3844" addr="30.30.30.100/28" mtu="1500"/>
    <ospfIfP authKey="tecom" authType="md5" authKeyId='1'>
      <ospfRslfPol tnOspfIfPolName="ospfIfPol"/>
    </ospflfP>
  </l3extLIfP>
</l3extLNodeP>
```

l3extOut ポリシーは、サービス デバイスが接続されているリーフ ポートと同じものに導入する必要があります。

scope=import-security 属性は次を実行します。

- データ プレーン内のトラフィックのフローを制御する
- このルートをアドバタイズする外部デバイスへのディレクティブとして機能する

（注） ルート ピアリングを正しく動作させるには、l3extRsPathL3OutAtt の関係が、デバイスを表す vnsCDev の下の RsCIfPathAtt の関係と同じファブリックの宛先を指している必要があります。

OspfExternal ポリシー

OspfInternal ポリシー

仮想サービス

```
<polUni>
  <fvTenant name="common">
    <fvCtx name="commonctx">
      <fvRsCtxToExtRouteTagPol tnL3extRouteTagPolName="myTagPol"/>
    </fvCtx>
    <l3extRouteTagPol tag="212" name="myTagPol"/>
    <l3extOut name="OspfExternal" status="created,modified">
      <l3extLNodeP name="bLeaf-101">
        <l3extRsNodeL3OutAtt tDn="topology/pod-1/node-101" rtrId="180.0.0.8/28"/>
        <l3extLIfP name="portIf">
          <l3extRsPathL3OutAtt tDn="topology/pod-1/paths-101/pathep-[eth1/23]"
            ifInstT="ext-svi" encap="vlan-3843" addr="40.40.40.100/28" mtu="1500"/>
          <ospfIfP authKey="tecom" authType="md5" authKeyId='1'>
            <ospfRsIfPol tnOspfIfPolName="ospfIfPol"/>
          </ospfIfP>
        </l3extLIfP>
      </l3extLNodeP>
      <ospfExtP areaId="100" areaType="regular" areaCtrl="redistribute"/>
      <l3extInstP name="ExtInstP">
        <l3extSubnet ip="40.40.40.100/28" scope="import-security"/>
        <l3extSubnet ip="10.10.10.0/24" scope="import-security"/>
      </l3extInstP>
      <l3extRsEctx tnFvCtxName="commonctx"/>
    </l3extOut>
   <ospfIfPol name="ospfIfPol" ctrl="mtu-ignore" nwT="bcast" xmitDelay="1" helloIntvl="10"

      deadIntvl="40" status="created,modified"/>
  </fvTenant>
</polUni>
```

```
<polUni>
  <fvTenant name="tenant1">
    <l3extRouteTagPol tag="213" name="myTagPol"/>
    <fvCtx name="tenant1ctx1">
      <fvRsCtxToExtRouteTagPol tnL3extRouteTagPolName="myTagPol"/>
    </fvCtx>
    <l3extOut name="OspfInternal" status="created,modified">
      <l3extLNodeP name="bLeaf-101">
        <l3extRsNodeL3OutAtt tDn="topology/pod-1/node-101" rtrId="180.0.0.11"/>
        <l3extLIfP name="portIf">
          <l3extRsPathL3OutAtt tDn="topology/pod-1/paths-101/pathep-[eth1/25]"
            ifInstT="ext-svi" encap="vlan-3844" addr="30.30.30.100/28" mtu="1500"/>
          <ospfIfP authKey="tecom" authType="md5" authKeyId='1'>
            <ospfRsIfPol tnOspfIfPolName="ospfIfPol"/>
          </ospfIfP>
        </l3extLIfP>
      </l3extLNodeP>
      <ospfExtP areaId="100" areaType="regular" areaCtrl="redistribute"/>
```

```
      <l3extInstP name="IntInstP">
        <l3extSubnet ip="30.30.30.100/28" scope="import-security"/>
        <l3extSubnet ip="20.20.20.0/24" scope="import-security"/>
      </l3extInstP>
      <l3extRsEctx tnFvCtxName="tenant1ctx1"/>
    </l3extOut>
   <ospfIfPol name="ospfIfPol" ctrl="mtu-ignore" nwT="bcast" xmitDelay="1" helloIntvl="10"

      deadIntvl="40" status="created,modified"/>
  </fvTenant>
</polUni>
```

`OspfExternalInstP` ポリシーは、プレフィクスの 40.40.40.100/28 と 10.10.10.0/24 をプレフィクス ベースのエンドポイントのアソシエーションに使用する必要があることを指定します。また、このポリシーは、プレフィックスの 20.20.20.0/24 をサービス デバイスにエクスポートするようにファブリックに指示します。

```
      <l3extInstP name="OspfExternalInstP">
        <l3extSubnet ip="40.40.40.100/28" scope="import-security"/>
        <l3extSubnet ip="10.10.10.0/24" scope="import-security"/>
        <l3extSubnet ip="20.20.20.0/24" scope="export"/>
      </l3extInstP>
```

`bleaf-101` ポリシーは、この `l3extOut` ポリシーを導入する場所を制御します。

```
      <l3extLNodeP name="bLeaf-101">
        <l3extRsNodeL3OutAtt tDn="topology/pod-1/node-101" rtrId="180.0.0.8/28"/>
        <l3extLIfP name="portIf">
          <l3extRsPathL3OutAtt tDn="topology/pod-1/paths-101/pathep-[eth1/23]"
            ifInstT="ext-svi" encap="vlan-3843" addr="40.40.40.100/28" mtu="1500"/>
          <!-- <ospfIfP authKey="tecom" authType="md5" authKeyId='1'> -->
          <ospfIfP>
            <ospfRsIfPol tnOspfIfPolName="ospfIfPol"/>
          </ospfIfP>
        </l3extLIfP>
      </l3extLNodeP>
```

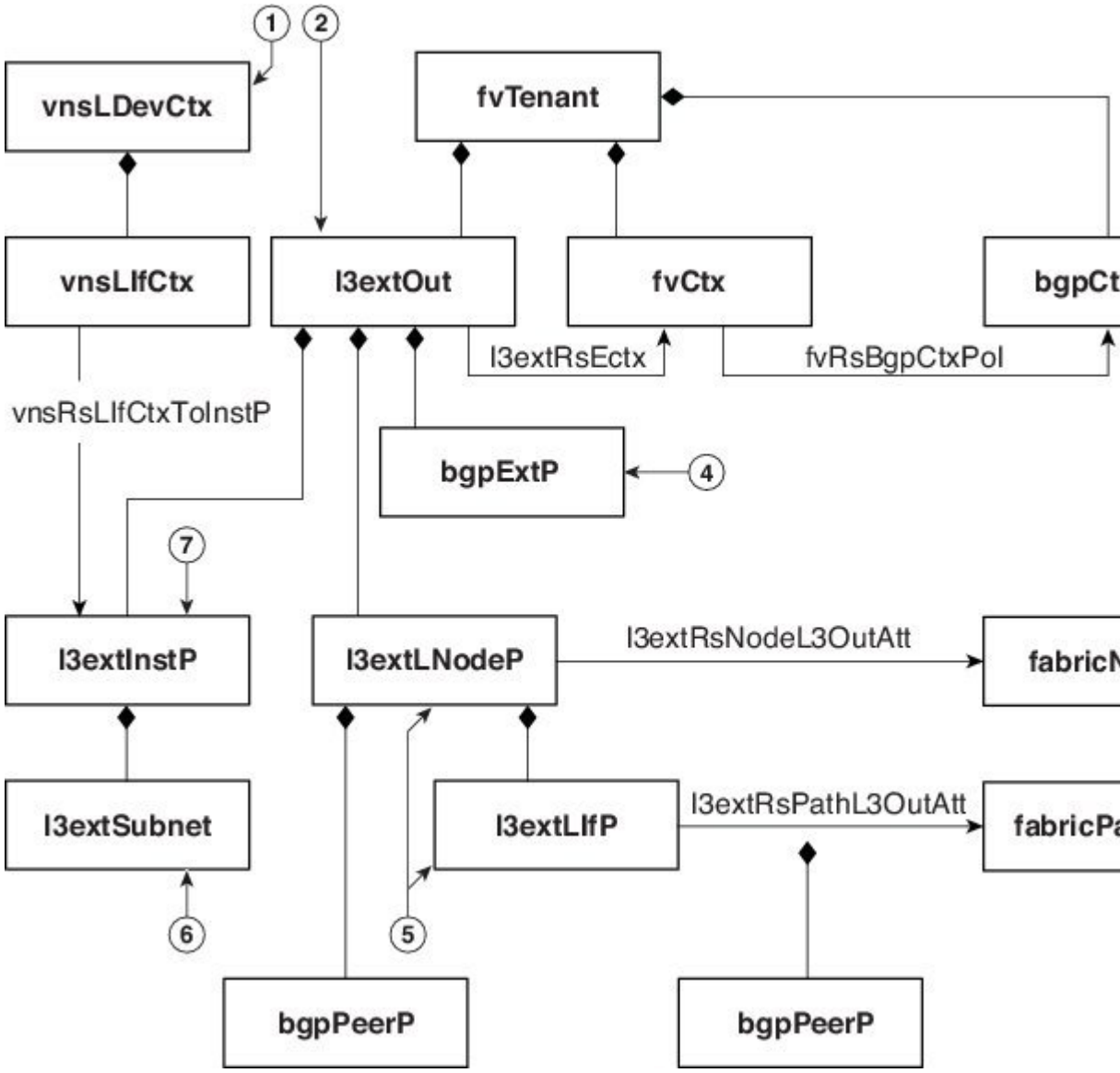
仮想サービスはルート ピアリングとともに導入できますが、`vnsCIf` オブジェクトでの `l3extRsPathL3OutAtt` 検証は実行されません。このデータ パスは、`l3extOut` オブジェクトが仮想サービス データが接続されている正しいリーフに導入されている場合にのみ動作します。

Border Gateway Protocol ポリシー

内部 Border Gateway Protocol（iBGP）を使用してデバイスの外部インターフェイスにルート ピアリングを設定し、内部インターフェイスに静的ルートを設定できます。追加設定なしにデバイスの内部インターフェイスと外部インターフェイスの両方に iBGP を設定することはできません。これは、インターフェイスが異なる自律システムに存在する必要があり、相互自律システム再配布ポリシーをプッシュ ダウンしないためです。

次の図に、ルート ピアリング オブジェクトの関係を示します。

図 *3 : iBGP* ルート ピアリング オブジェクトの関係



1. `vnsLDevCtx`：デバイス選択ポリシー。
2. `l3extOut`：単一の自律システム用のすべての BGP ポリシーが含まれます。
3. `bgpCtxPol`：コンテキスト単位の BGP タイマー。
4. `bgpExtP`：ASN ポリシー単位の BGP。
5. `l3extLIfP/l3extLNodeP`：これらのエンドポイント グループ（EPG）を導入するノードまたはポートを制御します。
6. `l3extSubnet`：ファブリックからのエクスポートするサブネットとファブリックにインポートするサブネット。

7. `l3extInstP`：プレフィックス ベースの EPG。

次のポリシーは、外部インターフェイスに iBGPv4/v6 を設定します。

```
<polUni>
  <fvTenant name="common">
    <fvCtx name="commonctx">
      <fvRsBgpCtxPol tnBgpCtxPolName="timer-3-9"/>
      <fvRsCtxToExtRouteTagPol tnL3extRouteTagPolName="myTagPol"/>
    </fvCtx>
    <l3extRouteTagPol tag="212" name="myTagPol"/>
   <bgpCtxPol grCtrl="helper" holdIntvl="9" kaIntvl="3" name="timer-3-9" staleIntvl="30"/>

    <l3extOut name="BgpExternal" status="created,modified">
      <l3extLNodeP name="bLeaf-101">
        <!-- <bgpPeerP addr="40.40.40.102/32 "ctrl="send-com"/> -->
        <l3extRsNodeL3OutAtt tDn="topology/pod-1/node-101" rtrId="180.0.0.8/28>"
          <l3extLoopBackIfP addr="50.50.50.100/32"/>
        </l3extRsNodeL3OutAtt>
        <l3extLIfP name="portIf">
          <l3extRsPathL3OutAtt tDn="topology/pod-1/paths-101/pathep-[eth1/23]"
            ifInstT="ext-svi" encap="vlan-3843" addr="40.40.40.100/28 "mtu="1500">
            <bgpPeerP addr="40.40.40.102/32 "ctrl="send-com"/>
          </l3extRsPathL3OutAtt>
        </l3extLIfP>
      </l3extLNodeP>
      <bgpExtP/>
      <l3extInstP name="ExtInstP">
        <l3extSubnet ip="40.40.40.100/28 "scope="import-security"/>
        <l3extSubnet ip="10.10.10.0/24 "scope="import-security"/>
        <l3extSubnet ip="20.20.20.0/24 "scope="export-rtctrl"/>
      </l3extInstP>
      <l3extRsEctx tnFvCtxName="commonctx"/>
    </l3extOut>
  </fvTenant>
</polUni>
```

iBGP ピアは、物理インターフェイス レベルまたはループバック レベルで設定できます。次に、物理インターフェイス レベルで設定された iBGP ピアの例を示します。

```
<l3extLIfP name="portIf">
    <l3extRsPathL3OutAtt tDn="topology/pod-1/paths-101/pathep-[eth1/23]"
      ifInstT="ext-svi" encap="vlan-3843" addr="40.40.40.100/28 "mtu="1500">
        <bgpPeerP addr="40.40.40.102/32 "ctrl="send-com"/>
    </l3extRsPathL3OutAtt>
</l3extLIfP>
```

この場合、ファブリック上で実行する iBGP プロセスはスイッチ仮想インターフェイス（SVI）IP アドレス 40.40.40.100/28 を使用して、ネイバーとピアリングします。ネイバーは、IP アドレス 40.40.40.102/32 のサービス デバイスです。

次に、iBGP ピアの定義が論理ノード レベル（`l3extLNodeP` の下）に移動され、ループバック インターフェイスが作成されている例を示します。

```
      <l3extLNodeP name="bLeaf-101">
        <bgpPeerP addr="40.40.40.102/32 "ctrl="send-com"/>
        <l3extRsNodeL3OutAtt tDn="topology/pod-1/node-101" rtrId="180.0.0.8/28>"
          <l3extLoopBackIfP addr="50.50.50.100/32"/>
        </l3extRsNodeL3OutAtt>
        <l3extLIfP name="portIf">
          <l3extRsPathL3OutAtt tDn="topology/pod-1/paths-101/pathep-[eth1/23]"
            ifInstT="ext-svi" encap="vlan-3843" addr="40.40.40.100/28 "mtu="1500">
```

```
          </l3extRsPathL3OutAtt>
        </l3extLIfP>
      </l3extLNodeP>
```

この例では、iBGPプロセスはループバックアドレスを使用してネイバーとピアリングします。ループバックが設定されていない場合は、ファブリックは rtrId で指定された IP アドレスを使用してネイバーとピアリングします。

次に、デバイスの内部インターフェイス用にファブリック上で静的ルートを設定する例を示します。

```
<polUni>
  <fvTenant name="tenant11">
    <l3extOut name="StaticInternal" status="created,modified">
      <l3extLNodeP name="bLeaf-201">
        <l3extRsNodeL3OutAtt tDn="topology/pod-1/node-101" rtrId="180.0.0.11>"
          <ipRouteP ip="20.20.20.0/24>"
            <ipNexthopP nhAddr="30.30.30.102/32"/>
          </ipRouteP>
        </l3extRsNodeL3OutAtt>
        <l3extLIfP name="portIf">
          <l3extRsPathL3OutAtt tDn="topology/pod-1/paths-101/pathep-[eth1/25]"
            ifInstT="ext-svi" encap="vlan-3844" addr="30.30.30.100/28 "mtu="1500"/>
        </l3extLIfP>
      </l3extLNodeP>
      <l3extInstP name="IntInstP">
        <l3extSubnet ip="20.20.20.0/24 "scope="import-security"/>
      </l3extInstP>
      <l3extRsEctx tnFvCtxName="tenant1ctx1"/>
    </l3extOut>
  </fvTenant>
</polUni>
```

クラスタ用の L3extOut ポリシーの選択

特定の l3extOut ポリシーを、選択ポリシー vnsLIfCtx を使用して論理デバイスのインターフェイスに関連付けることができます。次に、これを実現する例を示します。

```
<vnsLDevCtx ctrctNameOrLbl="webCtrct1" graphNameOrLbl="WebGraph" nodeNameOrLbl="FW">
    <vnsRsLDevCtxToLDev tDn="uni/tn-tenant1/lDevVip-Firewall"/>
    <vnsLIfCtx connNameOrLbl="internal">
        <vnsRsLIfCtxToInstP tDn="uni/tn-tenant1/out-OspfInternal/instP-IntInstP"
          status="created,modified"/>
        <vnsRsLIfCtxToLIf tDn="uni/tn-tenant1/lDevVip-Firewall/lIf-internal"/>
    </vnsLIfCtx>
    <vnsLIfCtx connNameOrLbl="external">
        <vnsRsLIfCtxToInstP tDn="uni/tn-common/out-OspfExternal/instP-ExtInstP"
          status="created,modified"/>
        <vnsRsLIfCtxToLIf tDn="uni/tn-tenant1/lDevVip-Firewall/lIf-external"/>
    </vnsLIfCtx>
</vnsLDevCtx>
```

vnsRsLIfCtxToInstP の関係を使用して、サービスデバイスのこのレッグと関連付ける特定のプレフィックスベースの EPG（l3extInstP）を選択します。この関係に、redistribute プロトコル再配布プロパティを指定できます。redistribute プロパティのデフォルト値は「ospf,bgp」です。redistribute をデフォルト値のままにすると、各レッグで設定されているルーティングプロトコルが Application Policy Infrastructure Controller（APIC）によって自動検出され、適切な

再配布設定にプッシュされます。自動設定は、常にInterior Gateway Protocol（OSPF）から外部ゲートウェイ プロトコル（BGP）に再配布します。

静的または接続済みといった特定の再配布設定を使用する場合は、それらの設定をこの関係に追加します。たとえば、`redistribute="ospf,bgp,static"` は、自動検出設定と `redistribute-static` をサービス デバイスにプッシュします。

このプロパティをデフォルト値を含まない特定の値（たとえば、`redistribute="ospf,static,connected"`）に設定すると、それらの設定がそのままサービス デバイスにプッシュされます。これは、APICによって選択されたデフォルト値を上書きする場合に役に立ちます。

（注） この関係は `l3extOut` 自体でなく、EPG（`l3extInstP`）を指します。これは、`l3extOut` ポリシーにはこのようなEPGが複数存在する可能性があり、別のデバイス選択ポリシーがそれらのEPGを指していることがあるためです。これにより、さまざまなサービス グラフによってインポートまたはエクスポートされるプレフィックスを細かく制御できます。

関連付けられた具象デバイスには `vnsRsCIfPathAtt` オブジェクトが必要です。このオブジェクトでは、デバイスを同じファブリック リーフに導入します（下記参照）。

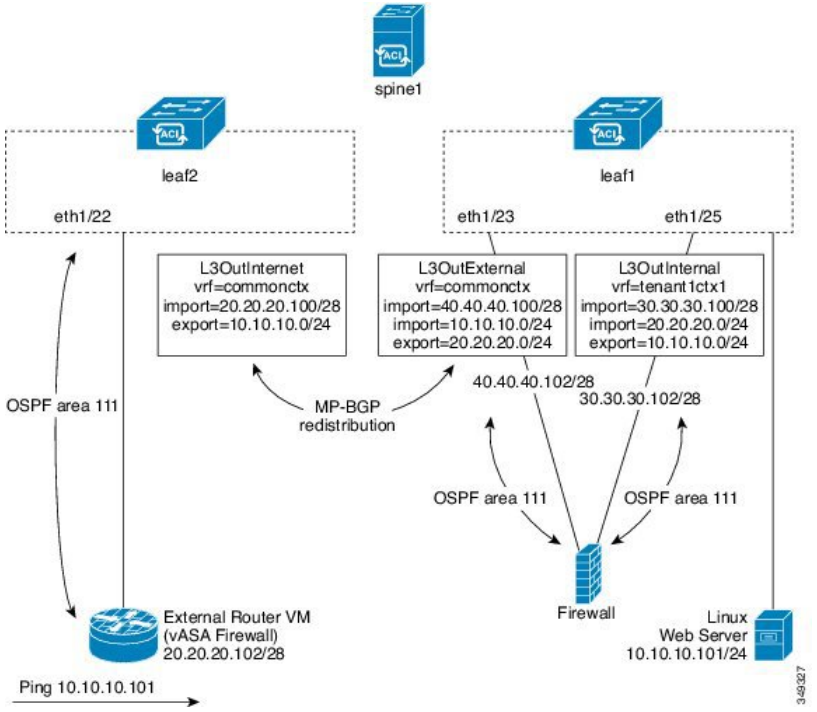
```
<vnsCDev name="ASA">
    <vnsCIf name="Gig0/0">
      <vnsRsCIfPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1/23]"/>
    </vnsCIf>
    <vnsCIf name="Gig0/1">
      <vnsRsCIfPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1/25]"/>
    </vnsCIf>
</vnsCDev>
```

（注） ルート ピアリングを設定した場合は、`vnsLIfCtx` セレクタにブリッジ ドメインを設定する必要がありません。ブリッジ ドメインの関係（`vnsRsLIfCtxToBD`）と `l3extInstP` の関係（`vnsRsLIfCtxToInstP`）の両方を設定しようとすると、エラーになります。

ルート ピアリングのエンドツーエンド フロー

次の図に、ルート ピアリングがエンドツーエンドでどのように動作するかを示します。

図 *4*: ルート ピアリングのエンドツーエンド フロー



この図には、ルート ピアリングを使用して Linux Web サーバの IP アドレスが外部ルータにアドバタイズされる、単一スパイン スイッチ トポロジである 2 台のリーフ スイッチの例が示されています。Linux Web サーバは IP アドレス 10.10.10.101 にあり、`leaf1` に接続する ESX サーバ上でホストされています。通常のブリッジドメインベースのエンドポイント グループ（EPG）が導入されており、Web サーバから発信されるトラフィックを表しています。

2 アームのルーティング可能なファイアウォールから構成され、両方のアームを `leaf1` に接続したサービス グラフを導入します。ファイアウォール デバイスでは、Virtual Routing and Forwarding (VRF) 分割が行われています。つまり、ファイアウォールの各アームが異なる VRF のリーフ（コンテキスト）に接続されています。VRF 分割は、トラフィックがリーフ スイッチによって短絡されるのではなく、サービスデバイスを通じて確実にルーティングされるようにするために必要です。外部トラフィックは `leaf2` に導入されている `l3extOut`（`L3OutInternet`）で表されます。このシナリオでは、`leaf2` をファブリックの境界リーフ スイッチと見なすことができます。`L3OutInternet` と Web サーバ EPG 間にコントラクトを導入できます。このコントラクトは、ファイアウォール デバイスを含むサービス グラフに関連付けられます。

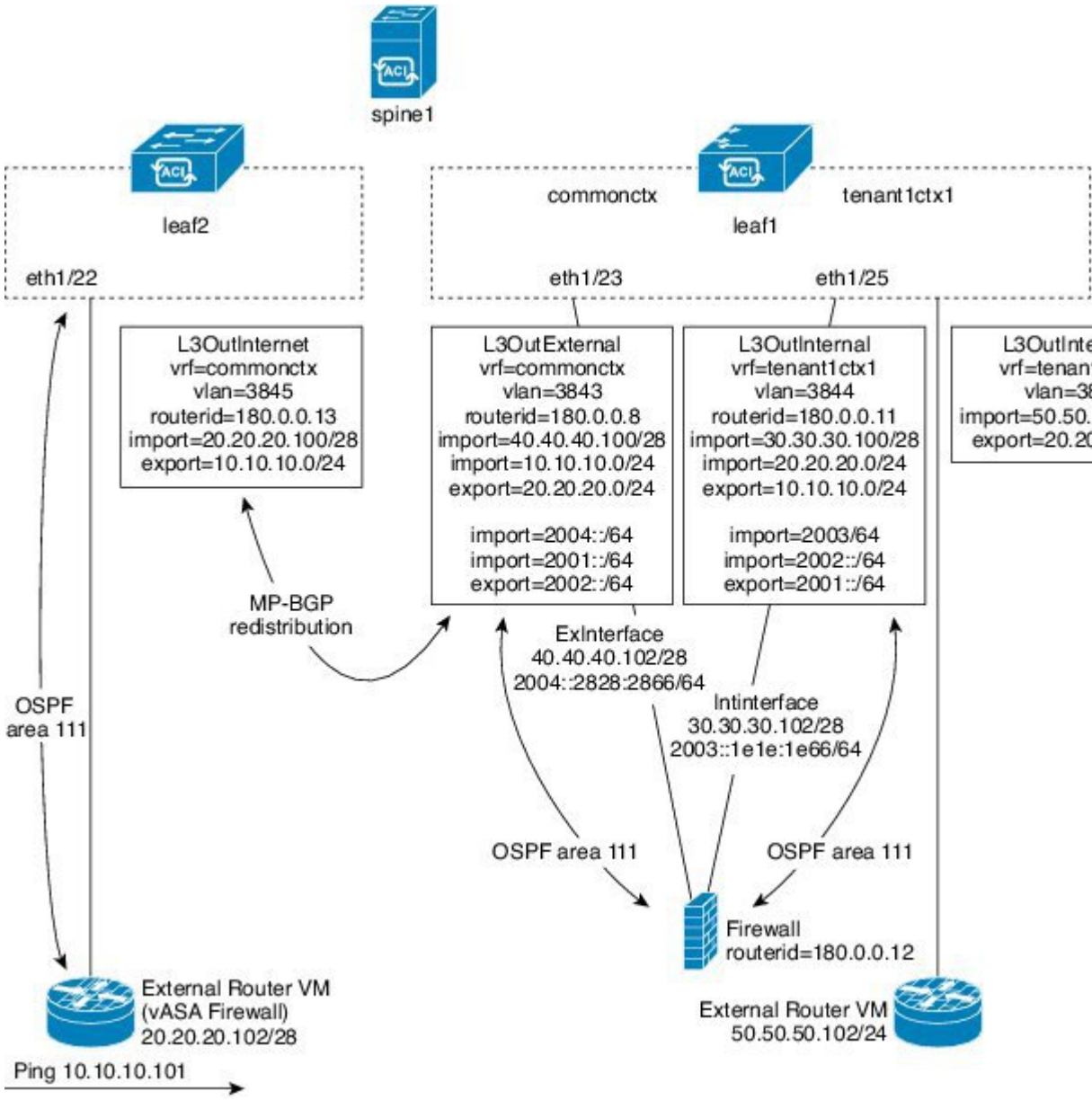
Web サーバ ルートを外部にパブリッシュするには、2 つの `l3extOut`（`L3OutExternal` と `L3OutInternal`）を、サービス デバイスを接続するリーフ スイッチ ポートに展開します。その結果、Open Shortest Path First (OSPF) ピアリング セッションが、両方のコンテキスト（`commonctx` と `tenant1ctx1`）のリーフ スイッチとファイアウォール間で確立されます。これらの `l3extOut` の export 属性が境界リーフ スイッチへのルーティング情報のアドバタイズ方法を制御します。ルートはマルチプロトコル Border Gateway Protocol (MP-BGP) の再配布を使用して、ファブリック リーフ スイッチの間で内部的に交換されます。

最終的に、別の OSPF セッションを使用して Web サーバ ルートが外部ルータ（IP アドレス 20.20.20.102）にアドバタイズされます。これにより、静的ルートを手動で設定することなく、外部ルータから Web サーバを ping できるようになります。

Cisco Application Centric Infrastructure トランジット ルーティング ドメインとして機能するファブリック

Cisco Application Centric Infrastructure（ACI）ファブリックをトランジット ルーティング ドメインとして導入できるので、ACI の受渡しポイント（POD）が他の POD 間のトランジット ルーティング ドメインとして機能している場合に便利です。次の図に、2 つの境界リーフ スイッチへの 2 つの 外部 `l3extOut`（`L3OutInternet` と `L3OutInternet2`）の展開を示します。これらの `3extOut` 間には関連付けられているコントラクトがあり、そのコントラクトはファイアウォール サービス デバイスを含む単一ノードのサービス グラフに適用されています。

図 *5 : ACI* トランジット ルーティング ドメインとして機能するファブリック



2 つの追加 `l3extOut` は、ファイアウォール デバイスの外部レッグと内部レッグに導入され、それらの間に Open Shortest Path First（OSPF）ピアリング セッションを確立します。インポート セキュリティ制御（`import-security` 属性）を適切に設定することで、境界リーフ スイッチへの ACI ファブリックの通過を許可するルートを制御できます。

GUI を使用したルート ピアリングの設定

ルート ピアリングを設定するには、次のタスクを実行する必要があります。

1. デバイスとCisco Application Centric Infrastructure（ACI）ファブリック間のカプセル化VLANに使用するスタティック VLAN プールを作成します。

   GUI を使用したスタティック VLAN プールの作成 （14 ページ）を参照してください。

2. デバイスの場所（リーフ ノード/パス）と VLAN プールを結びつける外部ルーテッド ドメインを作成します。

   GUI を使用した外部ルーテッド ドメインの作成 （14 ページ）を参照してください。

3. ルート ピアリングで ACI ファブリックのルーティング設定を指定するために使用する外部ルーテッド ネットワークを作成します。

   GUI を使用した外部ルーテッド ネットワークの作成 （15 ページ）を参照してください。

4. デバイスで使用するルータ ID を指定する新しいルータ設定を作成します。

   GUI を使用したルータ設定の作成 （18 ページ）を参照してください。

5. サービス グラフのアソシエーションを作成します。これには、外部ルーテッドネットワーク ポリシーおよびルータ設定とデバイス選択ポリシーの関連付けが含まれます。

   「GUI を使用したサービス グラフ アソシエーションの作成 （18 ページ）」を参照してください。

GUI を使用したスタティック VLAN プールの作成

外部ルーテッド ネットワーク設定を作成する前に、デバイスとファブリック間のカプセル化 VLAN に使用するスタティック VLAN プールを作成する必要があります。

ステップ 1 メニュー バーで、**[Fabric]** > **[Access Policies]** の順に選択します。

ステップ 2 [Navigation] ペインで、**[Pools]** > **[VLAN]** の順に選択します。

ステップ 3 [Work] ペインで、**[Actions]** > **[Create VLAN Pool]** の順に選択します。

ステップ 4 **[Create VLAN Pool]** ダイアログボックスで、下記で指定している項目を除き、必要に応じてフィールドに入力します。

a) **[Allocation Mode]** オプション ボタンでは **[Static Allocation]** を選択します。

b) **[Encap Blocks]** セクションでは、**[+]** をクリックします。

ステップ 5 **[Create Ranges]** ダイアログボックスで、一意の VLAN 範囲を入力し、**[OK]** をクリックします。

ステップ 6 **[Create VLAN Pool]** ダイアログボックスで、**[Submit]** をクリックします。

GUI を使用した外部ルーテッド ドメインの作成

デバイスの場所 (リーフ ノード/パス) とルート ピアリング用に作成するスタティック VLAN プールを結びつける外部ルーテッド ドメインを作成する必要があります。

ステップ 1 メニュー バーで、**[ファブリック（FABRIC）]** > **[アクセス ポリシー（Access Policies）]** の順に選択します。

ステップ 2 ナビゲーションウィンドウで、[**スイッチポリシー（Switch Policies**）] を右クリックして、[**インターフェイス、PC、VPC の設定（Configure Interface, PC, and VPC**）]を選択します。

ステップ 3 **[Configure Interface, PC, and VPC]** ダイアログボックスで、Application Policy Infrastructure Controller (APIC) に接続されるスイッチ ポートを設定し、次の操作を実行します。

a) スイッチ図の横にある大きい **[+]** アイコンをクリックし、新しいプロファイルを作成して VLAN を APIC 用に設定します。

b) **[Switches]** フィールドのドロップダウン リストから、APIC を接続するスイッチのチェックボックスをオンにします

c) **[Switch Profile Name]** フィールドに、プロファイルの名前を入力します。

d) **[+]** アイコンをクリックして、ポートを設定します。

e) **[Interface Type]** 領域で、**[Individual]** オプション ボタンが選択されていることを確認します。

f) **[Interfaces]** フィールドで、APIC が接続されるポートを入力します。

g) **[Interface Selector Name]** フィールドに、ポート プロファイルの名前を入力します。

h) **[Interface Policy Group]** フィールドで、**[Create One]** オプション ボタンをクリックします。

i) **[Attached Device Type]** ドロップダウン リストで、**[External Routed Devices]** を選択します。

j) **[Domain]** オプション ボタンでは、**[Create One]** オプション ボタンをクリックします。

k) **[Domain Name]** フィールドに、ドメイン名を入力します

l) VLAN プールを前に作成していた場合は、**[VLAN]** オプション ボタンとして、**[Choose One]** オプション ボタンをクリックします。その他の場合は、**[Create One]** オプション ボタンをクリックします。

既存の VLAN プールを選択する場合は、**[VLAN Pool]** ドロップダウン リストで、VLAN プールを選択します。

VLAN プールを作成する場合は、**[VLAN Range]** フィールドに VLAN 範囲を入力します。

m) **[Save]** をクリックし、**[Save]** をもう一度クリックします。

n) [送信（Submit）] をクリックします。

GUI を使用した外部ルーテッド ネットワークの作成

外部ルーテッド ネットワークは、ルート ピアリングでCisco Application Centric Infrastructure（ACI）ファブリックのルーティング設定を指定します。

ステップ 1 メニュー バーで、**[Tenants]** > **[All Tenants]** の順に選択します。

ステップ 2 [Work] ペインで、テナントの名前をダブルクリックします。

ステップ 3 [Navigation] ペインで、***[tenant_name]*** > **[Networking]** > **[External Routed Networks]** を選択します。

ステップ 4 [Work] ペインで、**[Actions]** > **[Create Routed Outside]** を選択します。

ステップ 5 [Create Routed Outside] ダイアログボックスで、下記で指定している項目を除き、必要に応じてフィールドに入力します。

a) ダイナミック ルーティングの場合は、[BGP] チェックボックスまたは [OSPF] チェックボックスをオンにします。

Open Shortest Path Firs （OSPF ）の場合は、追加の OSPF 固有のフィールドに入力します。

b) [Private Network] ドロップダウン リストで、デバイスがルートを交換するプライベート ネットワークを選択します。

c) [External Routed Domain] ドロップダウン リストで、ルート ピアリング用に作成した外部ルーテッド ドメインを選択します。

d) [Nodes and Interfaces Protocol Profiles] セクションで、[+] をクリックします。

ステップ 6 [Create Node Profile] ダイアログボックスで、下記で指定している項目を除き、必要に応じてフィールドに入力します。

a) [Nodes] セクションで、[+] をクリックします。

ステップ 7 [Select Node] ダイアログボックスで、下記に指定している項目を除き、必要に応じてフィールドに入力します。

a) [Node ID] ドロップダウン リストで、デバイスを接続するノード ID を選択します。

- 物理デバイスの場合は、物理デバイスをファブリックに接続するノードの ID にする必要があります。
- 仮想デバイスの場合は、仮想マシンをホストしているサーバが接続するノードの ID にする必要があります。

b) [Router ID] フィールドに、ACI ファブリックがルーティング プロトコル プロセスで使用するルータ ID を入力します。

c) ACI ファブリックとデバイスの間でスタティック ルーティングを使用する場合は、[Static Routes] セクションで [+] をクリックします。それ以外の場合は、ステップ 10 （16 ページ） に進みます。

ステップ 8 [Create Static Route] ダイアログボックスで、下記で指定している項目を除き、必要に応じてフィールドに入力します。

a) [Prefix] セクションには、静的ルートのプレフィックスを入力します。

b) [Next Hop Addresses] セクションでは、[+] をクリックします。

c) 静的ルートのネクスト ホップ IP アドレスを入力します。

d) [Update] をクリックします。

ステップ 9 **OK** をクリックします。

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

ステップ 11 ダイナミック ルーティング プロトコルとしてデバイスで BGP を使用する場合は、[BGP Peer Connectivity Profiles] セクションで、[+] をクリックします。それ以外の場合は、ステップ 14 （17 ページ） に進みます。

ステップ 12 [Create Peer Connectivity Profile] ダイアログボックスで、下記で指定している項目を除き、必要に応じてフィールドに入力します。

a) [Peer Address] フィールドで、BGP セッションを確立するデバイスの IP アドレスであるピア アドレスを入力します。

ステップ 13 [Create Peer Connectivity Profile] ダイアログボックスで、[OK] をクリックします。

ステップ 14 [Interface Profiles] セクションで、[+] をクリックします。

ステップ 15 [Create Interface Profile] ダイアログボックスで、必要に応じてフィールドに入力します。

a) ダイナミック ルーティング プロトコルとして OSPF を使用する場合は、OSPF プロファイル情報を入力します。

ステップ 16 [Interface] セクションでは、[SVI] タブを選択します。

ステップ 17 [Interface] セクションで、[+] をクリックします。

ステップ 18 [Select SVI Interface] ダイアログボックスで、下記に指定している項目を除き、必要に応じてフィールドに入力します。

a) [Path Type] オプション ボタンでは、デバイスのファブリックへの接続方法と一致するタイプを選択します。

b) [Path] ドロップダウン リストで、デバイスをファブリックに接続するパスを選択します。

- 物理デバイスの場合は、物理デバイスをファブリックに接続するパスです。
- 仮想デバイスの場合は、仮想マシンをホストしているサーバを接続するパスです。

c) [Encap] フィールドで、カプセル化 VLAN を指定します。

d) [IP Address] フィールドで、ファブリック SVI インターフェイスで使用する IP アドレスを指定します。

e) [MTU (bytes)] フィールドで、最大伝送ユニット サイズをバイト単位で指定します。

デフォルト値の「inherit」の場合、ACI ではデフォルト値の「9000」が使用され、リモート デバイスでは通常はデフォルト値の「1500」が使用されます。異なる MTU 値を指定すると、ACI とリモート デバイス間のピアリングで問題が発生する可能性があります。リモート デバイスの MTU 値を「1500」に設定した場合は、リモート デバイスの `L3Out` オブジェクトの MTU 値を「9000」に設定して ACI の MTU 値と一致させます。

ステップ 19 [OK] をクリックします。

ステップ 20 [Create Interface Profile] ダイアログボックスで、[OK] をクリックします。

ステップ 21 [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 22 [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 23 [External EPG Networks] セクションで、[+] をクリックします。

ステップ 24 [Create External Network] ダイアログボックスで、下記で指定している項目を除き、必要に応じてフィールドに入力します。

a) [Subnet] セクションで、[+] をクリックします。

ステップ 25 [Create Subnet] ダイアログボックスで、下記で指定している項目を除き、必要に応じてフィールドに入力します。

a) [IP Address] フィールドに IP アドレスまたはサブネット マスクを入力します。

サブネットマスクは、従来のルーティングプロトコル設定で定義するネットワーク ステートメントと同等です。

ステップ 26 [OK] をクリックします。

ステップ 27 （任意） 必要に応じて、さらにサブネットを作成します。

ステップ 28 **[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 29 **[Create Routed Outside]** ダイアログボックスで、**[Finish]** をクリックします。

GUI を使用したルータ設定の作成

ルーティング プロトコル設定の一部として、デバイスで使用するルータ ID を指定する必要があります。

ステップ 1 メニュー バーで、**[Tenants]** > **[All Tenants]** の順に選択します。

ステップ 2 [Work] ペインで、テナントの名前をダブルクリックします。

ステップ 3 [Navigation] ペインで、**テナント名** > **[Services]** > **[L4-L7]** > **[Router configurations]** を選択します。

ステップ 4 [Work] ペインの [Router Configurations] テーブルで、[+] をクリックします。

ステップ 5 デバイスでルータ ID として使用する IP アドレスを入力します。

ステップ 6 [更新（Update）] をクリックします。

GUI を使用したサービス グラフ アソシエーションの作成

サービス グラフのアソシエーションを作成する必要があります。これには、外部ルーテッド ネットワーク ポリシーおよびルータ設定とデバイス選択ポリシーの関連付けが含まれます。

ステップ 1 メニュー バーで、**[テナント（Tenants）]** > **[すべてのテナント（ALL Tenants）]** の順に選択します。

ステップ 2 [Work] ペインで、テナントの名前をダブルクリックします。

ステップ 3 ナビゲーションウィンドウで、**[テナント（Tenant）]*[テナント名（tenant_name）]*** > **[サービス（Services）]** > **[L4-L7]** > **[デバイス選択ポリシー（Device Selection Policies）]** > ***[デバイス選択ポリシー（device_selection_policy）]*** の順に選択します。

ステップ 4 ナビゲーションウィンドウで、***[テナント名（tenant_name）]*** > **[L4 ～ L7 サービス（L4-L7 Services）]** > **[デバイス選択ポリシー（Device Selection Policies）]** > ***[デバイス選択ポリシー（device_selection_policy）]*** の順に選択します。*[デバイス選択ポリシー（device_selection_policy）]* は、Cisco Application Centric Infrastructure（ACI）ファブリックでルートピアリングを実行する際に使用するデバイス選択ポリシーです。

ステップ 5 [Work] ペインの [properties] セクションにある **[Router Config]** ドロップダウン リストで、ルーティング ピアリング用に作成したルータ設定を選択します。

ステップ 6 [Navigation] ペインで、選択したデバイス選択ポリシーを展開し、ACI ファブリックとピアリングするインターフェイスを選択します。

ステップ 7 [Work] ペインの [properties] セクションにある [Associated Network] オプション ボタンで、[L3 External Network] を選択します。

ステップ 8 **[L3 External Network]** ドロップダウン リストで、ルート ピアリング用に作成した外部ルーテッド ネットワークを選択します。

次のように変更されます。

- 外部ルーテッド ネットワークと関連付けたインターフェイスのカプセル化 VLAN が、外部ルーテッド ネットワーク インターフェイス プロファイルの一部として設定した VLAN と一致するようにプログラミングされる
- 外部ルーテッド ネットワーク インターフェイスとルーティング プロトコル設定がルーフ スイッチにプッシュされる
- ルーティングプロトコル設定がデバイスにプッシュされます

NX-OS スタイルの CLI を使用したルート ピアリングの設定

ここでは、ルート ピアリングを設定する NX OS スタイルの CLI のコマンドの例を示します。

ステップ 1 コンフィギュレーション モードを開始します。

例：

```
apic1# configure
```

ステップ 2 テナントのコンフィギュレーション モードを開始します。

例：

```
apic1(config)# tenant 101
```

ステップ 3 サービス グラフを追加し、それをコントラクトと関連付けます。

例：

```
apic1(config-tenant)# l4l7 graph g1 contract c1
```

ステップ 4 デバイス クラスタに関連付けるノード（サービス）を追加します。

例：

```
apic1(config-graph)# service ASA_FW device-cluster-tenant 101 device-cluster ASA_FW1
```

ステップ 5 サービス機能で、コンシューマ コネクタとプロバイダー クラスタ インターフェイスを設定します。

例：

```
apic1(config-service)# connector consumer cluster-interface provider
```

ステップ 6 クラスタ インターフェイスで、サービス デバイスでのルート ピアリングで使用するレイヤ 3 Outside（l3extOut）とエンドポイント グループ（l3extInstP）を指定し、コネクタのコンフィギュレーション モードを終了します。

例：

```
apic1(config-connector)# l4l7-peer tenant 101 out l101 epg e101 redistribute bgp
apic1(config-connector)# exit
```

ステップ 7 プロバイダー コネクタとコンシューマのクラスタ インターフェイスにステップ 5 とステップ 6 を繰り返します。

例：

```
apic1(config-service)# connector provider cluster-interface consumer
apic1(config-connector)# l4l7-peer tenant 101 out l101 epg e101 redistribute bgp
apic1(config-connector)# exit
```

ステップ 8 （任意） コネクタからエンドポイント グループの関連付けを解除する場合は、**no l4l7-peer** コマンドを使用します。

例：

```
apic1(config-connector)# no l4l7-peer tenant 101 out l101 epg e101 redistribute bgp
```

ステップ 9 ルータ設定ポリシーをテナントに作成し、ピア レイヤ 4 ～ レイヤ 7 デバイスにルータ ID を指定し、コンフィギュレーション モードに戻ります。

例：

```
apic1(config)# tenant 102
apic1(config-tenant)# rtr-cfg bgp1
apic1(config-router)# router-id 1.2.3.5
apic1(config-router)# exit
```

ステップ 10 ルータ設定ポリシーを特定のサービス デバイスに関連付け、テナント コンフィギュレーション モードに戻ります。

例：

```
apic1(config-tenant)# l4l7 graph g2 contract c2 subject http
apic1(config-graph)# service ASA_FW device-cluster-tenant 102 device-cluster ASA_FW2
apic1(config-service)# rtr-cfg bgp1
apic1(config-service)# exit
apic1(config-graph)# exit
```

ステップ 11 レイヤ 3 Outside をリーフ インターフェイスおよび VRF に関連付けます。

例：

```
apic1(config-tenant)# external-l3 epg e101 l3out l101
apic1(config-tenant-l3ext-epg)# vrf member v101
apic1(config-tenant-l3ext-epg)# match ip 101.101.1.0/24
apic1(config-tenant-l3ext-epg)# exit
apic1(config-tenant)# exit
apic1(config)# leaf 101
apic1(config-leaf)# vrf context tenant 101 vrf v101 l3out l101
apic1(config-leaf-vrf)# ip route 101.101.1.0/24 99.1.1.2
apic1(config-leaf-vrf)# exit
apic1(config-leaf)# interface ethernet 1/10
apic1(config-leaf-if)# vrf member tenant 101 vrf v101 l3out l101
apic1(config-leaf-if)# vlan-domain member dom101
```

```
apic1(config-leaf-if)# no switchport
apic1(config-leaf-if)# ip address 99.1.1.1/24
apic1(config-leaf-if)# exit
apic1(config-leaf)# exit
```

ルーティング プロトコル（BGP、OSPF）やルート マップなど、名前付きモードを使用したレイヤ 3 外部接続（レイヤ 3 Outside）の詳細な設定については、『*Cisco APIC NX-OS Style CLI Command Reference*』ドキュメントを参照してください。

（注） CLI での外部レイヤ3設定は、2つのモード（基本モードと名前付きモード）で使用できます。特定のテナントまたは VRF では、すべての外部レイヤ 3 設定にこれらのモードの 1 つのみを使用します。ルート ピアリングは名前付きモードでのみサポートされています。

ルート ピアリングのトラブルシューティング

Cisco Application Centric Infrastructure（ACI）ファブリックにルート ピアリングまたはデータ トラフィックの問題がある場合に、その問題をトラブルシーティングするために ACI ファブリック リーフ スイッチ上で実行できるコマンドがいくつかあります。

次の表に、ファブリック リーフ スイッチのスイッチ シェルで実行できるトラブルシューティング コマンドを示しますスイッチ。

コマンド	説明
show ip route vrf all	動的に取得したルートを含む特定のコンテキストのすべてのルートを表示します。
show ip ospf neighbor vrf all	隣接デバイスとの Open Shortest Path First（OSPF）ピアリング セッションを表示します。
show ip ospf vrf all	各コンテキスト内のランタイム OSPF 設定を表示します。
show ip ospf traffic vrf all	Virtual Routing and Forwarding（VRF）の各コンテキストの OSPF トラフィックを確認します。
show system internal policymgr stats	特定のリーフ スイッチのコントラクト フィルタ ルールを表示し、ルールのパケット ヒット カウントを確認します。

次の表に、**vsh_lc** シェルで実行できるトラブルシューティング コマンドを示します。

コマンド	説明
show system internal aclqos prefix	特定のリーフ スイッチの IPv4 プレフィックス アソシエーション ルールとルールのトラフィック ヒット カウントを確認します。

シェル コマンドに加えて、トラブルシューティングに役立つ次の点を確認できます。

- デバイスの健全性カウント
- 特定のテナントの下のすべてのエラーと `NwIssues`

CLI を使用したリーフ スイッチのルート ピアリング機能の確認

ファブリック リーフ上でスイッチ シェル コマンドを使用して、リーフ スイッチ設定とルート ピアリング機能を確認することができます。

ステップ 1 デバイスが接続されているファブリック リーフ スイッチで、SVI インターフェイスが設定されていることを確認します。

```
fab2-leaf3# show ip interface vrf user1:global
IP Interface Status for VRF "user1:global"
vlan30, Interface status: protocol-up/link-up/admin-up, iod: 134,
  IP address: 1.1.1.1, IP subnet: 1.1.1.0/30
  IP broadcast address: 255.255.255.255
  IP primary address route-preference: 1, tag: 0
lo3, Interface status: protocol-up/link-up/admin-up, iod: 133,
  IP address: 10.10.10.1, IP subnet: 10.10.10.1/32
  IP broadcast address: 255.255.255.255
  IP primary address route-preference: 1, tag: 0

fab2-leaf3#
```

インターフェイス vlan30 には SVI インターフェイス設定が含まれており、インターフェイス lo3 には外部ルーテッド ネットワーク設定に指定されているルータ ID が含まれています。

ステップ 2 ファブリック リーフ スイッチの Open Shortest Path First（OSPF）の設定を確認します。

```
fab2-leaf3# show ip ospf vrf user1:global

 Routing Process default with ID 10.10.10.1 VRF user1:global
 Stateful High Availability enabled
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Table-map using route-map exp-ctx-2949120-deny-external-tag
 Redistributing External Routes from
   static route-map exp-ctx-st-2949120
   bgp route-map exp-ctx-proto-2949120
   eigrp route-map exp-ctx-proto-2949120
 Maximum number of non self-generated LSA allowed 100000
    (feature configured but inactive)
    Current number of non self-generated LSA 1
    Threshold for warning message 75%
    Ignore-time 5 minutes, reset-time 10 minutes
    Ignore-count allowed 5, current ignore-count 0
 Administrative distance 110
```

```
 Reference Bandwidth is 40000 Mbps
 SPF throttling delay time of 200.000 msecs,
   SPF throttling hold time of 1000.000 msecs,
   SPF throttling maximum wait time of 5000.000 msecs
 LSA throttling start time of 0.000 msecs,
   LSA throttling hold interval of 5000.000 msecs,
   LSA throttling maximum wait time of 5000.000 msecs
 Minimum LSA arrival 1000.000 msec
 LSA group pacing timer 10 secs
 Maximum paths to destination 8
 Number of external LSAs 0, checksum sum 0x0
 Number of opaque AS LSAs 0, checksum sum 0x0
 Number of areas is 1, 1 normal, 0 stub, 0 nssa
 Number of active areas is 1, 1 normal, 0 stub, 0 nssa
   Area (0.0.0.200)
        Area has existed for 00:17:55
        Interfaces in this area: 1 Active interfaces: 1
        Passive interfaces: 0  Loopback interfaces: 0
        SPF calculation has run 4 times
         Last SPF ran for 0.000273s
        Area ranges are
        Area-filter in 'exp-ctx-proto-2949120'
        Number of LSAs: 3, checksum sum 0x0
fab2-leaf3#
```

ステップ 3 ファブリック リーフ スイッチの OSPF ネイバーの関係を確認します。

```
fab2-leaf3# show ip ospf neighbors vrf user1:global
 OSPF Process ID default VRF user1:global
 Total number of neighbors: 1
 Neighbor ID     Pri State            Up Time  Address         Interface
 10.10.10.2        1 FULL/BDR         00:03:02 1.1.1.2         Vlan30
fab2-leaf3#
```

ステップ 4 ルートがファブリック リーフ スイッチによって取得されることを確認します。

```
fab2-leaf3# show ip route vrf user1:global
IP Route Table for VRF "user1:global"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

1.1.1.0/30, ubest/mbest: 1/0, attached, direct
    *via 1.1.1.1, vlan30, [1/0], 00:26:50, direct
1.1.1.1/32, ubest/mbest: 1/0, attached
    *via 1.1.1.1, vlan30, [1/0], 00:26:50, local, local
2.2.2.0/24, ubest/mbest: 1/0
    *via 1.1.1.2, vlan30, [110/20], 00:06:19, ospf-default, type-2
10.10.10.1/32, ubest/mbest: 2/0, attached, direct
    *via 10.10.10.1, lo3, [1/0], 00:26:50, local, local
    *via 10.10.10.1, lo3, [1/0], 00:26:50, direct
10.122.254.0/24, ubest/mbest: 1/0
    *via 1.1.1.2, vlan30, [110/20], 00:06:19, ospf-default, type-2
fab2-leaf3#
```

ステップ 5 OSPF がデバイス（この例では Cisco ASAv）に設定されていることを確認します。

```
ciscoasa# show running-config
: Saved
:
: Serial Number: 9AGRM5NBEXG
: Hardware:   ASAv, 2048 MB RAM, CPU Xeon 5500 series 2133 MHz
:
```

```
ASA Version 9.3(1)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface GigabitEthernet0/0
 nameif internalIf
 security-level 100
 ip address 2.2.2.1 255.255.255.0
!
interface GigabitEthernet0/1
 nameif externalIf
 security-level 50
 ip address 1.1.1.2 255.255.255.252
!
<<..>>
router ospf 1
 router-id 10.10.10.2
 network 1.1.1.0 255.255.255.252 area 200
 area 200
 log-adj-changes
 redistribute connected
 redistribute static
!
```