Cisco Application Centric Infrastructure Border Gateway Protocol Configuration Guide for External Network Reachability
Contents

1. Introduction ........................................................................................................................................ 3
2. BGP Network Topology .................................................................................................................. 4
3. Fabric Setup for External Network Peering .................................................................................... 5
   3.1 Fabric BGP ASN and Route Reflector Configuration ................................................................. 6
   3.1.1 XML Output for Fabric Setup for BGP Peering .................................................................... 8
4. iBGP Peering Options with an External Network ............................................................................ 8
5. WAN Router Sample Configuration ................................................................................................. 10
6. ACI BGP Sample Configuration for ISP1 ....................................................................................... 10
   6.1 Private Network .......................................................................................................................... 10
      6.1.1 XML Output for Private Network (CTX1) ........................................................................... 11
   6.2 Bridge Domain ............................................................................................................................ 11
      6.2.1 XML Output for Bridge Domain (BD1) .............................................................................. 13
   6.3 External Routed Network .......................................................................................................... 13
      6.3.1 Create Layer 3 outside Network Profiles .......................................................................... 14
      6.3.2 Create Node Profiles .......................................................................................................... 16
      6.3.3 Configure a BGP Peer Connectivity Profile for ISP1 ......................................................... 18
      6.3.4 Create an Interface Profile for ISP1 .................................................................................... 18
      6.3.5 Completed Node Profile Output ......................................................................................... 20
      6.3.6 Create an External Endpoint Group ................................................................................... 21
      6.3.7 Configure a Contract for the External Network ................................................................. 23
      6.3.8 Associate the Layer 3 outside Network with a Bridge Domain .......................................... 24
      6.3.9 XML Output for BGP Setup with ISP1 .............................................................................. 28
   6.4 Route Profile ............................................................................................................................... 28
      6.4.1 Create a Route Profile ......................................................................................................... 29
      6.4.2 Associate the Route Profile ................................................................................................ 30
      6.4.3 The default-export Route Profile ....................................................................................... 30
7. ACI BGP Sample Configuration for ISP2 ....................................................................................... 31
8. BGP Configuration and Statistic Validation ................................................................................... 33
1. Introduction

The Border Gateway Protocol (BGP) is an inter-autonomous system routing protocol. An autonomous system is a network or group of networks under a common administration and with common routing policies. BGP is used to exchange routing information for the Internet and is the protocol used between ISPs. Customer networks, such as universities and corporations, usually employ an Interior Gateway Protocol (IGP) such as Routing Information Protocol (RIP) or Open Shortest Path First (OSPF) for the exchange of routing information within their networks. Customers connect to ISPs, and ISPs use BGP to exchange customer and ISP routes. When BGP is used between autonomous systems, the protocol is referred to as External BGP (eBGP). If a service provider is using BGP to exchange routes within an autonomous system, the protocol is referred to as Interior BGP (iBGP).

Cisco® Application Centric Infrastructure (ACI) fabric uses routed links to communicate with external networks. The fabric leaf switches are able to peer with external networks and redistribute the routing information throughout the fabric. The routing protocols supported initially are OSPF, iBGP, and static routing.

This document focuses on how the Cisco ACI fabric can establish iBGP peering with external entities outside of the ACI fabric (part of the same autonomous system) in the network.

For this document, the term “external network” is used to refer to external entities. The leaf switches that connect the devices over the WAN link are commonly referred to as border leaf switches or simply leaf switches. The border leaf switch physically connects with the external network over a dedicated link and runs iBGP to learn information about the external network. The border leaves are ACI leaves that provide Layer 3 connections to outside networks. Any ACI leaf can be a border leaf.

This document describes how to establish two BGP sessions, advertise public networks, access an external network via BGP peering, and provide the following functionalities:

- Fabric setup for autonomous system number (ASN) and route reflectors
- Options for BGP peering with external routers
- MD5 authentication
- Advertising prefixes from fabric to external routers
- Advertising routes to multiple Layer 3 outside networks
- Configuring a route profile to send standard and extended BGP communities

The external network routing within the fabric involves two major steps:

- Setting up the fabric for propagation of external routing
- Configuring a border leaf for external network peering
2. BGP Network Topology

Besides static routes and OSPF, customers have the choice of running iBGP between the Cisco ACI border leaf switches and external routers. As of this writing, the ACI border leaf switches support iBGP only, with eBGP support planned for a future software release.

This document explains how to use iBGP to create a Layer 3 outside connection with two ISPs. Figure 1 shows the topology used in this document.

Figure 1. BGP Topology for Layer 3 Outside Connectivity

- As mentioned earlier, the ACI border leaf switches support only iBGP at this point.
- ISP1 and ISP2 can be considered customer premises equipment (CPE) routers.
- Loopback and interface IPs, on both sides, are used for iBGP peering.
- BGP ASN 666 is used as an example.
- Prefixes 192.168.1.0/24 and 192.168.2.0/24 are advertised to ISP1.
- Prefix 192.168.2.0/24 is advertised to ISP2.
- ISP1 advertises external network prefixes to Leaf1 (10.10.10.0/24, 10.10.20.0/24, 0.0.0.0/0).
- ISP2 advertises external network prefixes to Leaf2 (172.16.10.0/24, 172.16.20.0/24, 0.0.0.0/0).
Figure 2 provides a conceptual view of the BGP setup in ACI.

**Figure 2.** BGP Topology from the Cisco ACI Perspective

As shown in Figure 2, tenant “Acme” is configured with one private network (CTX1) and two bridge domains (BD1 and BD2). Two Layer 3 outside networks are created to control the route advertisement to selected ISPs. If we create one bridge domain with a single Layer 3 outside network, all the public subnets within the bridge domain will get advertised to all ISPs. At this point there is no control mechanism available for outbound advertisement from fabric to outside network.

Note that:

- If the network type is defined as *shared* or *private*, those prefixes will not be advertised to the external network.
- Border leaves don’t have iBGP sessions among themselves. This is not required because border leaf switches can learn routes from each other through Multiprotocol BGP (MP-BGP) through the spine.

3. Fabric Setup for External Network Peering

The fabric internally uses MP-BGP to distribute external routing information through the domain to each of the leaf switches that require the information. MP-BGP is not enabled by default in the fabric; it must be turned on explicitly by assigning a BGP autonomous system number (ASN) and configuring spine nodes as BGP route reflectors. The Cisco Application Policy Infrastructure Controller (APIC) then configures all leaf switches as route-reflector clients. Spine nodes as route reflectors eliminate the need for full-mesh BGP connectivity inside the fabric. MP-BGP runs in overlay (infra) Virtual Route Forwarding (VRF), with sessions established among route-reflector spine and client leaves using reachability information learned via the Intermediate System-to-Intermediate System (IS-IS) Protocol.
Redistribution of the external routes into the fabric BGP occurs at the border leaf switches (that is, at the point of connection to the external device). In summary, before external routing redistribution occurs across leaves, the fabric needs to be ready with following critical steps:

- **Configure the fabric BGP ASN:** This is done once in ACI at the fabric level.
- **Configure spine nodes as route reflectors:** To enable route reflectors in the ACI fabric, the fabric administrator must select the spine switches that will be the route reflectors and provide the ASN.

Once the fabric administrator has completed these two steps, other users/tenants can configure connectivity to external networks. The following section shows how to set up fabric for BGP ASN and route reflector configuration.

### 3.1 Fabric BGP ASN and Route Reflector Configuration

MP-BGP is not enabled in ACI fabric by default. To turn on MP-BGP, you need to assign an ASN explicitly and configure spine nodes as BGP route reflectors. For redundancy purposes, a maximum of two spines can be configured as router reflector nodes. In this topology we are using:

- 666 as the internal ASN
- Spines (node IDs 201 and 202) as route reflectors

Following are the configuration steps to configure the ASN and define route reflector nodes.

1. On the menu bar, choose Fabric and click Fabric Policies.
2. In the Navigation pane, expand Pod Policies and then expand Policies under it. Click BGP Route Reflector default.
3. In the Properties window, click the + sign next to Route Reflector Nodes.
4. Specify the ASN in the Autonomous System Number field.
Figure 4 shows the configuration screen.

**Figure 4.** Setting up the Fabric for ASN and Route Reflectors

Once the ASN and route reflectors are configured, the APIC will push the configuration to all switch nodes to set up iBGP peering between the leaf and spine. All leaves will be configured as route reflector clients. It also automatically generates the required configuration for route redistribution on the border leaf.

The following are key points to note for the MP-BGP session between the leaf and spines:

- MP-BGP is run in overlay (infra) VRF, and sessions are established between the TEP (Tunnel End Point) IP addresses of leaves and route reflector spines.
- APIC automatically assigns the TEP IP addresses during the fabric setup from the internal pool of infra IP addresses.
- The fabric relies on IS-IS for reachability of the TEP IP addresses of nodes.

This can be checked on the APIC by using the `acidiag fnvread` command (Figure 5).

**Figure 5.** Node Switch Details

Figure 5 shows the details of the node switches discovered on the APIC along with the TEP IP addresses. Note that the IP address of spine1 is 10.0.224.94, and the address of spine2 is 10.0.24.95. All leaf switches will be peering with both spines by using the default value VRF `overlay-1`. 
The MP-BGP session can be validated on any leaf or spine switch by using the `show bgp sessions vrf overlay-1` command (Figure 6).

**Figure 6.** Validating the Route Reflector Client Setup on the Leaf Switch

As shown in Figure 6, leaf2 has MP-BGP sessions with spine1 and spine2 in the VRF overlay-1.

### 3.1.1 XML Output for Fabric Setup for BGP Peering

Figure 7 shows XML equivalent code for the configuration screen shown in Figure 7.

**Figure 7.** XML Output for ASN and Route Reflector Configuration

### 4. iBGP Peering Options with an External Network

Cisco ACI fabric uses its loopback address as a source interface for peering with external devices. There are two ways fabric can establish iBGP peering with an external router:

1. BGP peering using a loopback interface on the fabric and WAN router. A loopback interface needs to be configured on both sides, as well as a static/OSPF route for the loopback interface IP address, for reachability of the loopback address (Figure 8).
Figure 8. iBGP Peering Using Loopback IP on Both Sides

2. BGP peering with a loopback IP on the fabric and an interface IP on the WAN routers. This approach doesn’t require configuring additional loopback interfaces on remote routers for BGP peering (Figure 9).

Figure 9. iBGP Peering Using Loopback IP on the Leaf Switch and Interface IP on the ISP Device
5. WAN Router Sample Configuration

Figure 10 shows the sample configuration of WAN ISP1 and ISP2 routers as described in Section 2, BGP Network Topology. Cisco Nexus® 3000 Series Switches are used to simulate external WAN routers that connect the ACI fabric.

Figure 10. Sample BGP Configurations of ISP1 and ISP2

<table>
<thead>
<tr>
<th>ISP1</th>
<th>ISP2</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf context ISP1</td>
<td>vrf context ISP2</td>
</tr>
<tr>
<td></td>
<td>vrf route 10.100.100.1/32 10.2.1.1</td>
</tr>
<tr>
<td>!</td>
<td>!</td>
</tr>
<tr>
<td>interface loopback581</td>
<td>interface loopback582</td>
</tr>
<tr>
<td></td>
<td>vrf member ISP1</td>
</tr>
<tr>
<td></td>
<td>ip address 10.100.100.2/32</td>
</tr>
<tr>
<td></td>
<td>ip address 10.10.254/24 secondary</td>
</tr>
<tr>
<td></td>
<td>ip address 10.10.254/24 secondary</td>
</tr>
<tr>
<td>!</td>
<td>!</td>
</tr>
<tr>
<td>interface vlan581</td>
<td>interface vlan582</td>
</tr>
<tr>
<td></td>
<td>description SVI connected to Leaf1</td>
</tr>
<tr>
<td></td>
<td>vrf member ISP1</td>
</tr>
<tr>
<td></td>
<td>ip address 10.1.1.2/30</td>
</tr>
<tr>
<td></td>
<td>no shutdown</td>
</tr>
<tr>
<td>!</td>
<td>!</td>
</tr>
<tr>
<td>router bgp 666</td>
<td>router bgp 666</td>
</tr>
<tr>
<td>vrf ISP1</td>
<td>vrf ISP2</td>
</tr>
<tr>
<td></td>
<td>address-family ipv4 unicast</td>
</tr>
<tr>
<td></td>
<td>network 10.10.10.0/24</td>
</tr>
<tr>
<td></td>
<td>network 10.10.20.0/24</td>
</tr>
<tr>
<td></td>
<td>neighbor 10.100.100.1</td>
</tr>
<tr>
<td></td>
<td>remote-as 666</td>
</tr>
<tr>
<td></td>
<td>password cisco123</td>
</tr>
<tr>
<td></td>
<td>update-source loopback581</td>
</tr>
<tr>
<td></td>
<td>address-family ipv4 unicast</td>
</tr>
<tr>
<td></td>
<td>default-originate</td>
</tr>
<tr>
<td></td>
<td>address-family ipv4 unicast</td>
</tr>
<tr>
<td></td>
<td>network 172.16.10.0/24</td>
</tr>
<tr>
<td></td>
<td>network 172.16.20.0/24</td>
</tr>
<tr>
<td></td>
<td>neighbor 10.200.200.1</td>
</tr>
<tr>
<td></td>
<td>remote-as 666</td>
</tr>
<tr>
<td></td>
<td>password cisco123</td>
</tr>
<tr>
<td></td>
<td>update-source loopback582</td>
</tr>
<tr>
<td></td>
<td>address-family ipv4 unicast</td>
</tr>
<tr>
<td></td>
<td>default-originate</td>
</tr>
</tbody>
</table>

6. ACI BGP Sample Configuration for ISP1

6.1 Private Network

A private network is used to define a unique Layer 3 forwarding domain within the fabric. One or more private networks can be created inside a tenant. A private network is also known as a context and can be viewed as the equivalent of a VRF in the traditional networking world. Because each context defines a separate Layer 3 domain, IP addresses residing within a context can overlap with addresses in other contexts.

In this topology, the single private network CTX1 is configured (assuming that tenant “Acme” is preconfigured) as follows:

1. On the menu bar, click Tenants, and click the name of the tenant on which the private network needs to be created.
2. Right-click Networking and click Create Private Network.
3. In the Create Private Network area, specify the private tenant network name (CTX1), and click Next.
The APIC controller instantiates the required VRF for a tenant private network only when there are endpoints attached to the leaf. This helps preserve the hardware resources on the leaf switches.

Layer 3 outside connections, or external routed networks, provide IP connectivity between a private network of a tenant and an external IP network. Each Layer 3 outside connection is associated with one private network only. A private network may not have a Layer 3 outside connection if IP connectivity to the outside is not required.

6.1.1 XML Output for Private Network (CTX1)
Figure 12 shows equivalent XML output to create a context CTX1.

Figure 12. XML Output to Create Context (CTX1)

```
<fvCtx dn="uni/tn-tnAcme/ctx-CTX1" knwMcastAct="permit" name="CTX1" pcEnfPref="enforced">
  <fvRsBgpCtxPol tnBgpCtxPolName=""/>
  <fvRsAny descr="" matchT="AtleastOne" name=""/>
  <fvRsOspfCtxPol tnOspfCtxPolName=""/>
  <fvRsCtxToEpRet tnFvEpRetPolName=""/>
</fvCtx>
```

6.2 Bridge Domain
A bridge domain is a construct used to define a Layer 2 boundary within the fabric. A bridge domain can be viewed as somewhat similar to regular VLANs in a traditional switching environment.

1. Specify a bridge domain in the private network.
2. Specify the bridge domain name in the Name field (BD1).
3. Click the + sign next to Subnets to add a public subnet (192.168.1.254/24) to associate with BD1. This public subnet will advertise to ISP1 (Figure 13).
Figure 13. Configuring a Bridge Domain (BD1)

Border leaves are the place where tenant subnets are injected into the protocol running between the border leaves and external routers. Users have control of which tenant subnets they want to advertise to the external routers. When specifying subnets under a bridge domain for a given tenant, the user has the choice to specify the scope of a subnet, as indicated in Figure 13.

- **Public subnet** indicates that this subnet will be advertised to the external router by the border leaf.
- **Private subnet** indicates that this subnet will be contained within the ACI fabric and will not be advertised to external routers by the border leaf.
- **Shared subnet** is for shared services. It is used to indicate that this subnet needs to be leaked to one or more private networks. The shared subnet attribute is applicable to both public and private subnets.

As shown in Figure 13, subnet 192.168.1.254/24 is defined as a public subnet. In addition to specifying a tenant subnet as a public subnet, the user also needs to associate a Layer 3 outside connection with a bridge domain in order for the border leaf to advertise the tenant subnet to an external router. Refer to the section [Associate the Layer 3 Outside Network with a Bridge Domain](#) for details.
To validate the tenant’s private network (CTX1) and bridge domain (BD1), in the submenu bar under the Tenants tab, click the tenant name Acme. In the Navigation pane, expand the tenant name. Under Bridge Domains, the new bridge domain is displayed. Under Private Networks, the new network is displayed (Figure 14).

**Figure 14.** Validating the Private Network (CTX1) and Bridge Domain (BD1) Configuration

6.2.1 XML Output for Bridge Domain (BD1)

Figure 15 shows equivalent XML output for BD1 configuration.

**Figure 15.** Figure 1: XML Output to Create Bridge Domain (BD1)

6.3 External Routed Network

External routed networks are used to access an external network via routed links. The Cisco ACI fabric distinguishes internal endpoints from external routes. All the endpoints that are internal to the fabric are known by means of discovery of the endpoint itself. The external routes are known by peering with OSPF or BGP with neighboring routers or by configuring static routes. As mentioned earlier, fabric leaf switches are able to peer with external networks and redistribute the routing information throughout the fabric.

The following will be configured in the external routed network:

- Layer 3 outside network and a dynamic routing protocol (in this case BGP)
- Node ID, router ID, and static route for the loopback address of the external WAN device
- BGP peering detail with MD5 password and BGP community attributes
- Interface IP and VLAN to connect with external WAN device
6.3.1 Create Layer 3 outside Network Profiles

The configuration of Layer 3 connectivity requires identification of the leaf that will be the border leaf for this specific tenant, the interfaces that will be used, the IP addresses that should be used, and the routing instance of the tenant with which the routes should be associated.

The external routed network configuration requires border leaf switches and ports to be identified that connect to the external Layer 3 devices by using an attachable entity profile (AEP). On a high level, this is a mechanism to instruct the APIC to allow certain VLANs on selected ports. Detailed configuration steps for AEPs can be found at the following link.


**Note:** A private network can have only one Layer 3 outside network per leaf. If more than one Layer 3 outside network is required per private network, these must be spread across multiple leaf switches.

On the menu bar, choose **Tenants** and click the tenant on which the external routers needs to be created.

- In the **Navigation** pane, perform the following actions:
  - Expand Tenant “Acme” > Networking > External Routed Networks.
  - Right-click Create Routed Outside.

**Figure 16.** Selecting “Create Routed Outside” Under “Networking”
4. In the **Create Routed Outside** dialog box (Figure 17), do the following:
   
   1. In the Name field, enter the name of the routed outside policy (L3-OUT1).
   2. In the Private Network drop-down list, choose the network (CTX1).
   3. Select BGP as the routing protocol.
6.3.2 Create Node Profiles

Expand **Nodes and Interfaces Protocol Profiles** to display the Create Node Profile dialog box (Figure 18).

**Figure 18.** The Create Node Profile Dialog Box

In the Create Node Profile dialog box, you will configure the following:

- Node and router IDs with static routes for the next-hop address
- BGP peering detail, such as neighbor IP
- Interface ID with IP and VLAN encapsulation detail

1. In the Name field, enter the profile name (ISP1).
2. Click the + sign next to Nodes to display the Select Node dialog box (Figure 19). In the Node ID field, choose a leaf switch from the drop-down list. In this example, port 1/40 of leaf1 is connected with a WAN router (switched virtual interface [SVI] and VLAN ID is 581).
3. In the Router ID field, enter the router ID, which will be used for iBGP peering with the external WAN device.

**Note:** For the router ID, a corresponding loopback interface will be created on the border leaf switch (Figure 20).

**Figure 20.** Loopback Interface Configuration on Leaf Switches
6.3.3 Configure a BGP Peer Connectivity Profile for ISP1

BGP peer configuration is done in the Create Peer Connectivity Profile dialog box. In this example, the loopback IP address of the external WAN device is being used, which is 10.100.100.2. A static route is configured for the loopback IP address of the external device. The MD5 password and BGP community (standard and extended) need to be configured in the same dialog box (Figure 21).

1. Click the + sign next to BGP Peer Connectivity Profiles.
2. In the Create Peer Connectivity Profile dialog box, enter the BGP peer IP address in the Peer Address field.

Figure 21. Configuring the BGP Peer Connectivity Profile

6.3.4 Create an Interface Profile for ISP1

An interface profile is required to connect the ACI fabric with external devices. This profile associates the configuration with interfaces on the leaf switches. In the following example, port 1/40 on leaf1 (node 101) is attached to the external WAN device. The interface profile object can be created and port 1/40 added to it with the required VLANs. More ports' VLANs can be added later to apply the same configuration to all ports connected to the external WAN device. The fabric administrator needs to create this configuration beforehand. Detailed configuration steps can be found at the following link:

Three different types of interfaces are supported on border leaf switches to connect to an external router:

- Layer 3 interface.
- Subinterface with 802.1Q tagging: With a subinterface, the same physical interface can be used to provide a Layer 2 outside connection for multiple private networks.
- Switched virtual interface (SVI): With an SVI, the same physical interface that supports Layer 2 and Layer 3 can be used for a Layer 2 outside connection as well as a Layer 3 outside connection.

In this example, an SVI is used with VLAN 581 to connect with the external device (Figure 22). The interface IP is 10.1.1.1/30, as described in the BGP Network Topology section. Follow these steps to configure:

1. Select **SVI** as the interface type.
2. Enter the encapsulation VLAN ID in the **Encap** field, for ISP1 connectivity. VLAN 581 is used in this case.
3. Enter the point-to-point IP address of the SVI in the **IP Address** field.

**Figure 22.** Creating the SVI
6.3.5 Completed Node Profile Output

Figure 23 shows the output with the completed node profile.

**Figure 23.** Completed Node Profile

![CREATE NODE PROFILE](image)

The interface IP address can be viewed on leaf1 by using the command `show ip interface vrf Acme:CTX1` (Figure 24).

**Figure 24.** Interface IP Detail on Leaf1

```
leaf1# show ip interface vrf Acme:CTX1
IP Interface Status for VRF "Acme:CTX1"(8)
Vlan21, Interface status: protocol-up/link-up/admin-up, iod: 100, mode: pervasive, vrf_vnid: 2719744
 IP address: 192.168.1.254, IP subnet: 192.168.1.0/24
 IP primary address route-preference: 1, tag: 0
Vlan26, Interface status: protocol-up/link-up/admin-up, iod: 102, mode: pervasive, vrf_vnid: 2719744
 IP address: 192.168.2.254, IP subnet: 192.168.2.0/24
 IP primary address route-preference: 1, tag: 0
Vlan39, Interface status: protocol-up/link-up/admin-up, iod: 111, mode: external, vrf_vnid: 2719744
 IP address: 10.1.1.1, IP subnet: 10.1.1.0/30
 IP primary address route-preference: 1, tag: 0
loopback6, Interface status: protocol-up/link-up/admin-up, iod: 110, mode: unspecified, vrf_vnid: 2719744
 IP address: 10.100.100.1, IP subnet: 10.100.100.0/32
 IP primary address route-preference: 1, tag: 0
leaff1
```
Once these steps are completed, validate the IP connectivity between the border leaf and the external WAN router by pinging the leaf switch interface and loopback IP address from the ISP1 router (Figure 25).

**Figure 25.** Interface and Loopback IP Reachability Test from ISP1 to Leaf1

---

### 6.3.6 Create an External Endpoint Group

An external endpoint group (EPG) carries the external network/prefix information. The ACI fabric maps external Layer 3 endpoints to the external EPG by using the IP prefix and mask. One or more external EPGs can be supported for each Layer 3 outside connection, depending on whether the user wants to apply a different policy for different groups of external endpoints. In this example we treat all outside endpoints equally and create only one external EPG.

1. Click **Next** in the **Create Routed Outside** dialog box (Figure 26).
2. Click the + sign below External EPG Networks (Figure 27).

Figure 26. Selecting an External EPG Network

Figure 27. Creating an External EPG Network
3. In the **Create External Network** dialog box, in the **Name** field, add a name (ISP1-Net).

4. Define external **subnets** (Figure 28).

With the Layer 3 external EPG configuration, the user can map external endpoints to this EPG by adding IP prefixes and network masks. The network prefix and mask don’t need to be the same as the ones in the routing table. We can use simply use 0.0.0.0/0 to assign all external endpoints to this external EPG.

### 6.3.7 Configure a Contract for the External Network

Without a contract for the external network, traffic will not flow and a BGP session will not establish. Apply the common/default contract; it’s a **permit any** contract.

1. In the **Work** pane, expand the **Consumed Contracts** area, and from the **Name** drop-down list, choose the default contract of tenant **Common**. Choose **Update** (Figure 29).
Figure 29. Selecting the External Network

At this point a BGP session between ISP1 and leaf1 is established, but the prefix is still not advertised from leaf1 to ISP1 (Figure 30).

Figure 30. BGP Session on ISP1 with Leaf1

In order to advertise prefixes from leaf1 to ISP1, you need to associate the Layer 3 outside network with BD1. Refer to the following section for details.

6.3.8 Associate the Layer 3 outside Network with a Bridge Domain

BD1 is configured with a public subnet (192.168.1.254/24) to advertise it to BGP peers. As shown in Figure 30 in the previous section, the BGP session is up, but no prefixes are being advertised from leaf1. By default, when a BGP session is configured, the fabric (leaf) automatically associates/applies an inbound and outbound route map to each BGP peer to control the route advertisement.

Figure 31. Route Map Configuration on the Leaf Switch
As shown in Figure 31, the outbound route map `exp-epg491532719744` is associated with a BGP neighbor but is still not created, and so, as per standard BGP policy, all prefixes will be denied.

To advertise routes from the fabric (leaf), you need to associate a Layer 3 outside network with the bridge domain. The public routes will then be advertised to all peers of the associated Layer 3 outside network. In this example, BD1 will be associated with the L3-OUT1 network (Figure 32).

**Figure 32.** Associating L3-OUT1 with BD1

![Figure 32](image)

After associating L3-OUT1 with BD1, leaf1 automatically creates that route map, as shown in Figure 33.

**Figure 33.** Route Map Created After Associating L3-OUT1 with BD1

```
leaf1# show ip bgp Acme:CTX1 neighbors 10.100.100.2 | in route-map
Inbound route-map configured is permit-all
Outbound route-map configured is `exp-epg491532719744`
leaf1#
leaf1# show route-map | in exp-epg491532719744
route-map exp-epg491532719744, permit, sequence 2001
leaf1#
```

`now route-map found`
However, prefixes are not yet advertised from leaf1 to ISP1 (Figure 34).

**Figure 34.** Route Advertisement from Leaf1 to ISP1

![Image of route advertisement output]

One more step is needed to advertise prefixes from leaf1 to ISP1: creating an EPG on leaf1. Figure 35 shows an EPG-Host1 EPG being created in the application profile (AP1).

**Figure 35.** Creating EPG-Host1

![Image of EPG creation in application profile]

After you configure one EPG (EPG-Host1 in this example), leaf1 should start advertising the 19.168.1.0/24 prefix to ISP1 (Figure 36).
Figure 36. Route Advertisement from Leaf1 to ISP1

As shown in Figure 36, Host1 cannot ping to external networks and vice versa. To enable end-to-end data connectivity, you need to create a contract for the EPG Host1. Apply the common/default contract, as shown in Figure 37.

Figure 37. Applying the Common/Default Contract to EPG-Host1

After applying the common/default contract to EPG-Host1, ISP1 can ping internal networks such as Host1 (Figure 38).

Figure 38. Successful Ping from ISP1 to Host1
6.3.9 XML Output for BGP Setup with ISP1

Figure 39 shows XML equivalent code for BGP setup.

Figure 39. XML Output for BGP Setup with ISP1

```xml
<!-- L3-OUT1 -->
<l3extOut dn='uni/tn-Acme/out-L3-OUT1' name='L3-OUT1' targetDscp='unspecified'>
  <l3extRsEctx tnFvCtxName='CTX1'/>
  <l3extRsNodeL3OutAtt rtrId='10.100.100.1' tDn='topology/pod-1/path-101/nod-101'>
    <ipRouteP pm='10.100.2.32' name=''/>
  </ipRouteP>
  <l3extRsNodeL3OutAtt>
    <l3extLIFP name='ISP1-int' ownerKey=''' ownerTag=''' tag='yellow-green'
      addr='10.1.1.30' encaps='vlan-581' ifInst='ext-svi'
      tDn='topology/pod-1/path-101/nod-101/eth1/40'>
      <bgpPeerP addr='10.100.100.2' ctrl='' descr=''' name=''/>
    </l3extLIFP>
  </l3extRsNodeL3OutAtt>
  <l3extInstP name='ISP-Net' pri='unspecified'>
    <vRsCons pri='unspecified' tnVzBrCPName='default'/>
    <l3extSubnet descr='' ip='10.0.0.8'/>
    <vRsCstQosPol tnQosCustomPolName=''/>
    <vRsProv match='AtleastOne' pri='unspecified' tnVzBrCPName='default'/>
  </l3extInstP>
</l3extOut>
```

6.4 Route Profile

A route profile provides a control mechanism for routes with BGP peers. This can be viewed as a standard route map in the classic BGP configuration.

A route profile can be associated with any of the following:

- Prefix
- Bridge domain
- Layer 3 outside network
When a route profile is associated with a bridge domain, all of the subnets under the bridge domain will be advertised with the same BGP community value. The software also allows the user to associate a route profile with a subnet of a bridge domain; this capability provides the flexibility to mark different BGP community values for different subnets. When a route profile is specified under both the bridge domain and the subnets of a bridge domain, the route profile under the subnet takes precedence.

A route profile with the name default-export can be configured and will be applied automatically to the Layer 3 outside network.

6.4.1 Create a Route Profile
In Figure 40, a route profile (RouteProfile1) is created to advertise a standard community (666:1001) to its BGP peer.

Figure 40. Creating a Route Profile

The ACI border leaf switches support outbound BGP policy to set community or extended community values for tenant routes. The BGP community attributes (standard and extended) are commonly used by network architects to group together certain BGP routes and apply route policy by matching community values.

The following two types of communities are supported:

   a) regular:as2-nn2 is a keyword for the standard community
   b) 666:1001 is used as an example for a standard community value
2. Extended community: extended:as4-nn2: <community_value>
   a) extended:as4-nn2 is a keyword for the extended community
6.4.2 Associate the Route Profile

After a route profile is created, it can be associated with a prefix or bridge domain. Figure 41 shows how a route profile can be associated with a prefix.

Figure 41. Associating a Route Profile with a Prefix

The route profile (RouteProfile1) is used with prefix 192.168.1.0/24 and is advertised to its BGP peer through the L3-OUT1 network. Figure 42 shows the confirmation of the BGP community value.

Figure 42. Checking the BGP Community Value on the ISP1 Router

6.4.3 The default-export Route Profile

When a default-export route profile is created under a Layer 3 outside network, it is automatically associated with the Layer 3 outside network.

In Figure 43:

- A default-export route profile is created under L3-OUT1.
- The policy name is policy1.
- The advertised community is 666:1009 the default-export route profile.
- The route profile is removed from the prefix and bridge domain.
Figure 43. Configuring a Default-Export Route Profile in the L3-OUT1 Network

Now L3-OUT1 will advertise all prefixes to ISP1 with the community value 666:1009. This can be verified on the ISP1 router to check prefix 192.168.1.0/24 (Figure 44).

Figure 44. Prefix Advertised by Using the Default-Export Route Profile

7. ACI BGP Sample Configuration for ISP2
Repeat all the steps described in the section ACI BGP Sample Configuration for ISP1 to configure BGP for ISP2. The key difference between ISP1 and ISP2 setup is to associate a different Layer 3 outside network (Figure 45).
If one of the bridge domain's public prefixes needs to advertise to one or more than one of the Layer 3 outside networks, the respective bridge domain needs to associate with all of the Layer 3 outside networks. In Figure 46, BD2 will be associated with the L3-OUT1 and L3-OUT2 external networks. In other words, ISP1 will receive two routes, one from BD1 and the second from BD2, while ISP2 will receive only one prefix from BD2.

**Figure 46.** Associating Two Layer 3 Outside Networks with BD2
ISP1 must be receiving the 192.168.2.0/24 prefix along with the 192.168.1.0/24 prefix now (Figures 47 and 48).

Figure 47. Routes Received from Leaf1 to ISP1

![BGP routing table information for VRF ISP1, address family IPv4 Unicast](terable.png)

Figure 48. Routes Received from Leaf2 to ISP2

![BGP routing table information for VRF ISP2, address family IPv4 Unicast](terable.png)

8. BGP Configuration and Statistic Validation

BGP protocol statistics can be viewed under Fabric > Inventory (Figure 49).

1. In the Navigation pane, expand Pod ID > Leaf Switch ID > Protocols > BGP and click the corresponding tenant and private network.

2. Click various options, such as Neighbors, Interfaces, Routes, and Traffic to check different statistic related to BGP.
Figure 49. Configuring BGP and Validating Statistics

![BGP and Validating Statistics Configuration](image)

<table>
<thead>
<tr>
<th>Name</th>
<th>PRI</th>
<th>PATH-ID</th>
<th>Peer</th>
<th>Properties</th>
<th>NEXT-HOP</th>
<th>METRIC</th>
<th>LOCAL_PREF</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP Route 172.16.52.0/24</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>BGP Route 172.16.53.0/24</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>BGP Route 172.16.54.0/24</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td>100</td>
<td></td>
</tr>
</tbody>
</table>

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.