Understanding Fabric Policies

Now that ACME has been provisioned with ACI fabric and infrastructure space has been configured between the leaf and spine switches, access privileges, and basic management policies, it is time to start creating connectivity policies within the ACI fabric. The fabric tab in the APIC GUI is used to configure system-level features including, but not limited to, device discovery and inventory management, diagnostic tools, configuring domains, and switch and port behavior. The fabric pane is split into three sections: inventory, fabric policies, and access policies. Understanding how fabric and access policies configure the fabric is key for the ACME network teams, as they will be maintaining these policies for the purposes of internal connections between fabric leaf nodes, connections to external entities such as servers, networking equipment, and storage arrays. It is important that other teams such as server teams understand these concepts as well, as they will be interacting with them, particularly in the case of their build processes for adding additional capacity.

This chapter will review the key objects in the access policies subsection of the fabric tab -- many of which are reusable; demonstrate how to add and pre-provision switches, and walk through the steps and objects required when new devices are added to the fabric to effectively operate an ACI fabric. While many policies are reusable, it is also key to understand the implications of deleting policies on the ACI fabric.

The access policies subsection is split into folders separating out different types of policies and objects that affect fabric behavior. For example, the interface policies folder is where port behavior is configured, like port speed, or whether or not to run protocols like LACP on leaf switch interfaces is set. Domains and AEPs are also created in the access policies view. The fabric access policies provide the fabric with the base configuration of the access ports on the leaf switches.
Fabric - Access Policies

Domains

Endpoint groups are considered the "who" in ACI; contracts are considered the "what/when/why"; AEPs can be considered the "where" and domains can be thought of as the "how" of the fabric. Different domain types are created depending on how a device is connected to the leaf switch. There are four different domain types: physical domains, external bridged domains, external routed domains, and VMM domains.

- Physical domains are generally used for bare metal servers or servers where hypervisor integration is not an option.
- External bridged domains are used for Layer 2 connections. For example, an external bridged domain could be used to connect an existing switch trunked-up to a leaf switch.
- External routed domains are used for Layer 3 connections. For example, an external routed domain could be used to connect a WAN router to the leaf switch.
- Domains act as the glue between the configuration done in the fabric tab to the policy model and endpoint group configuration found in the tenant pane. The fabric operator creates the domains, and the tenant administrators associate domains to endpoint groups.

Ideally, policies should be created once and reused when connecting new devices to the fabric. Maximizing the reusability of policy and objects makes day-to-day operations exponentially faster and easier to make large-scale changes. The usage of these policies can be viewed by clicking the Show Usage button in the Application Policy Infrastructure Controller (APIC) GUI. Use this to determine what objects are using a certain policy to understand the impact when making changes.

For an in-depth whiteboard explanation on domains, watch the following video titled "How Devices Connect to the Fabric: Understanding Cisco ACI Domains": https://www.youtube.com/watch?v=_iQvoC9zQ_A.

VLAN Pools

VLAN pools contain the VLANs used by the EPGs the domain will be tied to. A domain is associated to a single VLAN pool. VXLAN and multicast address pools are also configurable. VLANs are instantiated on leaf switches based on AEP configuration. Allow/deny forwarding decisions are still based on contracts and the policy model, not subnets and VLANs.

Attachable Access Entity Profiles

Attachable Access Entity Profiles (AEPs) can be considered the "where" of the fabric configuration, and are used to group domains with similar requirements. AEPs are tied to interface policy groups. One or more domains can be added to an AEP. By grouping domains into AEPs and associating them, the fabric knows where the various devices in the domain live and the Application Policy Infrastructure Controller (APIC) can push the VLANs and policy where it needs to be. AEPs are configured under the global policies section.

Policy Types

Most of the policies folders have subfolders. For example, under the interface policies folder there are folders for configuration called policies, policy groups, and profiles.
Switch Policies

There are also policies for switches - for example, configuring vPC domains, which are called explicit vPC protection groups in the Application Policy Infrastructure Controller (APIC) GUI and vPC policies. Ideally, policies should be created once and reused when connecting new devices to the fabric. Maximizing reusability of policy and objects makes day-to-day operations exponentially faster and easier to make large-scale changes.

Switch Policy Groups

Switch policy groups allow leveraging of existing switch policies like Spanning Tree and monitoring policies.

Switch Profiles

Switch profiles allow the selection of one or more leaf switches and associate interface profiles to configure the ports on that specific node. This association pushes the configuration to the interface and creates a Port Channel or vPC if one has been configured in the interface policy.

The following figure highlights the relationship between the various global, switch, and interface policies:

Figure 1: Relationships to allow a physical interface or interfaces to be attached to an EPG

Interface Policies

Interface policies dictate interface behavior, and are later tied to interface policy groups. For example, there should be a policy that dictates if CDP is disabled and a policy that dictates if CDP is enabled; these can be reused as new devices are connected to the leaf switches.
**Interface Policy Groups**

Interface policy groups are templates to dictate port behavior and are associated to an AEP. Interface policy groups use the policies described in the previous paragraph to specify how links should behave. These are also reusable objects as many devices are likely to be connected to ports that will require the same port configuration. There are three types of interface policy groups depending on link type: Access Port, Port Channel, and vPC.

The ports on the leaf switches default to 10GE, and a 1GE link level policy must be created for devices connected at that speed. Regarding Port Channels and vPC, each policy group designated a single logical interface on the switches. If you want to create 10 PCs/vPCs, you must create 10 policy groups. Access port policy groups can be reused between interfaces. Policy groups do not actually specify where the protocols and port behavior should be implemented. The "where" happens by associating one or more interface profiles to a switch profile, covered in the following paragraphs.

**Interface Profiles**

Interface profiles help tie the pieces together. Interface profiles contain blocks of ports - interface selectors - and are also tied to the interface policy groups described in the previous paragraphs. Again, this is just an arbitrary port, such as e1/1, the profile must be associated to a specific switch profile to configure the ports.

**Layer 2 Interface Policy**

In the Cisco APIC release 1.1, a configurable interface policy was added to allow a per port-VLAN significance. To connect devices to the Cisco Application Centric Infrastructure (Cisco ACI) fabric we can use untagged traffic, 802.1Q tagged traffic, or VXLAN encapsulation. A per-port VLAN allows the same VLAN to be used for different endpoint groups, providing that traffic is coming in on a different port. Prior to release 1.1, a VLAN could only be tied to one endpoint group per leaf switch.

In traditional networking one of the limitations related to VLAN encapsulation is scalability and reusability due to the limit of 4096 VLANs in networking devices.

In Cisco ACI, with the default configuration (global), EPGs can use the same VLAN encapsulation as long as the EPGs are bound to separate switches and use different physical domains that are bound to different VLAN pools. This allows tenants to re-use VLAN encapsulation IDs through the fabric without allowing communication between tenants. However, global configuration assumes that tenants do not share leaf switches and therefore there is no VLAN overlapping within the same leaf switch.

Per port-VLAN limitations and considerations

- When per port-VLAN is used, a port and VLAN pair (P,V) is registered internally instead of just a VLAN encapsulation ID. This increases the consumption of hardware resources at a per switch level.
- Two EPGs belonging to a single bridge domain cannot share the same encapsulation ID on a given leaf switch.
- It is expected that the port will flap when the Layer 2 interface policy changes between global and local. That is, traffic will get affected.

**DWDM-SFP10G-C Optic Interface Policy**

The Cisco APIC release 3.1(1) added support for the DWDM-SFP10G-C optic, which includes an interface policy for the optic. When a DWDM-SFP10G-C port is inserted, the port by default has channel number 32. In the DWDM-SFP10G-C optic interface policy, you can change the channel number to any number between 1 to 96, which tunes the optic to the corresponding wavelength.
Table 1: DWDM-SFP10G-C Port Wavelength by Channel

<table>
<thead>
<tr>
<th>Channel Number</th>
<th>Frequency (THz)</th>
<th>Wavelength (nm)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>191.35</td>
<td>1566.72</td>
</tr>
<tr>
<td>2</td>
<td>191.40</td>
<td>1566.31</td>
</tr>
<tr>
<td>3</td>
<td>191.45</td>
<td>1565.90</td>
</tr>
<tr>
<td>4</td>
<td>191.50</td>
<td>1565.50</td>
</tr>
<tr>
<td>5</td>
<td>191.55</td>
<td>1565.09</td>
</tr>
<tr>
<td>6</td>
<td>191.60</td>
<td>1564.68</td>
</tr>
<tr>
<td>7</td>
<td>191.65</td>
<td>1564.27</td>
</tr>
<tr>
<td>8</td>
<td>191.70</td>
<td>1563.86</td>
</tr>
<tr>
<td>9</td>
<td>191.75</td>
<td>1563.45</td>
</tr>
<tr>
<td>10</td>
<td>191.80</td>
<td>1563.05</td>
</tr>
<tr>
<td>11</td>
<td>191.85</td>
<td>1562.64</td>
</tr>
<tr>
<td>12</td>
<td>191.90</td>
<td>1562.23</td>
</tr>
<tr>
<td>13</td>
<td>191.95</td>
<td>1561.83</td>
</tr>
<tr>
<td>14</td>
<td>192.00</td>
<td>1561.42</td>
</tr>
<tr>
<td>15</td>
<td>192.05</td>
<td>1561.01</td>
</tr>
<tr>
<td>16</td>
<td>192.10</td>
<td>1560.61</td>
</tr>
<tr>
<td>17</td>
<td>192.15</td>
<td>1560.20</td>
</tr>
<tr>
<td>18</td>
<td>192.20</td>
<td>1559.79</td>
</tr>
<tr>
<td>19</td>
<td>192.25</td>
<td>1559.39</td>
</tr>
<tr>
<td>20</td>
<td>192.30</td>
<td>1558.98</td>
</tr>
<tr>
<td>21</td>
<td>192.35</td>
<td>1558.58</td>
</tr>
<tr>
<td>22</td>
<td>192.40</td>
<td>1558.17</td>
</tr>
<tr>
<td>23</td>
<td>192.45</td>
<td>1557.77</td>
</tr>
<tr>
<td>24</td>
<td>192.50</td>
<td>1557.36</td>
</tr>
<tr>
<td>25</td>
<td>192.55</td>
<td>1556.96</td>
</tr>
<tr>
<td>26</td>
<td>192.60</td>
<td>1556.55</td>
</tr>
<tr>
<td>27</td>
<td>192.65</td>
<td>1556.15</td>
</tr>
<tr>
<td>28</td>
<td>192.70</td>
<td>1555.75</td>
</tr>
<tr>
<td>29</td>
<td>192.75</td>
<td>1555.34</td>
</tr>
<tr>
<td>30</td>
<td>192.80</td>
<td>1554.94</td>
</tr>
<tr>
<td>31</td>
<td>192.85</td>
<td>1554.54</td>
</tr>
<tr>
<td>Channel Number</td>
<td>Frequency (THz)</td>
<td>Wavelength (nm)</td>
</tr>
<tr>
<td>----------------</td>
<td>----------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>32</td>
<td>192.90</td>
<td>1554.13</td>
</tr>
<tr>
<td>33</td>
<td>192.95</td>
<td>1553.73</td>
</tr>
<tr>
<td>34</td>
<td>193.00</td>
<td>1553.33</td>
</tr>
<tr>
<td>35</td>
<td>193.05</td>
<td>1552.93</td>
</tr>
<tr>
<td>36</td>
<td>193.10</td>
<td>1552.52</td>
</tr>
<tr>
<td>37</td>
<td>193.15</td>
<td>1552.12</td>
</tr>
<tr>
<td>38</td>
<td>193.20</td>
<td>1551.72</td>
</tr>
<tr>
<td>39</td>
<td>193.25</td>
<td>1551.32</td>
</tr>
<tr>
<td>40</td>
<td>193.30</td>
<td>1550.92</td>
</tr>
<tr>
<td>41</td>
<td>193.35</td>
<td>1550.52</td>
</tr>
<tr>
<td>42</td>
<td>193.40</td>
<td>1550.12</td>
</tr>
<tr>
<td>43</td>
<td>193.45</td>
<td>1549.72</td>
</tr>
<tr>
<td>44</td>
<td>193.50</td>
<td>1549.32</td>
</tr>
<tr>
<td>45</td>
<td>193.55</td>
<td>1548.91</td>
</tr>
<tr>
<td>46</td>
<td>193.60</td>
<td>1548.51</td>
</tr>
<tr>
<td>47</td>
<td>193.65</td>
<td>1548.11</td>
</tr>
<tr>
<td>48</td>
<td>193.70</td>
<td>1547.72</td>
</tr>
<tr>
<td>49</td>
<td>193.75</td>
<td>1547.32</td>
</tr>
<tr>
<td>50</td>
<td>193.80</td>
<td>1546.92</td>
</tr>
<tr>
<td>51</td>
<td>193.85</td>
<td>1546.52</td>
</tr>
<tr>
<td>52</td>
<td>193.90</td>
<td>1546.12</td>
</tr>
<tr>
<td>53</td>
<td>193.95</td>
<td>1545.72</td>
</tr>
<tr>
<td>54</td>
<td>194.00</td>
<td>1545.32</td>
</tr>
<tr>
<td>55</td>
<td>194.05</td>
<td>1544.92</td>
</tr>
<tr>
<td>56</td>
<td>194.10</td>
<td>1544.53</td>
</tr>
<tr>
<td>57</td>
<td>194.15</td>
<td>1544.13</td>
</tr>
<tr>
<td>58</td>
<td>194.20</td>
<td>1543.73</td>
</tr>
<tr>
<td>59</td>
<td>194.25</td>
<td>1543.33</td>
</tr>
<tr>
<td>60</td>
<td>194.30</td>
<td>1542.94</td>
</tr>
<tr>
<td>61</td>
<td>194.35</td>
<td>1542.54</td>
</tr>
<tr>
<td>62</td>
<td>194.40</td>
<td>1542.14</td>
</tr>
<tr>
<td>63</td>
<td>194.45</td>
<td>1541.75</td>
</tr>
<tr>
<td>Channel Number</td>
<td>Frequency (THz)</td>
<td>Wavelength (nm)</td>
</tr>
<tr>
<td>----------------</td>
<td>----------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>64</td>
<td>194.50</td>
<td>1541.35</td>
</tr>
<tr>
<td>65</td>
<td>194.55</td>
<td>1540.95</td>
</tr>
<tr>
<td>66</td>
<td>194.60</td>
<td>1540.56</td>
</tr>
<tr>
<td>67</td>
<td>194.65</td>
<td>1540.16</td>
</tr>
<tr>
<td>68</td>
<td>194.70</td>
<td>1539.77</td>
</tr>
<tr>
<td>69</td>
<td>194.75</td>
<td>1539.37</td>
</tr>
<tr>
<td>70</td>
<td>194.80</td>
<td>1538.98</td>
</tr>
<tr>
<td>71</td>
<td>194.85</td>
<td>1538.58</td>
</tr>
<tr>
<td>72</td>
<td>194.90</td>
<td>1538.19</td>
</tr>
<tr>
<td>73</td>
<td>194.95</td>
<td>1537.79</td>
</tr>
<tr>
<td>74</td>
<td>195.00</td>
<td>1537.40</td>
</tr>
<tr>
<td>75</td>
<td>195.05</td>
<td>1537.00</td>
</tr>
<tr>
<td>76</td>
<td>195.10</td>
<td>1536.61</td>
</tr>
<tr>
<td>77</td>
<td>195.15</td>
<td>1536.22</td>
</tr>
<tr>
<td>78</td>
<td>195.20</td>
<td>1535.82</td>
</tr>
<tr>
<td>79</td>
<td>195.25</td>
<td>1535.43</td>
</tr>
<tr>
<td>80</td>
<td>195.30</td>
<td>1535.04</td>
</tr>
<tr>
<td>81</td>
<td>195.35</td>
<td>1534.64</td>
</tr>
<tr>
<td>82</td>
<td>195.40</td>
<td>1534.25</td>
</tr>
<tr>
<td>83</td>
<td>195.45</td>
<td>1533.86</td>
</tr>
<tr>
<td>84</td>
<td>195.50</td>
<td>1533.47</td>
</tr>
<tr>
<td>85</td>
<td>195.55</td>
<td>1533.07</td>
</tr>
<tr>
<td>86</td>
<td>195.60</td>
<td>1532.68</td>
</tr>
<tr>
<td>87</td>
<td>195.65</td>
<td>1532.29</td>
</tr>
<tr>
<td>88</td>
<td>195.70</td>
<td>1531.90</td>
</tr>
<tr>
<td>89</td>
<td>195.75</td>
<td>1531.51</td>
</tr>
<tr>
<td>90</td>
<td>195.80</td>
<td>1531.12</td>
</tr>
<tr>
<td>91</td>
<td>195.85</td>
<td>1530.72</td>
</tr>
<tr>
<td>92</td>
<td>195.90</td>
<td>1530.33</td>
</tr>
<tr>
<td>93</td>
<td>195.95</td>
<td>1529.94</td>
</tr>
<tr>
<td>94</td>
<td>196.00</td>
<td>1529.55</td>
</tr>
<tr>
<td>95</td>
<td>196.05</td>
<td>1529.16</td>
</tr>
</tbody>
</table>
Best Practices

Cisco has established several best practices for fabric configuration. These are not requirements and might not work for all environments or applications, but might help simplify day-to-day operation of the Cisco Application Centric Infrastructure (ACI) fabric.

- **Policies**
  
  - Reuse policies whenever possible. For example, there should be policies for LACP active/passive/off, 1GE port speed, and 10GE port speed.
  
  - When naming policies, use names that clearly describe the setting. For example, a policy that enables LACP in mode active could be called "LACP-Active". There are many "default" policies out of the box. However, it can be hard to remember what all the defaults are, which is why policies should be clearly named to avoid making a mistake when adding new devices to the fabric.
  
  - Create a switch profile for each leaf switch individually, and additionally, create a switch profile for each vPC pair (if using vPC).

- **Domains**
  
  - Build one physical domain per tenant for bare metal servers or servers without hypervisor integration requiring similar treatment.
  
  - Build one physical domain per tenant for external connectivity.
  
  - If a VMM domain needs to be leveraged across multiple tenants, a single VMM domain can be created and associated with all leaf ports where VMware ESXi servers are connected.

- **AEPs**
  
  - Multiple domains can be associated to a single AEP for simplicity's sake. There are some cases where multiple AEPs may need to be configured to enable the infrastructure VLAN, such as overlapping VLAN pools, or to limit the scope of the presence of VLANs across the fabric.

Adding New Devices to the Fabric

This section will demonstrate how to configure ACI to re-use the fabric access policies, simplifying day-to-day operation of the fabric. This section will walk through setting up profiles from scratch, with a focus on how to re-use these profiles across the fabric. As outlined in the previous section, these various profiles are linked together and have dependencies. The following diagram reiterates the object relationships:
Whereas a traditional command line interface on a switch generally requires a port-by-port configuration, ACI allows definition of objects and policies that can be re-used. The re-usability of these policies makes it possible to replicate the configuration of a switch very easily. The following diagram depicts how this re-usability simplifies the operation of the fabric over time.

In any data center, the configuration of a couple of switches does not require many processes or automation. As the data center size increases, automation becomes more and more critical as it has a direct impact on the cost of business operations. In traditional networks, when changes that impact a large set of devices need to be made, the operator is faced with the cost of designing processes to manage these devices. These can be network management tools, scripts, or specialized applications. Leveraging the Cisco ACI policy model, an operator can leverage profiles to streamline the operation of adding devices and managing those devices. This is what is depicted as the policy re-use inflection point in the previous diagram.
Sample Configuration

The following sections will walk through sample configuration of setting up individually connected devices, Port Channel-connected devices, and vPC-connected devices from scratch, and will include a review of the objects as they are configured. These are the steps to be taken in the APIC GUI when new devices are connected to the leaf switches to ensure the access ports on the leaf switches have the right switchport configuration, and the verification steps to ensure proper configuration. The following steps represent the use case of adding a new bare metal server connected to a leaf switch.

Before getting into the configuration of vPC's, which are a popular server connectivity methodology, it is important to understand what vPC’s are and how they are different from traditional methods of server connectivity. This section of the chapter attempts to clarify at a high level what vPC’s are, the benefits they provide and how vPC's in the ACI fabric differ from how they are deployed on Cisco Nexus switches running NX-OS software.

At a high level, vPC extends link aggregation to two separate physical switches.

In the figure above, a single server is dual homed to two different switches for redundancy. Without vPC’s, the server will likely use an active-standby configuration, or a special configuration on the NIC driver or the kernel that allows it to intelligently load-balance traffic using an algorithm.

By configuring ports on two different switches as the same port-channel and using an inter-switch messaging channel (such as the inter-switch port-channel in the green box on the left hand side) to cover redundancy scenarios, we provide a logical topology that greatly simplifies server provisioning and management.

This allows for several key advantages from a server deployment perspective:

- You can create resilient Layer 2 topologies based on link aggregation
- You do not need STP
- You have increased bandwidth, as all links are actively forwarding
- Your server configurations are simplified since the configurations simply appears as port-channels without the need for special software, from a driver or kernel-tuning standpoint

vPCs can also be used to connect other downstream devices, such as Cisco UCS fabric-interconnects, to provide similar benefits.

The figure below shows a single traditional Layer 2 switch connected to a VPC enabled Cisco switch pair.
The components of a traditional vPC domain are illustrated below:

**Figure 6: Traditional vPC topology**

As illustrated above, in Cisco switching products running NX-OS software, vPC configurations need to be done manually by the operator and require a pair of dedicated “inter-switch” links also called a peer-link. There is also a peer-keepalive link, typically on the out-of-band management port, that is used to determine peer liveliness to detect a vPC peer-switch failure. Making configuration changes in such scenarios without the config-sync feature enabled may lead to scenarios where there are mismatched vPC parameters between the vPC primary and the vPC secondary switches that may cause partial connectivity loss during the change itself if a type-1 inconsistency is detected.

The ACI fabric greatly simplifies VPC configurations.
The key differences to note here are that relative to traditional vPC design, there is no requirement for setting up vPC peer-links. There are also no keepalives being sent on the management ports. The fabric itself serves as the peer-link. The rich interconnectivity between fabric nodes makes it unlikely that peers will have an active path between them.

Note that attempting to cable a leaf switch to another leaf switch will lead to a "wiring mismatch" fault in the GUI and result in a blacklisted port that will have to be manually recovered.

The following are some other key behavioral changes to vPC as it applies to the ACI fabric relative to classic vPC that are important for operators to understand:

- Configurations are automatically synchronized to avoid an error-free configuration by the APIC which is the central point of control for all configurations in the ACI fabric.
- In traditional vPC solution, the slave switch brings down all its vPC links if the MCT goes down.
- In the ACI fabric, it is very unlikely that all the redundant paths between vPC peers fail at the same time. Hence if the peer switch becomes unreachable, it is assumed to have crashed. The slave switch does not bring down vPC links.
- Role election still happens, peers assume master-slave roles.
- Role is used in case of vpc type-1 consistency failure. Slave switch brings down all its vPC ports. A list of type-1 parameters used for consistency checking for a given vPC domain specific to the ACI fabric are listed below.
- Global type-1 parameters:
  - STP
- Interface type-1 parameters:
  - STP: Only BPDUGuard is configurable
  - EthPM
  - Port speed
  - Duplex mode
  - Port mode
  - MTU
  - Native VLAN
    - PCM: Channel mode, static vs lacp
• LACP: Lag ID

The following diagrams illustrate how the ACI fabric forwards traffic from a vPC domain to a non-vPC connected host in the fabric, and vice-versa.

*Figure 8: vPC forwarding*

Unicast packet flow H2 -> H1
1. H2 sends a pkt towards H1 on its link to S3.
2. S3 does a table lookup and routes with vPC Virtual IP (VIP).
3. Spine switch sees multiple routes for VIP and picks one of them (S2 in this case).
4. S2 delivers the pkt to locally attached host H1.

H1 -> H2
1. H1 sends a pkt towards H2 on one of its PC link (S1 in this case).
2. S1 does a table lookup and routes with IP of S3.
3. Spine switch routes to S3.
4. S3 delivers the pkt to locally attached host H2.

**Creating VLAN Pools**

In this example, configuring newly-connected bare metal servers first requires creation of a physical domain and then association of the domain to a VLAN pool. As mentioned in the previous section, VLAN pools define a range of VLAN IDs that will be used by the EPGs.

The servers are connected to two different leaf nodes in the fabric. Each server will be tagging using 802.1Q or VXLAN encapsulation. The range of VLANs used in the configuration example is 100-199. As depicted in the following figure, the ACI fabric can also act as a gateway between disparate encapsulation types such as untagged traffic, 802.1Q VLAN tags, VXLAN VNIDs, and NVGRE tags. The leaf switches normalize the traffic by stripping off tags and reapplying the required tags on fabric egress. In ACI, it is important to understand that the definition of VLANs as they pertain to the leaf switch ports is utilized only for identification purposes. When a packet arrives ingress to a leaf switch in the fabric, ACI has to know beforehand how to classify packets into the different EPGs, using identifiers like VLANs, VXLAN, NVGRE, physical port IDs, virtual port IDs.
Creating a VLAN Pool Using the GUI

This procedure creates a VLAN pool using the GUI.

Procedure

**Step 1** On the menu bar, choose Fabric > Access Policies.

**Step 2** In the Navigation pane, choose Pools > VLAN.

**Step 3** In the Work pane, choose Actions > Create VLAN Pool.

**Step 4** In the Create VLAN Pool dialog box, perform the following actions:

a) Enter a name for the VLAN pool.

b) (Optional) Enter a description for the VLAN pool.

c) Choose an allocation mode:

   - **Dynamic Allocation**—The Application Policy Infrastructure Controller (APIC) selects VLANs from the pool dynamically. This is common in VMM integration mode where the actual VLAN ID is not important since policies are applied to the EPG itself.

   - **Static Allocation**—This is typically used when the pool will be referenced from a static source, such as a static path binding for an EPG for use with bare metal servers.

d) Add one or more encapsulation blocks.

   The encapsulation blocks define the range of VLANs in the VLAN pool. Multiple ranges can be added to a single pool. Choose an allocation mode for each encapsulation block:

   - **Dynamic Allocation**—The Application Policy Infrastructure Controller (APIC) selects VLANs from the pool dynamically. This is common in VMM integration mode where the actual VLAN ID is not important since policies are applied to the EPG itself.

   - **Inherit Allocation Mode from parent**—The encapsulation block inherits its mode based on the VLAN pool.

   - **Static Allocation**—This is typically used when the pool will be referenced from a static source, such as a static path binding for an EPG for use with bare metal servers.
Creating a VLAN Pool Using the REST API

The following example REST request creates a VLAN pool:

```xml
<fvnsVlanInstP allocMode="static" configIssues="" descr="">
    dn="uni/infra/vlanns-[bsprint-vlan-pool]-static" lcOwn="local"
    modTs="2015-02-23T15:58:33.353-08:00"
    monPolDn="uni/fabric/monfab-default" name="bsprint-vlan-pool"
    ownerKey="" ownerTag="" status="" uid="8131">
        <fvnsRtVlanNs childAction="" lcOwn="local"
            modTs="2015-02-25T11:35:33.365-08:00"
            rn="rtinfraVlanNs-[uni/l2dom-JC-L2-Domain]" status="" tCl="l2extDomP"
            tDn="uni/l2dom-JC-L2-Domain"/>
        <fvnsRtVlanNs childAction="" lcOwn="local"
            modTs="2015-02-23T16:13:22.007-08:00"
            rn="rtinfraVlanNs-[uni/phys-bsprint-PHY]" status="" tCl="physDomP"
            tDn="uni/phys-bsprint-PHY"/>
        <fvnsEncapBlk childAction="" descr="" from="vlan-100" lcOwn="local"
            modTs="2015-02-23T15:58:33.353-08:00"
            name="" rn="from-[vlan-100]-to-[vlan-199]" status="" to="vlan-199" uid="8131"/>
    </fvnsVlanInstP>
```}

Creating a Physical Domain

A physical domain acts as the link between the VLAN pool and the Access Entity Profile (AEP). The domain also ties the fabric configuration to the tenant configuration, as the tenant administrator is the one who associates domains to EPGs, while the domains are created under the fabric tab. When configuring in this order, only the profile name and the VLAN pool are configured. The creation of the AEP and its association will be covered later in this section.

XML Object

```xml
<physDomP childAction="" configIssues="" dn="uni/phys-bsprint-PHY" lcOwn="local"
    name="bsprint-PHY" ownerKey="" ownerTag="" status="" uid="8131">
    <infraRsVlanNs childAction="" forceResolve="no" lcOwn="local"
        modTs="2015-02-23T16:13:22.065-08:00"
        monPolDn="uni/fabric/monfab-default"
        rType="mo"
        rn="rsvlanNs"
        state="formed"
        stateQual="none"
        status=""
        tCl="fvnsVlanInstP"
        tDn="uni/infra/vlanns-[bsprint-vlan-pool]-static"
        tType="mo"
        uid="8131"/>
    <infraRsVlanNsDef childAction="" forceResolve="no" lcOwn="local"
        modTs="2015-02-23T16:13:22.065-08:00"
        rType="mo"
        rn="rsvlanNsDef"
        state="formed"
        stateQual="none"
        status=""
        tCl="fvnsVlanInstP"
        tDn="uni/infra/vlanns-[bsprint-vlan-pool]-static"
        tType="mo"
        uid="8131"/>
    <infraRtDomP childAction="" lcOwn="local"
        modTs="2015-02-23T16:13:52.945-08:00"
        rtDn="[uni/infra/attentp-bsprint-AEP]"
        status="" tCl="infraAttEntityP"
        tDn="uni/infra/attentp-bsprint-AEP"/>
</physDomP>
```}

Creating an Attachable Access Entity Profile Using the GUI

This procedure creates an attachable access entity profile (AEP) using the GUI.

**Procedure**

**Step 1** On the menu bar, choose Fabric > Access Policies.

**Step 2** In the Navigation pane, choose Global Policies > Attached Acess Entity Profile.
Step 3  In the Work pane, choose Actions > Create Attached Entity Profile.

Step 4  In the Create Attached Entity Profile dialog box, perform the following actions:
   a) Enter a name for the AEP.
   b) (Optional) Enter a description for the AEP.
   c) Put a check in the Enable Infrastructure VLAN box if you want to allow the infrastructure VLAN to be passed over the links that are associated with this AEP.
   d) Click + to associate the domain to the AEP.
   e) Choose the physical domain that was previously configured.

Step 5  Click Next.

Step 6  Click Submit.

Creating an Attachable Access Entity Profile Using the REST API

The following example REST request creates an attachable access entity profile (AEP):

```xml
<infraAttEntityP childAction="" configIssues="" descr="" dn="uni/infra/attentpbsprint-AEP" lcOwn="local" modTs="2015-02-23T16:13:52.874-08:00" monPolDn="uni/fabric/monfab-default" name="bsprint-AEP" ownerKey="" ownerTag="" status="" uid="8131">
   <infraContDomP childAction="" lcOwn="local" modTs="2015-02-23T16:13:52.874-08:00" rn="domcont" status=""/>
      <infraAssocDomP childAction="" dompDn="uni/phys-bsprint-PHY" lcOwn="local" modTs="2015-02-23T16:13:52.961-08:00" rn="assocomp-[uni/phys-bsprint-PHY]" status=""/>
      <infraAssocDomP childAction="" dompDn="uni/l2dom-JC-L2-Domain" lcOwn="local" modTs="2015-02-25T11:35:33.570-08:00" rn="assocomp-[uni/l2dom-JC-L2-Domain]" status=""/>
   </infraContDomP>
   <infraContNS childAction="" lcOwn="local" modTs="2015-02-23T16:13:52.874-08:00" monPolDn="uni/fabric/monfab-default" rn="nscont" status=""/>
      <infraRsToEncapInstDef childAction="" deplSt="" forceResolve="no" lcOwn="local" modTs="2015-02-23T16:13:52.961-08:00" monPolDn="uni/fabric/monfab-default" rType="mo" rn="rstoEncapInstDef-[allocencap-[uni/infra]/encapsdef-[uni/vlanns-[bsprint-vlan-pool]-static]]" state="formed" stateQual="" status="" tCl="stpEncapInstDef" tDn="allocencap-[uni/infra]/encapsdef-[uni/vlanns-[bsprint-vlan-pool]-static]" tType="mo">
      <fabricCreatedBy childAction="" creatorDn="uni/l2dom-JC-L2-Domain" deplSt="" domainDn="uni/l2dom-JC-L2-Domain" lcOwn="local" modTs="2015-02-25T11:35:33.570-08:00" monPolDn="uni/fabric/monfab-default" profileDn=""
      rn="source-[uni/l2dom-JC-L2-Domain]" status=""/>
      <fabricCreatedBy childAction="" creatorDn="uni/phys-bsprint-PHY" deplSt="" domainDn="uni/phys-bsprint-PHY" lcOwn="local" modTs="2015-02-23T16:13:52.961-08:00" monPolDn="uni/fabric/monfab-default" profileDn=""
      status=""/>
   </infraRsToEncapInstDef>
   <infraRtAttEntP childAction="" lcOwn="local" modTs="2015-02-24T11:59:37.980-08:00" rn="rattEntP-[uni/infra/funcprof/accportgrp-bsprint-AccessPort]" tCl="infraAccPortGrp" tDn="uni/infra/funcprof/accportgrp-bsprint-AccessPort"/>
   <infraRsDomP childAction="" forceResolve="no" lcOwn="local" modTs="2015-02-25T11:35:33.570-08:00" monPolDn="uni/fabric/monfab-default" rType="mo" rn="rdomP-[uni/l2dom-JC-L2-Domain]" state="formed" stateQual="" status="" tCl="l2extDomP" tDn="uni/l2dom-JC-L2-Domain" tType="mo" uid="8754"/>
   <infraRsDomP childAction="" forceResolve="no" lcOwn="local" modTs="2015-02-23T16:13:52.961-08:00" monPolDn="uni/fabric/monfab-default" rType="mo"
Create Interface Policies

Next, define the interface profiles and showcase the re-usability of the fabric policies. Interface policies can be re-used as needed by different interface profile definition requirements. This section will illustrate creation of new profiles, but ideally there are already policies in place that can simply be selected.

Creating a Link Level Policy

Link level policies dictate configuration like the speed of ports.

XML Object

```xml
<fabricHIfPol autoNeg="on" childAction="" descr="" dn="uni/infra/hintfpol-1G-Auto" lcOwn="local" linkDebounce="100" modTs="2015-01-14T06:47:15.693-08:00" name="1G-Auto" ownerKey="" ownerTag="" speed="1G" status="" uid="15374"/>
```

Creating a CDP Interface Policy

XML Object

```xml
<cdpIfPol adminSt="enabled" childAction="" descr="" dn="uni/infra/cdpIfP-CDP-Enable" lcOwn="local" modTs="2015-01-14T06:47:25.470-08:00" name="CDP-Enable" ownerKey="" ownerTag="" status="" uid="15374"/>
```

Creating an LLDP Interface Policy

XML Object

```xml
<lldpIfPol adminRxSt="enabled" adminTxSt="enabled" childAction="" descr="" dn="uni/infra/lldpIfP-LLDP-Enable" lcOwn="local" modTs="2015-02-11T07:40:35.664-08:00" status=""/>
Creating a Port Channel Policy Using the GUI

This procedure creates a Port Channel policy using the GUI.

Procedure

**Step 1** On the menu bar, choose **Fabric > Access Policies**.

**Step 2** In the Navigation pane, choose **Interface Policies > Policies > Port Channel Policies**.

**Step 3** In the Work pane, choose **Actions > Create Port Channel Policy**.

**Step 4** In the **Create Port Channel Policy** dialog box, perform the following actions:

a) Enter a name for the Port Channel policy.

b) (Optional) Enter a description for the Port Channel policy.

c) Choose the LACP mode that is required for the server.

   If LACP is enabled on the leaf switch, LACP must also be enabled on the server or other connected device.

d) (Optional) Choose a control state.

e) (Optional) Specify the minimum and maximum number of links in the Port Channel.

**Note** Click i icon in the top-right corner of the **Create Port Channel Policy** dialog box to access the **Cisco APIC Online Help** file and view the full list of options.

**Step 5** Click **Submit**.

Creating a Port Channel Policy Using the REST API

The following example REST request creates a Port Channel policy:

```xml
<lacpLagPol childAction="" ctrl="fast-sel-hot-stdby,graceful-conv,susp-individual" descr="" dn="uni/infra/lacplagp-LACP-Active" lcOwn="local" maxLinks="16" minLinks="1" modTs="2015-02-24T15:58:36.547-08:00" mode="active" name="LACP-Active" ownerKey="" ownerTag="" status="" uid="8131" /
<lacpRtLacpPol childAction="" lcOwn="local" modTs="2015-02-24T14:59:11.154-08:00" rn="rtinfraLacpPol-[uni/infra/funcprof/accbundle-ACI-VPC-IPG]" status=""
 tCl="infraAccBndlGrp" tDn="uni/infra/funcprof/accbundle-ACI-VPC-IPG" />
<lacpLagPol>
```
• To enable symmetric hashing, add `ctrl="symmetric-hash"` to the REST request.

• Symmetric hashing is not supported on the following switches:
  - Cisco Nexus 93128TX
  - Cisco Nexus 9372PX
  - Cisco Nexus 9372PX-E
  - Cisco Nexus 9372TX
  - Cisco Nexus 9372TX-E
  - Cisco Nexus 9396PX
  - Cisco Nexus 9396TX

---

**Creating a Port Channel Member Profile Using the GUI (Optional)**

This procedure creates a Port Channel member profile using the GUI.

**Procedure**

**Step 1**
On the menubar, choose **Fabric > Access Policies**.

**Step 2**
In the Navigation pane, choose **Interface Policies > Policies > Port Channel Member Policies**.

**Step 3**
In the Work pane, choose **Actions > Create Port Channel Member Policy**.

**Step 4**
In the **Create Port Channel Member Policy** dialog box, perform the following actions:

a) Enter a name for the policy.
b) (Optional) Enter a description for the policy.
c) If required, change the priority.
d) If required, change the transmit rate.

**Step 5**
Click **Submit**.

---

**Creating a Spanning Tree Interface Policy Using the GUI (optional)**

The Spanning Tree policy dictates the behavior of southbound leaf port Spanning Tree features. It is a common best practice to enable BPDU guard on interfaces connected to servers.

**Note**
ACI does not run Spanning Tree on the fabric between the leaves and spines. The Spanning Tree interface policy simply defines the port behavior.

1. On the menu bar, choose **Fabric > Access Policies**.
2. In the Navigation pane, choose **Interface Policies > Policies > Spanning Tree Interface**.
3. In the Work pane, choose **Actions > Create Spanning Tree Interface Policy**.

4. In the **Create Spanning Tree Interface Policy** dialog box, perform the following actions:
   
   a. Define a meaningful name for the policy.
   
   b. Optionally, provide a description for the policy.
   
   c. Enable BPDU filter and/or BPDU guard.

5. Click **Submit**.

**Creating a Storm Control Policy Using the GUI (optional)**

A traffic storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance. The traffic storm control feature can be used to prevent disruptions on ports by a broadcast, multicast, or unicast traffic storm on physical interfaces.

1. On the menu bar, choose **Fabric > Access Policies**.

2. In the Navigation pane, choose **Interface Policies > Policies > Storm Control**.

3. In the Work pane, choose **Actions > Create Storm Control Policy**.

4. In the **Create Storm Control Policy** dialog box, perform the following actions:
   
   a. Define a meaningful name for the policy.
   
   b. Optionally, provide a description for the policy.
   
   c. Specify how the control policy is to be applied, either through percentage of the total bandwidth or as a packet per second definition that matches the requirement for the data center.

5. Click **Submit**.

**Creating a Mis-cabling Protocol Interface Policy Using the GUI (Optional)**

The mis-cabling protocol (MCP) was designed to handle misconfigurations that Link Layer Discovery Protocol (LLDP) and Spanning Tree Protocol (STP) are unable to detect. MCP has a Layer 2 packet that it uses, and MCP disables ports that form a loop within the Fabric. Cisco Application Centric Infrastructure (ACI) fabric leafs do not participate in spanning tree protocol (STP) and act as hub with respect to STP. The untagged MCP packet is sent, and if the fabric sees that the packet comes back in, then the fabric knows that there is a loop and the fabric takes action based on that event. Faults and events are generated when this happens. MCP can be enabled globally and per-interface. By default, MCP is disabled globally and is enabled on each port. For MCP to work, it must be enabled globally, regardless of the per-interface configuration.

The following procedure creates an MPC interface policy using the GUI.

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>On the menu bar, choose <strong>Fabric &gt; Access Policies</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>In the Navigation pane, choose <strong>Interface Policies &gt; Policies &gt; MCP Interface</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the Work pane, choose <strong>Actions &gt; Create Mis-cabling Protocol Interface Policy</strong>.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the <strong>Create Mis-cabling Protocol Interface Policy</strong> dialog box, perform the following actions:</td>
</tr>
</tbody>
</table>
a) Enter a name for the policy.
b) (Optional) Enter a description for the policy.
c) For the Admin State, choose Enable to enable the policy, or Disable to disable the policy.

Step 5

Click Submit.

Creating a Layer 2 Interface Policy to Enable Per Port-VLAN Using the GUI

2. In the Navigation pane, choose Interface Policies > Policies > L2 Interface.
3. In the Work pane, choose Actions > Create L2 Interface Policy.
4. In the Create L2 Interface Policy dialog box, perform the following actions:
   a. Give the L2 Interface name and an optional description.
   b. Select VLAN scope to Port Local scope to enable per port-VLAN.

Create Interface Policy Groups

The interface policy groups comprise the interface policies as a functional group that is associated to an interface. The following diagram shows how previously created items are grouped under the policy group.

Figure 10: Policies contained in a policy group

Once all the interface policies have been defined, the individual policies can be brought together to form a policy group that will be linked to the interface profile. The policy group is defined from a master definition that encompasses being one of the following:

- Access Policy Group
- Port Channel Policy Group
- VPC Policy Group

Creating an Access Port Policy Group Using the GUI

The access port policy is defined for an individual link (non-Port Channel or vPC).

2. In the Navigation pane, choose Interface Policies > Policy Groups.


4. In the Create Access Policy Group dialog box, perform the following actions:
   a. Define a meaningful name for the policy group.
   b. Optionally, provide a description for the policy group.
   c. Use the profiles created previously that are relevant for this policy group.

5. Click Submit.

**Creating a Port Channel Interface Policy Group Using the GUI**

Port Channeling also load-balances traffic across the physical interfaces that are members of the channel group. For every group of interfaces that needs to be configured into a port channel, a different policy group has to be created. This policy group defines the behaviour. For example, if ports 1/1-4 are to be configured into one port channel, and ports 1/5-8 into a separate port channel, each of those groups would require the creation of a separate policy group.


2. In the Navigation pane, choose Interface Policies > Policy Groups.

3. In the Work pane, choose Actions > Create PC Interface Policy Group.

4. In the Create PC Interface Policy Group dialog box, perform the following actions:
   a. Define a meaningful name for the policy group.
   b. Optionally, provide a description for the policy group.
   c. Select the policies created previously that are relevant for this PC policy group.

5. Click Submit.

**Create VPC Interface Policy Group**

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>This object must be unique for each vPC created.</td>
</tr>
</tbody>
</table>

A virtual Port Channel (vPC) allows links that are physically connected to two different devices to appear as a single Port Channel to a third device. In the world of ACI, pairs of leaf switches may be configured in a vPC domain so that downstream devices can be active-active dual-homed.

For every group of interfaces that are to be configured into a vPC, a different interface policy group needs to be created. The vPC policy group contains both the definition for the behaviour of the port channel, and the identifier. For example, if ports 1/1-4 are to be configured into one vPC across two switches, and ports 1/5-8 into a separate vPC across two switches, each of those groups would require the definition of a separate policy group.
For vPC you will also require a unique vPC domain definition between the two paired switches. More details to follow.

1. On the menu bar, choose **Fabric > Access Policies**.
2. In the Navigation pane, choose **Interface Policies > Policy Groups**.
3. In the Work pane, choose **Actions > Create VPC Interface Policy Group**.
4. In the **Create VPC Interface Policy Group** dialog box, perform the following actions:
   a. Define a meaningful name for the policy group.
   b. Optionally, provide a description for the policy group.
   c. Choose the policies created previously that are relevant for this vPC policy group.
5. Click **Submit**.

**Interface Profile**

The interface profile in ACI links the policy groups that define how the interface is going to behave, and assigns them to specific ports via the concept of interface selector. In turn, the interface profile is eventually tied to a switch profile to specify which leaf switch the referenced ports should be configured. As we continue the process of defining the port profiles, you can observe how we have started at the bottom of this object tree configuring the different profiles. The purposes for all these individual policies that tie together is to maximize policy re-use.

*Figure 11: Interface Profile links to Interface Selector and Interface Policy Group*

The diagram in the previous section provides a visual description of what can be accomplished by grouping the policies that have been defined under the interface profile, and then assigned to ports with interface selectors and the access port policy groups.

**Create Interface Profile**

The interface profile is composed of two primary objects. The interface selector and the access port policy group. The interface selector defines what interfaces will apply the access port policy. The ports that share the same attributes can then be grouped under the same interface profile.

1. On the menu bar, choose **Fabric > Access Policies**.
2. In the Navigation pane, choose **Interface Policies > Profiles**.

3. In the Work pane, choose **Actions > Create Interface Profile**.

4. In the **Create Interface Profile** dialog box, perform the following actions:
   a. Define a meaningful name for the profile.
   b. Optionally, provide a description for the profile.

5. Click **Submit**.

---

**Creating an Interface Selector Using the GUI**

This procedure creates an interface selector using the GUI.

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>On the menu bar, choose <strong>Fabric &gt; Access Policies</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>In the Navigation pane, choose <strong>Interface Policies &gt; Profiles &gt; Name_of_Interface_Profile</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the Work pane, choose <strong>Actions &gt; Create Access Port Selector</strong>.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the <strong>Create Access Port Selector</strong> dialog box, perform the following actions:</td>
</tr>
<tr>
<td></td>
<td>a) Enter a name for the profile.</td>
</tr>
<tr>
<td></td>
<td>b) (Optional) Enter a description for the profile.</td>
</tr>
<tr>
<td></td>
<td>c) Enter the interface IDs.</td>
</tr>
<tr>
<td></td>
<td>d) If the port is connected to a FEX, put a check in the <strong>Connected to FEX</strong> box.</td>
</tr>
<tr>
<td></td>
<td>e) Choose the interface policy group that should be associated to these ports.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click <strong>Submit</strong>.</td>
</tr>
</tbody>
</table>

**Creating an Interface Profile for a Port Channel Using the GUI**

If a server has two or more uplinks to a leaf switch, the links can be bundled into a Port Channel for resiliency and load distribution. To configure this in ACI, create an interface policy group of type **Port Channel** to bundle the interfaces. Different Port Channels require different policy groups.
This procedure creates an interface profile for a Port Channel using the GUI.

**Procedure**

**Step 1**
On the menu bar, choose **Fabric > Access Policies**.

**Step 2**
In the Navigation pane, choose **Interface Policies > Profiles**.

**Step 3**
In the Work pane, choose **Actions > Create Interface Profile**.

**Step 4**
In the **Create Interface Profile** dialog box, perform the following actions:

a) Enter a name for the profile.

b) (Optional) Enter a description for the profile.

**Step 5**
Click **Submit**.

Next, create an interface port selector. Since you will be configuring a Port Channel, the operator will add all of the interfaces required in the Port Channel interface. In this example, interfaces Ethernet 1/1-2 will be configured in one Port Channel and interfaces Ethernet 1/3-4 will be configured in another Port Channel.

**Step 6**
On the menu bar, choose **Fabric > Access Policies**.

**Step 7**
In the Navigation pane, choose **Interface Policies > Profiles > Name_of_Interface_Profile**.
Step 8  In the Work pane, choose Actions > Create Access Port Selector.

Step 9  In the Create Access Port Selector dialog box, perform the following actions:
   a) Enter a name for the profile.
   b) (Optional) Enter a description for the profile.
   c) Enter interface IDs for the first port channel.
   d) Choose the interface policy group.

Step 10 Click Submit.

Step 11 Repeat steps 8 through 10 if you have another Port Channel to add.

Create an Interface Profile for Virtual Port Channel

A vPC domain is always made up of two leaf switches, and a leaf switch can only be a member of one vPC domain. In ACI, that means that the definition of the policies is significant between the two switches. The same policy can be reused between the two switches, and through the vPC domain the pair association can be defined. vPC Switch domain members should be taken into consideration when configuring firmware maintenance groups. By keeping this in mind, firmware upgrades should never impact both vPC switch peers at the same time. More details on this can be found in the Upgrading and Downgrading Firmware section.

For this reason, a switch profile that would represent two separate switch IDs needs to be created. The relationship of these switches to the two ports in the same policy group is defined through the interface profile.

Figure 13: vPC Policy Group

The same process would have to be repeated for every grouped interface on each side that will be a member of the vPC.


2. In the Navigation pane, choose Interface Policies > Profiles.

3. In the Work pane, choose Actions > Create Interface Profile.

4. In the Create Interface Profile dialog box, perform the following actions:
   a. Define a meaningful name for the profile.
   b. Optionally, provide a description for the profile.

5. Click Submit.

6. In the Navigation pane, choose Interface Policies > Profiles > Name_of_Interface_Profile_Created.
7. In the Work pane, choose **Actions > Create Access Port Selector**.

8. In the **Create Access Port Selector** dialog box, perform the following actions:
   a. Define a meaningful name for the profile.
   b. Optionally, provide a description for the profile.
   c. Enter interface IDs.
   d. Select the interface policy group to be used for the vPC port behavior.

9. Click **Submit**.

---

**Create a vPC Domain for Virtual Port Channel**

When configuring a vPC, there is one additional step to be configured once to put two leaf switches into the same vPC domain.

*Figure 14: Creating a vPC Domain*

---

1. On the menu bar, choose **Fabric > Access Policies**.

2. In the Navigation pane, choose **Switch Policies > VPC Domain > Virual Port Channel default**.

3. In the Work pane, choose **Actions > Create Explicit VPC Protection Group**.

4. In the **Create Explicit VPC Protection Group** dialog box, perform the following actions:
   a. Define a meaningful name for the vPC domain.
   b. Provide a unique ID to represent the vPC domain.
   c. Choose the first switch you want to be part of the vPC domain.
   d. Choose the second switch you want to be part of the vPC domain.

5. Click **Submit**.

---

**Switch Profiles**

A switch profile groups all the interface profiles that define the behavior of its respective switch ports. A switch profile could be the definition of a single switch or it could be the definition of multiple switches. As
a best practice, there should be a switch profile for each leaf switch, and an additional switch profile for each vPC domain pair of leaf switches.

The interface profiles that you have created can be associated to the switch through a single switch profile or they can be associated through different switch profiles. If you have various racks that are identical in the way the interface ports are configured, it could be beneficial to utilize the same switch profile. This would make it possible to modify the configuration of many switches during operations without having to configure each switch individually.

Reusability

The capability of policy reusability is crucial to re-emphasize from an operational perspective. If a profile has been defined to configure a port as 1GB speed for example, that profile can be reused for many interface policy groups. When looking at whole switch configurations, the re-usability of the profile can be extended to simplify data center operations and ensure compliance. The following figure illustrates the reusability of profiles across racks of switches.

*Figure 15: Policy re-use at scale*

In the previous diagram, each of the top of rack switches is based on the same switch profile. If all these racks are configured in the same fashion (meaning they are wired in the same way) the same policies could be reused by simply assigning the switches to the same switch profile. It would then inherit the profile tree and be configured the exact same way as the other racks.

It is also important to be aware of the implication of deleting profiles. If a profile has been reused across many devices, make sure to check where it is being used before you delete the profile or policy.
Sample vPC Creation

The following procedure demonstrates what a vPC bringup looks like and also API POST configuration assessment of the vPC. The following topology will be configured:

*Figure 16: Sample Topology*

Creating VLAN Pools
REST :: /api/node/class/fvnsVlanInstP.xml

Creating a Physical Domain
REST :: /api/node/class/physDomP.xml

Creating Access Entity Profile
REST :: /api/node/class/infraAttEntityP.xml

Creating a Link Level Policy
REST :: /api/node/class/fabricHIfPol.xml

Creating a Port Channel Policy
REST :: /api/node/class/lacpLagPol.xml

Creating a vPC Interface Policy Group
REST :: /api/node/class/infraAccBndlGrp.xml

Creating an Interface Profile
REST :: /api/node/class/infraAccPortP.xml

Creating a Switch Profile
REST :: /api/node/class/infraNodeP.xml
Creating a vPC Domain

REST :: /api/node/class/fabricExplicitGEp.xml

Validating the Operation of a Configured vPC Using the GUI

1. On the menu bar, choose Fabric > Inventory.
2. In the Navigation pane, choose POD 1 > Node_Name > Interfaces > vPC Interfaces.
3. In the Work pane, there will be a table that shows the status of the vPC interface. If configured correctly, the status should be displayed and you should see successful establishment of the vPC domain.

Validating the Operation of a Configured vPC Using the CLI

You can validate the operation of the vPC directly from the CLI of the switch itself. If you connect to the console or the out of band management interface of the leaf node you should be able to see the status with the command show vpc.

Leaf-3# show vpc
Legend:
(*) - local vPC is down, forwarding via vPC peer-link
vPC domain id : 100
Peer status : peer adjacency formed ok
vPC keep-alive status : Disabled
Configuration consistency status : success
Per-vlan consistency status : success
Type-2 consistency status : success
vPC role : primary
Number of vPCs configured : 1
Peer Gateway : Disabled
Dual-active excluded VLANs : -
Graceful Consistency Check : Enabled
Auto-recovery status : Enabled (timeout = 240 seconds)
Operational Layer3 Peer : Disabled
vPC Peer-link status
---------------------------------------------------------------------
id Port Status Active vlans
--- ---- ------ --------------------------------------------------
1 up -
vPC status
---------------------------------------------------------------------
id Port Status Consistency Reason Active vlans
-- ---- ------ ------------- ------ ------------
1 Po1 up success success

The following REST API call can be used to build vPCs and attach vPCs to static port bindings.

URL: https://{{apic-ip}}/api/policymgr/mo/.xml
<polUni>
<infraInfra>
<!-- Switch Selector -->
<infraNodeP name="switchProfileforVPC_201">
<infraLeafS name="switchProfileforVPC_201" type="range">
infraNodeBlk name="nodeBlk" from="201" to="201"/>
</infraLeafS>
infraRsAccPortP tDn="uni/infra/accportprof-intProfileforVPC_201"/>
</infraNodeP>
infraRsAccPortP tDn="uni/infra/accportprof-intProfileforVPC_202"/>
</infraNodeP>
infraLeafS name="switchProfileforVPC_202" type="range">
infraNodeBlk name="nodeBlk" from="202" to="202"/>
</infraLeafS>
infraRsAccPortP tDn="uni/infra/accportprof-intProfileforVPC_202"/>
Server Connectivity

Server connectivity is necessary for all application workloads to function properly on the Cisco Application Centric Infrastructure (ACI) fabric. The fabric connectivity requirements that are dictated by the server infrastructure must be carefully considered. In the case of Cisco Unified Computing System (UCS), fabric access policies must be provisioned to match these requirements. These policies are all governed by interface policy groups. ACME Inc. has several different models of servers in their data centers, such as Cisco UCS B and C series, as well as some third party servers that all need to be connected to the ACI fabric.

Cisco UCS B-Series Servers

When connecting UCS to the ACI fabric, the type of Layer 2 connection needed on the Fabric Interconnect facing ports must be determined first. A best practice is to leverage a virtual port channel (vPC) to connect the UCS environment so as to create a multi-chassis etherchannel. In this scenario, individual link and fabric switch failures are mitigated to maintain a higher expected up time.
For more information on the process needed to configure links to UCS as either a vPC or a traditional port channel, see the Adding New Devices to the Fabric section.

**Standalone Rack Mount Servers or Non-Cisco Servers**

Any non-UCS server architecture can also be connected directly to the ACI fabric or to a Cisco Nexus 2000 Fabric Extender (FEX). When being connected to the ACI fabric, the kind of traffic expected out of the server links needs to be determined. If the workload is a bare metal server, traffic can be classified on a per port basis and associated AEPs and EPGs can be mapped appropriately to match the tagged or untagged traffic. If a supported hypervisor is to be used, a Virtual Machine Manager (VMM) domain must be properly configured, and then associated with the corresponding ports on the fabric as a hypervisor that is facing through EPG and AEP mapping. The key is to map the expected traffic classification to the ports that are connected to the server infrastructure.

Utilizing a FEX is an alternative way to connect host devices into the ACI fabric. Restrictions that are present in NX-OS mode such that non-host-facing ports are not supported, are still true. Ports must only be connected to hosts, and connectivity to any other network device will not function properly. When utilizing a FEX, all host-facing ports are treated the same way as if they were directly attached to the ACI fabric.

## Virtual Machine Networking

### Understanding VM Networking in ACI

One of the most common uses of the Cisco Application Centric Infrastructure (ACI) will be to help manage and deploy applications in virtual environments. The ACI provides the ability to manage both virtual and physical endpoints with the same set of policies. This chapter will look at various operational tasks that will be performed throughout the daily operations.

The following list describes some virtual machine manager (VMM) system terms:

- A virtual machine controller is an external VMM entity, such as VMware vCenter, VMware vShield, and Microsoft Systems Center Virtual Machine Manager (SCVMM). The Application Policy Infrastructure Controller (APIC) communicates with the VMM to publish network policies that are applied to virtual workloads. A virtual machine controller administrator provides an APIC administrator with a virtual machine controller authentication credential; multiple controllers of the same type can use the same credential.
- Credentials represent the authentication credentials to communicate with virtual machine controllers. Multiple controllers can use the same credentials.
- A pool represents a range of traffic encapsulation identifiers, such as VLAN and VXLAN IDs, and multicast addresses. A pool is a shared resource and can be consumed by multiple domains, such as VMM and Layer 4 to Layer 7 services. A leaf switch does not support overlapping VLAN pools. Different overlapping VLAN pools must not be associated with the same attachable entity profile (AEP).
- The two types of VLAN-based pools are as follows:
  - Dynamic pools - Managed internally by the APIC to allocate VLANs for endpoint groups (EPGs). A VMware vCenter domain can associate only to a dynamic pool. This is the pool type that is required for VMM integration.
  - Static pools - The EPG has a relation to the domain, and the domain has a relation to the pool. The pool contains a range of encapsulated VLANs and VXLANs. For static EPG deployment, the user
defines the interface and the encapsulation. The encapsulation must be within the range of a pool that is associated with a domain with which the EPG is associated.

When creating dynamic VLAN pools for VMM integration, the VLAN range must also be created on any intermediate devices, such as traditional switches or blade switches. This includes creating the VLANs on Unified Computing System (UCS).

**ACI VM Integration Workflow**

*Figure 17: ACI VM Integration Workflow*

For detailed information on how to deploy the VMware vSphere Distributed Switch with the Application Policy Infrastructure Controller (APIC) Application Policy Infrastructure Controller (APIC), see the *Cisco APIC Getting Started Guide*.

For detailed information and the workflow for how to enable integration of Microsoft SCVMM with Cisco Application Centric Infrastructure (ACI), see the *Cisco ACI with Microsoft SCVMM Workflow* document.
VMware Integration

When integrating Cisco Application Centric Infrastructure (ACI) into your VMware infrastructure, you have two options for deploying networking. VMware domains can be deployed, leveraging the VMware vSphere Distributed Virtual Switch (DVS) or the Cisco Application Virtual Switch (AVS). Both provide similar basic virtual networking functionality; however, the AVS provides additional capabilities, such as VXLAN and microsegmentation support. ACME Inc. has chosen to leverage the additional features provided by AVS. For organizations interested in using the standard DVS provided by VMware, see the following document:


The ACI 1.2 release supports vCenter 6.0 and the following features for DVS only:

- vMotion across DVS with a data center
- vMotion across a data center within the same vCenter
- vMotion across vCenter
- Upgrading an ACI deployment using vSphere 5.1 and 5.5 to vSphere 6.0
- vShield 5.5 with vSphere 6.0
- NSX manager 6.1 with vSphere 6.0

The following feature is not supported:

- Long distance vMotion

VMM Policy Model Interaction

Shown below are some of the various ACI policies which are involved with setting up VM Integration. This serves as a reference for the ways the various policies are related to each other.

*Figure 18: VMM Policy Model Interaction*
Publishing EPGs to a VMM Domain

This section will detail how to publish an existing endpoint group (EPG) to a Virtual Machine Manager (VMM) domain. For details on how to create EPGs, see the Tenants section.

For an EPG to be pushed to a VMM domain, a domain binding within the tenant EPG must be created.

1. On the menu bar, choose Tenants > ALL TENANTS
2. In the Work pane, choose the Tenant_Name.
3. In the Navigation pane, choose Tenant_Name > Application Profiles > Application_Profile_Name > Application EPGs > Application_EPG_Name > Domains (VMs and Bare-Metals).
4. In the Work pane, choose Actions > Add VM Domain Association.
5. In the Add VM Domain Association dialog box, choose the VMM Domain Profile that you previously created.
   a. For the Deployment and Resolution Immediacy, Cisco recommends keeping the default option of On Demand. This provides the best resource usage in the fabric by only deploying policies to Leaf nodes when endpoints assigned to this EPG are connected. There is no communication delay or traffic loss by keeping the default selections.
6. Click Submit. The EPG will now be available as a Port Group to your VMM.

Connecting Virtual Machines to the Endpoint Group Port Groups on vCenter

1. Connect to your vCenter using the VI Client.
2. From the Host and Clusters view, right click on your Virtual Machine and choose Edit Settings.
3. Click on the Network Adapter, and in the Network Connection drop-down box, choose the Port Group which corresponds to your EPG. It should display in the format of [TENANT | APPLICATION_PROFILE | EPG | VMM_DOMAIN_PROFILE]

If you do not see your Cisco Application Centric Infrastructure (ACI) EPG in the Network Connection list, it means one of the following:

- The VM is running on a host which is not attached to the Distributed Switch managed by the Application Policy Infrastructure Controller (APIC).
- There may be a communication between your APIC and vCenter either through the OOB or INB management network.

Microsoft SCVMM Integration

The following figure shows a representative topology of a System Center Virtual Machine Manager (SCVMM) deployment with Cisco Application Centric Infrastructure (ACI). Hyper-V clustering connectivity between SCVMM virtual machines and the Application Policy Infrastructure Controller (APIC) can run over the management network.
The following figure illustrates the workflow for integrating Microsoft SCVMM with Cisco Application Centric Infrastructure (ACI):
Figure 20: ACI SCVMM Workflow

For more information about the workflow for integrating Microsoft SCVMM with ACI, see the Cisco ACI with Microsoft SCVMM Workflow document.

Mapping of ACI and SCVMM Constructs

The following figure shows the mapping of Cisco Application Centric Infrastructure (ACI) and SCVMM constructs (SCVMM Controller, Cloud, and Logical Switches).
One VMM domain cannot map to the same SCVMM more than once. An Application Policy Infrastructure Controller (APIC) controller can be associated up to 5 SCVMM controllers. For additional information on other limitations, see the Verified Scalability Guide for Cisco ACI.

Mapping Multiple SCVMMs to an APIC Controller

When multiple SCVMMs are associated with an Application Policy Infrastructure Controller (APIC) controller, the Opflex certificate from the first SCVMM controller must be copied to the secondary controller and other controllers, as applicable. Use the `certlm.msc` command on the local SCVMM controller to import the certificate to the following location:

```
Certificates - Local Computer > Personal > Certificates
```

The same Opflex certificate is deployed on the Hyper-V servers that are managed by this SCVMM controller. Use the `mmc` command to install the certificate on the Hyper-V servers.

Verifying that the OpFlex Certificate is Deployed for a Connection from the SCVMM to the APIC

You can verify that the OpFlex certificate is deployed for a connection from the SCVMM to the Application Policy Infrastructure Controller (APIC) by viewing the `Cisco_APIC_SCVMM_Service.log` file, which is located in the `C:\Program Files (x86)\ApicVMMService\Logs\` directory. In the file, check for the following things:

- The correct certificate is used
- There was a successful login to the APIC

The following example log file highlights these things:

```
2/22/2016 1:14:07 PM-1044-13||UpdateCredentials||new: EndpointAddress: Called_from_SCVMM_PS,
```
Verifying VMM deployment from the APIC to the SCVMM

You can verify that the OpFlex certificate is deployed on the Hyper-V server by viewing log files in the C:\Program Files (x86)\ApicHyperAgent\Logs directory. In the file, check for the following things:

- The correct certificate is used.
- The connection with the Hyper-V servers on the fabric leaves is established.

In the SCVMM, check for the following things:

- Under Fabric > Logical Switches, verify that "apicVswitch_VMMdomainName" is deployed from the Application Policy Infrastructure Controller (APIC) to the SCVMM.
- Under Fabric > Logical Networks, verify that "apicLogicalNetwork_VMMdomainName" is deployed from APIC to the SCVMM.
- Under Fabric > Port Profiles, verify that "apicUplinkPortProfile_VMMdomainName" is deployed. If not, go to the host under Servers; right click the host and choose Properties. Go to Virtual Switches and ensure that the physical adapters are attached to the virtual switches.
- A VTEP Virtual Network Adapter is added to the virtual switch and an IP address is assigned to the VTEP adapter.

In the APIC GUI, the Hyper-V servers and the virtual machines will not appear under the Microsoft SCVMM inventory until the first 3 bullets items for the SCVMM are satisfied.

Other Troubleshooting Tips for Verifying VMM Deployment

- The logs for the APIC_SCVMM_Service agent and the APIC_Hyper-V agent are in the respective C:\Program Files (x86)\ApicVMMService and C:\Program Files (x86)\ApicHypervAgent directories.
- There are support scripts for these services. The support scripts can be run in debug mode to provide more insight on the service status/configuration on the SCVMM controller or Hyper-V server respectively.

To use the support scripts:
Verifying Virtual Endpoint Learning

Once the VMs are connected to the appropriate port group/EPG, you should verify the APIC has learned your virtual endpoint.

Verifying VM Endpoint Learning on the APIC from the GUI

1. On the menu bar, choose Tenants > ALL TENANTS.
2. In the Work pane, choose the Tenant_Name.
3. In the Navigation pane, choose Tenant_Name > Application Profiles > Application_Profile_Name > Application EPGs > Application_EPG_Name.
4. In the Work pane, choose the Operational tab. Note: The current tab should display CLIENT ENDPOINTS. All endpoints either virtual or physical will be displayed. From here you should be able to find your Virtual Machine by filtering the "Learning Source" column for rows with values of "Learned VMM".

Verifying VM Endpoint Learning on the APIC from the CLI

You can verify the same info as above from the CLI by using the 'moquery' (ManagedObject Query) command and adding two filters. One for the Distinguished Name (DN) name of your EPG, and one for the Class Name of 'fvCEp' (Fabric Vector Client Endpoint)

`moquery -c fvCEp --dn uni/tn-<TENANT_NAME>/ap-<APP_PROFILE_NAME>/epg-<EPG_NAME>`

You can determine the DN of your EPG by right clicking on the EPG in the GUI, selecting "Save As" and looking at the XML object. From this file you will see the DN entry for the particular EPG:

```
<imdata totalCount="1"><fvAEPg uid="15374" triggerSt="triggerable" status="" scope="2588672" prio="unspecified" pcTag="49159" name="epg-od" monPolDn="uni/tn-common/monepg-default" modTs="2015-02-06T06:46:24.729+11:00" matchT="AtleastOne" lcOwn="local" dn="uni/tn-mb-tennant1/ap-mb-app-pro/epg-epg-od" descr="" configSt="applied" configIssues="" childAction="" /></imdata>
```

Next, use this DN with the moquery to return the list of client Enpoints for this EPG:

```
admin@apic1:~> moquery -c fvCEp --dn uni/tn-mb-tennant1/ap-mb-app-pro/epg-epg-od
Total Objects shown: 1
# fv.CEp
name : 00:50:56:BB:8C:6A
childAction :
dn : uni/tn-mb-tennant1/ap-mb-app-pro/epg-epg-od/cep-00:50:56:BB:8C:6A
encap : vlan-211
id : 0
idepdn :
ip : 10.10.10.10
lcC : learned,vmm
lcOwn : local
mac : 00:50:56:BB:8C:6A
```
VMware Integration Use Case

A VMware administrator in ACME requests the network team to trunk a set of VLANs down to the ESX hosts to provide connectivity to their DVS switches. Rather than trunking VLANs on a per server basis, the network team decides to leverage a new methodology to be more agile and leverage the on-demand provisioning of resources where and when they are needed, as well as providing unlimited Layer 2 mobility for all the VM hosts within the ACI fabric.

To do so, the network admins work with the VMware admins to decide on a range of VLANs that will be provided dynamically by APIC to the ESX hosts that need them. They decide on an unused VLAN range of (600 - 800). This is their dynamic VLAN pool. Once this is decided, the APIC administrator proceeds to configure VMM integration in the APIC GUI by providing the vCenter credentials to APIC. APIC dynamically provisions all EPGs and makes them available to the ESX hosts as a port-group.

Note: The APIC does not automatically move VMNICs into the port-group. This allows VMware admins to maintain control and move virtual NICs into these port-groups on demand.

As the VMware admin provisions ESX hosts and selects the appropriate port-groups for VMs, the APIC dynamically communicates with vCenter to make EPGs available through port groups. The APIC also configures VLAN IDs on the leaf-switches as needed.

During a vMotion event, APIC is automatically informed of the VM move and then updates the endpoint tracking table to allow seamless communication. VMs are allowed to move anywhere within the ACI fabric with no restrictions other than those imposed by vCenter.

It is important to note that ACME can still choose to deploy traditional VLAN trunking down to VMware DVS switches by statically provisioning EPGs on a per-port basis, and still reap the advantages of the Layer 2-anywhere ACI fabric. However, ACME chose VMM integration as the preferred deployment model as it is the most effective method of breaking down organizational challenges, doing on-demand resource allocation, and getting enhanced visibility and telemetry into both the virtual and physical environments.

Deploying the Application Virtual Switch

Prerequisites for Deploying the Application Virtual Switch

- All switch nodes have been discovered by the fabric
- INB or OOB management connectivity is configured.
- VMware vCenter is installed, configured, and available.
- One or more vSphere hosts are available for deployment to the AVS.
- (Optional) A DNS server policy has been configured to enable connection to a VMM using a hostname.
- A dynamic VLAN pool has been created with enough VLAN IDs to accommodate one VLAN per EPG you plan on deploying to each VMM domain.
Getting Started

The AVS software was designed to operate independently of the APIC software version. This allows either device to be upgraded independently. Always refer to the AVS release notes to confirm if any special considerations may exist.

Just like any software, new versions of the AVS will be released to include new features and improvements. The initial AVS software released was version 4.2.1, followed by version 5.2.1. Refer to the *ACI Ecosystem Compatibility List* document to ensure your desired version of AVS is compatible with the APIC and vSphere versions being run.

The AVS package for either version will include vSphere Installation Bundles (VIBs). Each version of AVS software includes the VIB files for all supported vSphere versions. As of this publication there are two VIBs to support vSphere versions 5.1 and 5.5 (vSphere 5.0 is not supported). These can be downloaded from CCO at the following location:

**AVS 4.2.1 Bundle**
- cross_cisco-vem-v165-4.2.1.2.2.3.0-3.1.1.vib 5.1 VIB
- cross_cisco-vem-v165-4.2.1.2.2.3.0-3.2.1.vib 5.5 VIB

**AVS 5.2.1 Bundle**
- cross_cisco-vem-v172-5.2.1.3.1.3.0-3.1.1.vib
- cross_cisco-vem-v172-5.2.1.3.1.3.0-3.2.1.vib

Install the AVS VIB

Before setting up the AVS configuration on the APIC, the AVS software must be installed in vSphere, referred to as the Virtual Ethernet Module (VEM). This can be achieved in a variety of ways, all of which are discussed in *Cisco Application Virtual Switch Installation Guide*. For a few hosts, this can easily be done manually, but for 10+ hosts it may be easier to leverage the Virtual Switch Update Manager (VSUM) to help automate the installation process.

**Manual Installation**

1. Place the host in **Maintenance mode**.

2. Copy the VIB file to a host. The easiest way to copy the VIB to the host is to leverage the VMware VI Client, navigate to the **Host > Configuration > Storage > Datastore_X**. Right click on the desired datastore and choose **Browse Datastore**. From here, the VIB can be uploaded directly to the host's datastore.

3. SSH into the vSphere host on which the AVS VIB is to be installed. If SSH is not enabled, it can be enabled under the **Host Configuration > Security Profile > SSH**.

4. Install or upgrade the VIB using the **esxcli** command:

   To install the AVS VIB:
   ```bash
   esxcli software vib install -v /<path>/<vibname> --maintenance-mode --no-sig-check
   ```

   To upgrade an existing AVS VIB:
   ```bash
   esxcli software vib update -v /<path>/<vibname> --maintenance-mode --no-sig-check
   ```

   A sample output is shown below:
   ```bash
   # esxcli software vib install -v /vmfs/volumes/datastore1/cross_cisco-vem-v172-5.2.1.3.1.3.0-3.2.1.vib --maintenance-mode --no-sig-check
   ```
Installation Result
Message: Operation finished successfully.
Reboot Required: false
VIBs Installed: Cisco_bootbank_cisco-vem-v172=5.2.1.3.1.3.0-3.2.1
VIBs Removed:
VIBs Skipped:
/vmfs/volumes/53cab6da-55209af3-0ef2-24e9b391de3e # vem version
Running esx version -1623387 x86_64
VEM Version: 5.2.1.3.1.3.0-3.2.1
VSM Version:
System Version: VMware ESXi 5.5.0 Releasebuild-1623387

5. Confirm the VEM is loaded and running.

$ vem status

VEM modules are loaded
Switch Name Num Ports Used Ports Configured Ports MTU Uplinks
vSwitch0 3072 6 128 1500 VMNIC0

VEM Agent (vemdpa) is running

Attachable Access Entity Profile (AEP) and AVS

An important component used by the AVS is the Attachable Entity Profile (AEP). Regardless of using an existing AEP or creating a new one, the Enable Infrastructure VLAN check box must be checked for the AEP policy. This is to ensure that the traffic of interest, such as DHCP request/offer or data packets, can flow through the infrastructure VLAN to the AVS. The AEP defines which VLANs will be permitted on a host facing interface. When a domain is mapped to an endpoint group, the AEP validates that the VLAN can be deployed on certain interfaces. Referring back to the "VMM Policy Model Interaction" diagram from the "VM Networking Overview" chapter, the AEP is what ties the VMM domain to the physical interfaces where the vSphere hosts are connected. The AEP can be created on-the-fly during the creation of the VMM domain itself, but this guide will detail creating the AEP separately first.

Create a New AEP

2. In the Navigation pane, choose Global Policies > Attachable Access Entity Profile.
3. In the Work pane, choose Actions > Create Attachable Access Entity Profile.
4. In the Create Attachable Access Entity Profile dialog box, perform the following actions:
   a. Fill in the AEP wizard information then click Next.
      1. Name: Provide any name to identify the AEP, such as "AVS-AEP".
      2. Enable Infrastructure VLAN: Put a check in this box.
      3. Domains (VMs or Baremetal): Leave blank. This will be covered later in the Publishing EPGs to VMM Domains chapter.
   b. From the next page of the wizard, select the Interface Policy Group your AEP will be associated to. This procedure assumes your Interface Policy Group has already been created. Click the All Interfaces radio button for the desired Interface Policy Group.
Modify an Existing AEP

2. In the Navigation pane, choose Global Policies > Attachable Access Entity Profile.
   a. In the Navigation pane, choose the existing AEP.
   b. In the Work pane, put a check in the Enable Infrastructure VLAN check box.

Note: As mentioned early in this chapter, the Infrastructure VLAN is required for AVS communication to the fabric using the OpenFlex control channel.

VMM Domains for vCenter

A Virtual Machine Manager (VMM) domain defines a virtual infrastructure that will be integrated into ACI. This allows the same policies applied to physical endpoints, to also be applied to virtual endpoints. vCenter VMM Domains are created using either the VMware DVS or Cisco AVS. You cannot change from one to the other. A new VMM Domain will be created from scratch to support AVS deployment.

AVS Switching Modes

The AVS can operate in the following switching modes:

- Local Switching: Supports VXLAN encapsulation or VLAN encapsulation.
  - This switching mode allows Inter-EPG traffic to be switched locally on the AVS.
- No Local Switch only supports VLAN encapsulation.
  - This switching mode sends all traffic (Inter-EPG included) to the Leaf switch.
The decision between using VLAN or VXLAN encapsulation will mandate different VLAN extension requirements outside of the fabric. When using VXLAN encapsulation, only the infra VLAN is required to be extended to the AVS hosts. All traffic between the AVS uplinks and ACI fabric will be encapsulated by VXLAN and transferred using the infrastructure VLAN.

If VLAN encapsulation is preferred, you will need to ensure every VLAN in the VM Domain VLAN pool has been extended between the fabric and AVS host. This includes creating the VLANs on intermediate devices such as UCS and the vNICs for any AVS vSphere hosts.

**Create the VMM Domain for AVS**

Now that the DHCP server policy has been created and AEP created/modified, you can create the VMM domain for the AVS.

1. On the menu bar, choose **VM NETWORKING**.
2. In the Navigation pane, choose the **Policies** tab.
3. In the Work pane, choose **Actions > Create VCenter Domain**.
4. In the **Create vCenter Domain** dialog box, perform the following actions:
   a. **Name**: This value will be used as the AVS "Switchname" displayed in vCenter.
   b. **Virtual Switch**: Cisco AVS
c. **Switching Preference: <Choose Local or No Local Switching>**
   - For **No Local Switching** mode:
     - Multicast Address: <Assign a multicast address to represent your AVS>
     - Multicast Address Pool: <Create a unique Multicast Address Pool large enough to include each AVS vSphere host.>
   - For **Local Switching** mode:
     - Encapsulation: <Choose VLAN or VXLAN based on preference>
       - For **VLAN** Encapsulation:
         - VLAN Pool: <Choose/Create a VLAN pool>
       - For **VXLAN** Encapsulation:
         - Multicast Address: <Assign a multicast address to represent your AVS>
         - Multicast Address Pool: <Create a unique Multicast Address Pool large enough to include each AVS vSphere host.>

d. **Attachable Access Entity Profile**: <Choose the AEP previously created/modified>

e. **vCenter Credentials**: Create a credential set with administrator/root access to vCenter

f. **vCenter**: Add the vCenter details.
   - Name: Friendly name for this vCenter
   - Hostname/IP Address: <DNS or IP Address of vCenter>
   - DVS Version: vCenter Default
   - Datacenter: <Enter the exact Datacenter name displayed in vCenter>
   - Management EPG: <Set to oob or inb Management EPG>
   - Associated Credentials: <Choose the Credential set previously created>
   - Click **OK** to complete the creation of the vCenter.

5. **Click Submit**.

**Verify AVS Deployment on vCenter**

1. In the vCenter client, navigate to **HOME > INVENTORY > NETWORKING** and confirm a new Distributed Virtual Switch folder has been created.
2. Expand this folder to find your AVS, and a few default Port Groups including "uplink" and "vtep".
Adding vSphere Hosts to the AVS

After the AVS has been created in vCenter, you then need to attach hosts to it. To do this you will need at least one unused physical interface (VMNIC) to act as the uplink on each host. AVS uplinks cannot be shared with any other existing vSwitch or vDS.

1. From the vCenter client, navigate to HOME > INVENTORY > NETWORKING.
2. Right click on the newly created AVS switch (not the folder) and choose Add Host...
3. In the Add Host dialog box, choose any vSphere hosts to add to the AVS, and select an unassigned VMNIC uplink.
4. Click Next until the wizard completes, skipping the migration of any virtual adapters or virtual machine networking at this time.

   Note: For blade switch systems such as UCS, the VMNIC interface used must have all necessary VLANS allowed on the interface. In UCS terms, this requires the vNIC within the service profile to have all relevant VLANS active on the vNICs.
5. You should see a new vmk interface created on your distributed switch within vCenter and assigned to the 'vtep' port group. This VMK is your Virtual Tunnel Endpoint (VTEP) interface. The VTEP should have pulled a DHCP address from the APIC from the TEP subnet. As can be seen from the screenshot below, we see that the VMkernel port has received the IP address from the APIC. The APIC uses the same 10.0.0.0/16 pool that is created during the APIC setup to provision the IP address. This implies that we are ready for Opflex communication in between the AVS and the APIC.

   ~ # esxcfg-VMKNIC -l
   Interface Port Group/DVPort IP Family IP Address Netmask Broadcast
   vmk0 Management Network IPv4 172.16.176.54 255.255.255.0 172.16.176.255
   vmk1 vmotion IPv4 192.168.99.54 255.255.255.0 192.168.99.255
   vmk2 9 IPv4 10.0.16.95 255.255.0.0 10.0.255.255

   MAC Address MTU TSO MSS Enabled Type
   00:25:b5:00:00:29 1500 65535 true STATIC
   00:50:56:61:1c:92 1500 65535 true STATIC
   00:50:56:65:3d:b3 1500 65535 true DHCP

Verify AVS on ESX

On the ESX command line, issue the `vemcmd show openflex` command.

Verify that the status: `12 (Active)` is seen as well as the switching mode. Also verify that the GiPO address is the same as the multicast address that was used while creating the VMM domain.

   ~ # vemcmd show openflex
   Status: 12 (Active)
   Dvs name: comp/prov-VMware/ctrlr-[AVS-TEST]-VC/sw-dvs-87
   Remote IP: 10.0.0.30 Port: 8000
   Infra vlan: 4093
   FTEP IP: 10.0.0.32
   Switching Mode: LS
   NS GiPO: 225.127.1.1

Verify on the AVS host - there should be one multicast group per deployed EPG on the host. In the output below, there are three different Virtual Machines connected to different EPGs.
VXLAN Load Balancing

VXLAN load balancing is automatically enabled as soon as more than one VMKNIC is connected to the Cisco AVS. Each VMKNIC can use only one uplink port; you should have an equal number of VMKNICs and uplinks. A maximum of eight VMKNICs can be attached to a Cisco AVS switch. Each of the VMKNICs that you create has its own software-based MAC address. In VXLAN load balancing, the VMKNICs provide a unique MAC address to packets of data that can then be directed to use certain physical NICs (VMNICs).

You need to have as many VMKNICs as the host has VMNICs, up to a maximum of eight. For example, if the host has five VMNICs, you need to add four VMKNICs to enable VXLAN load-balancing; the Cisco Application Policy Infrastructure Controller (APIC) already created one VMKNIC when the host was added to the distributed virtual switch (DVS).

In VMware vSphere Client, you will need to create an additional virtual adapter (VMK) for each AVS uplink. Each vmk interface created for the AVS should be attached to the vtep port group and configured for DHCP. Each VMK interface added is assigned a unique DHCP address from the fabric TEP pool.

IGMP Snooping Policy for AVS

Cisco UCS-B Series Considerations with AVS Deployments

This section of the article will focus the necessary steps to enable AVS through the Cisco UCS-B series.

By default, USC-B FI has IGMP snooping enabled. Due to this, we have to configure an IGMP querier policy on the APIC. The IGMP snooping policy needs to be enabled on the infra tenant.

If we disable IGMP snooping on UCS or other intermediate blade switches, then IGMP policy is not needed since the blade switch will flood the multicast traffic on all the relevant ports.

Create an IGMP Snooping Policy for AVS

1. On the menu bar, choose Tenants > ALL TENANTS.
2. In the Work pane, choose infra.
3. In the Navigation pane, choose infr > Networking > Bridge Domain > default.
   a. In the IGMP Snoop Policy drop-down list, choose Create IGMP Snooping Policy.
   b. Provide a name for the policy, such as "IGMP_Infra".
   c. Click the Fast Leave check box.
   d. Click the Enable Querier check box.
4. Click Submit.
Verify if the IGMP snooping querier is being seen on the UCS Fabric interconnects. In this example, VLAN 4093 is the infra VLAN, and 192.168.0.30 is the bridge domain subnet for the infra bridge domain:

```
ucsb-A(nxos)# show ip igmp snooping querier vlan 4093
Vlan  IP Address   Version Expires Port
4093  192.168.0.30 v3      00:03:46 port-channel1
```

Note
You can verify if IGMP snooping is working properly on the vSphere host CLI by using the `vemcmd show epp multicast` command. The alternate method would be to create an IGMP policy on UCS to disable IGMP snooping, which will cause flooding of the multicast traffic to all endpoints.

Microsegmentation with the Cisco Application Virtual Switch

Microsegmentation (uSeg) with the Cisco Application Virtual Switch (AVS) provides the ability to assign endpoints to endpoint groups automatically based on various attributes. Microsegmentation with Cisco AVS was introduced in Cisco AVS Release 5.2(1)SV3(1.5). This feature is available in the Cisco Application Centric Infrastructure (ACI) for Cisco AVS only; it is not available with VMware Distributed Virtual Switch (DVS). Endpoint groups are now divided into two categories: application endpoint groups and uSeg endpoint groups. Application endpoint groups are what will appear in your VMM, such as vCenter, to be assigned to virtual machines as network port groups. uSeg endpoint groups are implicitly applied to any virtual machine within the same tenant and VMM domain, pending an attribute match.

Microsegmentation policies used by the Cisco AVS are centrally managed by the Application Policy Infrastructure Controller (APIC) and enforced by the fabric. uSeg endpoint groups will not appear to vCenter. When changing a virtual machine's network binding, "uSeg EPG" will not appear as a port group binding option. However, virtual machines are still assigned to their regular application endpoint group in the fabric.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Attribute Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM Name</td>
<td>VM</td>
</tr>
<tr>
<td>VM ID</td>
<td>VM</td>
</tr>
<tr>
<td>VNIC ID</td>
<td>VM</td>
</tr>
<tr>
<td>Hypervisor</td>
<td>VM</td>
</tr>
<tr>
<td>DVS Port-Group</td>
<td>VM</td>
</tr>
<tr>
<td>DVS Name</td>
<td>VM</td>
</tr>
<tr>
<td>MAC Sets</td>
<td>Network</td>
</tr>
<tr>
<td>IP Sets</td>
<td>Network</td>
</tr>
</tbody>
</table>
External Connectivity

Extending ACI to External Layer 2

As mentioned in the introduction of this book, ACME Inc. is a multinational company with multiple data centers. Therefore, ACME Inc. must configure some Layer 2 connectivity. This is necessary for extending Layer 2 connectivity to a Data Center Interconnect (DCI) platform, to further extend connectivity to a remote data center, or simply to extend a Layer 2 domain outside of the fabric to connect in an existing Layer 2 network in a non-ACI fabric.

Extending Endpoint Groups Outside the ACI Fabric

The simplest way to extend an endpoint group (EPG) outside of the ACI fabric is to statically assign a leaf port and VLAN ID to an existing endpoint group. After doing so, all of the traffic received on this leaf port with the configured VLAN ID will be mapped to the EPG, and as such, the configured policy for this EPG will be enforced. The endpoints do not need to be directly connected to the ACI leaf, as the traffic classification will be based on the encapsulation received on a port.

To assign a Layer 2 connection statically on an ACI leaf port to an EPG:

1. On the menu bar, choose Tenants > ALL TENANTS.
2. In the Work pane, choose the Tenant_Name.
3. In the Navigation pane, choose Tenant_Name > Application Profiles > App_Profile_Name > Application EPGs > EPG_Name > Static Bindings (Paths).
4. In the Work pane, choose Action > Deploy Static EPG on PC, vPC or Interface.
   a. In the Path field, specify a port as well as a VLAN ID.
   b. Click one of the Deployment Immediacy radio buttons. Deployment immediacy determines when the actual configuration will be applied on the leaf switch hardware. The immediacy also determines when the hardware resource, such as a VLAN resource and policy content-addressable memory (CAM) to support the related contract for this EPG, will be consumed on the leaf switch. The option Immediate means that the EPG configuration and its related policy configuration will be programmed in the hardware right away. The option On Demand instructs the leaf switch to program the EPG and its related policy in the hardware only when traffic matching this policy is received for this EPG.
   c. Click one of the Mode radio buttons. The mode option specifies whether the ACI leaf expects incoming traffic to be tagged with a VLAN ID or not.
      1. Tagged - The tagged option means that the leaf node expects incoming traffic to be tagged with the specified VLAN ID previously established. This is the default deployment mode. Choose this mode if the traffic from the host is tagged with a VLAN ID. Multiple EPGs can be statically bound to the same interface as long as the encap VLAN/VXLAN ID is unique.
      2. Untagged - The untagged option means that the leaf expects untagged traffic without a VLAN ID. Similar to the switchport access vlan vlan_ID command, with this option you can only assign the interface to one EPG. This option can be used to connect a leaf port to a bare metal server whose network interface cards (NICs) typically generate untagged traffic. A port can have only one EPG statically bound to a port as untagged.
3. **802.1P** - The 802.1P option refers to traffic tagged with 802.1P headers. 802.1P mode is useful when its necessary to handle the traffic on one EPG as untagged to the interface (similar to the `switchport trunk native vlan vlan_ID` command), but (unlike the untagged mode) 802.1P will allow other ‘tagged’ EPGs to be statically bound to the same interface. Any traffic received on links with this mode classification will have the following conditions applied to them.

d. Create a physical domain and VLAN pool that are associated to this physical domain.

e. Associate the physical domain to the EPG in question.

f. Create an attachable access entity profile (AEP) to map the interfaces and policies together.

See the Adding New Devices to the Fabric section for more information on how to configure an AEP and a physical domain.

**Extending an ACI Bridge Domain Outside of the Fabric**

A Layer 2 outside connection is associated with a bridge domain and is designed to extend the whole bridge domain, not just an individual EPG under the bridge domain, to the outside network.

To accomplish an extension of the bridge domain to the outside, a Layer 2 outside connection must be created for the bridge domain. During this process, create a new external EPG to classify this external traffic. This new EPG will be part of the existing bridge domain. Classify any outside connections or endpoints into this new external EPG. With two separate EPGs, you will also need to select which traffic you would like to traverse between the two EPGs. Similar to the previous example of adding an endpoint to a pre-existing EPG, this method will also allow the endpoints to share the same subnet and default gateway.

To create an external Layer 2 domain:

1. On the menu bar, choose **Tenants > ALL TENANTS**.

2. In the Work pane, choose the **Tenant_Name**.

3. In the Navigation pane, choose **Tenant_Name > Networking > External Bridged Network**.

4. In the Work pane, choose **Action > Create Bridged Outside**.

5. In the **Create Bridged Outside** dialog box, perform the following actions:

a. Associate the Layer 2 outside connection with the bridge domain and a VLAN ID. This VLAN must be configured on the external Layer 2 network. This Layer 2 outside connection will put this VLAN and the bridge domain of the ACI fabric under the same Layer 2 domain. This VLAN ID must be in the range of the VLAN pool that is used for the Layer 2 outside connection.

   1. For the **External Bridged Domain** drop-down list, create a Layer 2 domain if one does not already exist.

   2. While creating the Layer 2 domain, if it does not already exist, create a VLAN pool to associate to the VLAN on the Layer 2 outside connection. This is a means to specify the range of the VLAN IDs that will be used for creating a Layer 2 outside connection. This helps avoid any overlapping in the VLAN range between VLANs used for an EPG and those in use for a Layer 2 outside connection.

b. Add a Layer 2 border leaf node and Layer 2 interface for a Layer 2 outside connection.
c. After adding a Layer 2 border leaf and Layer 2 interface, click **Next** to start creating a Layer 2 EPG. Simply provide a name for the Layer 2 EPG. All of the traffic entering the ACI fabric with the designated VLAN (the VLAN ID provided in step 1) will be classified into this Layer 2 EPG.

d. Configure a contract to allow communication between your existing endpoints in the existing EPG and your new external Layer 2 EPG. In the Navigation pane, choose **External Bridged Networks > Networks** and specify a contract to govern this policy as the consumed contract. After specifying this contract as the provided contract for your internal EPG, the communication between this external Layer 2 EPG and your existing internal EPG will be allowed.

e. Create an AEP. This is a policy object that tells the APIC to allow certain encapsulation (VLANs) on selected ports. For more information on how to create a Access Attachable Entity Profile, see the Adding New Devices to the Fabric section.

You should now have the desired reachability between the inside and outside Layer 2 segments.

### Extending ACI to External Layer 3

The most important component of any application is the user or customer, which generally does not directly attach to the fabric, and therefore there must be connected to the external network. ACME must be able to connect to both their internal corporate backbone, as well as to the Internet to provide access to the mobile application. This integration is possible with Cisco Application Centric Infrastructure (ACI) at the tenant policy level. Layer 3 connectivity to a device like a router is known as an **External Routed Network**, and provides IP connectivity between a tenant private network and an external IP network. Each Layer 3 external connection is associated with one tenant private network. The requirement of the Layer 3 external network is only needed when a group of devices in the application profile require Layer 3 connectivity to a network outside of the ACI fabric.

An application profile enables an operator to group the different components, or tiers, of an application into endpoint groups (EPGs). These application components might have requirements for external connectivity into them. The following figure shows part of a simplified fabric:

**Figure 23: A sample application profile for a three-tiered application with contracts between the tiers**

For example, web servers need a connection to the outside world for users to reach them. With ACI, the connectivity is defined by a contract to a defined external Layer 3 endpoint group. As the operator of the fabric, you can provide the tenant administrator with the ability to interface to an external Layer 3 connection in various ways by using a uniquely-defined Layer 3 construct for the tenant application profile or a shared common infrastructure.

External Layer 3 connections are usually established on the border leaf construct of the ACI. Any ACI leaf can become a border leaf. In large scale ACI designs it might be productive to have dedicated ACI leaves as border leaves. It is important to note that the spine nodes cannot have connections to external routers. A border leaf is simply terminology to refer to a leaf that happens to be connected to a Layer 3 device. Other devices, like servers, can still connect to the border leaves. In the ACI fabric, the external Layer 3 connection can be one of the following types:

1. Physical Layer 3 interface
2. Subinterface with 8021.Q tagging
3. Switched Virtual Interface (SVI)

The following figure depicts the logic of public and private networks:

*Figure 24: Application profile with external consumers, public and private networks annotated*

With devices connecting through the external Layer 3 connection, the external network has learned of the internal ACI network 10.1.1.0/24, as it is advertised to the adjacent router through the Layer 3 external connection. For the private networks, ACI does not advertise the networks through the routing protocol to the adjacent Layer 3 router, and the networks are not reachable to devices external to the fabric.

In releases prior to version 1.1 of Cisco Application Policy Infrastructure Controller (APIC), the fabric only advertises subnets that are marked public in the associated bridge domain. Routes that are learned externally from the fabric are not advertised through other ports. This behavior is known as a non-transit fabric. In release version 1.1 and later, ACI is capable of acting as a transit network, and routes learned from one external Layer 3 connection can be advertised out to a different external Layer 3 connection, not just fabric routes.

The network team will provide the external Layer 3 connectivity for their tenants. One common mechanism is to use sub-interfaces on a router to create different Layer 3 domains since each tenant will likely not have their own external router.

**Supported Routing Protocols**

The following routing protocols are supported at time of writing:

- **Static routes** - You can define static routes to the outside world. Using static routes reduces the sizing and complexity of the routing tables in the leaf nodes, but increases administrator overhead. With static routes, you must also configure the static path back to the internal network that you wish to be reachable from the outside world.

- **OSPF NSSA** - Using not-so-stubby area (NSSA) reduces the size of the Open Shortest Path First (OSPF) database and the need to maintain the overhead of the routing protocols with large tables of routes. With OSPF NSSA, the router learns only a summarization of routes, including a default path out of the fabric. OSPF NSSA advertises to the adjacent router the internal public subnets part of the Layer 3 external.

- **iBGP peering leaf and external router** - With internal Border Gateway Protocol (iBGP), ACI supports only one autonomous system (AS) number that has to match the one that is used for the internal Multiprotocol Border Gateway Protocol (MP-BGP) route reflector. Without MP-BGP, the external routes (static, OSPF, or BGP) for the Layer 3 outside connections are not propagated within the ACI fabric, and the ACI leaves that are not part of the border leaf do not have IP connectivity to any outside networks. Given that the same AS number is used for both cases, the user must find out the AS number on the router to which the ACI border leaf will connect, and use that AS number as the BGP AS number for the ACI fabric.

**Configure MP-BGP Spine Route Reflectors**

The ACI fabric route reflectors use multiprotocol border gateway protocol (MP-BGP) to distribute external routes within the fabric so a full mesh BGP topology is not required. To enable route reflectors in the ACI
fabric, the fabric administrator must select at least one spine switch that will be a route reflector, and provide the autonomous system (AS) number for the fabric. Once route reflectors are configured, administrators can setup connectivity to external networks.

To connect external Layer 3 devices to the ACI fabric, the fabric infrastructure operator must configure a Route Reflector policy to designate which spines act as the route reflector(s). For redundancy purposes, configure more than one spine as a router reflector node.

When a tenant requires a Layer 3 connection, the infrastructure operator configures the leaf node to which the WAN router is being connected as border leaf node, which pairs the border leaf node with one of the route reflector nodes as a BGP peer. After the route reflectors are configured, they can advertise routes in the fabric.

Each leaf node can store up to 4000 routes at time of writing. If a WAN router must advertise more than 4000 routes, the router should peer with multiple leaf nodes. The infrastructure operator configures each of the paired leaf nodes with the routes (or route prefixes) that the nodes can advertise.

To configure the Route Reflector policy:
2. In the Navigation pane, choose Pod Policies > Policies > BGP Route Deflector default.
3. In the Work pane, perform the following actions:
   a. Change the Autonomous System Number to match the required number for your network.
   b. Add the two spine nodes that will be members of this reflector policy.
   c. Click Submit.
4. In the Navigation pane, choose Pod Policies.
5. In the Work pane, choose Actions > Create Pod Policy Group.
6. In the Create Pod Policy Group dialog box, perform the following actions:
   a. In the BGP Route Reflector Policy drop-down list, choose default.
   b. In the Navigation pane, choose Pod Policies > Profiles > default.
   c. In the Work pane, in the Fabric Policy Group drop-down list, choose Create Pod Policy Group.
   d. In the Create Pod Policy Group dialog box, in the Date Time Policy drop-down list, choose default.
   e. In the BGP Route Reflector Policy drop-down list, choose default.
   f. Complete the remainder of the dialog box as appropriate to your setup.
7. Click Submit.

The following figure illustrates the objects and their relationships for external Layer 3 connections:
Layer 3 Integration Through Tenant Network with OSPF NSSA

The following figure shows a simple integration of a Layer 3 external into ACI using OSPF:

The setup includes a single router with two interfaces connected to leaf switches.

**Note:** See the "Adding New Devices to The Fabric" section to setup the access policies for the interfaces of the leaves that are connected to the router.

To integrate Layer 3 through a tenant network with OSPF/NSSA:

1. On the menu bar, choose Tenants > ALL TENANTS.
2. In the Work pane, choose the tenant.
3. In the Navigation pane, choose Tenant_Name > Networking > External Routed Networks.
4. In the Work pane, choose Action > Create Routed Outside.
5. In the Create Routed Outside dialog box, perform the following actions:
   a. In the Name field, enter a name for the profile.
b. In the **Private Network** drop-down list, choose the private network for this tenant.

c. Click the **OSPF** check box.

d. In the **OSPF Area ID** field, enter the OSPF area ID, such as "1".

e. In the **OSPF Area Control** section, click the **Send redistributed LSAs into NSSA area** check box.

f. In the **OSPF Area Type** section, click the **NSSA Area** radio button.

g. In the **Nodes and Interfaces Protocol Profiles** section, click + to add a profile.

h. In the **Create Node Profile** dialog box, perform the following actions:
   1. In the Name field, enter a name for the profile.
   2. In the **Nodes** section, click + to add a node.
   3. In the **Select Node** dialog box, perform the following actions:
      a. In the **Node ID** drop-down list, choose a node, such as Leaf-1.
      b. In the **Router ID** field, enter the router’s IP address as the ID, such as "10.0.1.1".
      c. Uncheck the **Router ID as Loopback Address** check box.
      d. In the **Loopback Addresses** section, click + to add a loopback address.
      e. Enter the loopback address, such as "10.254.254.1", and click **Update**.
      f. Click **OK**.

4. In the **OSPF Interface Profiles** section, click + to create an OSPF interface profile.

5. In the **Create Interface Profile** dialog box, perform the following actions:
   a. In the **Name** field, enter a name for the profile.
   b. In the **OSPF Policy** drop-down list, choose **Create OSPF Interface Policy**. When defining the interaction with another OSPF router, you must specify the policy interaction. This document does not explain the different OSPF parameters.
   c. In the **Create OSPF Interface Policy** dialog box, perform the following actions:
      Ordered List Number 5 In the **Name** field, enter a name for the OSPF policy, such as "OSPF-Point2Point".
      Ordered List Number 5 In the **Network Type** section, click the radio button that matches the adjacent router, such as **Point to Point**.
      Ordered List Number 5 Complete the remainder of the dialog box as appropriate to your setup.
      Ordered List Number 5 Click **Submit**.

d. In the **Interfaces** section, click on the **Routed Interfaces** tab.

e. Click the + sign to select a routed interface.

f. In the **Select Routed Interface** dialog box, perform the following actions:
Ordered List Number 5
In the Path drop-down list, choose the interface on the leaf, such as e1/9 on Leaf-1.

Ordered List Number 5
In the IP Address field, enter the IP address of the path that is attached to the layer 3 outside profile, such as "10.0.1.1/24".

Ordered List Number 5
In the MTU (bytes) field, enter the maximum MTU of the external network, such as "1500" to match the example peering router.

Ordered List Number 5
Complete the remainder of the dialog box as appropriate to your setup and click OK.

6. Click OK.

i. Click Next.

j. In the External EPG Networks section, click + create an external network.

k. In the Create External Network dialog box, perform the following actions:

   1. In the IP Address field, enter 0.0.0.0/0 to permit the learning of any subnet and click OK.

l. Click Finish. Next, you must configure the external network EPG.

External Layer 3 for Multiple Tenants

In ACI, you can use various mechanisms to reuse the same external Layer 3 router for multiple tenants. If the adjacent router is a Cisco Nexus Series Switch with a Layer 2 trunk interface, the external Layer 3 connection can be configured to route via SVI. For routers capable of using sub-interfaces, those can be used to provide multiple external Layer 3 connection for multiple VRFs and/or tenants. The fabric operator can configure multiple external Layer 3 connections using either sub-interface or SVI and provide that to each tenant.

Application Migration Use Case

When operating the ACI fabric, there can be occasions when you will have to migrate workloads, servers or virtualization hosts from outside the ACI fabric, onto the fabric. One common example is when migrating from a traditional data center configuration over to a policy-driven data center using ACI. As ACME starts to use ACI in more of their data centers, it will be come necessary to perform these migrations. In this example, ACME must manage the migration of switched virtual interfaces (SVI) as well as the policy allowing traffic to traverse a Layer 2 outside network and then on to the ACI fabric.

At a high level, you must start by configuring the Layer 2 outside network to allow traffic from the source VLAN to communicate with the same VLAN residing on the ACI fabric. You will also need to configure Layer 3 connectivity from the fabric out to the existing Layer 3 networks in preparation for full connectivity after SVI migration.

Further information and steps on how to create this Layer 2 and Layer 3 connectivity including the policy, can be found in the Fabric Connectivity chapter of this book.
Once they have successfully established connectivity between the outside Layer 2 network (where the workload or host is coming from) and the existing internal fabric EPG, you can then start the migration process of moving application workloads onto the fabric. One key consideration should be when to switch over the SVI interfaces from the existing environment into the ACI fabric and when to start advertising routes to this SVI network. Assuming that the SVIs reside on the external Layer 2 network, Cisco recommends that you move the SVIs over to the ACI fabric once a majority of the hosts have been migrated over.

**Extending the Network to ACI**

One of the ACME sites would like to migrate from the legacy data center architecture to the next generation Cisco Application Centric Infrastructure (ACI) Fabric. They would like to migrate with minimal service interruption while taking advantage of ACI innovations where applicable. ACME would like to perform the migration in multiple stages.

The Legacy data center prior to migration:

*Figure 27: Traditional pre-migration data center*

The ACI data center following migration:
The first stage will provide connectivity from the legacy data center to the ACI fabric. In this state, you logically map a VLAN=EPG. The interconnect from the legacy network to the ACI fabric will be accomplished through standard Layer 2 extensions (VLAN/VXLAN).

Provide physical connectivity from the existing aggregation layer to the ACI border leafs. This connectivity can be accomplished in either the form of a Virtual Port Channel, Port Channel, or a single interface.

1. Provide a physical connection from aggregation switch #1 to the ACI border leaf #1.
2. Provide a physical connection from aggregation switch #2 to the ACI border leaf #1.

**Note:** Before connecting external physical connections into the fabric, the Fabric Access Policies for the access ports that you will be used for the DCI must be configured. For details on configuring the access policies please reference the Fabric Connectivity section of this book.

Configure the aggregation links as a Layer 2 trunk.

1. Trunk the VLAN representing the host connectivity. This allows for the host VLAN to be extended into the fabric.

In the Application Policy Infrastructure Controller (APIC) you will now configure a single tenant. The created tenant will represent the legacy data center into the ACI fabric.