Intra-EPG Isolation Enforcement and Cisco ACI

This chapter contains the following sections:

Intra-EPG Isolation for VMware VDS or Microsoft Hyper-V Virtual Switch

Intra-EPG Isolation is an option to prevent physical or virtual endpoint devices that are in the same base EPG or microsegmented (uSeg) EPG from communicating with each other. By default, endpoint devices included in the same EPG are allowed to communicate with one another. However, conditions exist in which total isolation of the endpoint devices from on another within an EPG is desirable. For example, you may want to enforce intra-EPG isolation if the endpoint VMs in the same EPG belong to multiple tenants, or to prevent the possible spread of a virus.

A Cisco Application Centric Infrastructure (ACI) virtual machine manager (VMM) domain creates an isolated PVLAN port group at the VMware VDS or Microsoft Hyper-V Virtual Switch for each EPG that has intra-EPG isolation enabled. A fabric administrator specifies primary encapsulation or the fabric dynamically specifies primary encapsulation at the time of EPG-to-VMM domain association. When the fabric administrator selects the VLAN-pri and VLAN-sec values statically, the VMM domain validates that the VLAN-pri and VLAN-sec are part of a static block in the domain pool.

Primary encapsulation is defined per EPG VLAN. In order to use primary encapsulation for Intra-EPG isolation, you must deploy it in one of the following ways:

- Segregate primary and secondary VLAN defined ports on different switches. EPG VLAN is created per switch. If you have port encapsulation, and only static ports on a switch for an EPG, primary encapsulation is not associated.
- Use a different encapsulation for static ports that use only port encapsulation. This creates a second EPG VLAN that does not have primary encapsulation associated with it.

  In the example below, consider egress traffic on two interfaces (Eth1/1, Eth1/3) with primary VLAN-1103. Eth1/1 port encap was changed to VLAN-1132 (from VLAN-1130), so that it does not share the secondary VLAN with Eth1/3.

  ```
  Port encap with VLAN-1130 on Eth1/1
  Eth1/1: Port Encap only VLAN-1130
  Eth1/6: Primary VLAN-1103 and Secondary VLAN-1130
  ```

```
fab2-leaf3# show vlan id 53 ext

VLAN Name                              Encap            Ports
---- --------------------------------- ---------------- ------------------------
53   JT:jt-ap:EPG1-1                   vlan-1130        Eth1/1, Eth1/3

module-1# show sys int eltmc info vlan access_encap_vlan 1130
             vlan_id:             53   :::           isEpg:              1
          bd_vlan_id:             52   :::         hwEpgId:          11278
      srcpolicyincom:              0   :::       data_mode:              0
        accencaptype:              0   :::    fabencaptype:              2
       accencapval:             1130   :::     fabencapval:          12192
             sclass:            49154   :::         sglabel:             12
          sclassprio:                1   :::     floodmetptr:             13
          maclearnen:                1   :::       iplearnen:              1
         sclasslrnen:                1   :::   bypselffwdchk:              0
            qosusetc:                0   :::       qosuseexp:              0
            isolated:                1   :::   primary_encap:           1103
           proxy_arp:                0   :::       qinq core:              0
           ivxlan_dl:                0   :::       dtag_mode:              0
      is_service_epg:                0

Port encap changed to VLAN-1132 on Eth1/1
fab2-leaf3# show vlan id 62 ext

VLAN Name                              Encap            Ports
---- --------------------------------- ---------------- ------------------------
62   JT:jt-ap:EPG1-1                   vlan-1132        Eth1/1

module-1# show sys int eltmc info vlan access_encap_vlan 1132
          [SDK Info]:
             vlan_id:             62   :::           isEpg:              1
          bd_vlan_id:             52   :::         hwEpgId:          11289
      srcpolicyincom:              0   :::       data_mode:              0
        accencaptype:              0   :::    fabencaptype:              2
        accencapval:            1132   :::     fabencapval:          11224
             sclass:            49154   :::         sglabel:             12
          sclassprio:                1   :::     floodmetptr:             13
          maclearnen:                1   :::       iplearnen:              1
         sclasslrnen:                1   :::   bypselffwdchk:              0
            qosusetc:                0   :::       qosuseexp:              0
            isolated:                1   :::   primary_encap:              0
           proxy_arp:                0   :::       qinq core:              0
           ivxlan_dl:                0   :::       dtag_mode:              0
      is_service_epg:                0

fab2-leaf3# show vlan id 53 ext

VLAN Name                              Encap            Ports
---- --------------------------------- ---------------- ------------------------
53   JT:jt-ap:EPG1-1                   vlan-1130        Eth1/3

module-1# show sys int eltmc info vlan access_encap_vlan 1130
          [SDK Info]:
             vlan_id:             53   :::           isEpg:              1
          bd_vlan_id:             52   :::         hwEpgId:          11278
      srcpolicyincom:              0   :::       data_mode:              0
        accencaptype:              0   :::    fabencaptype:              2
        accencapval:             1130   :::     fabencapval:          12192
             sclass:            49154   :::         sglabel:             12
          sclassprio:                1   :::     floodmetptr:             13
          maclearnen:                1   :::       iplearnen:              1
```

```
sclasslrnen:              1   :::   bypselffwdchk:              0
   qosusetc:              0   :::       qosuseexp:              0
   isolated:              1   :::   primary_encap:           1103
  proxy_arp:              0   :::       qinq core:              0
  ivxlan_dl:              0   :::       dtag_mode:              0
```

Note

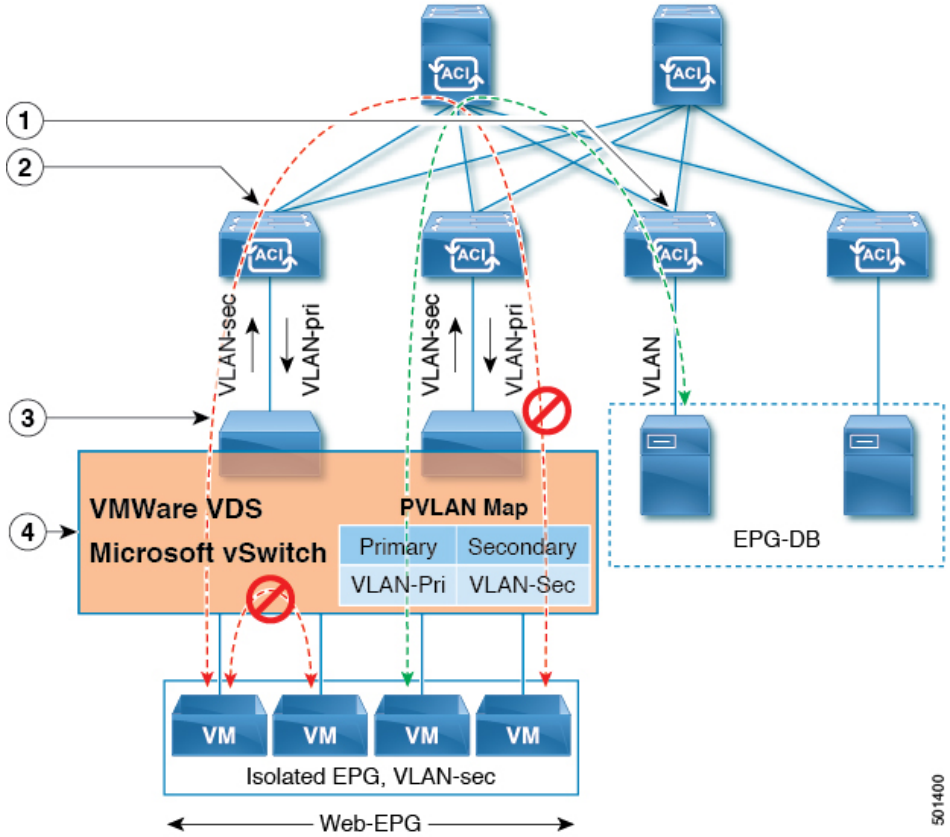
- When intra-EPG isolation is not enforced, the VLAN-pri value is ignored even if it is specified in the configuration.
- A VMware distributed virtual switch (DVS) domain with EDM UCSM integration may fail. The domain fails if you configure intra-EPG isolation on the endpoint group (EPG) attached to the domain and you use UCSM Mini 6324, which does not support private VLANs.

BPDUs are not forwarded through EPGs with intra-EPG isolation enabled. Therefore, when you connect an external Layer 2 network that runs spanning tree in a VLAN that maps to an isolated EPG on Cisco ACI, Cisco ACI might prevent spanning tree in the external network from detecting a Layer 2 loop. You can avoid this issue by ensuring that there is only a single logical link between Cisco ACI and the external network in these VLANs.

VLAN-pri/VLAN-sec pairs for the VMware VDS or Microsoft Hyper-V Virtual Switch are selected per VMM domain during the EPG-to-domain association. The port group created for the intra-EPG isolation EPGs uses the VLAN-sec tagged with type set to `PVLAN`. The VMware VDS or the Microsoft Hyper-V Virtual Switch and fabric swap the VLAN-pri/VLAN-sec encapsulation:

- Communication from the Cisco ACI fabric to the VMware VDS or Microsoft Hyper-V Virtual Switch uses VLAN-pri.
- Communication from the VMware VDS or Microsoft Hyper-V Virtual Switch to theCisco ACI fabric uses VLAN-sec.

Figure 1: Intra-EPG Isolation for VMware VDS or Microsoft Hyper-V Virtual Switch



Note these details regarding this illustration:

1. EPG-DB sends VLAN traffic to the Cisco ACI leaf switch. The Cisco ACI egress leaf switch encapsulates traffic with a primary VLAN (PVLAN) tag and forwards it to the Web-EPG endpoint.
2. The VMware VDS or Microsoft Hyper-V Virtual Switch sends traffic to the Cisco ACI leaf switch using VLAN-sec. The Cisco ACI leaf switch drops all intra-EPG traffic because isolation is enforced for all intra VLAN-sec traffic within the Web-EPG.
3. The VMware VDS or Microsoft Hyper-V Virtual Switch VLAN-sec uplink to the Cisco ACI leaf switch is in isolated trunk mode. The Cisco ACI leaf switch uses VLAN-pri for downlink traffic to the VMware VDS or Microsoft Hyper-V Virtual Switch.
4. The PVLAN map is configured in the VMware VDS or Microsoft Hyper-V Virtual Switch and Cisco ACI leaf switches. VM traffic from WEB-EPG is encapsulated in VLAN-sec. The VMware VDS or Microsoft Hyper-V Virtual Switch denies local intra-WEB EPG VM traffic according to the PVLAN tag. All intra-ESXi host or Microsoft Hyper-V host VM traffic is sent to the Cisco ACI leaf switch using VLAN-Sec.

Configuring Intra-EPG Isolation for VMware VDS or Microsoft Hyper-V Virtual Switch using the GUI

Procedure

Step 1 Log into Cisco APIC.

Step 2 Choose **Tenants** > ***tenant***.

Step 3 In the left navigation pane expand the **Application Profiles** folder and appropriate application profile.

Step 4 Right-click the **Application EPGs** folder and then choose **Create Application EPG**.

Step 5 In the **Create Application EPG** dialog box, complete the following steps:

a) In the **Name** field, add the EPG name.
b) In the **Intra EPG Isolation** area, click **Enforced**.
c) In the **Bridge Domain** field, choose the bridge domain from the drop-down list.
d) Associate the EPG with a bare metal/physical domain interface or with a VM Domain.

- For the VM Domain case, check the **Associate to VM Domain Profiles** check box.
- For the bare metal case, check the **Statically Link with Leaves/Paths** check box.

e) Click **Next**.
f) In the **Associated VM Domain Profiles** area, click the + icon.
g) From the **Domain Profile** drop-down list, choose the desired VMM domain.

For the static case, in the **Port Encap (or Secondary VLAN for Micro-Seg)** field, specify the secondary VLAN, and in the **Primary VLAN for Micro-Seg** field, specify the primary VLAN. If the Encap fields are left blank, values will be allocated dynamically.

Note
For the static case, a static VLAN must be available in the VLAN pool.

Step 6 Click **Update** and click **Finish**.