BPDU Features

This chapter contains the following sections:

Understanding Bridge Protocol Data Unit Features

The following sections describe supported bridge protocol data unit (BPDU) features on the Cisco ACI Virtual Edge with the Cisco APIC. BPDU Guard and BPDU filtering are switch-wide features, and they are applicable only for VM virtual Ethernet (vEth) ports.

BPDU Guard

BPDU Guard prevents loops by moving a nontrunking port into an errdisable state when a BPDU is received on that port. When you enable BPDU Guard on the switch, the interface is moved to blocking state on receiving a BPDU.

BPDU Guard provides a secure response to invalid configurations because the administrator must manually put the interface back in service. To put the interface back in service, disconnect the VM port and then reconnect it to the Cisco ACI Virtual Edge or an EPG port group through vCenter.

BPDU Filtering

BPDU filtering prevents sending and receiving of BPDUs on ports. Any BPDU that is received is dropped when filtering is enabled. BPDU filtering is enabled on VM vEth ports by default. When you enable this feature, Cisco ACI Virtual Edge drops all BPDUs received on uplink ports.

Note We recommend that you configure BPDU policy in a single policy interface group. Configuring BPDU in multiple policy interface groups leads to inconsistent behavior.

Note In an L2 switch extended topology, we recommend that you configure BPDU policy through an attached entity profile vSwitch policy override. If the interface policy group is used for configuration, then BPDU Guard or filter is enabled on the Leaf ports. This causes those ports to become error-disabled when they receive BPDU packets from an L2 switch.

For information about configuring BPDU policy through an override policy, see the section "Modifying the Interface Policy Group to Override the vSwitch-Side Policies" in the *Cisco Application Virtual Edge Installation Guide*.

Configuring BPDU Features Using the GUI

Procedure

Step 1 Log in to the Cisco APIC.

Step 2 On the menu bar, choose **Fabric** > **Access Policies**.

Step 3 In the **Policies** navigation pane, expand the **Policies** and the **Interface** folders.

Step 4 Right-click the **Spanning Tree Interface** folder and choose **Create Spanning Tree Interface Policy**.

Step 5 In the **Create Spanning Tree Interface Policy** dialog, complete the following actions:

a) In the **Name** field, enter a name for the policy.
b) (Optional) In the **Description** field, enter a description of the policy.
c) In the **Interface controls** area, check the **BPDU Guard enabled** check box or the **BPDU filter enabled** check box.
d) Click **Submit** to save the policy.

Step 6 Attach the spanning tree interface policy that you created in Step 5 by completing the following steps:

a) Go to **Virtual Networking** > **Inventory** and then expand the **VMM Domains** and **VMware** folders.
b) Click the VMM domain where you want to attach the policy.
c) Click the **VSwitch Policy** tab on the right side of the work pane.
d) From the **STP Policy** drop-down list, choose the policy that you created in Step 5.
e) Click **Submit**.

Step 7 Verify the configuration by opening an ESXi CLI session to the ESXi hypervisor and entering the **vemcmd show card** command.

Example:

```
cisco-ave# vemcmd show card
Global BPDU Guard: Enabled && Global BPDU Filter: Enabled
```

The output indicates that BPDU filtering and BPDU Guard are enabled.

Configure BPDU Features Using the NX-OS Style CLI

Procedure

Step 1 Enter the vmware-domain mode.

Example:

```
apic1# configure
apic1(config)# vmware-domain domain name
AVE-Vlan  AVE2-VXLAN  Test  Test2
```

Step 2 Create a spanning-tree interface policy.

Example:

```
apic1(config-vmware)# configure-ave
apic1(config-vmware-ave)# spanning-tree
              bpdu-filter  bpdu-guard
apic1(config-vmware-ave)# spanning-tree
              bpdu-filter  Configure BPDU filter override on AVE uplink ports
              bpdu-guard   Configure BPDU guard override on AVE uplink ports
```

Step 3 Disable or enable BPDU filter.

Example:

```
apic1(config-vmware-ave)# spanning-tree bpdu-filter
                 default  disable  enable
apic1(config-vmware-ave)# spanning-tree bpdu-filter
                 default  Remove BPDU filter/guard override policy
                 disable  Disable BPDU filter
                 enable   Enable BPDU filter
```

Step 4 Disable or enable BPDU guard.

```
apic1(config-vmware-ave)# spanning-tree bpdu-guard
               default  disable  enable
```

Configure BPDU Features Using the REST API

Procedure

Step 1 Configure BPDU Guard.

Example:

```
<polUni>
  <infraInfra>
      <stpIfPol name="testStp5" ctrl="bpdu-guard"/>
      <infraFuncP>
```

```
        <infraAccBndlGrp name="test51">
        <infraRsStpIfPol tnStpIfPolName="testStp5"/>
        <infraRsAttEntP tDn="uni/infra/attentp-test-bpdu"/>
        </infraAccBndlGrp>
      </infraFuncP>
  </infraInfra>
</polUni>


<vmmProvP vendor="VMware">
     <vmmDomP name="mininet">
        <vmmVSwitchPolicyCont>
           <vmmRsVswitchOverrideStpPol tDn="uni/infra/ifPol-testStp5"/>
        </vmmVSwitchPolicyCont>
     </vmmDomP>
</vmmProvP
```

Step 2 Configure BPDU filtering.

Example:

```
<polUni>
  <infraInfra>
      <stpIfPol name="testStp5" ctrl="bpdu-filter"/>
      <infraFuncP>
        <infraAccBndlGrp name="test51">
        <infraRsStpIfPol tnStpIfPolName="testStp5"/>
        <infraRsAttEntP tDn="uni/infra/attentp-test-bpdu"/>
        </infraAccBndlGrp>
      </infraFuncP>
 </infraInfra>
</polUni>

<vmmProvP vendor="VMware">
     <vmmDomP name="mininet">
        <vmmVSwitchPolicyCont>
           <vmmRsVswitchOverrideStpPol tDn="uni/infra/ifPol-testStp5"/>
        </vmmVSwitchPolicyCont>
     </vmmDomP>
</vmmProvP>
```