IGMP Querier and Snooping

This chapter contains the following sections:

Guidelines and Limitations for Configuring IGMP Snooping and Querier

Depending on your setup, you may need to configure IGMP on Layer 2 switches or on infra tenant or administrator-created tenant bridge domains. This section provides guidelines for two common scenarios when you must configure IGMP protocol snooping and querier.

Note Cisco ACI Virtual Edge does not support IGMP snooping. The guidelines and limitations and configuration procedures for IGMP snooping in this section are for configuring IGMP snooping on the leaf switch.

Multi-destination Flood for VXLAN-Encapsulated Traffic

To receive multi-destination flood on Cisco ACI Virtual Edge for VXLAN-encapsulated traffic and minimize multicast flooding traffic originating from and terminating on the Cisco ACI Virtual Edge if there is a Layer 2 device between the leaf and the Cisco ACI Virtual Edge, do the following:

- Apply IGMP snooping policy and enable IGMP querier on the infra tenant bridge domain subnet through the Cisco APIC. See the instructions in the section Configure IGMP Querier Using the GUI, on page 2 in this guide.

- Enable IGMP snooping on each of any Layer 2 devices between the leaf and the Cisco ACI Virtual Edge. Follow the instructions that are specific to the device. For example, if the Layer 2 device is a Cisco Nexus 5000 Series switch, see the instructions in the configuration guide for that switch.

Sending or Receiving Multicast Streams with Virtual Machines

If you have virtual machines connected to the Cisco ACI Virtual Edge and want to send or receive multicast streams, do the following:

- Apply IGMP snoop policy and enable IGMP querier for administrator-created tenant bridge domain. If you have multiple administrator-created tenant bridge domains, you must apply IGMP snoop policy and configure IGMP querier on each administrator-created tenant bridge domain through the Cisco APIC. See the instructions in the section Configure IGMP Querier Using the GUI, on page 2 in this guide.
- Enable IGMP snooping on each Layer 2 device between the leaf and the Cisco ACI Virtual Edge. Follow the instructions that are specific to the device. For example, if the Layer 2 device is a Cisco Nexus 5000 Series switch, see the instructions in the configuration guide for that switch.
- If the multicast traffic that originates from or terminates on the VMs is VXLAN-encapsulated, follow all the guidelines in the previous section as well as this one.

Order of Configuration

Configure IGMP querier before you configure IGMP snooping.

Configure IGMP Querier Using the GUI

Procedure

Step 1 Log in to the Cisco APIC.

Step 2 Complete one of the following series of steps, depending on the type of tenant:

If you have ...	Then...
An infra tenant	**a.** Choose **Tenants** > **infra**. **b.** In the navigation pane, open the following folders: **Networking** > **Bridge Domains** > **default** > **Subnets**. **c.** Choose the subnet in the **Subnets** folder. **d.** In the **Properties** work pane, in the **Subnet Control** area, make sure that the **Querier IP** check box is checked. **e.** Click **Submit**.
An administrator-created tenant	**a.** Choose **Tenants** and then choose the tenant on which you want to configure the IGMP querier. **b.** In the tenant navigation pane, open the **Networking** folder, the **Bridge Domains** folder, and then the folder for the bridge domain created earlier for the tenant.

If you have ...	Then...
	If the selected bridge domain already has a subnet with a gateway IP, you can use it to enable IGMP querier in the **Subnet Control** area. Or you can follow the remaining steps to create a new subnet to enable IGMP querier. **c.** Right-click the **Subnets** folder inside the bridge domain folder and choose **Create Subnet**. **d.** In the **Create Subnet** dialog box, complete the following steps: **1.** Specify a gateway IP address. **Note** You can configure any IP address except one from the 10.0.0.0/16 network because that network is reserved for Cisco APIC fabric devices. **2.** In the **Subnet Control** area, make sure that the **Querier IP** check box is checked. **3.** Click **Submit**.

Configure IGMP Querier Using the NX-OS Style CLI

Procedure

Configure IGMP querier.

Example:

```
apic1# configure
apic1(config)# tenant t1
apic1(config-tenant)# interface bridge-domain bd1
apic1(config-tenant-interface)# ip address <192.168.1.1/24> snooping-querier
 <CR>
multi-site  Set the address as multi-site address
scope       Scope of the address among ['public', 'private']
secondary   Set the address as secondary address
```

Enable IGMP Querier on the Bridge Domain Subnet Using the REST API

Procedure

Enable IGMP querier on the bridge domain subnet.

Example:

```
<fvTenant name="ms10">

<fvCtx name="msv10"/>

<fvBD name="msb10">
  <fvSubnet ctrl="querier" descr="" ip="1.1.9.1/24" name="" nameAlias=""
preferred="no" scope="private" virtual="no"/>
  <fvRsCtx tnFvCtxName="msv10"/>

</fvBD></fvTenant>
```

Configure IGMP Snooping to Take Effect Immediately Using the GUI

Procedure

Step 1 Log in to the Cisco APIC.

Step 2 Take one of the following actions:

- If you have an infra tenant, choose **Tenants** > **infra**.
- If you have an administrator-created tenant, choose **Tenants** and then choose the tenant on which you want to configure the IGMP snooping.

Step 3 Take one of the following actions in the tenant navigation pane:

- If you have an infra tenant, open the **Networking** folder, open the **Bridge Domains** folder, and then choose the **default** folder.
- If you have an administrator-created tenant, open the **Networking** folder, open the **Bridge Domains** folder, and then choose the bridge domain created earlier for the tenant.

Step 4 In the **Properties** work pane, from the **IGMP Snoop Policy** drop-down list, choose **Create IGMP Snoop Policy**.

Step 5 In the **Create IGMP Snoop Policy** dialog box, complete the following steps:

a) In the **Name** field, enter a name for the policy.

b) In the **Control** area, check the **Enable querier** check box.

c) (Optional) Configure any other relevant IGMP parameters.
d) Click **Submit**.

Step 6 In the **Properties** pane, click **Submit**.

Configure IGMP Snooping to Take Effect Immediately Using the NX-OS Style CLI

Procedure

Configure IGMP snooping to take effect immediately.

Example:

```
apic1# configure
apic1(config)# tenant t1
apic1(config-tenant)# interface bridge-domain bd1
apic1(config-tenant-interface)# ip igmp snooping querier
```

Configure IGMP Snooping to Take Effect Later Using the GUI

Procedure

Step 1 Log in to the Cisco APIC.

Step 2 Take one of the following actions:

- If you have an infra tenant, choose **Tenants** > **infra**.
- If you have an administrator-created tenant, choose **Tenants** and then choose the tenant on which you want to configure the IGMP snooping.

Step 3 In the tenant navigation pane, open the **Policies** and **Protocol** folders.

Step 4 Right-click the **IGMP Snoop** folder and then choose **Create IGMP Snoop Policy**.

Step 5 In the **Create IGMP Snoop Policy** dialog box, complete the following steps:

a) In the **Name** field, enter a name for the policy.
b) In the **Control** area, check the **Enable querier** check box.
c) (Optional) Configure any other relevant IGMP parameters.
d) Click **Submit**.

What to do next

Once you configure IGMP snooping, you can apply it at any time to a bridge domain by completing the following steps:

1. Take one of the following actions:
   - If you have an infra tenant, choose **Tenants** > **infra**.
   - If you have an administrator-created tenant, choose **Tenants** and then choose the tenant on which you want to configure the IGMP snooping.
2. Take one of the following actions in the **Tenant** navigation pane:
   - If you have an infra tenant, click the + icons to open the **Networking** and **Bridge Domain** folders, and then choose the **default** folder.
   - If you have an administrator-created tenant, open the **Networking** and **Bridge Domain** folders, and then choose the bridge domain created earlier for the tenant.
3. In the **Properties** pane, in the **IGMP Snoop Policy** drop-down list, choose the IGMP snooping policy that you want to apply.
4. Click **Submit** for the IGMP policy to go into effect for the bridge domain.

Configure IGMP Snooping to Take Effect Later Using the NX-OS Style CLI

Procedure

Configure IGMP snooping to take effect later.

Example:

```
apic1# configure
apic1(config)# tenant t1
apic1(config-tenant)# template ip igmp snooping policy <foo_igmp>
apic1(config-tenant-template-ip-igmp-snooping)# ip igmp snooping querier
```

Configure an IGMP Snooping Policy Using the REST API

Procedure

Create an IGMP snooping policy and apply it to the bridge domain.

Example:

```
<igmpSnoopPol name="igmp_snp_bd_21"
              adminSt="enabled"
              ctrl="fast-leave,querier"
              lastMbrIntvl="1"
              queryIntvl="125"
              rspIntvl="10"
              startQueryCnt="2"
              startQueryIntvl="31"
              />
<fvCtx name="msv10"/>

<fvBD name="msb10">
  <fvRsCtx tnFvCtxName="msv10"/>

  <!-- Bind IGMP snooping to a BD -->
  <fvRsIgmpsn tnIgmpSnoopPolName="igmp_snp_bd_21"/>
</fvBD></fvTenant>
```