Cisco APIC and IGMP Snoop Layer 2 Multicast Configuration

New and Changed  2
About Cisco APIC and IGMP Snooping  2
Configuring and Assigning an IGMP Snoop Policy  5
Enabling IGMP Snoop Static Port Groups  9
Enabling IGMP Snoop Access Groups  12
EPG Static Port Deployment  16
New and Changed

The following table provides an overview of the significant changes up to this current release. The table does not provide an exhaustive list of all changes or of the new features up to this release.

Table 1: New Features and Changed Behavior in Cisco APIC

<table>
<thead>
<tr>
<th>Cisco APIC Release Version</th>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 2.1(1h)</td>
<td>IGMP snoop static group support</td>
<td>This feature is introduced.</td>
</tr>
<tr>
<td></td>
<td>IGMP snoop access group support</td>
<td>This feature is introduced.</td>
</tr>
</tbody>
</table>

About Cisco APIC and IGMP Snooping

IGMP snooping is the process of listening to Internet Group Management Protocol (IGMP) network traffic. The feature allows a network switch to listen in on the IGMP conversation between hosts and routers and filter multicasts links that do not need them, thus controlling which ports receive specific multicast traffic.

Cisco APIC provides support for the full IGMP snooping feature included on a traditional switch such as the N9000 standalone.

- Policy-based IGMP snooping configuration per bridge domain
  APIC enables you to configure a policy in which you enable, disable, or customize the properties of IGMP Snooping on a per bridge-domain basis. You can then apply that policy to one or multiple bridge domains.

- Static port group implementation
  IGMP static port grouping enables you to pre-provision ports, already statically-assigned to an application EPG, as the switch ports to receive and process IGMP multicast traffic. This pre-provisioning prevents the join latency which normally occurs when the IGMP snooping stack learns ports dynamically.

  Static group membership can be pre-provisioned only on static ports (also called, static-binding ports) assigned to an application EPG.

- Access group configuration for application EPGs
  An “access-group” is used to control what streams can be joined behind a given port.
  An access-group configuration can be applied on interfaces that are statically assigned to an application EPG in order to ensure that the configuration can be applied on ports that will actually belong to the that EPG.

  Only Route-map-based access groups are allowed.
How IGMP Snooping is Implemented in the ACI Fabric

We recommend that you do not disable IGMP snooping on the bridge domain. If you disable IGMP snooping, you might see reduced multicast performance because of excessive false flooding within the bridge domain.

Note IGMP snooping software examines Layer 2 IP multicast traffic within a bridge domain to discover the ports where interested receivers reside. Using the port information, IGMP snooping can reduce bandwidth consumption in a multi-access bridge domain environment to avoid flooding the entire bridge domain. By default, IGMP snooping is enabled on the bridge domain.

This figure shows the IGMP routing functions and IGMP snooping functions both contained on an ACI leaf switch with connectivity to a host. The IGMP snooping feature snoops the IGMP membership reports and Leave messages and forwards them only when necessary to the IGMP router function.

Figure 1: IGMP Snooping function

IGMP snooping operates upon IGMPv1, IGMPv2, and IGMPv3 control plane packets where Layer 3 control plane packets are intercepted and influence the Layer 2 forwarding behavior.

IGMP snooping has the following proprietary features:

- Source filtering that allows forwarding of multicast packets based on destination and source IP addresses
- Multicast forwarding based on IP addresses rather than the MAC address
- Multicast forwarding alternately based on the MAC address
For more information about IGMP snooping, see RFC 4541.

**Virtualization Support**

You can define multiple virtual routing and forwarding (VRF) instances for IGMP snooping. On leaf switches, you can use the `show` commands with a VRF argument to provide a context for the information displayed. The default VRF is used if no VRF argument is supplied.

**The APIC IGMP Snooping Function, IGMPv1, IGMPv2, and the Fast Leave Feature**

Both IGMPv1 and IGMPv2 support membership report suppression, which means that if two hosts on the same subnet want to receive multicast data for the same group, the host that receives a member report from the other host suppresses sending its report. Membership report suppression occurs for hosts that share a port.

If no more than one host is attached to each switch port, you can configure the fast leave feature in IGMPv2. The fast leave feature does not send last member query messages to hosts. As soon as APIC receives an IGMP leave message, the software stops forwarding multicast data to that port.

IGMPv1 does not provide an explicit IGMP leave message, so the APIC IGMP snooping function must rely on the membership message timeout to indicate that no hosts remain that want to receive multicast data for a particular group.

**Note**

The IGMP snooping function ignores the configuration of the last member query interval when you enable the fast leave feature because it does not check for remaining hosts.

**The APIC IGMP Snooping Function and IGMPv3**

The IGMPv3 snooping function in APIC supports full IGMPv3 snooping, which provides constrained flooding based on the (S, G) information in the IGMPv3 reports. This source-based filtering enables the device to constrain multicast traffic to a set of ports based on the source that sends traffic to the multicast group.

By default, the IGMP snooping function tracks hosts on each VLAN port in the bridge domain. The explicit tracking feature provides a fast leave mechanism. Because every IGMPv3 host sends membership reports, report suppression limits the amount of traffic that the device sends to other multicast-capable routers. When report suppression is enabled, and no IGMPv1 or IGMPv2 hosts requested the same group, the IGMP snooping function provides proxy reporting. The proxy feature builds the group state from membership reports from the downstream hosts and generates membership reports in response to queries from upstream queriers.

Even though the IGMPv3 membership reports provide a full accounting of group members in a bridge domain, when the last host leaves, the software sends a membership query. You can configure the parameter last member query interval. If no host responds before the timeout, the IGMP snooping function removes the group state.

**Cisco APIC and the IGMP Snooping Querier Function**

When PIM is not enabled on an interface because the multicast traffic does not need to be routed, you must configure an IGMP snooping querier function to send membership queries. Within APIC, you define within the IGMP Snoop policy, the querier in a bridge domain that contains multicast sources and receivers but no other active querier.
The querier function can be configured to use any IP address in the bridge domain. As a best practice, a unique IP address, one that is not already used by the switch interface or the Hot Standby Router Protocol (HSRP) virtual IP address, should be configured so as to easily reference the querier function.

**Note**  
The IP address for the querier should not be a broadcast IP address, multicast IP address, or 0 (0.0.0.0).

When an IGMP snooping querier is enabled, it sends out periodic IGMP queries that trigger IGMP report messages from hosts that want to receive IP multicast traffic. IGMP snooping listens to these IGMP reports to establish appropriate forwarding.

The IGMP snooping querier performs querier election as described in RFC 2236. Querier election occurs in the following configurations:

- When there are multiple switch queriers configured with the same subnet on the same VLAN on different switches.
- When the configured switch querier is in the same subnet as with other Layer 3 SVI queriers.

### Prerequisites for IGMP Snooping in APIC

IGMP snooping has the following prerequisites:

- You are logged onto the device.

### Guidelines and Limitations for the APIC IGMP Snooping Function

The APIC IGMP snooping has the following guidelines and limitations:

- Layer 3 IPv6 multicast routing is not supported.
- Layer 2 IPv6 multicast packets will be flooded on the incoming bridge domain.

### Configuring and Assigning an IGMP Snoop Policy

#### Configuring and Assigning an IGMP Snoop Policy to a Bridge Domain in the Advanced GUI

To implement IGMP snooping functionality, you configure an IGMP Snoop policy then assign that policy to one or more bridge domains.

#### Configuring an IGMP Snoop Policy Using the Advanced GUI

Create an IGMP Snoop policy whose IGMP settings can be assigned to one or multiple bridge domains.

**Procedure**

1. Click the **Tenants** tab and the name of the tenant on whose bridge domain you intend to configure IGMP snooping support.
2. Then, in the **Navigation** pane, click **Networking > Protocol Policies > IGMP Snoop**.
3. Right-click **IGMP Snoop** and select **Create IGMP Snoop Policy**.
4. In the **Create IGMP Snoop Policy** dialog, configure a policy as follows:
a) Name and Description fields, enter and policy name and description.
b) In the Admin State field, select Enabled or Disabled to enable or disable this entire policy.
c) Select or unselect Fast Leave to enable or disable IGMP V2 immediate dropping of queries through this policy.
d) Select or unselect Enable querier to enable or disable the IGMP querier activity through this policy.

Note: For this option to be effectively enabled, the Subnet Control: Querier IP setting must also be enabled in the subnets assigned to the bridge domains to which this policy is applied. The navigation path to the properties page on which this setting is located is Tenants > tenant_name > Networking > Bridge Domains > bridge_domain_name > Subnets > subnet_name.

e) Specify in seconds the Last Member Query Interval value for this policy.
IGMP uses this value when it receives an IGMPv2 Leave report. This means that at least one host wants to leave the group. After it receives the Leave report, it checks that the interface is not configured for IGMP Fast Leave and if not, it sends out an out-of-sequence query.

f) Specify in seconds the Query Interval value for this policy.
This value is used to define the amount of time the IGMP function will store a particular IGMP state if it does not hear any reports on the group.

g) Specify in seconds Query Response Interval value for this policy.
When a host receives the query packet, it starts counting to a random value, less that the maximum response time. When this timer expires, host replies with a report.

h) Specify the Start query Count value for this policy.
Number of queries sent at startup that are separated by the startup query interval. Values range from 1 to 10. The default is 2.

i) Specify in seconds a Start Query Interval for this policy.
By default, this interval is shorter than the query interval so that the software can establish the group state as quickly as possible. Values range from 1 to 18,000 seconds. The default is 31 seconds.

Step 5 Click Submit.

The new IGMP Snooping policy is listed in the Protocol Policies - IGMP Snooping summary page.

What to Do Next
To put this policy into effect, assign it to any bridge domain.

Assigning an IGMP Snooping Policy to a Bridge Domain Using the Advanced GUI
Assigning an IGMP Snooping policy to a bridge domain configures that bridge domain to use the IGMP Snooping properties specified in that policy.

Before You Begin

- Configure a bridge domain for a tenant.
- Configure the IGMP Snooping policy that will be attached to the bridge domain.
Procedure

Step 1  Click the APIC Tenants tab and select the name of the tenant whose bridge domains you intend to configure with an IGMP Snoop policy.

Step 2  In the APIC navigation pane click Networking > Bridge Domains, then select the bridge domain to which you intend to apply your policy-specified IGMP Snoop configuration.

Note  For the Enable Querier option on the assigned policy to be effectively enabled, the Subnet Control: Querier IP setting must also be enabled in the subnets assigned to the bridge domains to which this policy is applied. The navigation path to the properties page on which this setting is located is Tenants > tenant_name > Networking > Bridge Domains > bridge_domain_name > Subnets > subnet_name.

Step 3  In the Bridge-Domain - page select the Policy tab and the Main sub-tab.

Step 4  Scroll down to the IGMP Snoop Policy field and select the appropriate IGMP policy from the drop-down menu.

Step 5  Click Submit.

The target bridge domain is now associated with the IGMP Snoop configuration specified in its assigned policy.

Configuring and Assigning an IGMP Snoop Policy to a Bridge Domain using the NX-OS Style CLI

Before You Begin

- Create the tenant that will consume the IGMP Snoop policy.
- Create the bridge domain for the tenant, where you will attach the IGMP Snoop policy.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Create a snooping policy based on default values.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>The example NX-OS style CLI sequence:</td>
</tr>
<tr>
<td><code>apic1(config-tenant)# template ip igmp snooping policy cookieCut1</code></td>
<td>• Creates an IGMP Snoop policy named cookieCut1 with default values.</td>
</tr>
<tr>
<td><code>apic1(config-tenant-template-ip-igmp-snooping)# show run all</code></td>
<td>• Displays the default IGMP Snoop values for the policy cookieCut1.</td>
</tr>
</tbody>
</table>

```
# Command: show running -config all tenant foo template ip igmp snooping policy cookieCut1
# Time: Thu Oct 13 18:26:03 2016
tenant t_10
  template ip igmp snooping policy cookieCut1
    ip igmp snooping
    no ip igmp snooping fast-leave
    ip igmp snooping last-member-query-interval 1
    no ip igmp snooping querier
    ip igmp snooping query-interval 125
    ip igmp snooping query-max-response-time 10
    ip igmp snooping startup-query-count 2
    ip igmp snooping startup-query-interval 31
    no description
  exit
```
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>exit</td>
<td></td>
</tr>
<tr>
<td>apic1(config-tenant-template-ip-igmp-snooping)#</td>
<td></td>
</tr>
</tbody>
</table>

### Step 2
Modify the snooping policy as necessary.

**Example:**

```bash
apic1(config-tenant-template-ip-igmp-snooping)# ip igmp snooping query-interval 300
apic1(config-tenant-template-ip-igmp-snooping)# show run all
# Command: show running-config all tenant foo template ip igmp snooping policy cookieCut1
#Time: Thu Oct 13 18:26:03 2016
tenant foo
template ip igmp snooping policy cookieCut1
  ip igmp snooping
  no ip igmp snooping fast-leave
  ip igmp snooping last-member-query-interval 1
  no ip igmp snooping querier
  ip igmp snooping query-interval 300
  ip igmp snooping query-max-response-time 10
  ip igmp snooping startup-query-count 2
  ip igmp snooping startup-query-interval 31
  no description
exit
exit
apic1(config-tenant-template-ip-igmp-snooping)# exit
apic1(config-tenant)#
```

**Note**
The `ip igmp optimise-multicast-flood` command is deprecated. It is only allowed for backward compatibility.

The example NX-OS style CLI sequence:

- Specifies a custom value for the query-interval value in the IGMP Snooping policy named cookieCut1.
- Confirms the modified IGMP Snooping value for the policy cookieCut1.

### Step 3
Assign the policy to a bridge domain.

**Example:**

```bash
apic1(config-tenant)# int bridge-domain bd3
apic1(config-tenant-interface)# ip igmp snooping policy cookieCut1
```

**What to Do Next**
You can assign the IGMP Snooping policy to multiple bridge domains.

**Configuring and Assigning an IGMP Snooping Policy to a Bridge Domain using the REST API**

**Procedure**

To configure an IGMP Snooping policy and assign it to a bridge domain, send a post with XML such as the following example:

**Example:**

```xml
https://apic-ip-address/api/node/mo/uni/.xml
<fvTenant name="mcast_tenant1">
<!-- Create an IGMP snooping template, and provide the options -->
<igmpSnoopPol name="igmp_snp_bd_21"
```

8
This example creates and configures the IGMP Snoop policy, igmp_snp_bd_12 with the following properties, and binds the IGMP policy, igmp_snp_bd_21, to bridge domain, bd_21:

- Administrative state is enabled
- Last Member Query Interval is the default 1 second.
- Query Interval is the default 125.
- Query Response interval is the default 10 seconds
- The Start Query Count is the default 2 messages
- The Start Query interval is 35 seconds.

Enabling IGMP Snoop Static Port Groups

IGMP static port grouping enables you to pre-provision ports, already statically-assigned to an application EPG, as the switch ports to receive and process IGMP multicast traffic. This pre-provisioning prevents the join latency which normally occurs when the IGMP snooping stack learns ports dynamically.

Static group membership can be pre-provisioned only on static ports assigned to an application EPG.

Static group membership can be configured through the APIC GUI, CLI, and REST API interfaces.

Enabling IGMP Layer 2 Multicast on Static Ports in the Advanced GUI

You can enable IGMP snooping and Layer 2 multicasting on ports that have been statically assigned to an EPG. Afterwards you can create and assign access groups of users that are permitted or denied access to the IGMP snooping and multicast traffic enabled on those ports.

Before You Begin

Before you begin to enable IGMP snooping and Layer 2 multicasting for an EPG, complete the following tasks.

- Identify the interfaces to enable this function and statically assign them to that EPG

Note: For details on static port assignment, see Deploying an EPG on a Specific Port with APIC Using the GUI, on page 16

- Identify the IP addresses that you want to be recipients of IGMP snoop layer 2 multicast traffic.
Procedure

Step 1  Click Tenant > tenant_name > Application Profiles > application_name > Application EPGs > epg_name > Static Ports.
Navigating to this spot displays all the ports you have statically assigned to the target EPG.

Step 2  Click the port to which you intend to statically assign group members for IGMP snooping. This action displays the Static Port Configuration page.

Step 3  On the Static Port Configuration page, click Actions > Create IGMP Snoop Address Group Group to display the IGMP Static Group table at the bottom of the page.

Step 4  Locate the IGMP Snoop Static Group table and click + to add an IGMP Snoop Address Group entry. Adding an IGMP Snoop Address Group entry associates the target static port with a specified multicast IP address and enables it to process the IGMP snoop traffic received at that address.

a) In the Group Address field, enter the multicast IP address to associate with his interface and this EPG.

b) In the Source Address field enter the IP address of the source to the multicast stream, if applicable.

c) Click Submit.
When configuration is complete, the target interface is enabled to process IGMP Snooping protocol traffic sent to its associated multicast IP address.

Note  You can repeat this step to associate additional multicast addresses with the target static port.

Step 5  Click Submit.

Enabling IGMP Layer 2 Multicast on Static Ports in the NX-OS Style CLI

You can enable IGMP snooping and Layer 2 multicasting on ports that have been statically assigned to an EPG. Then you can create and assign access groups of users that are permitted or denied access to the IGMP snooping and multicast traffic enabled on those ports.

The steps described in this task assume the pre-configuration of the following entities:

- Tenant: tenant_A
- Application: application_A
- EPG: epg_A
- Bridge Domain: bridge_domain_A
- vrf: vrf_A -- a member of bridge_domain_A
- VLAN Domain: vd_A (configured with a range of 300-310)
- Leaf switch: 101 and interface 1/10
  The target interface 1/10 on switch 101 is associated with VLAN 305 and statically linked with tenant_A, application_A, epg_A
- Leaf switch: 101 and interface 1/11
  The target interface 1/11 on switch 101 is associated with VLAN 309 and statically linked with tenant_A, application_A, epg_A
Before You Begin

Before you begin to enable IGMP snooping and Layer 2 multicasting for an EPG, complete the following tasks.

- Identify the interfaces to enable this function and statically assign them to that EPG

Note

- Identify the IP addresses that you want to be recipients of IGMP snoop layer 2 multicast traffic.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>On the target interfaces enable IGMP snooping and layer 2 multicasting</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>The example sequences enable:</td>
</tr>
<tr>
<td>apic1# conf t</td>
<td>• IGMP snooping on the statically-linked target interface 1/10 and associates it with a multicast IP address, 225.1.1.1</td>
</tr>
<tr>
<td>apic1(config)# tenant tenant_A</td>
<td>• IGMP snooping on the statically-linked target interface 1/11 and associates it with a multicast IP address, 227.1.1.1</td>
</tr>
<tr>
<td>apic1(config-tenant)# application application_A</td>
<td></td>
</tr>
<tr>
<td>apic1(config-tenant-app)# epg epg_A</td>
<td></td>
</tr>
<tr>
<td>apic1(config-tenant-app-epg)# ip igmp snooping static-group 225.1.1.1 leaf 101 interface ethernet 1/10 vlan 305</td>
<td></td>
</tr>
<tr>
<td>apic1(config-tenant-app-epg)# end</td>
<td></td>
</tr>
<tr>
<td>apic1# conf t</td>
<td></td>
</tr>
<tr>
<td>apic1(config)# tenant tenant_A; application application_A; epg epg_A</td>
<td></td>
</tr>
<tr>
<td>apic1(config-tenant-app-epg)# ip igmp snooping static-group 227.1.1.1 leaf 101 interface ethernet 1/11 vlan 309</td>
<td></td>
</tr>
<tr>
<td>apic1(config-tenant-app-epg)# exit</td>
<td></td>
</tr>
<tr>
<td>apic1(config-tenant-app)# exit</td>
<td></td>
</tr>
</tbody>
</table>

Enabling IGMP Layer 2 Multicast on Static Ports Using the REST API

You can enable IGMP snoop and layer 2 multicast processing on ports that have been statically assigned to an EPG. You can create and assign access groups of users that are permitted or denied access to the IGMP snoop and multicast traffic enabled on those ports.

Before You Begin

Procedure

To configure application EPGs with static ports, enable those ports to receive and process IGMP snoop and layer 2 multicast traffic, and assign groups to access or be denied access to that traffic, send a post with XML such as the following example.
In the following example, IGMP snoop is enabled on leaf 102 interface 1/10 on VLAN 202. Multicast IP addresses 224.1.1.1 and 225.1.1.1 are associated with this port.

Example:
https://apic-ip-address/api/node/mo/uni.xml

```xml
<fvTenant name="tenant_A">
  <fvAp name="apppllication_A">
    <fvAEPg name="epg_A">
      <fvRsPathAtt encap="vlan-202" instrImedcy="immediate" mode="regular" tDn="topology/pod-1/paths-102/pathep-[eth1/10]">
        <!-- IGMP snooping static group case -->
        <igmpSnoopStaticGroup group="224.1.1.1" source="0.0.0.0"/>
        <igmpSnoopStaticGroup group="225.1.1.1" source="2.2.2.2"/>
      </fvRsPathAtt>
    </fvAEPg>
  </fvAp>
</fvTenant>
```

### Enabling IGMP Snoop Access Groups

An "access-group" is used to control what streams can be joined behind a given port.

An access-group configuration can be applied on interfaces that are statically assigned to an application EPG in order to ensure that the configuration can be applied on ports that will actually belong to the that EPG.

Only Route-map-based access groups are allowed.

IGMP snoop access groups can be configured through the APIC GUI, CLI, and REST API interfaces.

### Enabling Group Access to IGMP Layer 2 Multicast in the GUI

After you enable IGMP snooping and Layer 2 multicasting on ports that have been statically assigned to an EPG, you can then create and assign access groups of users that are permitted or denied access to the IGMP snooping and multicast traffic enabled on those ports.

**Before You Begin**

Before you enable access to IGMP snooping and Layer 2 multicasting for an EPG, Identify the interfaces to enable this function and statically assign them to that EPG.

**Note**

For details on static port assignment, see Deploying an EPG on a Specific Port with APIC Using the GUI, on page 16

**Procedure**

**Step 1**

Click Tenant > tenant_name > Application Profiles > application_name > Application EPGs > epg_name > Static Ports.

Navigating to this spot displays all the ports you have statically assigned to the target EPG.

**Step 2**

Click the port to which you intend to assign multicast group access.to display the page.
This action displays the **Static Port Configuration** window.

**Step 3**
Click **Actions > Create IGMP Snoop Access Group** to display the IGMP Snoop Access Group table.

**Step 4**
Locate the IGMP Snoop Access Group table and click + to add an access group entry. Adding an IGMP Snoop Access Group entry creates a user group with access to this port, associates it with a multicast IP address, and permits or denies that group access to the IGMP snoop traffic received at that address.

- a) select **Create RouteMap Policy** to display the **Create RouteMap Policy** window.
- b) In the **Name** field assign the name of the group that you want to allow or deny multicast traffic.
- c) In the **RouteMaps** table click + to display the route map dialog.
- d) In the **Order** field, if multiple access groups are being configured for this interface, select a number that reflects the order in which this access group will be permitted or denied access to the multicast traffic on this interface. Lower-numbered access groups are ordered before higher-numbered access groups.
- e) In the **Group IP** field enter the multicast IP address whose traffic is to be allowed or blocked for this access group.
- f) In the **Source IP** field, enter the IP address of the source if applicable.
- g) In the **Action** field, choose **Deny** to deny access for the target group or **Permit** to allow access for the target group.
- h) Click **OK**.
- i) Click **Submit**.

When the configuration is complete, the configured IGMP snoop access group is assigned a multicast IP address through the target static port and permitted or denied access to the multicast streams that are received at that address.

**Note**
- You can repeat this step to configure and associate additional access groups with multicast IP addresses through the target static port.
- To review the settings for the configured access groups, click to the following location: **Tenant > tenant_name > Networking > Protocol Policies > Route Maps > route_map_access_group_name**.

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

---

**Enabling Group Access to IGMP Layer 2 Multicast using the NX-OS Style CLI**

After you have enabled IGMP snooping and Layer 2 multicasting on ports that have been statically assigned to an EPG, you can then create and assign access groups of users that are permitted or denied access to the IGMP snooping and multicast traffic enabled on those ports.

The steps described in this task assume the pre-configuration of the following entities:

- Tenant: tenant_A
- Application: application_A
- EPG: epg_A
- Bridge Domain: bridge_domain_A
- vrf: vrf_A -- a member of bridge_domain_A
- VLAN Domain: vd_A (configured with a range of 300-310)
- Leaf switch: 101 and interface 1/10

The target interface 1/10 on switch 101 is associated with VLAN 305 and statically linked with tenant_A, application_A, epg_A

- Leaf switch: 101 and interface 1/11

---

13
The target interface 1/11 on switch 101 is associated with VLAN 309 and statically linked with tenant_A, application_A, epg_A

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Define the route-map &quot;access groups.&quot;</td>
<td>The example sequences configure:</td>
</tr>
<tr>
<td><strong>Example:</strong> apic1# conf t</td>
<td>- Route-map-access group &quot;foobroker&quot; linked to multicast group 225.1.1.1/24, access permitted</td>
</tr>
<tr>
<td>apic1(config)# tenant tenant_A; application application_A; epg epg_A</td>
<td>- Route-map-access group &quot;foobroker&quot; linked to multicast group 227.1.1.1/24, access denied</td>
</tr>
<tr>
<td>apic1(config-tenant)# route-map fooBroker permit</td>
<td>- Route-map-access group &quot;newbroker&quot; connected through leaf switch 101, interface 1/10, and VLAN 305.</td>
</tr>
<tr>
<td>apic1(config-tenant-rtmap)# match ip multicast group 225.1.1.1/24</td>
<td>- Route-map-access group &quot;newbroker&quot; connected through leaf switch 101, interface 1/10, and VLAN 305.</td>
</tr>
<tr>
<td>apic1(config-tenant-rtmap)# exit</td>
<td>- Route-map-access group &quot;newbroker&quot; connected through leaf switch 101, interface 1/10, and VLAN 305.</td>
</tr>
<tr>
<td>apic1(config-tenant)# route-map fooBroker deny</td>
<td>- Route-map-access group &quot;newbroker&quot; connected through leaf switch 101, interface 1/10, and VLAN 305.</td>
</tr>
<tr>
<td>apic1(config-tenant-rtmap)# match ip multicast group 227.1.1.1/24</td>
<td>- Route-map-access group &quot;newbroker&quot; connected through leaf switch 101, interface 1/10, and VLAN 305.</td>
</tr>
<tr>
<td>apic1(config-tenant-rtmap)# exit</td>
<td>- Route-map-access group &quot;newbroker&quot; connected through leaf switch 101, interface 1/10, and VLAN 305.</td>
</tr>
<tr>
<td><strong>Step 2</strong> Verify route map configurations.</td>
<td>The example sequences configure:</td>
</tr>
<tr>
<td><strong>Example:</strong> apic1(config-tenant)# show running-config tenant test route-map fooBroker</td>
<td>- Route-map-access group &quot;newbroker&quot; connected through leaf switch 101, interface 1/10, and VLAN 305.</td>
</tr>
<tr>
<td># Command: show running-config tenant test route-map fooBroker</td>
<td>- Route-map-access group &quot;newbroker&quot; connected through leaf switch 101, interface 1/10, and VLAN 305.</td>
</tr>
<tr>
<td># Time: Mon Aug 29 14:34:30 2016</td>
<td>- Route-map-access group &quot;newbroker&quot; connected through leaf switch 101, interface 1/10, and VLAN 305.</td>
</tr>
<tr>
<td>tenant test</td>
<td>- Route-map-access group &quot;newbroker&quot; connected through leaf switch 101, interface 1/10, and VLAN 305.</td>
</tr>
<tr>
<td>route-map fooBroker permit 10</td>
<td>- Route-map-access group &quot;newbroker&quot; connected through leaf switch 101, interface 1/10, and VLAN 305.</td>
</tr>
<tr>
<td>match ip multicast group 225.1.1.1/24</td>
<td>- Route-map-access group &quot;newbroker&quot; connected through leaf switch 101, interface 1/10, and VLAN 305.</td>
</tr>
<tr>
<td>exit</td>
<td>- Route-map-access group &quot;newbroker&quot; connected through leaf switch 101, interface 1/10, and VLAN 305.</td>
</tr>
<tr>
<td>route-map fooBroker deny 20</td>
<td>- Route-map-access group &quot;newbroker&quot; connected through leaf switch 101, interface 1/10, and VLAN 305.</td>
</tr>
<tr>
<td>match ip multicast group 227.1.1.1/24</td>
<td>- Route-map-access group &quot;newbroker&quot; connected through leaf switch 101, interface 1/10, and VLAN 305.</td>
</tr>
<tr>
<td>exit</td>
<td>- Route-map-access group &quot;newbroker&quot; connected through leaf switch 101, interface 1/10, and VLAN 305.</td>
</tr>
<tr>
<td>exit</td>
<td>- Route-map-access group &quot;newbroker&quot; connected through leaf switch 101, interface 1/10, and VLAN 305.</td>
</tr>
<tr>
<td><strong>Step 3</strong> Specify the access group connection path.</td>
<td>The example sequences configure:</td>
</tr>
<tr>
<td><strong>Example:</strong> apic1(config-tenant)# application application_A</td>
<td>- Route-map-access group &quot;newbroker&quot; connected through leaf switch 101, interface 1/10, and VLAN 305.</td>
</tr>
<tr>
<td>apic1(config-tenant-app)# epg epg_A</td>
<td>- Route-map-access group &quot;newbroker&quot; connected through leaf switch 101, interface 1/10, and VLAN 305.</td>
</tr>
<tr>
<td>apic1(config-tenant-app-epg)# ip igmp snooping access-group route-map newBroker leaf 101 interface ethernet 1/10 vlan 305</td>
<td>- Route-map-access group &quot;newbroker&quot; connected through leaf switch 101, interface 1/10, and VLAN 305.</td>
</tr>
<tr>
<td>apic1(config-tenant-app-epg)# ip igmp snooping access-group route-map newBroker leaf 101 interface ethernet 1/10 vlan 305</td>
<td>- Route-map-access group &quot;newbroker&quot; connected through leaf switch 101, interface 1/10, and VLAN 305.</td>
</tr>
<tr>
<td><strong>Step 4</strong> Verify the access group connections.</td>
<td>The example sequences configure:</td>
</tr>
<tr>
<td><strong>Example:</strong> apic1(config-tenant-app-epg)# show run</td>
<td>- Route-map-access group &quot;newbroker&quot; connected through leaf switch 101, interface 1/10, and VLAN 305.</td>
</tr>
<tr>
<td># Command: show running-config tenant tenant_A application application_A epg epg_A</td>
<td>- Route-map-access group &quot;newbroker&quot; connected through leaf switch 101, interface 1/10, and VLAN 305.</td>
</tr>
<tr>
<td># Time: Mon Aug 29 14:43:02 2016</td>
<td>- Route-map-access group &quot;newbroker&quot; connected through leaf switch 101, interface 1/10, and VLAN 305.</td>
</tr>
<tr>
<td>tenant tenant_A</td>
<td>- Route-map-access group &quot;newbroker&quot; connected through leaf switch 101, interface 1/10, and VLAN 305.</td>
</tr>
</tbody>
</table>
### Enabling Group Access to IGMP Layer 2 Multicast using REST API

After you have enabled IGMP snooping and Layer 2 multicasting on ports that have been statically assigned to an EPG, you can then create and assign access groups of users that are permitted or denied access to the IGMP snooping and multicast traffic enabled on those ports.

#### Procedure

Define the access group, "foobroker."

The following example sequence configures: Access group "foobroker" associated with tenant_A, Rmap_A, application_A, epg_A, on leaf 102, interface 1/10, VLAN 202. By association with Rmap_A, the access group "foobroker" has access to multicast traffic received at multicast address 226.1.1.1/24 and is denied access to traffic received at multicast address 227.1.1.1/24.

#### Example:

```xml
<!-- api/node/mo/uni/.xml -->
<fvTenant name="tenant_A">
    <pimRouteMapPol name="Rmap_A">
        <pimRouteMapEntry action="permit" grp="226.1.1.1/24" order="10"/>
        <pimRouteMapEntry action="deny" grp="227.1.1.1/24" order="20"/>
    </pimRouteMapPol>
    <fvAp name="application_A">
        <fvAEPg name="epg_A">
            <fvRsPathAtt encap="vlan-202" instrImedcy="immediate" mode="regular" tDn="topology/pod-1/paths-102/pathep-[eth1/10]">
                <!-- IGMP snooping access group case -->
                <igmpSnoopAccessGroup name="foobroker"/>
            </fvRsPathAtt>
            <fvRsSnoopAccessGroupFilterRMap tPimRouteMapPolName="Rmap_A"/>
        </fvAEPg>
    </fvAp>
</fvTenant>
```
EPG Static Port Deployment

Enabling IGMP snooping processing on ports requires as a prerequisite that the target ports be statically-assigned to associated EPGs. Static deployment of ports can be configured through the APIC GUI, CLI, or REST API interfaces.

Deploying an EPG on a Specific Port with APIC Using the GUI

Before You Begin
The tenant where you deploy the EPG is already created.

Procedure

Step 1 On the menubar, click TENANTS.
Step 2 In the Navigation pane, expand the appropriate Tenant_name > Application Profiles.
Step 3 Right-click Application Profiles and click Create Application Profile.
Step 4 In the Create Application Profile dialog box, perform the following actions:
   a) In the Name field, enter a name for the application profile.
   b) Expand EPGs.
   c) In the Create Application EPG dialog box, in the Name field, enter an EPG name.
   d) In the Statically Link with Leaves/Paths field, check the checkbox for Statically Link with Leaves/Paths. (this is selected to specify on which port the EPG is required to be deployed). Click Next.
   e) In the Leaves/Paths area, expand Paths.
      In this example we are deploying the EPG on the port of a node. Alternatively, you could choose to deploy the EPG on a node.
      f) From the Path drop-down list, choose the appropriate node and port.
      g) In the Deployment Immediacy field drop-down list, choose the preferred deployment time.
      h) In the Mode field, choose the appropriate mode.
      i) In the Port Encap field, enter the secondary VLAN to be deployed.
      j) In the Primary Encap field, enter the primary VLAN to be deployed.
      k) Click Update, and click Finish.
Step 5 In the Navigation pane, expand Application Profiles to view the new application profile.
Step 6 Expand Application EPGs, to view the new EPG.
Step 7 Expand the EPG and click Static Bindings (Paths), and in the Properties pane, view the details of the static binding paths that are established.
# Deploying an EPG on a Specific Port with APIC Using the NX-OS Style CLI

## Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Step 1** | Configure a VLAN domain:  
**Example:**  
```  
apic1(config)# vlan-domain dom1  
apic1(config-vlan)# vlan 10-100  
``` |
| **Step 2** | Create a tenant:  
**Example:**  
```  
apic1# configure  
apic1(config)# tenant t1  
``` |
| **Step 3** | Create a private network/VRF:  
**Example:**  
```  
apic1(config-tenant)# vrf context ctx1  
apic1(config-tenant-vrf)# exit  
``` |
| **Step 4** | Create a bridge domain:  
**Example:**  
```  
apic1(config-tenant)# bridge-domain bd1  
apic1(config-tenant-bd)# vrf member ctx1  
apic1(config-tenant-bd)# exit  
``` |
| **Step 5** | Create an application profile and an application EPG:  
**Example:**  
```  
apic1(config-tenant)# application AP1  
apic1(config-tenant-app)# epg EPG1  
apic1(config-tenant-app-epg)# bridge-domain member bd1  
apic1(config-tenant-app-epg)# exit  
apic1(config-tenant-app)# exit  
apic1(config-tenant)# exit  
``` |
| **Step 6** | Associate the EPG with a specific port:  
**Example:**  
```  
apic1(config)# leaf 1017  
apic1(config-leaf)# interface ethernet 1/13  
apic1(config-leaf-if)# vlan-domain member dom1  
apic1(config-leaf-if)# switchport trunk allowed vlan 20 tenant t1 application AP1 epg EPG1  
``` |

**Note**  
The vlan-domain and vlan-domain member commands mentioned in the above example are a pre-requisite for deploying an EPG on a port.
Deploying an EPG on a Specific Port with APIC Using the REST API

Before You Begin
The tenant where you deploy the EPG is created.

Procedure
Deploy an EPG on a specific port.

Example:
```xml
<fvTenant name="<tenant_name>" dn="uni/tn-test1">
  <fvCtx name="<network_name>" pcEnfPref="enforced" knwMcastAct="permit"/>
  <fvBD name="<bridge_domain_name>" unkMcastAct="flood">
    <fvRsCtx tnFvCtxName="<network_name/>
  </fvBD>
  <fvAp name="<application_profile>">
    <fvAEPg name="<epg_name>">
      <fvRsPathAtt tDn="topology/pod-1/paths-1017/pathep-[eth1/13]" mode="regular" instrImedcy="immediate" encap="vlan-20">
      </fvRsPathAtt>
    </fvAEPg>
  </fvAp>
</fvTenant>
```
Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.