Multicast support

IP multicast is a method of sending Internet Protocol (IP) datagrams to a group of interested receivers in a single transmission. It is often employed for streaming media applications on the Internet and private networks. Since traffic is sent from the source once in total, instead of once per recipient, throughput can be saved.

Each host (and in fact each application on the host) that wants to be a receiving member of a multicast group (i.e. receive data corresponding to a particular multicast address) must use the Internet Group Management Protocol (IGMP) to join. A detailed article on how nodes join and leave multicast groups can be found [here](#). Below is a packet capture with details of the joining process.

IGMP membership

<table>
<thead>
<tr>
<th>No</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Length</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.000000</td>
<td>192.168.1.2</td>
<td>224.0.0.1</td>
<td>IGMPv2</td>
<td>60</td>
<td>Membership Query, general</td>
</tr>
<tr>
<td>2</td>
<td>0.928423</td>
<td>192.168.1.64</td>
<td>239.255.255.250</td>
<td>IGMPv2</td>
<td>48</td>
<td>Membership Report group 239.255.255.250</td>
</tr>
<tr>
<td>3</td>
<td>7.062878</td>
<td>192.168.1.201</td>
<td>225.10.10.10</td>
<td>IGMPv2</td>
<td>60</td>
<td>Membership Report group 225.10.10.10</td>
</tr>
<tr>
<td>4</td>
<td>8.412740</td>
<td>192.168.1.201</td>
<td>225.1.1.3</td>
<td>IGMPv2</td>
<td>60</td>
<td>Membership Report group 225.1.1.3</td>
</tr>
<tr>
<td>5</td>
<td>19.522691</td>
<td>192.168.1.201</td>
<td>224.0.0.2</td>
<td>IGMPv2</td>
<td>60</td>
<td>Leave Group 225.1.1.3</td>
</tr>
<tr>
<td>6</td>
<td>19.532213</td>
<td>192.168.1.2</td>
<td>225.1.1.3</td>
<td>IGMPv2</td>
<td>60</td>
<td>Membership Query, specific for group 225.1.1.3</td>
</tr>
</tbody>
</table>

The first packet, a membership query, is sent when a member wants to know about the other members of a multicast group. The membership reports are sent by the various members, announcing that they belong to the group. These membership reports are also how a member joins the group in the first place. The leave group message is the opposite of a membership report, and indicates that the member is no longer part of the multicast group.

**IGMP snooping** is the process of listening to IGMP network traffic. The feature allows a network switch to listen in on the IGMP conversation between hosts and routers. By listening to these conversations the switch maintains a map of which links need which IP multicast streams. Multicasts are filtered from the links which do not need them and thus controls which ports receive specific multicast traffic.

IGMP Support on the Cisco Meraki Security Appliance

MX Security Appliances will forward IGMP traffic for a single broadcast domain. It does not forward multicast traffic upstream, between VLANs, or over a VPN.

IGMP Support on the Cisco Meraki Switch

MS Switches can forward IGMP traffic, but will run IGMP snooping by default. This prevents the switch from sending multicast traffic to hosts who are not yet joined with the proper multicast group. IGMP Snooping can be disabled under the **Switch > Switch Settings** page in Dashboard.

Certain Cisco Meraki switches support multicast routing; specifically, Protocol Independent Multicast - Sparse Mode (PIM-SM). For more information, see **MS Multicast Routing Overview**.

**Note:** PIM-SM and IGMP Querier are available in switch-9. You can check your current firmware version on the **Organization > Firmware Upgrades** page.

**Note:** IGMPv1 is not supported with IGMP snooping. However, the switch will forward IGMPv1 packets with snooping disabled.
IGMP Querier

An IGMP querier is required for IGMP snooping to operate per RFC4604. To configure an IGMP querier:

1. Navigate to **Switch > Configure > Routing and DHCP**.
2. Select or **Add an interface**.
3. Enter **Name**, **Interface IP**, and **VLAN**.
4. Under **multicast support**, select **Enable IGMP snooping querier**.

   ![Interface Configuration](image)

5. Click **Save**.

**Note:** Adding a new L3 interface on an MS390 automatically enables an IGMP querier for that VLAN.

IGMP Support in the Cisco Meraki APs

The MR Access Points will forward multicast and IGMP traffic, but does not itself participate in the process. This means that an MR Access Point will not prevent clients from joining a multicast group, but it will not itself be a destination. In addition, multicast-to-unicast is enabled on all MR Access Points by default. More information on this behavior can be found [here](#).