VIP-NET-2804PP-1G
VIP-NET-4804PP-1G
VIP-NET-0424-1G

Multicast Configuration Guide

L2+
‘Media Hub’ Managed Switch
IGMP Overview

Internet Group Management Protocol (IGMP) allows devices to establish multicast group memberships. The routes between transmitters (sources) and receivers (outputs) is maintained by a table on each switch or router on the multicast network. The master route table is maintained by an IGMP Querier that is either statically or dynamically assigned (*Querier Election). An IGMP aware switch is crucial in sending large amounts of data through a network for time sensitive data like video or audio. IGMP aware switches are capable of treating multicast data packets as directed traffic rather than blindly broadcasting the data packets to every port of the switch. Only devices that have elected to join a multicast group will receive multicast data packets allowing for more efficient network routing.

With Querier Election, each switch starts off assuming it is the IGMP Querier and builds a table of all locally connected multicast devices. After it has identified each multicast device, and the associated groups, it looks for a Router Port (switch-to-switch interconnect). An IGMP Query is sent out each Router Port and the switches begin to elect a single switch as the IGMP Querier (the switch responsible for building the master route table between transmitters and receivers). This is repeated until the switch with the lowest management IP address is located and selected as the IGMP Querier.

Proper configuration allows this process to complete the routing table necessary for connecting transmitters and receivers across VIP-NET.

*Note: Querier Election is not supported by IGMPv1 devices.
IGMP Snooping

IGMP Snooping is passive and can take 1-2 minutes to build out the routing table when switches are first started up, particularly with a large deployment of multicast devices.

1. Login to the VIP-NET switch
2. On the left-hand menu, select Multicast → IGMP Snooping → Basic Configuration

   a. Global Configuration
      i. Snooping Enabled → Checked
      ii. Unregistered IPMCv4 Flooding Enabled → Unchecked
      iii. IGMP SSM Range → Default Value
      iv. Leave Proxy Enabled → Unchecked
      v. Proxy Enabled → Unchecked
   b. Port Related Configuration
      i. Any port that has an Encoder (Transmitter) connected needs to have the Fast Leave box checked.
ii. Ports 49-52 are used for SFP+ 10Gb switch interconnects. Any port that is connected to another switch should have Router Port checked.

ii. All other settings can be left as default values.

c. After any changes, click Apply at the bottom of the page, then Save to Startup Config in the top Right Corner.

3. On the left hand menu, select Multicast → VLAN Configuration

   a. If there is no VLAN defined, click “Add New IGMP VLAN”
      i. VLAN ID → 1
      ii. Snooping Enabled → Checked
      iii. Querier Election → Checked
iv. Querier Address → Blank or default
v. Compatibility → IGMP-Auto
vi. PRI → Default Value
vii. RV → Default Value
viii. QI (sec) → Default Value
ix. QRI (0.1 sec) → Default Value
x. LLQI (0.1 sec) → Default Value
xi. URI (sec) → Default Value

b. After any changes, click Apply at the bottom of the page, then Save to Startup Config in the top Right Corner.
Link Aggregation – LACP

Link Aggregation Control Protocol allows for automatic determination, configuration, and monitoring of Link Aggregation Group members. LACP will automatically discover any duplicate routes between any two switches and aggregate them into a single connection so long as LACP is enabled on each port utilized on both switches. Any two switches that are connected via two or more 10G switch-to-switch interconnects should utilize LACP to maximize available bandwidth.

1. Login to the VIP-NET switch
2. On the left hand menu, select Port Management → Link Aggregation → LACP Configuration
3. Locate the 10G ports that are connected switch-to-switch and check the checkbox for LACP Enabled
4. Set the Key value to a number e.g. 1 for each port that is connected to a second switch. You will need to follow the same guidelines for the second switch. If there is a third switch, you will
need to set a key value for the aggregated ports interlinked to that switch to a different Key value e.g. 2.

You can check the success of the settings in the Port Management>Internal Status and Port Management>Neighbor Status pages

5. After any changes, click Apply at the bottom of the page, then Save to Startup Config in the top Right Corner

In a two-switch configuration where switch 1 port 49-50 are connected to switch 2 port 49-50, only ports 49 and 50 on both switches will require the LACP Enabled checkbox to be checked.

In a configuration containing more than 2 switches connected in a series (S1 ←→ S2 ←→ S3), you may either enable LACP on all interconnect ports (49-52) or enable only ports 49-50 on the first and last switch in the series while enabling ports 49-52 on all intermediary switches between the first and last switch.

**IPMC Profile**

Port Filtering Profiles allow you to assign a filtering profile to a port for blocking or accepting traffic for specific multicast groups on a per port basis. IGMP Snooping should block multicast traffic to ports that have not elected to join a multicast group, but here you can define additional rules, or block multicast packets explicitly, rather than implicitly through IGMP Snooping built routing tables.

1. Login to the VIP-NET switch
2. On the left hand menu, select Multicast → Multicast Filtering Profile → Filtering Address Entry

   a. To block all Multicast traffic
      i. Select “Add New Address (Range) Entry”
      ii. Entry Name → NoMulticast
      iii. Start Address → 224.0.0.0
      iv. End Address → 239.255.255.254

   b. After any changes, click Apply at the bottom of the page, then Save to Startup Config in the top Right Corner
3. On the left-hand menu, select Multicast → Multicast Filtering Profile → Filtering Profile Table

   a. IPMC Profile Global Setting
      i. Multicast Filtering Profile Mode → Enabled

   b. IPMC Profile Table Setting
      i. If no profiles exist, click Add New IPMC Profile
         1. Profile Name → NoMulticast
         2. Profile Description → Blocks multicast traffic
c. Once a profile exists, click the edit icon under Rule on the right side of the IPMC Profile Table Setting table.

1. Click Add Last Rule

2. Under Entry Name, select NoMulticast.

3. Address Range will populate.

4. Action → Deny

5. Log → Disable

6. Click Commit

4. Apply the filtering profile to a specific port.
5. On the left-hand menu, select Multicast → IGMP Snooping → Basic Configuration

i. Locate the port number you would like to assign a filtering profile.

ii. Using the drop-down menu on the right side of the table, select the IPMC Profile for the port.

iii. After any changes, click Apply at the bottom of the page, then Save to Startup Config in the top Right Corner.