Multicast IGMP

This chapter describes how to identify and resolve problems that relate to multicast Internet Group Management Protocol (IGMP) snooping. This chapter contains the following sections:

Information About Multicast

IP multicast is a method of forwarding the same set of IP packets to a number of hosts within a network. You can use multicast in an IPv4 network to provide efficient delivery of data to multiple destinations.

Multicast involves both a method of delivery and discovery of senders and receivers of multicast data, which is transmitted on IP multicast addresses called groups. A multicast address that includes a group and source IP address is often referred to as a channel.

Multicast IGMP Snooping

IGMP snooping software examines Layer 2 IP multicast traffic within a VLAN to discover the ports where interested receivers reside. Using the port information, IGMP snooping can reduce bandwidth consumption in a multi-access LAN environment to avoid flooding the entire VLAN. The IGMP snooping feature tracks which ports are attached to multicast-capable routers to help the routers forward IGMP membership reports. The IGMP snooping software responds to topology change notifications.

In general, IGMP snooping works as follows:

- Ethernet switches, such as Cisco Catalyst 6000 Series switches, parse and intercept all IGMP packets and forward them to a CPU, such as a supervisor module, for protocol processing.
- Router ports are learned using IGMP queries. The switch returns IGMP queries, it remembers which port the query comes from, and marks the port as a router port.
- IGMP membership is learned using IGMP reports. The switch parses IGMP report packets and updates its multicast forwarding table to keep track of IGMP membership.
- When the switch receives multicast traffic, it check its multicast table and forwards the traffic only to those ports interested in the traffic.

- IGMP queries are flooded to the whole VLAN.
- IGMP reports are forwarded to the uplink port (the router ports).
- Multicast data traffic is forwarded to uplink ports (the router ports).

Multicast IGMP Troubleshooting Guidelines

Follow these guidelines when troubleshooting multicast IGMP issues:

- Verify that IGMP snooping is enabled by using the **show ip igmp snooping** command.
- Verify that the upstream switch has IGMP configured.
- Verify that the Cisco Nexus 1000V is configured correctly and is ready to forward multicast traffic by using the **show ip igmp snooping groups** command. In the displayed output of the command, look for the letter R under the port heading. The R indicates that the Virtual Supervisor Module (VSM) has learned the uplink router port from the IGMP query that was sent by the upstream switch, and means that the Cisco Nexus 1000V is ready to forward multicast traffic.

Note When high CPU utilization occurs on Cisco Nexus 1000V due to igmp and netstack processes, it is possible that it is caused by the UCS server looping a high amount of IGMP queries. For more troubleshooting information, see *UCS Troubleshooting Guide* or *UCS Release Notes*.

Upstream Switch Configuration for Multicast IGMP Snooping

The operation of multicast IGMP snooping depends on the correct configuration of the upstream switch. Because the IGMP process needs to know which upstream port connects to the router that supports IGMP routing, you must turn on the IP multicast routing on the upstream switch by entering the **ip multicast-routing** command.

The following example shows how to turn on global multicast routing, configure an SVI interface, and turn on the PIM routing protocol:

```
switch# conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ip multicast-routing
switch(config)# end

switch# conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# int vlan159
switch(config-if)# ip pim dense-mode
switch(config-if)# end
```

The following example shows a sample Cisco Nexus 5000 Series configuration that has an IGMP querier configured on a VLAN:

```
n5k-sw1(config)# vlan configuration 59
n5k-sw1(config-vlan-config)# ip igmp snooping querier 7.59.59.1
n5k-sw1(config-vlan-config)# ip igmp snooping query-interval 60
n5k-sw1(config-vlan-config)# ip igmp snooping version 3
n5k-sw1(config-vlan-config)#
```

Problems with Multicast IGMP Snooping

The following are symptoms, possible causes, and solutions for problems with multicast IGMP snooping.

Symptom	Solution
A VM is interested in the multicast traffic but is not receiving the multicast traffic.	Use the **debug ip igmp snooping vlan** command to determine if IGMP snooping is working as expected. Examine the output to see if the port is receiving the IGMP report and if the interface has been added to the multicast traffic interface list for the VM.
	Use the **module vem** *module-number* **execute vemcmd show vlan** command to verify that the multicast distribution table in the VEM has the correct information in it.
	Use the **module vem** *module-number* **execute vemcmd show port** command to see the port table. Make sure that the table has the correct information in it. Make sure that the state of the trunk port and the access port is UP/UP.

Enabling Debugging Commands for IGMP Snooping

You can enable debugging commands for IGMP snooping:

Procedure

Step 1 Enable logs files on the module that hosts the preferred VMs/Veths.

Example:

```
switch(config)# module vem 4 execute vemdpalog debug sfigmp_snoop d
switch(config)# module vem 4 execute vemlog debug sfigmp_snoop d
```

Step 2 (Optional) Clear existing log data.

Example:

```
switch(config)# module vem 4 execute vemlog clear
Cleared log
```

Step 3 Start collecting log data.

Example:

```
switch(config)# module vem 4 execute vemlog start
Started log
```

Step 4 Wait for the IGMP queries and reports to hit the VEM ports.

Step 5 Stop and verify the log data.

Example:

```
switch(config)# module vem 4 execute vemlog stop
Will suspend log after next 0 entries
switch(config)# module vem 4 execute vemlog show all
Timestamp                  Entry CPU  Mod Lv         Message
Jul 15 18:19:27.000679        0  0  99  16   Debug sf_igmp_snoop_thread: IGMP Snoop Thread
 waken up
```

```
Jul 15 18:19:27.000706        1  0  99  16   Debug sf_igmp_snoop_thread: Check timed-out
members in 0.0.0.0, BD: 52
Jul 15 18:19:27.000718        2  0  99  16   Debug sf_igmp_snoop_thread: Check timed-out
members in 0.0.0.0, BD: 55
Jul 15 18:19:27.000726        3  0  99  16   Debug sf_igmp_snoop_thread: Check timed-out
members in 0.0.0.0, BD: 59
Jul 15 18:19:27.000734        4  0  99  16   Debug sf_igmp_snoop_thread: Check timed-out
members in 224.6.7.8, BD: 59
Jul 15 18:19:27.112144        5  2   1  16   Debug IGMP pkt (snoop OFF): orig_src_ltl 0x15,
 src_ltl 0x40f vlan 232
Jul 15 18:19:27.603386        6  3   1  16   Debug IGMP pkt (snoop ON): orig_src_ltl 0x15,
 src_ltl 0x40f vlan 52
Jul 15 18:19:27.603390        7  3   1  16   Debug Notification size: 68
Jul 15 18:19:27.603393        8  3   1  16   Debug Sending IGMP pkt notif: swbd 52, pkt_size
 56, notif_size 68
Jul 15 18:19:27.609442        9  0  99  16   Debug sf_igmp_snoop_v4_pkt_notify_handler:
IGMP notify message from DP:
Jul 15 18:19:27.609459       10  0  99  16   Debug sf_igmp_snoop_v4_pkt_notify_handler:
SRC_LTL: 1039, SWBD: 52, pkt_size: 56
Jul 15 18:19:27.609470       11  0  99  16   Debug sf_igmp_snoop_v4_pkt_notify_handler: Got
 IGMP Query.
Jul 15 18:19:27.609479       12  0  99  16   Debug sf_igmp_snoop_handle_query: Received v3
 query.
Jul 15 18:19:27.609485       13  0  99  16   Debug sf_igmp_snoop_handle_query: Adding v3
router entry in BD 52 (len: 12).
Jul 15 18:19:27.609494       14  0  99  16   Debug sf_igmp_snoop_add_update_v4_grp: Existing
 Group 0.0.0.0 in BD 52.
Jul 15 18:19:27.609502       15  0  99  16   Debug sf_igmp_snoop_add_update_v4_grp: Existing
 Member 1039 in Group 0.0.0.0 in BD 52.
Jul 15 18:19:28.011257       16  5   1  16   Debug IGMP pkt (snoop OFF): orig_src_ltl 0x15,
 src_ltl 0x40f vlan 232
Jul 15 18:19:29.058442       17  0   1  16   Debug IGMP pkt (snoop OFF): orig_src_ltl 0x15,
 src_ltl 0x40f vlan 180
Jul 15 18:19:30.480455       18  3   1  16   Debug IGMP pkt (snoop OFF): orig_src_ltl 0x15,
 src_ltl 0x40f vlan 233
Jul 15 18:19:30.623668       19  2   0   0         Started log
Jul 15 18:19:32.002081       20  0  99  16   Debug sf_igmp_snoop_thread: IGMP Snoop Thread
 waken up
Jul 15 18:19:32.002103       21  0  99  16   Debug sf_igmp_snoop_thread: Check timed-out
members in 0.0.0.0, BD: 52
Jul 15 18:19:32.002111       22  0  99  16   Debug sf_igmp_snoop_thread: Check timed-out
members in 0.0.0.0, BD: 55
Jul 15 18:19:32.002117       23  0  99  16   Debug sf_igmp_snoop_thread: Check timed-out
members in 0.0.0.0, BD: 59
Jul 15 18:19:32.002122       24  0  99  16   Debug sf_igmp_snoop_thread: Check timed-out
members in 224.6.7.8, BD: 59
Jul 15 18:19:34.418381       25 12   1  16   Debug IGMP pkt (snoop ON): orig_src_ltl 0x0,
src_ltl 0x66 vlan 59
Jul 15 18:19:34.418385       26 12   1  16   Debug Notification size: 72
Jul 15 18:19:34.418389       27 12   1  16   Debug Sending IGMP pkt notif: swbd 59, pkt_size
 60, notif_size 72
Jul 15 18:19:34.418400       28 12   1  16   Debug Forward report to router port: 10347
.Jul 15 18:19:34.448932       29  0  99  16   Debug sf_igmp_snoop_v4_pkt_notify_handler:
IGMP notify message from DP:
Jul 15 18:19:34.448949       30  0  99  16   Debug sf_igmp_snoop_v4_pkt_notify_handler:
SRC_LTL: 102, SWBD: 59, pkt_size: 60
Jul 15 18:19:34.448961       31  0  99  16   Debug sf_igmp_snoop_v4_pkt_notify_handler: Got
 IGMP v1/v2 Report
Jul 15 18:19:34.448970       32  0  99  16   Debug Handle IGMPv2 report in BD 59, LTL:102,
 group: 224.3.4.5.
Jul 15 18:19:34.448978       33  0  99  16   Debug Handle IGMPv2 JOIN in BD 59, LTL:102,
group: 224.3.4.5.
Jul 15 18:19:34.448986       34  0  99  16   Debug sf_igmp_snoop_add_update_v4_grp: Adding
 Group 224.3.4.5 to BD 59.
```

```
Jul 15 18:19:34.448996       35  0  99  16   Debug sf_igmp_snoop_notify_vsm: Sending to
VSM: opcode : 1, swbd 59, grp_ip: 0xe0030405.
Jul 15 18:19:34.449087       36  0  99  16   Debug sf_igmp_snoop_add_update_v4_grp: Adding
 Member 102 to Group 224.3.4.5 in BD 59.
Jul 15 18:19:34.449102       37  0  99  16   Debug sf_igmp_snoop_update_dp: group update
for BD 59: IP: 224.3.4.5, with 2 members
Jul 15 18:19:34.449111       38  0  99  16   Debug sf_igmp_snoop_update_dp: Sending group
update to DP for BD 59: IP: 224.3.4.5, with 2 members
Jul 15 18:19:34.938394       39 14   1  16   Debug IGMP pkt (snoop ON): orig_src_ltl 0x0,
src_ltl 0x66 vlan 59
Jul 15 18:19:34.938400       40 14   1  16   Debug Notification size: 72
Jul 15 18:19:34.938406      41 14   1  16   Debug Sending IGMP pkt notif: swbd 59, pkt_size
 60, notif_size 72
Jul 15 18:19:34.938419       42 14   1  16   Debug Forward report to router port: 10347
.Jul 15 18:19:34.968621       43  0  99  16   Debug sf_igmp_snoop_v4_pkt_notify_handler:
IGMP notify message from DP:
Jul 15 18:19:34.968634       44  0  99  16   Debug sf_igmp_snoop_v4_pkt_notify_handler:
SRC_LTL: 102, SWBD: 59, pkt_size: 60
Jul 15 18:19:34.968645       45  0  99  16   Debug sf_igmp_snoop_v4_pkt_notify_handler: Got
 IGMP v1/v2 Report
Jul 15 18:19:34.968654       46  0  99  16   Debug Handle IGMPv2 report in BD 59, LTL:102,
 group: 224.3.4.5.
Jul 15 18:19:34.968661       47  0  99  16   Debug Handle IGMPv2 JOIN in BD 59, LTL:102,
group: 224.3.4.5.
Jul 15 18:19:34.968669      48  0  99  16   Debug sf_igmp_snoop_add_update_v4_grp: Existing
 Group 224.3.4.5 in BD 59.
Jul 15 18:19:34.968677      49  0  99  16   Debug sf_igmp_snoop_add_update_v4_grp: Existing
 Member 102 in Group 224.3.4.5 in BD 59.
Jul 15 18:19:37.000827       50  0  99  16   Debug sf_igmp_snoop_thread: IGMP Snoop Thread
 waken up
Jul 15 18:19:37.000853       51  0  99  16   Debug sf_igmp_snoop_thread: Check timed-out
members in 0.0.0.0, BD: 52
Jul 15 18:19:37.000895       52  0  99  16   Debug sf_igmp_snoop_thread: Check timed-out
members in 0.0.0.0, BD: 55
Jul 15 18:19:37.000905       53  0  99  16   Debug sf_igmp_snoop_thread: Check timed-out
members in 0.0.0.0, BD: 59
Jul 15 18:19:37.000912       54  0  99  16   Debug sf_igmp_snoop_thread: Check timed-out
members in 224.3.4.5, BD: 59
Jul 15 18:19:37.000919       55  0  99  16   Debug sf_igmp_snoop_thread: Check timed-out
members in 224.6.7.8, BD: 59
Jul 15 18:19:37.085327       56  8   1  16   Debug IGMP pkt (snoop ON): orig_src_ltl 0x0,
src_ltl 0x66 vlan 59
Jul 15 18:19:37.085331       57  8   1  16   Debug Notification size: 72
Jul 15 18:19:37.085335      58  8   1  16   Debug Sending IGMP pkt notif: swbd 59, pkt_size
 60, notif_size 72
Jul 15 18:19:37.085345       59  8   1  16   Debug Forward report to router port: 10347
.Jul 15 18:19:37.085998       60  1   1  16   Debug IGMP pkt (snoop ON): orig_src_ltl 0x15,
 src_ltl 0x40f vlan 59
Jul 15 18:19:37.086002       61  1   1  16   Debug Notification size: 68
Jul 15 18:19:37.086006      62  1   1  16   Debug Sending IGMP pkt notif: swbd 59, pkt_size
 56, notif_size 68
Jul 15 18:19:37.134375       63  0  99  16   Debug sf_igmp_snoop_v4_pkt_notify_handler:
IGMP notify message from DP:
Jul 15 18:19:37.134390       64  0  99  16   Debug sf_igmp_snoop_v4_pkt_notify_handler:
SRC_LTL: 102, SWBD: 59, pkt_size: 60
Jul 15 18:19:37.134400       65  0  99  16   Debug sf_igmp_snoop_v4_pkt_notify_handler: Got
 IGMP v1/v2 Report
Jul 15 18:19:37.134409       66  0  99  16   Debug Handle IGMPv2 report in BD 59, LTL:102,
 group: 224.3.4.5.
Jul 15 18:19:37.134416       67  0  99  16   Debug Handle IGMPv2 LEAVE in BD 59, LTL:102,
group: 224.3.4.5.
Jul 15 18:19:37.134439       68  0  99  16   Debug sf_igmp_snoop_v4_pkt_notify_handler:
IGMP notify message from DP:
Jul 15 18:19:37.134446       69  0  99  16   Debug sf_igmp_snoop_v4_pkt_notify_handler:
```

```
SRC_LTL: 1039, SWBD: 59, pkt_size: 56
Jul 15 18:19:37.134453       70  0  99  16   Debug sf_igmp_snoop_v4_pkt_notify_handler: Got
 IGMP Query.
Jul 15 18:19:37.134461       71  0  99  16   Debug sf_igmp_snoop_handle_query: Received v2
 query.
Jul 15 18:19:37.134467       72  0  99  16   Debug sf_igmp_snoop_handle_query: Got group
specific query for 0x50403e0.
Jul 15 18:19:37.134475       73  0  99  16   Debug sf_igmp_snoop_start_leave_timers: Found
 group 0xe0030405.
Jul 15 18:19:37.134482       74  1   1  16   Debug IGMP pkt (snoop ON): orig_src_ltl 0x15,
 src_ltl 0x40f vlan 59
Jul 15 18:19:37.134486       75  1   1  16   Debug Notification size: 68
Jul 15 18:19:37.134488      76  1   1  16   Debug Sending IGMP pkt notif: swbd 59, pkt_size
 56, notif_size 68
Jul 15 18:19:37.134483       77  0  99  16   Debug sf_igmp_snoop_start_leave_timers: Start
 leave timer on member 102 for 2 secs.
Jul 15 18:19:37.134504       78  0  99  16   Debug sf_igmp_snoop_v4_pkt_notify_handler:
IGMP notify message from DP:
Jul 15 18:19:37.134511       79  0  99  16   Debug sf_igmp_snoop_v4_pkt_notify_handler:
SRC_LTL: 1039, SWBD: 59, pkt_size: 56
Jul 15 18:19:37.134518       80  0  99  16   Debug sf_igmp_snoop_v4_pkt_notify_handler: Got
 IGMP Query.
Jul 15 18:19:37.134524       81  0  99  16   Debug sf_igmp_snoop_handle_query: Received v2
 query.
Jul 15 18:19:37.134530       82  0  99  16   Debug sf_igmp_snoop_handle_query: Got group
specific query for 0x50403e0.
Jul 15 18:19:37.134536       83  0  99  16   Debug sf_igmp_snoop_start_leave_timers: Found
 group 0xe0030405.
Jul 15 18:19:37.610484       84  5   1  16   Debug IGMP pkt (snoop ON): orig_src_ltl 0x15,
 src_ltl 0x40f vlan 52
Jul 15 18:19:37.610489       85  5   1  16   Debug Notification size: 68
Jul 15 18:19:37.610492      86  5   1  16   Debug Sending IGMP pkt notif: swbd 52, pkt_size
 56, notif_size 68
Jul 15 18:19:37.648380       87  0  99  16   Debug sf_igmp_snoop_v4_pkt_notify_handler:
IGMP notify message from DP:
Jul 15 18:19:37.648396       88  0  99  16   Debug sf_igmp_snoop_v4_pkt_notify_handler:
SRC_LTL: 1039, SWBD: 52, pkt_size: 56
Jul 15 18:19:37.648406       89  0  99  16   Debug sf_igmp_snoop_v4_pkt_notify_handler: Got
 IGMP Query.
Jul 15 18:19:37.648415       90  0  99  16   Debug sf_igmp_snoop_handle_query: Received v3
 query.
Jul 15 18:19:37.648422       91  0  99  16   Debug sf_igmp_snoop_handle_query: Adding v3
router entry in BD 52 (len: 12).
Jul 15 18:19:37.648431      92  0  99  16   Debug sf_igmp_snoop_add_update_v4_grp: Existing
 Group 0.0.0.0 in BD 52.
Jul 15 18:19:37.648439      93  0  99  16   Debug sf_igmp_snoop_add_update_v4_grp: Existing
 Member 1039 in Group 0.0.0.0 in BD 52.
Jul 15 18:19:42.002071       94  0  99  16   Debug sf_igmp_snoop_thread: IGMP Snoop Thread
 waken up
Jul 15 18:19:42.002099       95  0  99  16   Debug sf_igmp_snoop_thread: Check timed-out
members in 0.0.0.0, BD: 52
Jul 15 18:19:42.002112       96  0  99  16   Debug sf_igmp_snoop_thread: Check timed-out
members in 0.0.0.0, BD: 55
Jul 15 18:19:42.002121       97  0  99  16   Debug sf_igmp_snoop_thread: Check timed-out
members in 0.0.0.0, BD: 59
Jul 15 18:19:42.002128       98  0  99  16   Debug sf_igmp_snoop_thread: Check timed-out
members in 224.3.4.5, BD: 59
Jul 15 18:19:42.002135       99  0  99  16   Debug sf_igmp_snoop_thread: Check timed-out
members in 224.6.7.8, BD: 59
Jul 15 18:19:43.301931      100  6   0   0         Suspending log
switch(config)#
```

Multicast IGMP Snooping Troubleshooting Commands

Command	Description
show cdp neighbor	Displays if IGMP uses the packet VLAN to forward IGMP packets to the VSM, which is the same mechanism that CDP uses. However, if you have disabled the CDP protocol on the upstream switch using the **no cdp enable** command, the **show cdp neighbor** command does not display any information.
show ip igmp groups	Displays whether IGMP snooping is enabled on the VLAN.
show ip igmp snooping vlan	Displays IGMP snooping configuration by VLAN.
show ip igmp snooping groups vlan	Displays IGMP snooping group information.
debug ip igmp snooping vlan	Enables debugging for IGMP shopping. **Note** Even if you enable the **debug** command for IGMP snooping, log details are not available for multicast groups and their members.
module vem *module-number* **execute vemcmd show vlan**	
module vem *module-number* **execute vemcmd show igmp** *vlan* [**detail**]	

Command Examples

show cdp neighbor

```
switch# show cdp neighbor
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
S - Switch, H - Host, I - IGMP, r - Repeater,
V - VoIP-Phone, D - Remotely-Managed-Device,
s - Supports-STP-Dispute

Device ID Local Intrfce Hldtme Capability Platform Port ID
switch Eth3/2 179 R S I WS-C6506-E Gig5/16
switch Eth3/4 179 R S I WS-C6506-E Gig5/23
```

show ip igmp snooping vlan

```
switch# show ip igmp snooping vlan 159
IGMP Snooping information for vlan 159
IGMP snooping enabled <-- IGMP SNOOPING is enabled for vlan 159
IGMP querier none
Switch-querier disabled
```

```
IGMPv3 Explicit tracking enabled (initializing, time-left: 00:03:20)
IGMPv2 Fast leave disabled
IGMPv1/v2 Report suppression enabled
IGMPv3 Report suppression disabled
Router port detection using PIM Hellos, IGMP Queries
Number of router-ports: 0
Number of groups: 0
```

show ip igmp snooping groups

```
switch# show ip igmp snooping groups vlan 1784
Type: S - Static, D - Dynamic, R - Router port

Vlan Group Address Ver Type Port list
1784 */* - R Po1 Po2 Eth5/31
1784 227.0.0.1 v2 D Veth79 Veth80

VSM-DAO# show ip igmp snooping querier vlan 1784
Vlan IP Address Version Expires Port
1784 184.184.0.12 v3 00:04:14 Po1
1784 184.184.0.12 v3 00:04:14 Po2
1784 184.184.0.12 v3 00:04:14 Eth5/31

switch# show ip igmp snooping groups vlan 1784 detail
IGMP Snooping group membership for vlan 1784
Group addr: 227.0.0.1
Group ver: v2 [old-host-timer: not running]
report-timer: not-running
Last reporter: 184.184.0.11
IGMPv1/v2 memb ports:
Veth79 [0 GQ missed]
Veth80 [0 GQ missed]


switch# show ip igmp snooping groups vlan 1784 summary
Legend: E - Enabled, D - Disabled

Vlan Snoop (*,G)-Count
1784 E 2
Total number of (*,G) entries: 2
switch#
```

debug ip igmp snooping vlan

```
switch(config)# debug ip igmp snooping vlan
2014 Jul 8 23:49:16.633077 igmp[3157]: SNOOP: Switchport interface Veth43 (308) has been
created,
obtaining any static mrouter/oif configs
2014 Jul 8 23:49:16.683929 igmp[3157]: SNOOP: Switchport interface Veth37 (128) has been
created,
obtaining any static mrouter/oif configs
2014 Jul 8 23:49:16.748355 igmp[3157]: SNOOP: <vlan 1> clear port:Veth43, vlan:1
2014 Jul 8 23:49:16.789832 igmp[3157]: SNOOP: Switchport interface Veth47 (428) has been
created,
obtaining any static mrouter/oif configs
2014 Jul 8 23:49:16.797079 igmp[3157]: SNOOP: Switchport interface Veth38 (158) has been
created,
obtaining any static mrouter/oif configs
2014 Jul 8 23:49:16.824702 igmp[3157]: SNOOP: <vlan 11> Added Veth43 to active ports for
vlan 11
2014 Jul 8 23:49:16.824854 igmp[3157]: SNOOP: Mode for if(Vethernet43): 0x80000 vlan: 11
2014 Jul 8 23:49:16.862531 igmp[3157]: SNOOP: <vlan 1> clear port:Veth37, vlan:1
2014 Jul 8 23:49:16.950490 igmp[3157]: SNOOP: <vlan 11> Added Veth37 to active ports for
```

```
vlan 11
2014 Jul 8 23:49:16.950638 igmp[3157]: SNOOP: Mode for if(Vethernet37): 0x80000 vlan: 11
2014 Jul 8 23:49:16.998800 igmp[3157]: SNOOP: <vlan 1> clear port:Veth38, vlan:1
2014 Jul 8 23:49:16.999030 igmp[3157]: SNOOP: <vlan 1> clear port:Veth47, vlan:1
2014 Jul 8 23:49:17.089056 igmp[3157]: SNOOP: Switchport interface Veth40 (218) has been
created,
obtaining any static mrouter/oif configs
2014 Jul 8 23:49:17.121007 igmp[3157]: SNOOP: Switchport interface Veth39 (188) has been
created,
obtaining any static mrouter/oif configs
2014 Jul 8 23:49:17.131549 igmp[3157]: SNOOP: <vlan 11> Added Veth38 to active ports for
vlan 11
2014 Jul 8 23:49:17.131693 igmp[3157]: SNOOP: Mode for if(Vethernet38): 0x80000 vlan: 11
2014 Jul 8 23:49:17.156004 igmp[3157]: SNOOP: <vlan 11> Added Veth47 to active ports for
vlan 11
2014 J
```

module vem execute vemcmd show vlan

```
switch# module vem 3 execute vemcmd show vlan 159
BD 159, vdc 1, vlan 159, 3 ports
Portlist:
18 vmnic3
47 fedora8.eth0

Multicast Group Table:
Group 224.1.2.3 RID 1 Multicast LTL 4408
47
18
Group 0.0.0.0 RID 2 Multicast LTL 4407
18
```

This example shows that LTL 18 corresponds to vmnic3, and LTL 47 corresponds to VM fedora8, interface eth0.

The multicast group table for 224.1.2.3 shows the interfaces that the VEM forwards to when it receives multicast traffic for group 224.1.2.3. If fedora8 has multicast group 224.1.2.3 on its eth0 interface, LTL 47 should be in the multicast group table for 224.1.2.3.

LTL 18 is also in multicast group 224.1.2.3, which means it is a VM and generates multicast traffic to 224.1.2.3. The traffic is forwarded to vmnic3, which is the uplink to the upstream switch.

The multicast group table entry for 0.0.0.0 serves as a default route. If any multicast group traffic does not match any of the multicast group, the address uses the default route, which means that the traffic is forwarded to an upstream switch through vmnic3.

module vem execute vemcmd show igmp

module vem 3 execute vemcmd show igmp 1784

In show ip igmp snooping groups , on page 8, global IGMP snooping is enabled on VLAN 1784 (the disabled global state takes precedence).

Multicast group table values are as follows:

```
Group 227.0.0.1, Multicast LTL: 10363

Group */*, Multicast LTL: 10358
```

module vem 3 execute vemcmd show igmp 1784 detail

In show ip igmp snooping groups , on page 8, global IGMP snooping is enabled on VLAN 1784 (the disabled global state takes precedence)

Multicast group table values are as follows:

```
Group 227.0.0.1, Multicast LTL: 10363

Members: 59, 1039

Group */*, Multicast LTL: 10358

Members: 1039

Querier Info -

IP Address: 184.184.0.12

Uptime: 241955 seconds

Version: 3

Timeout: 8 seconds
```