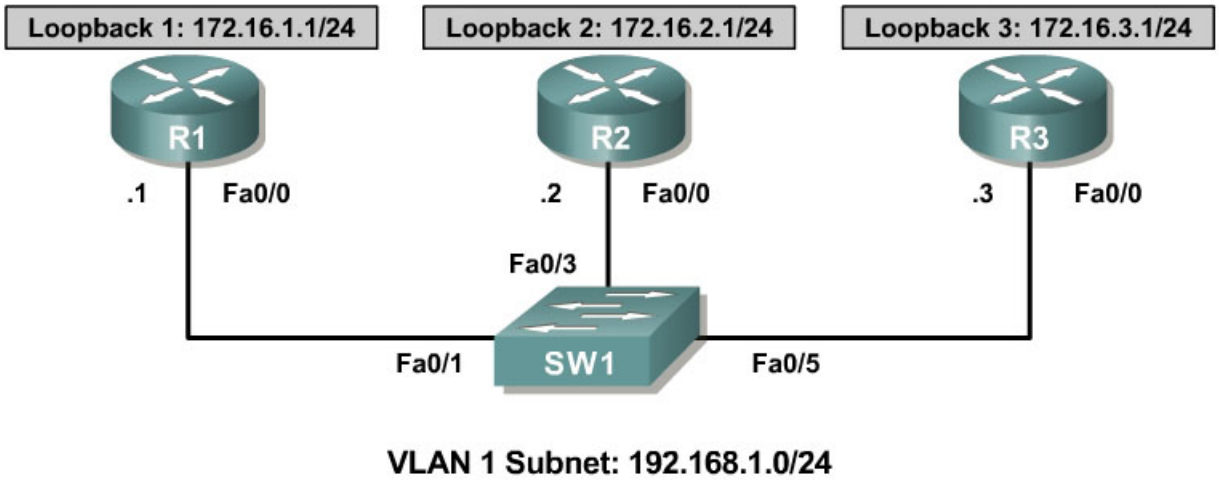
Lab 7-1 Implementing IGMP and IGMP Snooping

Learning Objectives

- Configure IGMP to join interfaces to a multicast group
- Verify the operation of IGMP at Layer 3
- Analyze IGMP packets and packets sent to multicast groups
- Enable PIM-DM
- Verify the operation of IGMP snooping on a Catalyst switch

Topology Diagram



Scenario

Configure IGMP to listen to the multicast group 229.7.7.7 on R2 and R3. Send multicast traffic from R1 to the LAN segment. Configure IGMP snooping to efficiently send multicast traffic through the switch.

Review IGMP, PIM-DM, and IGMP snooping in your course materials before completing this lab.

Overview

This set of multicast labs builds skills in working with multicast features and routing protocols so that the student can confidently configure PIM in sparse-dense mode. Sparse-dense mode is simply PIM sparse mode (PIM-SM) with a dense mode fallback control mechanism.

To grasp the principles involved in sparse-dense mode, students must understand the principles involved with IGMP and PIM routing protocols at Layer 3. Thus, considerable lab time will be spent understanding IGMP as well as each of the PIM protocols. IGMP snooping greatly improves multicast efficiency at Layer 2 and therefore receives thorough treatment.

Step 1: Configure Hosts on a LAN

Configure the basic addressing scheme in the diagram on each router. Disable IP routing using the **no ip routing** command. This command forces a router to act as a host connected to a specific VLAN via the switch. Routing between networks is not performed.

```
R1# conf t
R1(config)# no ip routing
R1(config)# interface fastethernet 0/0
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# interface loopback 1
R1(config-if)# ip address 172.16.1.1 255.255.255.0

R2# conf t
R2(config)# no ip routing
R2(config)# interface fastethernet 0/0
R2(config-if)# ip address 192.168.1.2 255.255.255.0
R2(config-if)# no shutdown
R2(config-if)# interface loopback 2
R2(config-if)# ip address 172.16.2.1 255.255.255.0

R3# conf t
R3(config)# no ip routing
R3(config)# interface fastethernet 0/0
R3(config-if)# ip address 192.168.1.3 255.255.255.0
R3(config-if)# no shutdown
R3(config-if)# interface loopback 3
R3(config-if)# ip address 172.16.3.1 255.255.255.0
```

With routing disabled, will the routers redirect packets between remote addresses on connected subnets?

Reload the switch with a blank configuration file and erase the vlan.dat file in flash memory. By default, all connected ports are assigned to VLAN 1.

Step 2: Subscribe Interfaces to Multicast Groups with IGMP

In IP multicast, hosts use the Internet Group Management Protocol (IGMP) to join and leave groups and to respond to membership queries.

Debug IP IGMP and all IP packets on all routers. This allows you to see any IGMP messages sent or received by any of the routers.


```
R1# debug ip igmp
R1# debug ip packet

R2# debug ip igmp
R2# debug ip packet

R3# debug ip igmp
R3# debug ip packet
```

On R1, issue the **ip igmp join-group** *group_address* command in interface configuration mode for FastEthernet0/0.

```
R1# conf t
R1(config)# interface fastethernet 0/0
R1(config-if)# ip igmp join-group 229.7.7.7

*Nov  3 20:54:57.114: IGMP(0): WAVL Insert group: 229.7.7.7 interface:
FastEthernet0/0Successful
*Nov  3 20:54:57.114: IGMP(0): Send v2 Report for 229.7.7.7 on FastEthernet0/0
*Nov  3 20:54:57.114: IP: s=192.168.1.1 (local), d=229.7.7.7
(FastEthernet0/0), len 28, sending broad/multicast
```

The **ip igmp join-group** command sends an IGMPv2 join message to the group-specific address, which is then propagated to all reachable members of the specified group. This message states that multicast traffic destined for the group should be forwarded to the local router's IP address. Because none of the other routers are listening to the 229.7.7.7 group at this point, R2 and R3 do not receive a broadcast sent to the group.

Issue the **show ip igmp interface** *interface_type interface_number* command on R1.

```
R1# show ip igmp interface fastethernet 0/0
FastEthernet0/0 is up, line protocol is up
  Internet address is 192.168.1.1/24
  IGMP is enabled on interface
  Current IGMP host version is 2
  Current IGMP router version is 2
  IGMP query interval is 60 seconds
  IGMP querier timeout is 120 seconds
  IGMP max query response time is 10 seconds
  Last member query count is 2
  Last member query response interval is 1000 ms
  Inbound IGMP access group is not set
  IGMP activity: 1 joins, 0 leaves
  Multicast routing is disabled on interface
  Multicast TTL threshold is 0
  Multicast groups joined by this system (number of users):
      229.7.7.7(1)
```

Which version of IGMP is R1's Fast Ethernet interface using?

Remove the **ip igmp join-group** command from R1's FastEthernet0/0 interface because it is not used for the remainder of this lab.

```
R1(config)# interface fastethernet 0/0
R1(config-if)# no ip igmp join-group 229.7.7.7

*Nov  3 20:59:10.582: IGMP(0): IGMP delete group 229.7.7.7 on FastEthernet0/0
*Nov  3 20:59:10.582: IGMP(0): Send Leave for 229.7.7.7 on FastEthernet0/0
*Nov  3 20:59:10.582: IP: s=192.168.1.1 (local), d=224.0.0.2
(FastEthernet0/0), len 28, sending broad/multicast
```

Note that the IGMPv2 leave messages are sent to 224.0.0.2, the link-local multicast group representing all routers on the subnet.

Use R1 as the originator of multicast traffic to the group 229.7.7.7, but do not subscribe it to the group. Use IGMP to subscribe R2 and R3 to the 229.7.7.7 group. If you turned debugging off on R2 and R3, re-enable debugging on both routers to watch the IGMP messages. Keep debugging on for IGMP and IP packets through the end of Step 4.

```
R2# debug ip igmp
R2# debug ip packet

R3# debug ip igmp
R3# debug ip packet

R2(config-if)# ip igmp join-group 229.7.7.7
*Nov  4 04:59:59.340: IGMP(0): WAVL Insert group: 229.7.7.7 interface:
FastEthernet0/0Successful
*Nov  4 04:59:59.340: IGMP(0): Send v2 Report for 229.7.7.7 on FastEthernet0/0
*Nov  4 04:59:59.340: IP: s=192.168.1.2 (local), d=229.7.7.7
(FastEthernet0/0), len 28, sending broad/multicast

R3(config-if)# ip igmp join-group 229.7.7.7
*Nov  4 05:02:11.696: IGMP(0): WAVL Insert group: 229.7.7.7 interface:
FastEthernet0/0Successful
*Nov  4 05:02:11.700: IGMP(0): Send v2 Report for 229.7.7.7 on FastEthernet0/0
*Nov  4 05:02:11.700: IP: s=192.168.1.3 (local), d=229.7.7.7
(FastEthernet0/0), len 28, sending broad/multicast
```

Display the IGMP groups to which R2 and R3 have subscribed with the **show ip igmp groups** and **show ip igmp membership** commands. Verify that the specified groups are being received.

```
R2# show ip igmp groups
IGMP Connected Group Membership
Group Address Interface       Uptime   Expires  Last Reporter  Group Accounted
229.7.7.7     FastEthernet0/0 00:07:56 stopped  192.168.1.2

R2# show ip igmp membership
Flags: A  - aggregate, T - tracked
       L  - Local, S - static, V - virtual, R - Reported through v3
       I - v3lite, U - Urd, M - SSM (S,G) channel
       1,2,3 - The version of IGMP the group is in
Channel/Group-Flags:
       / - Filtering entry (Exclude mode (S,G), Include mode (*,G))
Reporter:
       <mac-or-ip-address> - last reporter if group is not explicitly tracked
```



```
       <n>/<m>      - <n> reporter in include mode, <m> reporter in exclude

 Channel/Group              Reporter        Uptime   Exp.  Flags  Interface
 *,229.7.7.7                192.168.1.2     00:08:27 stop  2LA    Fa0/0

R3# show ip igmp groups
IGMP Connected Group Membership
Group Address Interface        Uptime   Expires  Last Reporter Group Accounted
229.7.7.7     FastEthernet0/0  00:09:00 stopped  192.168.1.3

R3# show ip igmp membership
Flags: A  - aggregate, T - tracked
       L  - Local, S - static, V - virtual, R - Reported through v3
       I - v3lite, U - Urd, M - SSM (S,G) channel
       1,2,3 - The version of IGMP the group is in
Channel/Group-Flags:
       / - Filtering entry (Exclude mode (S,G), Include mode (*,G))
Reporter:
       <mac-or-ip-address> - last reporter if group is not explicitly tracked
       <n>/<m>      - <n> reporter in include mode, <m> reporter in exclude

 Channel/Group              Reporter        Uptime   Exp.  Flags  Interface
 *,229.7.7.7                192.168.1.3     00:09:27 stop  2LA    Fa0/0
```

From R1, ping the multicast group 229.7.7.7. The output should appear similar to the following with debugging turned on:

```
R1# ping 229.7.7.7

Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 229.7.7.7, timeout is 2 seconds:

*Nov  4 16:10:18.413: IP: s=192.168.1.1 (local), d=229.7.7.7
(FastEthernet0/0), len 100, sending broad/multicast
*Nov  4 16:10:18.413: IP: s=172.16.1.1 (local), d=229.7.7.7 (Loopback1), len
100, sending broad/multicast
*Nov  4 16:10:18.413: IP: s=192.168.1.3 (FastEthernet0/0), d=192.168.1.1, len
100, rcvd 1
*Nov  4 16:10:18.413: IP: s=192.168.1.2 (FastEthernet0/0), d=192.168.1.1, len
100, rcvd 1
Reply to request 0 from 192.168.1.3, 1 ms
Reply to request 0 from 192.168.1.2, 1 ms
```

The output above indicates the expected result of a successful multicast ping: echo replies from all members of the multicast group. Notice that the ping is sent out all interfaces, including the loopback interface on R1. Because there could technically be multicast listeners to that group on other connected subnets or even remote networks, multicasts must be flooded out all interfaces, unless a multicast routing protocol informs the router that this is unnecessary.

If R2 and R3 received the multicast ping, how did SW1 treat the ping at OSI Layer 2?

To which address did R2 and R3 send their replies?

Is this a unicast or multicast address?

Ping from R2 to the multicast group. From which hosts do you expect replies?

If the output of your ping has only one reply, as shown below, re-issue the ping. With unicast pings, the first ping usually times out due to the delay at Layer 2 caused by the ARP request from the source to the destination.

```
R2# ping 229.7.7.7

Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 229.7.7.7, timeout is 2 seconds:

Reply to request 0 from 192.168.1.2, 1 ms
```

For R3 to send the ICMP echo reply to 192.168.1.2, it needs to locate a MAC address for that IP address via ARP. Thus, the ARP request from the multicast listener to the multicast receiver may cause the ICMP echo to time out at the source. Try to ping again with the same command. You should now receive all ICMP echo replies, as follows:

```
R2# ping 229.7.7.7

Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 229.7.7.7, timeout is 2 seconds:

*Nov  4 16:19:28.117: IP: s=192.168.1.2 (local), d=229.7.7.7
(FastEthernet0/0), len 100, sending broad/multicast
*Nov  4 16:19:28.117: IP: s=172.16.2.1 (local), d=229.7.7.7 (Loopback2), len
100, sending broad/multicast
*Nov  4 16:19:28.117: IP: s=192.168.1.2 (FastEthernet0/0), d=229.7.7.7, len
100, rcvd 1
*Nov  4 16:19:28.117: IP: tableid=0, s=192.168.1.2 (local), d=192.168.1.2
(FastEthernet0/0), routed via RIB
*Nov  4 16:19:28.117: IP: s=192.168.1.2 (local), d=192.168.1.2
(FastEthernet0/0), len 100, sending
*Nov  4 16:19:28.121: IP: s=192.168.1.3 (FastEthernet0/0), d=192.168.1.2, len
100, rcvd 1
*Nov  4 16:19:28.121: IP: s=192.168.1.2 (FastEthernet0/0), d=192.168.1.2, len
100, rcvd 1
Reply to request 0 from 192.168.1.3, 4 ms
```



```
Reply to request 0 from 192.168.1.2, 4 ms
```

For more information on IP multicast and IGMP, see RFC 1112 and RFC 2236: http://www.ietf.org/rfc/rfc1112.txt http://www.ietf.org/rfc/rfc2236.txt.

Step 3: Verify IGMP Snooping on the Switch

Up to this point, multicast has been simplified to be multicast hosts on a broadcast, multi-access medium of a switched VLAN. The switch treated these multicast packets as broadcasts at Layer 2 and forwarded them to every host on the VLAN, regardless of whether that host was subscribed to the group. Sending traffic to every host on the subnet effectively reduces multicasting to broadcasting with a different destination address. Multicast switching in an enterprise network should be designed in a more intelligent way at Layer 2.

Layer 2 switches can use IGMP snooping to constrain the flooding of multicast traffic by dynamically configuring Layer 2 interfaces. Multicast traffic is then forwarded to only those interfaces associated with IP multicast devices. IGMP snooping requires the LAN switch to snoop on the IGMP transmissions between the host and the router and to track multicast groups and member ports. When the switch receives an IGMP report from a host for a particular multicast group, the switch adds the host port number to the forwarding table entry. When it receives an IGMP Leave Group message from a host, it removes the host port from the table entry. It also periodically deletes entries if it does not receive IGMP membership reports from the multicast clients.

The multicast router sends out periodic IGMP general queries to all VLANs. When IGMP snooping is enabled, the switch responds to the router queries with only one join request per MAC multicast group, and the switch creates one entry per VLAN in the Layer 2 forwarding table for each MAC group from which it receives an IGMP join request. All hosts interested in this multicast traffic send join requests and are added to the forwarding table entry.

Layer 2 multicast groups learned through IGMP snooping are dynamic. However, you can statically configure MAC multicast groups by using the **ip igmp snooping vlan static** global configuration command. If you specify group membership for a multicast group address statically, your setting supersedes any automatic manipulation by IGMP snooping. Multicast group membership lists can consist of both user-defined and IGMP snooping-learned settings.

If a port spanning-tree, a port group, or a VLAN ID change occurs, the IGMP snooping-learned multicast groups from this port on the VLAN are deleted.

IGMP snooping is enabled on Catalyst switches by default.

Issue the **show ip igmp snooping** command on SW1.

```
SW1# show ip igmp snooping
vlan 1
```



```
----------
 IGMP snooping is globally enabled
 IGMP snooping is enabled on this Vlan
 IGMP snooping immediate-leave is disabled on this Vlan
 IGMP snooping mrouter learn mode is pim-dvmrp on this Vlan
 IGMP snooping is running in IGMP_ONLY mode on this Vlan
```

Notice that IGMP snooping is enabled by default globally and on a per-VLAN basis on SW1. In this case, IGMP snooping identifies a switchport as a multicast router port only if it see PIM or DVMRP messages sent toward the switch on that port.

IGMP snooping only subscribes other switchports to multicast groups at Layer 2 if it sees IGMP messages sent to the multicast router. Until you configure a supported multicast routing protocol (PIM or DVMRP) on the multicast router R1, IGMP snooping does not create MAC address table entries for the multicast groups. Verify this with the **show mac address-table multicast** command on SW1.

```
SW1# show mac address-table multicast
Vlan    Mac Address       Type       Ports
----    -----------       ----       -----
SW1#
```

Step 4: Configure a Multicast-Enabled Router on the VLAN

First, enable IP routing on R1 with the **ip routing** command.

```
R1(config)# ip routing
```

Enable multicast routing on R1 using the **ip multicast-routing** command in global configuration mode, which is similar to the **ip routing** command. The **ip multicast-routing** command allows R1 to start obtaining current information on multicast groups, sources, destination, and routing patterns.

```
R1(config)# ip multicast-routing
```

Enable PIM-DM on R1's FastEthernet0/0 interface with the **ip pim dense-mode** command. Identify the output with debugging turned on.

```
R1(config-if)# ip pim dense-mode
R1(config-if)#
*Nov  5 00:28:24.687: IP: s=192.168.1.1 (local), d=224.0.0.13
(FastEthernet0/0), len 54, sending broad/multicast
```

PIM attempts to make adjacencies out interfaces on which it is enabled. The multicast packet to 224.0.0.13 equates with a PIM Hello packet to all PIM-enabled routers on the subnet.

```
R1(config-if)#
*Nov  5 00:28:24.687: IGMP(0): Send v2 init  Query on FastEthernet0/0
*Nov  5 00:28:24.687: IP: s=192.168.1.1 (local), d=224.0.0.1
(FastEthernet0/0), len 28, sending broad/multicast
```


Next, IGMP sends the initial IGMP query to the multicast group referencing all devices on the subnet 224.0.0.1. Each IGMP-enabled interface connected to the VLAN should now send an IGMP join message to 192.168.1.1 indicating which multicast groups it wishes to join.

```
*Nov  5 00:28:24.691: IGMP(0): WAVL Insert group: 224.0.1.40 interface:
FastEthernet0/0Successful
*Nov  5 00:28:24.691: IGMP(0): Send v2 Report for 224.0.1.40 on
FastEthernet0/0
*Nov  5 00:28:24.691: IGMP(0): Received v2 Report on FastEthernet0/0 from
192.168.1.1 for 224.0.1.40
R1(config-if)#
*Nov  5 00:28:24.691: IGMP(0): Received Group record for group 224.0.1.40,
mode 2 from 192.168.1.1 for 0 sources
*Nov  5 00:28:24.691: IGMP(0): Switching to EXCLUDE mode for 224.0.1.40 on
FastEthernet0/0
*Nov  5 00:28:24.691: IGMP(0): Updating EXCLUDE group timer for 224.0.1.40
*Nov  5 00:28:25.331: IGMP(0): MRT Add/Update FastEthernet0/0 for
(*,224.0.1.40) by 0
*Nov  5 00:28:24.691: IP: s=192.168.1.1 (local), d=224.0.1.40
(FastEthernet0/0), len 28, sending broad/multicast
```

All PIM routers automatically subscribe to the 224.0.1.40 group. Therefore, R1 sends an IGMP join message on its Fast Ethernet interface for the 224.0.1.40 group. Then, R1 receives its own message and implicitly joins its Fast Ethernet interface to the group. You will learn more about the 224.0.1.40 group in Lab 7.4.

The relevant parts of the remaining output are highlighted.

```
*Nov  5 00:28:25.331: IP: s=192.168.1.2 (FastEthernet0/0), d=229.7.7.7, len
28, rcvd 0
*Nov  5 00:28:25.331: IGMP(0): Received v2 Report on FastEthernet0/0 from
192.168.1.2 for 229.7.7.7
*Nov  5 00:28:25.331: IGMP(0): Received Group record for group 229.7.7.7, mode
2 from 192.168.1.2 for 0 sources
*Nov  5 00:28:25.331: IGMP(0): WAVL Insert group: 229.7.7.7 interface:
FastEthernet0/0Successful
*Nov  5 00:28:25.331: IGMP(0): Switching to EXCLUDE mode for 229.7.7.7 on
FastEthernet0/0
*Nov  5 00:28:25.331: IGMP(0): Updating EXCLUDE group timer for 229.7.7.7
*Nov  5 00:28:25.331: IGMP(0): MRT Add/Update FastEthernet0/0 for
(*,229.7.7.7) by 0
*Nov  5 00:28:25.687: %PIM-5-DRCHG: DR change from neighbor 0.0.0.0 to
192.168.1.1 on interface FastEthernet0/0 (vrf default)
*Nov  5 00:28:53.979: IP: s=192.168.1.1 (local), d=224.0.0.13
(FastEthernet0/0), len 54, sending broad/multicast
*Nov  5 00:29:23.415: IP: s=192.168.1.1 (local), d=224.0.0.13
(FastEthernet0/0), len 54, sending broad/multicast
*Nov  5 00:29:23.695: IGMP(0): Send v2 general Query on FastEthernet0/0
*Nov  5 00:29:23.695: IGMP(0): Set report delay time to 4.6 seconds for
224.0.1.40 on FastEthernet0/0
*Nov  5 00:29:23.695: IP: s=192.168.1.1 (local), d=224.0.0.1
(FastEthernet0/0), len 28, sending broad/multicast
*Nov  5 00:29:28.695: IGMP(0): Send v2 Report for 224.0.1.40 on
FastEthernet0/0
*Nov  5 00:29:28.695: IGMP(0): Received v2 Report on FastEthernet0/0 from
192.168.1.1 for 224.0.1.40
```



```
*Nov  5 00:29:28.695: IGMP(0): Received Group record for group 224.0.1.40,
mode 2 from 192.168.1.1 for 0 sources
*Nov  5 00:29:28.695: IGMP(0): Updating EXCLUDE group timer for 224.0.1.40
*Nov  5 00:29:28.695: IP: s=192.168.1.1 (local), d=224.0.1.40
(FastEthernet0/0), len 28, sending broad/multicast
*Nov  5 00:29:29.331: IP: s=192.168.1.2 (FastEthernet0/0), d=229.7.7.7, len
28, rcvd 0
*Nov  5 00:29:29.331: IGMP(0): Received v2 Report on FastEthernet0/0 from
192.168.1.2 for 229.7.7.7
*Nov  5 00:29:29.331: IGMP(0): Received Group record for group 229.7.7.7, mode
2 from 192.168.1.2 for 0 sources
*Nov  5 00:29:29.331: IGMP(0): Updating EXCLUDE group timer for 229.7.7.7
*Nov  5 00:29:29.331: IGMP(0): MRT Add/Update FastEthernet0/0 for
(*,229.7.7.7) by 0
*Nov  5 00:29:53.111: IP: s=192.168.1.1 (local), d=224.0.0.13
(FastEthernet0/0), len 54, sending broad/multicast
*Nov  5 00:30:22.819: IP: s=192.168.1.1 (local), d=224.0.0.13
(FastEthernet0/0), len 54, sending broad/multicast
*Nov  5 00:30:23.695: IGMP(0): Send v2 general Query on FastEthernet0/0
*Nov  5 00:30:23.695: IGMP(0): Set report delay time to 4.8 seconds for
224.0.1.40 on FastEthernet0/0
*Nov  5 00:30:23.695: IP: s=192.168.1.1 (local), d=224.0.0.1
(FastEthernet0/0), len 28, sending broad/multicast
*Nov  5 00:30:27.331: IP: s=192.168.1.2 (FastEthernet0/0), d=229.7.7.7, len
28, rcvd 0
*Nov  5 00:30:27.331: IGMP(0): Received v2 Report on FastEthernet0/0 from
192.168.1.2 for 229.7.7.7
*Nov  5 00:30:27.331: IGMP(0): Received Group record for group 229.7.7.7, mode
2 from 192.168.1.2 for 0 sources
*Nov  5 00:30:27.331: IGMP(0): Updating EXCLUDE group timer for 229.7.7.7
*Nov  5 00:30:27.331: IGMP(0): MRT Add/Update FastEthernet0/0 for
(*,229.7.7.7) by 0
*Nov  5 00:30:28.695: IGMP(0): Send v2 Report for 224.0.1.40 on
FastEthernet0/0
*Nov  5 00:30:28.695: IGMP(0): Received v2 Report on FastEthernet0/0 from
192.168.1.1 for 224.0.1.40
*Nov  5 00:30:28.695: IGMP(0): Received Group record for group 224.0.1.40,
mode 2 from 192.168.1.1 for 0 sources
*Nov  5 00:30:28.695: IGMP(0): Updating EXCLUDE group timer for 224.0.1.40
*Nov  5 00:30:28.695: IP: s=192.168.1.1 (local), d=224.0.1.40
(FastEthernet0/0), len 28, sending broad/multicast
*Nov  5 00:30:52.155: IP: s=192.168.1.1 (local), d=224.0.0.13
(FastEthernet0/0), len 54, sending broad/multicast
*Nov  5 00:31:22.079: IP: s=192.168.1.1 (local), d=224.0.0.13
(FastEthernet0/0), len 54, sending broad/multicast
*Nov  5 00:31:23.695: IGMP(0): Send v2 general Query on FastEthernet0/0
*Nov  5 00:31:23.695: IGMP(0): Set report delay time to 9.8 seconds for
224.0.1.40 on FastEthernet0/0
*Nov  5 00:31:23.695: IP: s=192.168.1.1 (local), d=224.0.0.1
(FastEthernet0/0), len 28, sending broad/multicast
*Nov  5 00:31:27.503: IP: s=192.168.1.3 (FastEthernet0/0), d=229.7.7.7, len
28, rcvd 0
*Nov  5 00:31:27.503: IGMP(0): Received v2 Report on FastEthernet0/0 from
192.168.1.3 for 229.7.7.7
*Nov  5 00:31:27.503: IGMP(0): Received Group record for group 229.7.7.7, mode
2 from 192.168.1.3 for 0 sources
*Nov  5 00:31:27.503: IGMP(0): Updating EXCLUDE group timer for 229.7.7.7
*Nov  5 00:31:27.503: IGMP(0): MRT Add/Update FastEthernet0/0 for
(*,229.7.7.7) by 0
```

The highlighted messages indicate the IGMP queries and responses. In each case, R1 sends a periodic IGMP query to all devices on the subnet. R2 and R3

periodically respond to those queries as necessary, requesting that multicast traffic to the 229.7.7.7 group be allowed onto this subnet. PIM-DM periodically floods traffic to a Layer 2 segment and then prunes that traffic from that segment if no listeners are configured.

At this point, disable debugging on all routers.

```
Router# undebug all
```

Step 5: Verify Multicast Operation at Layer 2

Which IP multicast groups do you expect to see in the IGMP records on R1?

On R1, issue the **show ip igmp groups** command to display the multicast groups for which IGMP has currently recorded information from connected interfaces.

```
R1# show ip igmp groups
IGMP Connected Group Membership
Group Address    Interface                Uptime    Expires   Last Reporter
Group Accounted
229.7.7.7        FastEthernet0/0          00:02:19  00:02:19  192.168.1.3
224.0.1.40       FastEthernet0/0          00:02:22  00:02:22  192.168.1.1
```

Display the IGMP membership for the IGMP groups reported by R1 using the **show ip igmp membership** command.

```
R1# show ip igmp membership
Flags: A  - aggregate, T - tracked
       L  - Local, S - static, V - virtual, R - Reported through v3
       I - v3lite, U - Urd, M - SSM (S,G) channel
       1,2,3 - The version of IGMP the group is in
Channel/Group-Flags:
       / - Filtering entry (Exclude mode (S,G), Include mode (*,G))
Reporter:
       <mac-or-ip-address> - last reporter if group is not explicitly tracked
       <n>/<m>      - <n> reporter in include mode, <m> reporter in exclude

 Channel/Group                  Reporter        Uptime   Exp.  Flags
Interface
 *,229.7.7.7                    192.168.1.3     00:02:20 02:20 2A     Fa0/0
 *,224.0.1.40                   192.168.1.1     00:02:23 02:23 2LA    Fa0/0
```

Display the IGMP status on R1's FastEthernet0/0 interface with the **show ip igmp interface** command.

```
R1# show ip igmp interface
FastEthernet0/0 is up, line protocol is up
  Internet address is 192.168.1.1/24
  IGMP is enabled on interface
  Current IGMP host version is 2
  Current IGMP router version is 2
```



```
IGMP query interval is 60 seconds
IGMP querier timeout is 120 seconds
IGMP max query response time is 10 seconds
Last member query count is 2
Last member query response interval is 1000 ms
Inbound IGMP access group is not set
IGMP activity: 2 joins, 0 leaves
Multicast routing is enabled on interface
Multicast TTL threshold is 0
Multicast designated router (DR) is 192.168.1.1 (this system)
IGMP querying router is 192.168.1.1 (this system)
Multicast groups joined by this system (number of users):
    224.0.1.40(1)
```

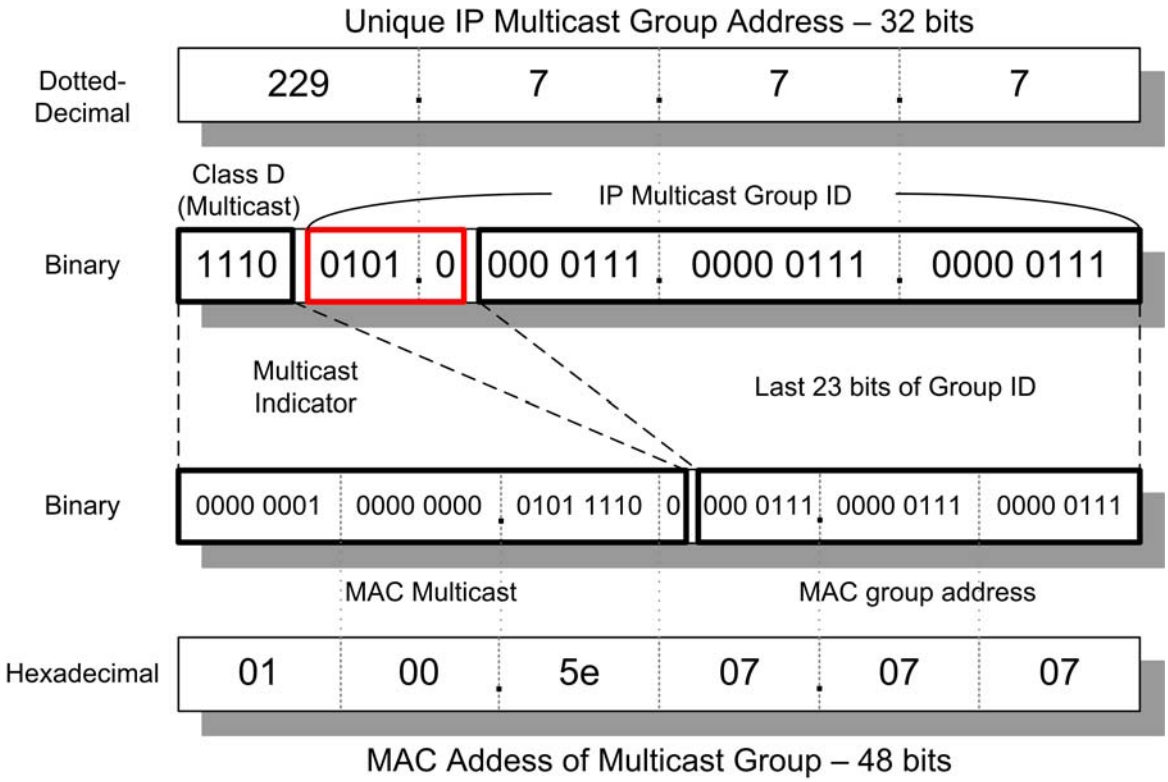
Step 6: Verify IGMP Snooping

On SW1, issue the **show mac address-table multicast**.

```
SW1# show mac address-table multicast
Vlan    Mac Address       Type       Ports
----    -----------       ----       -----
   1    0100.5e00.0128    IGMP       Fa0/1
   1    0100.5e07.0707    IGMP       Fa0/1, Fa0/3, Fa0/5
```

These MAC addresses are not unique to one IP multicast group, because there is a 1:32 correlation between each MAC address and the IP multicast groups it represents.

Consider the binary form of the group address for 229.7.7.7:



Because the center set of boxed bits in the binary representation of the IP address is not mapped to any bits in the MAC address, the MAC addresses of multicast groups are not unique to an IP multicast group. Class D addresses with any value in those 5 bits and a constant sequence of bits in the 23 least-significant digits all map to the same MAC address.

List at least three IP multicast groups with which the following MAC addresses correspond.

- 0100.5e00.0128

- 0100.5e07.0707

In this particular scenario, which IP multicast groups do the 0100.5e00.128 and 0100.5e07.0707 MAC addresses represent?

Although all 32 groups are forwarded at Layer 2 to the Layer 3 interfaces of the routers and hosts, IGMP only reads IP packets for groups to which the interface has subscribed or for which it is in a forwarding state. All other multicast traffic is dropped.

As discussed in Step 3, statically subscribe FastEthernet0/9 on SW1 to the multicast MAC group of 0100.5e07.07.07 via the **ip igmp snooping vlan static** global configuration command. This configuration does not affect the remainder of the lab.

```
SW1(config)# ip igmp snooping vlan 1 static 0100.5e07.0707 interface
fastethernet 0/9
```

Reissue the **show mac address-table multicast** command on SW1.

```
SW1# show mac address-table multicast
Vlan    Mac Address       Type       Ports
----    -----------       ----       -----
   1    0100.5e00.0128    IGMP       Fa0/1
   1    0100.5e07.0707    USER       Fa0/1, Fa0/3, Fa0/5,
                                     Fa0/9
```


Notice that the Type field for the 0100.5e07.0707 entry now indicates that it is a statically configured group address. Statically configured addresses override mappings dynamically learned via IGMP snooping.

Step 7: Verify Multicast Operation at Layer 3

Verify that multicast route state has been recorded on R1 using the **show ip mroute** command.

```
R1# show ip mroute
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group
Outgoing interface flags: H - Hardware switched, A - Assert winner
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode

(*, 229.7.7.7), 00:06:48/00:02:11, RP 0.0.0.0, flags: DC
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    FastEthernet0/0, Forward/Dense, 00:06:48/00:00:00

(*, 224.0.1.40), 00:07:33/00:02:15, RP 0.0.0.0, flags: DCL
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    FastEthernet0/0, Forward/Dense, 00:07:33/00:00:00
```

The **show ip mroute** command shows multicast state with reference to each multicast group. Multicast routes are more complex than unicast routes because the router needs to identify incoming interfaces which it considers the “upstream interface” to specific multicast sources using a reverse-path check. The multicast router must also store the outgoing interfaces that should forward the multicast traffic for each source and group.

Without PIM communicating between routers, much of the interface and RPF neighbor information the multicast routing table shown above is default information, such as RPF neighbors of 0.0.0.0. You will see more complex router state in the next lab.

Notice in the output shown that all traffic to the 229.7.7.7 group should be forwarded out FastEthernet0/0. Verify this by pinging from R1 to 229.7.7.7.

```
R1# ping 229.7.7.7
Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 229.7.7.7, timeout is 2 seconds:

Reply to request 0 from 192.168.1.3, 1 ms
Reply to request 0 from 192.168.1.2, 1 ms
```


Final Configurations

```
R1# show run
!
hostname R1
!
ip multicast-routing
!
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 ip pim dense-mode
 no shutdown
!
end


R2# show run
!
hostname R2
!
interface FastEthernet0/0
 ip address 192.168.1.2 255.255.255.0
 ip igmp join-group 229.7.7.7
 no shutdown
!
end


R3# show run
!
hostname R3
!
interface FastEthernet0/0
 ip address 192.168.1.3 255.255.255.0
 ip igmp join-group 229.7.7.7
 no shutdown
!
end


SW1# show run
!
hostname SW1
!
ip igmp snooping vlan 1 static 0100.5e07.0707 interface Fa0/9
!
interface FastEthernet0/1
 switchport mode access
!
interface FastEthernet0/3
 switchport mode access
!
interface FastEthernet0/5
 switchport mode access
!
interface Vlan1
 ip address 192.168.1.10 255.255.255.0
 no shutdown
!
end
```

