Understanding IGMP Snooping and Multicast Forwarding

IGMP snooping monitors the Internet Group Management Protocol (IGMP) traffic between hosts and multicast routers. The switch uses what IGMP snooping learns to forward multicast traffic only to interfaces that are connected to interested receivers. This conserves bandwidth by allowing the switch to send multicast traffic to only those interfaces that are connected to hosts that want to receive the traffic, instead of flooding the traffic to all interfaces in the VLAN. This topic describes how Juniper Networks EX Series Ethernet Switches forward multicast traffic when IGMP snooping is enabled.

This topic covers:

IGMP Snooping and Forwarding Interfaces

To determine how to forward multicast traffic, IGMP snooping maintains information about the following interfaces in its multicast cache table:

- Multicast-router interfaces—These interfaces lead toward multicast routers or IGMP queriers.
- Group-member interfaces—These interfaces lead toward hosts that are members of multicast groups.

IGMP snooping learns about these interfaces by monitoring IGMP traffic. If an interface receives IGMP queries or Protocol Independent Multicast (PIM) updates, IGMP snooping adds the interface to its multicast cache table as a multicast-router interface. If an interface receives IGMP group membership reports in response to IGMP group queries or receives unsolicited join group messages, IGMP snooping adds the interface to its multicast cache table as a group-member interface.

Interfaces that IGMP snooping learns about are subject to aging. For example, if a multicast-router interface does not receive IGMP queries or PIM hellos within a certain interval, IGMP snooping removes that interface from its multicast cache table.

Note: For a switch to learn multicast-router interfaces and group-member interfaces, an IGMP querier must exist in the network. For the switch itself to function as an IGMP querier, IGMP must be enabled on the switch.

You can statically configure an interface to be a multicast-router interface or a group-member interface. A statically configured interface is not subject to aging and does not require an IGMP querier for IGMP snooping to learn about the interface. You can have a mix of statically configured and dynamically learned interfaces on a switch.

General Forwarding Rules

Multicast traffic received on a switch interface in a VLAN on which IGMP snooping is enabled is forwarded according to the following rules.

IGMP traffic is forwarded as follows:

- IGMP general queries received on a multicast-router interface are forwarded to all other interfaces in the VLAN.
- IGMP group-specific queries received on a multicast-router interface are forwarded to only those interfaces in the VLAN that are members of the group.
- IGMP reports received on a host interface are forwarded to multicast-router interfaces in the same VLAN, but not to the other host interfaces in the VLAN.

Multicast traffic that is not IGMP traffic is forwarded as follows:

- A multicast packet with a destination address of 224.0.0.0/24 is flooded to all other interfaces on the VLAN.
- An unregistered multicast packet—that is, a packet for a group that has no current members—is forwarded to all multicast-router interfaces in the VLAN.
- A registered multicast packet is forwarded only to those host interfaces in the VLAN that are members of the multicast group and to all multicast-router interfaces in the VLAN.

Examples of IGMP Snooping Multicast Forwarding

The following examples are provided to illustrate how IGMP snooping forwards multicast traffic in different topologies:

- Scenario 1: Switch Forwarding Multicast Traffic to a Multicast Router and Hosts
- Scenario 2: Switch Forwarding Multicast Traffic to Another Switch
- Scenario 3: Switch Connected to Hosts Only (No IGMP Querier)
- Scenario 4: Layer 2/Layer 3 Switch Forwarding Multicast Traffic Between VLANs

Scenario 1: Switch Forwarding Multicast Traffic to a Multicast Router and Hosts

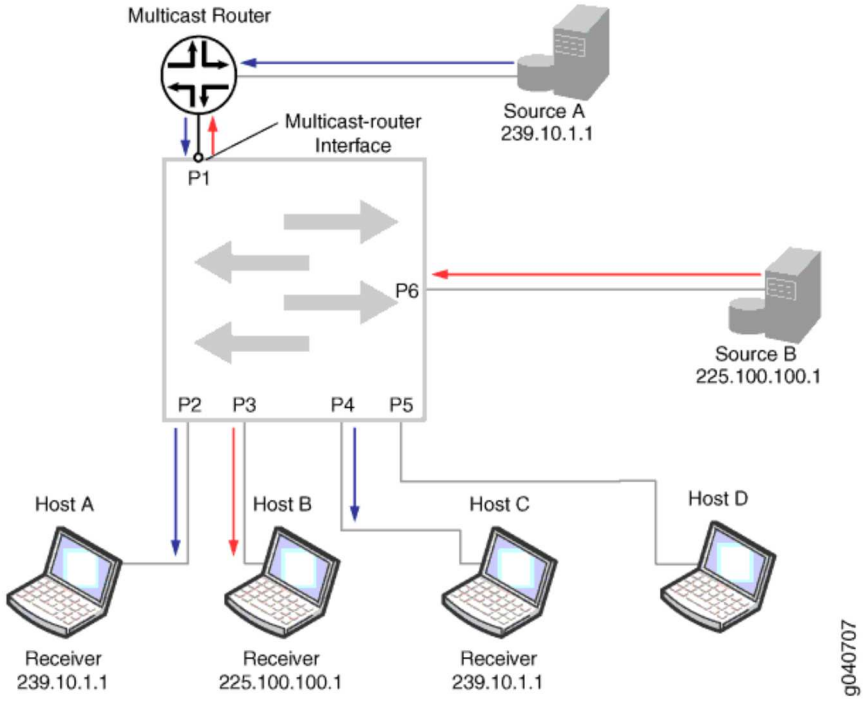
In the topology shown in Figure 1, a switch acting as a pure Layer 2 device receives multicast traffic belonging to multicast group `239.10.1.1` from Source A, which is connected to the multicast router. It also receives multicast traffic belonging to multicast group `225.100.100.1` from Source B, which is connected directly to the switch. All interfaces on the switch belong to the same VLAN.

Because the switch receives IGMP queries from the multicast router on interface P1, IGMP snooping learns that interface P1 is a multicast-router interface and adds the interface to its multicast cache table. It forwards any IGMP general queries it receives on this interface to all host interfaces on the switch, and, in turn, forwards membership reports it receives from hosts to the multicast-router interface.

In the example, Hosts A and C have responded to the membership queries with membership reports for group `239.10.1.1`. IGMP snooping adds interfaces P2 and P4 to its multicast cache table as member interfaces for group `239.10.1.1`. It forwards the group multicast traffic received from Source A to Hosts A and C, but not to Hosts B and D.

Host B has responded to the membership queries with a membership report for group `225.100.100.1`. The switch adds interface P3 to its multicast cache table as a member interface for group `225.100.100.1` and forwards multicast traffic it receives from Source B to Host B. The switch also forwards the multicast traffic it receives from Source B to the multicast-router interface P1.

Figure 1: Scenario 1: Switch Forwarding Multicast Traffic to a Multicast Router and Hosts

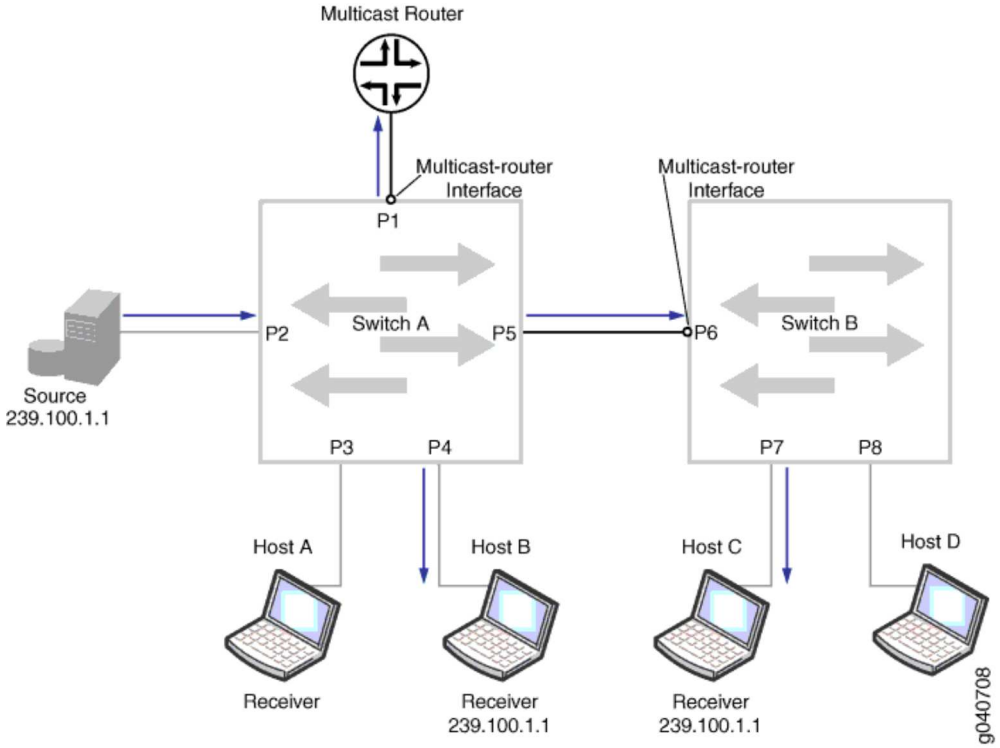


Scenario 2: Switch Forwarding Multicast Traffic to Another Switch

In the topology show in Figure 2, a multicast source is connected to Switch A. Switch A in turn is connected to another switch, Switch B. Hosts on both Switch A and B are potential members of the multicast group. Both switches are acting as Layer 2 devices and all interfaces on the switches are members of the same VLAN.

Switch A receives IGMP queries from the multicast router on interface P1, making interface P1 a multicast-router interface for Switch A. Switch A forwards all general IGMP queries it receives on this interface to the other interfaces on the switch, including the interface connecting Switch B. Because Switch B receives the forwarded IGMP queries on interface P6, P6 is the multicast-router interface for Switch B. Switch B forwards the group membership report it receives from Host C to Switch A through its multicast-router interface. Switch A forwards the membership report to its multicast-router interface, includes interface P5 in its multicast cache table as a group-member interface, and forwards multicast traffic from the source to Switch B.

Figure 2: Scenario 2: Switch Forwarding Multicast Traffic to Another Switch



You might have to configure P6 on Switch B as a static multicast-router interface in certain implementations. If Switch B receives unsolicited join messages from its hosts before it learns which interface is its multicast-router interface, it does not forward those reports to Switch A. When Switch A receives multicast traffic, it does not forward the traffic to Switch B, because it has not received any member reports on interface P5. You can statically configure interface P6 as a multicast-router interface to solve this issue.

Scenario 3: Switch Connected to Hosts Only (No IGMP Querier)

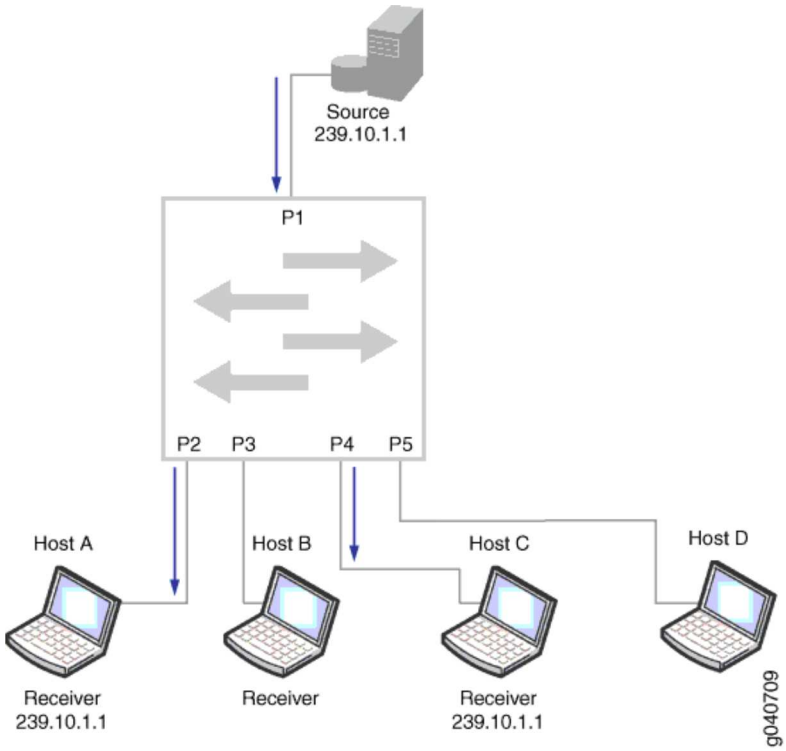
In the topology shown in Figure 3, a switch is connected to a multicast source and to hosts. There is no multicast router in this topology—hence there is no IGMP querier. Without an IGMP querier to respond to, a host does not send periodic membership reports. As a result, even if the host sends an unsolicited join to join a multicast group, its membership in the multicast group times out.

For IGMP snooping to work correctly in this network so that the switch forwards multicast traffic to Hosts A and C only, you can either:

- Configure interfaces P2 and P4 as static group-member interfaces.

- Configure a routed VLAN interface (RVI) on the VLAN and enable IGMP on it. In this case, the switch itself acts as an IGMP querier, and the hosts can dynamically join the multicast group and refresh their group membership by responding to the queries.

Figure 3: Scenario 3: Switch Connected to Hosts Only (No IGMP Querier)

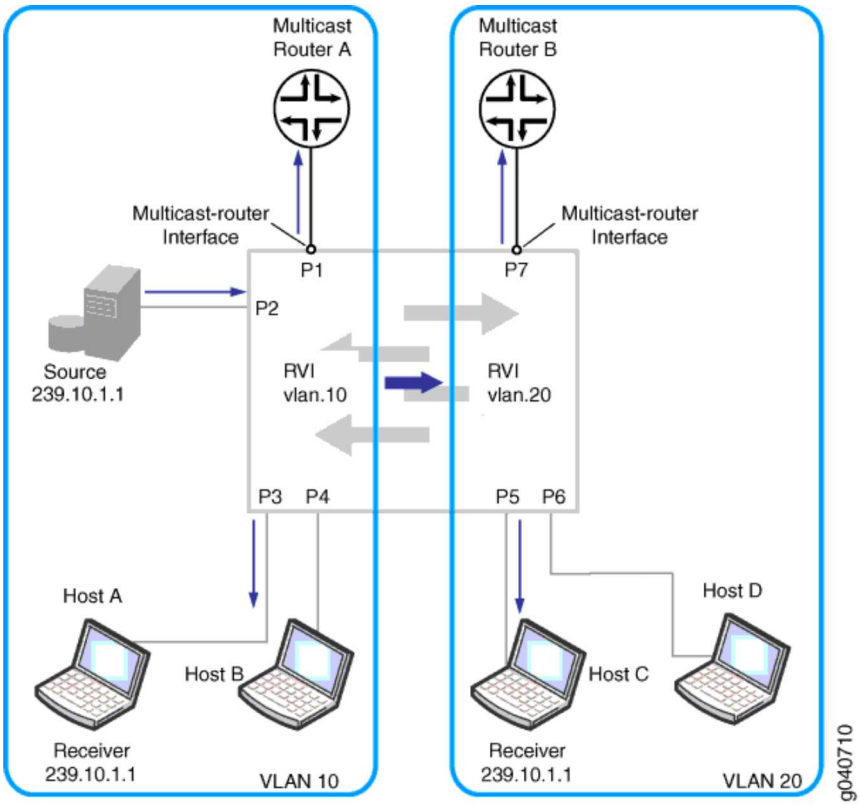


Scenario 4: Layer 2/Layer 3 Switch Forwarding Multicast Traffic Between VLANs

In the topology shown in Figure 4, a multicast source, Multicast Router A, and Hosts A and B are connected to the switch and are in VLAN 10. Multicast Router B and Hosts C and D are also connected to the switch and are in VLAN 20.

In a pure Layer 2 environment, traffic is not forwarded between VLANs. For Host C to receive the multicast traffic from the source on VLAN 10, RVIs must be created on VLAN 10 and VLAN 20 to permit routing of the multicast traffic between the VLANs. In addition, PIM must be enabled on the switch to perform the multicast routing.

Figure 4: Scenario 4: Layer 2/Layer 3 Switch Forwarding Multicast Traffic Between VLANs



Related Documentation

EX Series

- IGMP Snooping on EX Series Switches Overview
- Example: Configuring IGMP Snooping on EX Series Switches

- Configuring IGMP Snooping (CLI Procedure)
- Configuring IGMP Snooping (J-Web Procedure)
- Configuring Routed VLAN Interfaces (CLI Procedure)

Published: 2011-06-02