CHAPTER 17

Configuring Multicast Forwarding

This chapter describes configuring multicast forwarding and includes the following sections:

- Multicast Overview, page 17-1
- Multicast Forwarding and IGMP Snooping, page 17-1
- Multicast/Broadcast Configuration in Bridge-Groups, page 17-4
- Creating a Multicast Group, page 17-4

Multicast Overview

This section describes multicast forwarding and includes the following topics:

- IPv4 Multicast, page 17-1
- Multicast Forwarding and IGMP Snooping, page 17-1

Multicast support is implemented in hardware and functions at wire speed. This feature provides the automatic discovery of multicast groups.

IPv4 Multicast

IPv4 multicast is the only type of IP multicast that is supported by the Ethernet gateway.

IP multicasting enables a host to send packets to a specific subset of all hosts as a group transmission. Without the ability to multicast, a host is limited to sending to either a single host or to all hosts.

Point-to-multipoint—a single multicast stream that is replicated at branch points in a switched network to reach multiple viewers. This is useful for unidirectional, live broadcasts such as corporate communications or media events. It is also useful for content distribution from a central server to collocated servers or software distribution from a data center to multiple end station PCs or servers.

Multipoint-to-multipoint—a bidirectional hub-and-spoke architecture in which an MCU receives and redirects signals from each member of a multicast conference.

Multicast Forwarding and IGMP Snooping

This section describes multicast forwarding and IGMP snooping and includes the following topics:

- Multicast Groups, page 17-2
Multicast Overview

- Multicast Forwarding, page 17-2
- Internet Group Management Protocol, page 17-2
- IGMP Snooping, page 17-2
- Layer 2 Multicast Addresses, page 17-3

Multicast Groups

Each multicast group is identified by a unique LID and GID. Each switch is configured with routing information for the multicast traffic, which specifies all of the ports where the packet needs to travel.

Multicast Forwarding

Multicast forwarding allows the hardware engine to forward IP packets, instead of having multicast traffic sent to the line card CPU for slower path processing.

In multicast forwarding, the source sends traffic to an arbitrary group of hosts that are represented by a multicast group address. The multicast router must determine which direction is the upstream direction (toward the source) and which one is the downstream direction (or directions). If there are multiple downstream paths, the router replicates the packet and forwards it down the appropriate downstream paths (best unicast route metric)—which is not necessarily all paths. Forwarding multicast traffic away from the source, rather than to the receiver, is called RPF.

Internet Group Management Protocol

IGMP is used to dynamically register individual hosts in a multicast group on a particular LAN. Hosts identify group memberships by sending IGMP messages to their local multicast router. Under IGMP, routers listen to IGMP messages and periodically send out queries to discover which groups are active or inactive on a particular subnet.

IGMP is used by IP routers and their immediately connected IP hosts to communicate multicast group membership states to neighboring multicast routers.

Version 3 of IGMP supports source filtering, which is the ability of a multicast receiver host to signal to a router the groups from which it wants to receive multicast traffic, and from the sources this traffic is expected. This membership information enables software to forward traffic from only those sources from which receivers requested the traffic.

IGMP Snooping

IGMP snooping manages multicast traffic in switches by allowing directed switching of IP multicast traffic.

IGMP snooping is an IP multicast constraining mechanism that runs on a Layer 2 switch. IGMP snooping requires that the switch examine, or snoop, some Layer 3 information (specifically IGMP join/leave messages) in the IGMP packets that are sent between the hosts and the router. When the switch hears the IGMP host report from a host for a particular multicast group, the switch adds the port number of the host to the associated multicast table entry. When the switch hears the IGMP leave group messages from a host, the switch removes the table entry of the host.

Because IGMP control messages are sent as multicast packets, they are indistinguishable from multicast data at Layer 2. A switch running IGMP snooping must examine every multicast data packet to determine if it contains any pertinent IGMP control information.
When a host wants to join an IP multicast group, it sends an IGMP join message. A join message specifies the MAC address of the host and the IP multicast group that it wants to join.

The router then builds an IGMP join message and multicasts the join message to the well-known address to which the switches listen.

Upon receipt of the join message, each switch searches its multicast table to determine if it contains the MAC address of the host that is asking to join the multicast group.

If a switch finds the MAC address of the host in its table associating the MAC address with a non-trunking port, the switch creates a multicast forwarding entry in the forwarding table.

The host associated with that port receives multicast traffic for that multicast group. In this way, the switch automatically learns the MAC addresses and port numbers of the IP multicast hosts.

Layer 2 Multicast Addresses

Historically, NICs on a LAN segment could receive only packets destined for their burned-in MAC address or the broadcast MAC address. In IP multicast, several hosts must receive a single data stream with a common destination MAC address such that multiple hosts receive the same packet and are still able to differentiate between several multicast groups.

One method to accomplish this is to map IP multicast Class D addresses directly to a MAC address.

Today, using this method, NICs can receive packets destined to many different MAC addresses that are their own unicast, broadcast, and a range of multicast addresses.

Multicast Forwarding with the Ethernet Gateway

This section describes multicast forwarding with the Ethernet gateway.

The Ethernet gateway does not use IGMP snooping to discover IP multicast groups. The gateway queries or listens for IB traps from the Subnet Manager, and whether there is an IPoIB multicast listener provision, the hardware to forward the corresponding IP multicast group.

This is an example of a multicast scenario:

- No multicast members are in an IP multicast group in the IP subnet (both Ethernet and IB).
- A multicast sender is on a different IP subnet (there is an L3 switch on the Ethernet side).

1. An IPoIB host must receive this multicast and join the corresponding IP/IB multicast group.
2. The Subnet Manager sends a notification:
   - The Ethernet gateway receives an IB trap from the Subnet Manager that a new IB multicast group has been created.
   - The gateway inspects the MGID and sees that this is an IPoIB multicast group.
   - The Ethernet gateway provisions the Ethernet tables to forward the IPoIB multicast group (in less than a second). The L3 switch starts forwarding this multicast group, the Ethernet gateway is already provisioned, and the multicast traffic reaches the IPoIB host.

The IGMP message is sent by the IPoIB host at approximately the same time. The IPoIB host sends a notification at approximately the same time as the Subnet Manager sends a notification:

- The IPoIB host sends an IGMP notification to the L3 switch to inform that it is available to receive multicast groups. The L3 switch starts forwarding the multicast group to this subnet.
If the first IGMP notification comes after the first Subnet Manager trap, the IGMP notification can be dropped.

If the first IGMP notification is dropped, the host resends the IGMP announcement 2-3 times, and the next packets reach L3 on the Ethernet. The L3 switch starts forwarding this multicast group, the Ethernet gateway is already provisioned, and the multicast traffic reaches the IPoIB host.

### Multicast/Broadcast Configuration in Bridge-Groups

The bridge-group has a setting to enable/disable multicast/broadcast forwarding. This setting is used while the group is not a member of a redundancy group. If the bridging group is a member of a redundancy group, the redundancy group multicast/broadcast enable/disable flag overwrites that of the bridge-group. When the bridge-group is removed from the redundancy group, the original setting is restored.

### Creating a Multicast Group

This section describes how to create a multicast group and includes the following topics:

- Enabling Multicast Forwarding, page 17-4
- Disabling Multicast Forwarding, page 17-5

### Enabling Multicast Forwarding

To enable multicast forwarding, perform the following steps:

**Step 1** Start a CLI session, unless you have already done so.

**Step 2** Enter privileged EXEC mode:

```
SFS-3504> enable
SFS-3504#
```

**Step 3** Enter global configuration mode:

```
SFS-3504# configure
SFS-3504(config)#
```

**Step 4** Specify the bridge-group and enable multicast forwarding as follows:

a. Enter the `bridge-group <bridge-group number>` command.

b. Enter the `multicast` command.

```
SFS-3504(config)# bridge-group 1 multicast
SFS-3504(config)#
```

**Step 5** Return to privileged EXEC mode:

```
SFS-3504(config)# exit
SFS-3504#
```

**Step 6** Show the bridge-group by entering the `show bridge-group` command:
SFS-3504# show bridge-group

================================================================================
Bridge Groups
================================================================================
bridge-group-id : 1
bridge-group-name : BridgeGroupOne
        ip-addr : 10.0.0.101
eth-bridge-port : trunk 1 (not tagged)
ib-bridge-port : 1/2(gw) (pkey: ff:ff)
        broadcast-forwarding : false
broadcast-forwarding-mode : self
directed-broadcast : false
directed-broadcast-mode : self
        loop-protection-method : one
multicast : false
multicast-mode : self
gratuitous-igmp : false
gratuitous-igmp-mode : self
        igmp-version : v2
        igmp-version-mode : self
redundancy-group : 0
status-in-redundancy-group : none

Disabling Multicast Forwarding

To disable multicast forwarding, perform the following steps:

Step 1  Start a CLI session, unless you have already done so.

Step 2  Enter privileged EXEC mode:
SFS-3504> enable
SFS-3504#

Step 3  Enter global configuration mode:
SFS-3504# configure
SFS-3504(config)#

Step 4  Specify the bridge-group and disable multicast forwarding as follows:
1. Enter the no keyword with the bridge-group <bridge-group number> command
2. Enter the multicast command.
SFS-3504(config)# no bridge-group 2 multicast
SFS-3504(config)#

Step 5  Return to privileged EXEC mode:
SFS-3504(config)# exit
SFS-3504#

Step 6  Show the bridge-group by entering the show bridge-group command:
SFS-3504# show bridge-group

================================================================================
Bridge Groups
Creating a Multicast Group

bridge-group-id : 1
bridge-group-name : BridgeGroupOne
  ip-addr : 10.0.0.101
  eth-bridge-port : trunk 1 (not tagged)
  ib-bridge-port : 1/2(gw) (pkey: ff:ff)
  broadcast-forwarding : false
  broadcast-forwarding-mode : self
  directed-broadcast : false
  directed-broadcast-mode : self
  loop-protection-method : one
  multicast : false
  multicast-mode : self
  gratuitous-igmp : false
  gratuitous-igmp-mode : self
  igmp-version : v2
  igmp-version-mode : self
  redundancy-group : 0
  status-in-redundancy-group : none