Chapter 5

Configuring IPv4 Multicast

IPv4 multicast enables a device to send packets to a group of hosts rather than to a list of individual hosts. This chapter describes how to configure IP multicast on the E-series router; it contains the following sections:

Overview

IPv4 defines three types of addresses: *unicast*, *broadcast*, and *multicast*. Each type of address enables a device to send datagrams to selected recipients:

- A unicast address enables a device to send a datagram to a single recipient.
- A broadcast address enables a device to send a datagram to all hosts on a subnetwork.
- A multicast address enables a device to send a datagram to a specified set of hosts, known as a multicast group, in different subnetworks.

Multicast IP packets contain a class D address in the Destination Address fields of their headers. A class D address is the IP address of a multicast group. See *Chapter 6, Configuring IGMP* and *JUNOSe IP, IPv6, and IGP Configuration Guide, Chapter 1, Configuring IP*, for information about class D addresses.

IP multicast improves network efficiency by enabling a host to transmit a datagram to a targeted group of receivers. For example, for a host to send a large video clip to a group of selected recipients would be time-consuming to unicast the datagram to each recipient individually. If the host broadcasts the video clip throughout the network, network resources are not available for other tasks. The host uses only the resources it needs when multicasting the datagram.

Routers use multicast routing algorithms to determine the best route and transmit multicast datagrams throughout the network. E-series routers support a number of IP multicast protocols on virtual routers (VRs). Each VR handles the interoperability of IP multicast protocols automatically. To start multicast operation on a VR, you access the context for that VR and configure the desired protocols on the selected interfaces. Table 4 describes the function of each protocol that the router supports.

Table 4: Function of Multicast Protocols on a Router

Protocol	Function
Internet Group Membership Protocol (IGMP)	Discovers hosts that belong to multicast group.
Protocol Independent Multicast Protocol (PIM)	Discovers other multicast routers to receive multicast packets.
Distance Vector Multicast Routing Protocol (DVMRP)	Routes multicast datagrams within autonomous systems.
BGP Multicasting Protocol	Routes multicast datagrams between autonomous systems.

The router supports up to 16,384 multicast forwarding entries (multicast routes) at any time.

Reverse-Path Forwarding

IP multicasting uses reverse path forwarding (RPF) to verify that a router receives a multicast packet on the correct incoming interface. The RPF algorithm enables a router to accept a multicast datagram only on the interface from which the router sends a unicast datagram to the source of the multicast datagram.

When the router receives a multicast datagram from a source for a group, the router verifies that the packet was received on the correct RPF interface. If the packet was not received on the correct interface, the router discards the packet. Only packets received on the correct RPF interface are considered for forwarding to downstream receivers.

When operating in sparse-mode, the routers perform an RPF lookup to identify the upstream router from which to request the data and then send join messages for the multicast stream only to that router.

When operating in dense-mode, routers that have multiple paths to the source of the multicast stream initially receive the same stream on more than one interface. In this case, the routers perform an RPF lookup to identify multicast data streams that are not arriving on the best path and send prune messages to terminate these flows.

The RPF lookup need not always be towards the source of the multicast stream. The lookup is done towards the source only when the router is using a source-rooted tree to receive the multicast stream. If the router uses a shared tree instead, the RPF lookup is toward a rendezvous point and not toward the source of the multicast stream.

Multicast Packet Forwarding

Multicast packet forwarding is based on the source (S) of the multicast packet and the destination multicast group address (G). For each (S,G) pair, the router accepts multicast packets on an incoming interface (IIF), which satisfies the RPF check (RPF-IIF). The router drops packets received on IIFs other than the RPF-IIF and notifies the routing protocols that a packet was received on the wrong interface.

The router forwards packets received on the RPF-IIF to a list of outgoing interfaces (OIFs). The list of OIFs is determined by the exchange of routing information and local group membership information. The router maintains mappings of (S,G, IIF) to {OIF1, OIF2…} in the multicast routing table.

You can enable two or more multicast protocols on an IIF. However, only one protocol can forward packets on that IIF. The protocol that forwards packets on an IIF *owns* that IIF. A multicast protocol that owns an IIF also owns the (S,G) entry in the multicast routing table.

Platform Considerations

For information about modules that support IP multicasting on the ERX-7xx models, ERX-14xx models, and the ERX-310 router:

- See *ERX Module Guide, Table 1, Module Combinations* for detailed module specifications.
- See *ERX Module Guide, Appendix A, Module Protocol Support* for information about the modules that support IP multicasting.

For information about modules that support IP multicasting on the E120 router and the E320 router:

- See *E120 and E320 Module Guide, Table 1, Modules and IOAs* for detailed module specifications.
- See *E120 and E320 Module Guide, Appendix A, IOA Protocol Support* for information about the modules that support IP multicasting.

References

For more information about IP multicast, see the following resources:

- A “traceroute” Facility for IP Multicast—draft-ietf-idmr-traceroute-ipm-07.txt (January 2001 expiration)
- RFC 2858—Multiprotocol Extensions for BGP-4 (June 2000)
- RFC 2932—IPv4 Multicast Routing MIB (October 2000)
- RFC 3292—General Switch Management Protocol (GSMP) V3 (June 2002)

NOTE: IETF drafts are valid for only 6 months from the date of issuance. They must be considered as works in progress. Refer to the IETF Web site at http://www.ietf.org for the latest drafts.

Before You Begin

You can configure multicasting on IPv4 and IPv6 interfaces.

For information about configuring IP interfaces, see *JUNOSe IP, IPv6, and IGP Configuration Guide, Chapter 1, Configuring IP*. For information about configuring IPv6 interfaces, see *JUNOSe IP, IPv6, and IGP Configuration Guide, Chapter 2, Configuring IPv6*.

For information about configuring multicast on IPv6 interfaces, see *Chapter 10, Configuring IPv6 Multicast*.

Configuring the Switch Fabric Bandwidth

By default, the switch fabric for the ERX-1440, ERX-310, E120, and E320 routers uses a bandwidth weighting ratio of 15:2 for multicast-to-unicast weighted round robin (WRR). In the absence of strict-priority traffic, and when both unicast and multicast traffic compete for switch fabric bandwidth, the switch fabric allocates 15/17ths of the available bandwidth to multicast traffic and 2/17ths of the available bandwidth to unicast traffic.

You can use the **fabric weights** command to change the ratio for multicast-to-unicast traffic on the router switch fabric. For more information about the **fabric weights** command, see *JUNOSe System Basics Configuration Guide, Chapter 5, Managing the System*.

Enabling IP Multicast

In this implementation, IP multicast works on virtual routers (VRs). By default, IP multicast is disabled on a VR. To enable IP multicast on a VR, access the context for a VR, and then issue the **ip multicast-routing** command.

ip multicast-routing

- Use to enable IP multicast routing on the VR.
- By default, IP multicast is disabled on the VR. In the disabled state, all multicast protocols are disabled, and the VR forwards no multicast packets.
- Example

  host1(config)#**ip multicast-routing**

- Use the **no** version to disable IP multicast routing on the VR (the default).

Defining Static Routes for Reverse-Path Forwarding

Use the **ip rpf-route** command to define reverse-path forwarding (RPF) to verify that a router receives a multicast packet on the correct incoming interface.

ip rpf-route

- Use to customize static routes that the router may use for RPF.
- Specify the IP address and subnet mask of the destination network.
- Specify either a next-hop IP address or an interface type and specifier, such as atm 3/0. For details about interface types and specifiers, see *JUNOSe Command Reference Guide, About This Guide*.
- Optionally, specify the distance (number of hops) to the next-hop address.
- Optionally, specify a route’s tag number to identify a particular route in the routing table.
- Example

  host1(config)#**ip rpf-route 11.1.0.0 255.255.0.0 atm4/1.1 56 tag 25093**

- Use the **no** version to remove the static route.

Displaying Available Routes for Reverse-Path Forwarding

Use the **show ip rpf-route** command to display all available routes, only the routes to a particular destination, or routes associated with a specific unicast protocol that the router can use for Reverse-Path Forwarding (RPF).

show ip rpf-route

- Use to display routes that the router can use for RPF.
- Specify the IP address and the network mask to view routes to a particular destination.
- Specify a unicast routing protocol to view routes associated with that protocol.
- Field descriptions
  - Prefix—Value of the logical AND of the IP address of the destination network and the subnet address
  - Length—Length of the subnet mask in bits
  - Type—Protocol type for the interface
    - Connect—Subnet directly connected to the interface
    - Static—Static route
    - *protocol-name*—Route learned through the named protocol
  - Next Hop—IP address of the next hop for this route
  - Dist—Distance configured for this route
  - Met—Learned or configured cost associated with this route
  - Intf—Type of interface and interface specifier for the next hop. For details about interface types and specifiers, see *JUNOSe Command Reference Guide, About This Guide*.
- Example 1

```
host1#show ip rpf-route
Protocol/Route type codes:
  I1- ISIS level 1, I2- ISIS level2,
  I- route type intra, IA- route type inter, E- route type external,
  i- metric type internal, e- metric type external,
  O- OSPF, E1- external type 1, E2- external type2,
  N1- NSSA external type1, N2- NSSA external type2
  L- MPLS label, V- VR/VRF, *- indirect next-hop

  Prefix/Length    Type    Next Hop       Dist/Met   Intf
  -------------    ----    --------       --------   ------
  10.10.0.112/32    Static  192.168.1.1     1/1       fastEthernet0/0
  10.1.1.0/24       Connect 10.1.1.1        0/1       atm3/0.100
  25.25.25.25/32    Connect 25.25.25.25     0/1       loopback0
```

- Example 2

```
host1#show ip rpf-route static
Protocol/Route type codes:
  I1- ISIS level 1, I2- ISIS level2,
  I- route type intra, IA- route type inter, E- route type external,
  i- metric type internal, e- metric type external,
  O- OSPF, E1- external type 1, E2- external type2,
  N1- NSSA external type1, N2- NSSA external type2
  L- MPLS label, V- VR/VRF, *- indirect next-hop

 Prefix/Length  Type   Next Hop   Dist/Met  Intf
 -------------  ----   --------   --------  --------------
10.10.0.112/32  Static 192.168.1.1  1/1     fastEthernet0/0
```

Enabling and Disabling RPF Checks

By default, the router accepts multicast packets for each Source, Group (S,G) pair on an incoming interface (IIF), which satisfies the RPF check (RPF-IIF). When the router performs RPF checks, only the interface that first accepts traffic for an (S,G) pair accepts subsequent traffic for that pair. If traffic stops arriving on that interface and starts arriving on another interface, the router does not accept or forward the traffic.

Some network configurations require the router to accept traffic on any interface. To do so, you can disable the RPF check on a specified set of (S,G) pairs by issuing the **ip multicast-routing disable-rpf-check** command.

When you disable RPF checks, the router accepts multicast packets for (S,G) pairs on any incoming interface. When the router has added the new route to its multicast routing table, it then accepts multicast packets for these pairs on any interface in the virtual router and forwards them accordingly. Multicast routes established before you issue this command are not affected.

ip multicast-routing disable-rpf-check

- Use to disable RPF checks for specified (S,G) pairs.
- Specify a standard IP access list that defines the (S,G) pairs.
- Example

  host1(config)#**ip multicast-routing disable-rpf-check boston-list**

- Use the **no** version to restore the default, in which the router performs RPF checks for all (S,G) pairs.

Using Unicast Routes for RPF

You can specify that IS-IS, OSPF, or RIP routes be available for RPF. Routes available for RPF appear in the multicast view of the routing table.

ip route-type

- Use to specify whether IS-IS, OSPF, or RIP routes are available only for unicast forwarding, only for multicast RPF checks, or for both.
- Use the **show ip rpf-routes** command to view the routes available for RPF.
- By default, IS-IS, OSPF, and RIP routes are available both for unicast forwarding and multicast reverse-path forwarding checks.
- Example

  host1(config)#**router ospf**
  host1(config-router)#**ip route-type multicast**

- There is no **no** version.

Defining Permanent IP Multicast Forwarding Entries

An mroute is a multicast traffic flow (a (Source, Group) entry used for forwarding multicast traffic). By default, forwarding mroutes (with a valid RPF incoming interface) are timed out if data for them is not received for 210 seconds. However, you can specify an mroute as permanent by using the **ip multicast-routing permanent-mroute** command.

ip multicast-routing permanent-mroute

- Use to specify that any newly created mroutes that match the specified access-list do not time out.
- Using this command does not change existing mroutes.
- Permanent mroutes are removed if a topology change occurs that affects the mroute.
- Permanent mroutes may be removed due to certain protocol actions (for example, PIM sparse-mode switching from shared to shortest-path tree).
- Outgoing interface lists of permanent mroutes may change due to protocol actions.
- Example

  host1(config)#**ip multicast-routing permanent-mroute routes1**

- Use the **no** version to prevent any new mroutes from becoming permanent. To remove existing permanent mroutes, use the **clear ip mroute** command.

Defining a Multicast Bandwidth Map

Multicast interface-level admission control, port-level admission control, and QoS adjustment all use a single multicast bandwidth map. The multicast bandwidth map is a route map that uses the **set admission-bandwidth**, **set qos-bandwidth**, **set admission-bandwidth adaptive**, or **set qos-bandwidth adaptive** commands. The **adaptive** commands configure an autosense mechanism for measuring the multicast bandwidth.

NOTE: Even though you can include any of the preceding commands several times in a route map entry, only the last **admission-bandwidth** command or **qos-bandwidth** command in the bandwidth map is used. In other words, if you included the **set qos-bandwidth** command first and then the **set qos-bandwidth adaptive** command, the bandwidth map uses the **set qos-bandwidth adaptive** command.

Interface-level and port-level admission control is performed when an OIF on the interface or port is added to the mroute for a given (S,G) multicast data stream and the multicast bandwidth map contains a **set admission-bandwidth** or **set admission-bandwidth adaptive** action for that (S,G).

QoS adjustment is performed on the joining interface when an OIF is added to the mroute for a given (S,G) data stream and the multicast bandwidth map contains a **set qos-bandwidth** or **set qos-bandwidth adaptive** action for that (S,G).

You can prioritize the traffic by configuring a priority value for the <S, G> data stream on a physical port by issuing the **set priority** command. Dynamic multicast admission control enables only prioritized groups to join the interface after the configured priority limit is reached on the physical port. The system records the priority when a new <S, G> entry is created. For more information, see *Enabling Port Admission Bandwidth Control* on page 49.

NOTE: You can create a single route map with the **set admission-bandwidth** command, the **set qos-bandwidth** command, or both. However, creating an entry with only one of these **set** commands enables only that specific function for the matched address (that is, only multicast traffic admission control or only QoS adjustment). The same is true for the **adaptive** commands.

Using the Autosense Mechanism

Video bandwidth is typically considered to be a constant rate—2 Mbps for standard definition television (SDTV) and 10 Mbps for high definition television (HDTV). However, in reality, and depending on achievable video compression, the bit rate can vary. For example, HDTV streams (using MPEG4 or WM9 encoding) can vary between 6 Mbps (for low-action programs) to 10 Mbps (for a fast-paced, high-action programs). The autosense mechanism causes the bandwidth value, used for admission control and QoS adjustment, to be the actual measured rate of the stream. Using this feature to measure the actual bandwidth avoids the need to configure arbitrary bandwidth limits and enables a channel to be reassigned to a different (S, G) without requiring a bandwidth map to be changed.

How Adaptive Mode Works

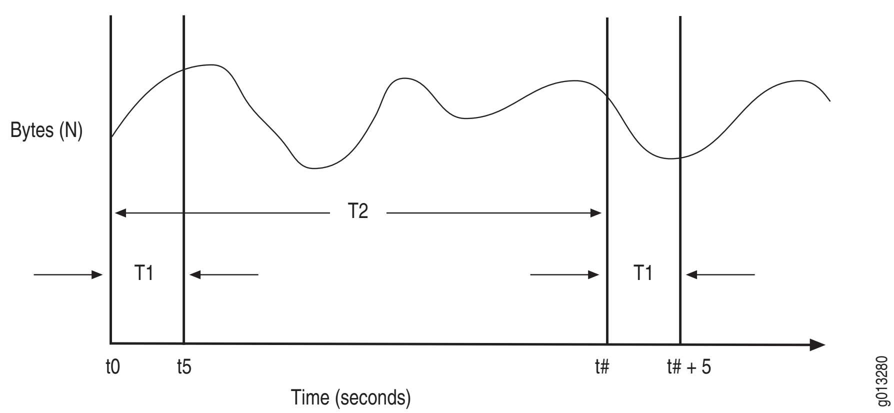
You configure the auto-sense mechanism in the multicast bandwidth using the **set admission-bandwidth adaptive** command, **set qos-bandwidth adaptive** command, or both. For example:

```
host1(config)#route-map mcast-bandwidths permit 10
host1(config-route-map)#match ip address sdtv
host1(config-route-map)#set admission-bandwidth adaptive
host1(config-route-map)#set qos-bandwidth adaptive
host1(config-route-map)#end
```

In this example, any stream with an (S,G) that matches the sdtv access list performs adaptive bandwidth detection for admission control and QoS adjustment.

A rate measurement mechanism runs on the ingress line card that polls the forwarding controller (FC) to obtain statistics for each mroute. This mechanism then reports the rate measurement to the SRP to update the bandwidth map. By computing the average bandwidth over a relatively short sampling period (T1; 5 seconds), the measurement approximates the peak bandwidth of the multicast stream.

As an example, assume that a new mroute (S1, G1) is added to the interface controller (IC) at time t0.



To calculate the measured bandwidth of a stream, the router uses the following equation:

$R = (N_{t+5} - N_t) / 5$

Where

R = Calculated bandwidth of the stream during each sampling interval

N_t = Bytes measured at the start of each sampling period (t seconds)

N_{t+5} = Bytes measured at the end of each sampling period (t + 5 seconds)

NOTE: When the mroute is first installed in the FC (at t = 0), R_0 is undetermined. For multicast admission control no joins are admitted until the first bandwidth measurement is computed (that is, for admission control, R_0 is considered to be infinite). Similarly, no QoS adjustment occurs until the first bandwidth measurement is computed (that is, for QoS adjustment, R_0 is considered to be zero [0]).

Using the previous graph as a reference, the first bandwidth rate (R_1) is determined by calculating the number of bytes received during the first sampling period, T_1. Mroute statistics are read at time t_0 (N_0) and at time t_5 (N_5) and the bytes received values are subtracted and divided by the sampling period T_1 to yield the average rate. This process is repeated every sampling interval, T_2, to yield rates R1, R2, R3, and so on.

The first two sampling interval calculations are as follows:

$R_1 = (N_5 - N_0)/5$

$R_2 = (N_{\#+5} - N_{\#})/5$

The router maintains a history of bandwidth measurements (H) for each mroute, up to a maximum of M measurements. The actual rate, R, reported to the SRP is the maximum rate measured in those H samples.

To minimize the IC to SRP traffic generated by the rate measurements, the IC reports a bandwidth change only when a newly computed rate (R#) differs from the current rate by a specified threshold. When R_s is computed at time t = 5 seconds, R is set to R_1. A rate update occurs whenever a newly calculated rate (R) differs from R_1 by at least a threshold value (specified as a percentage, P) of the measured peak bandwidth. This calculation is as follows:

R = Rt, if and only if the absolute value of (R - Rt) > P * R.

Table 5 lists values assigned to variables associated with this algorithm.

Table 5: Adaptive Mode Algorithm Values

Variable	Value	Units	Description
T1	5	Seconds	Sampling period; the time in which a sample is taken
T2	0	Seconds	Sampling interval; zero (0) seconds indicates continuous sampling
H	12	Samples	Number of history samples over which to compute measurement
M	12	Samples	Maximum number of samples maintained in history
P	1	Percent	Threshold value; percent difference by which a newly calculated rate must differ from the measured peak bandwidth before a rate update occurs

Multicast Bandwidth Map Example

The following example creates a multicast bandwidth map for both multicast traffic admission control and QoS adjustment:

NOTE: In this example, you can replace the **set admission-bandwidth** command and **set qos-bandwidth** command with their **adaptive** command counterparts.

1. Define a route-map using the **set admission-bandwidth** and **set qos-bandwidth** commands. You can optionally issue the **set priority** command.

   ```
   host1(config)#route-map mcast-bandwidths permit 10
   host1(config-route-map)#match ip address sdtv
   host1(config-route-map)#set admission-bandwidth 2000000
   host1(config-route-map)#set qos-bandwidth 2000000
   host1(config-route-map)#set priority 100
   host1(config-route-map)#route-map mcast-bandwidths permit 20
   host1(config-route-map)#match ip address hdtv
   host1(config-route-map)#set admission-bandwidth 10000000
   host1(config-route-map)#set qos-bandwidth 10000000
   host1(config-route-map)#set priority 200
   host1(config-route-map)#end
   ```

2. Define the access list for use by the **match ip address** command to match (S,G) and (*,G) entries.

   ```
   host1(config)#access-list sdtv permit ip host 31.0.0.1 232.0.0.0 0.0.0.255
   host1(config)#access-list hdtv permit ip host 32.0.0.1 232.0.0.0 0.0.0.255
   host1(config)#access-list hdtv permit ip host 32.0.0.2 232.0.0.0 0.0.0.255
   host1(config-route-map)#end
   ```

NOTE: You can also define a prefix-list or a prefix-tree for use by the **match ip address** command to match (S,G) and (*,G) entries.

For additional information about configuring QoS adjustment, see *Configuring Multicast QoS Adjustment* on page 35.

For additional information about configuring interface-level and port-level admission control, see *Blocking and Limiting Multicast Traffic* on page 46.

For additional information about creating route maps, see *JUNOSe IP Services Configuration Guide, Chapter 1, Configuring Routing Policy*.

set admission-bandwidth

- Use to set a multicast bandwidth for admission control.
- Use the **adaptive** keyword to define the bandwidth as adaptive (automatically sensed).
- Example

  ```
  host1(config-route-map)#set admission-bandwidth 2000000
  ```

- Use the **no** version to remove the set clause from a route map.

set priority

- Use to configure a priority value for the <S, G> data stream on a physical port.
- Dynamic multicast admission control enables only prioritized groups to join the interface after the configured priority limit is reached on the physical port. The system records the priority when a new <S, G> entry is created.
- Example

  host1(config-route-map)#**set priority 100**

- Use the **no** version to remove the priority value.

set qos-bandwidth

- Use to set a multicast bandwidth for QoS adjustment.
- Use the **adaptive** keyword to define the bandwidth as adaptive (automatically sensed).
- Example

  host1(config-route-map)#**set qos-bandwidth 10000000**

- Use the **no** version to remove the set clause from a route map.

Configuring Multicast QoS Adjustment

When the router uses multicast OIF mapping, any multicast streams that a subscriber receives bypass any configured QoS treatment for that subscriber interface. The Multicast QoS adjust feature provides a way in which the router can account for this multicast traffic.

NOTE: For additional information about how to configure OIF mapping, see *Configuring Group Outgoing Interface Mapping* on page 73.

The following sections provide two possible configuration cases for using multicast QoS adjustment.

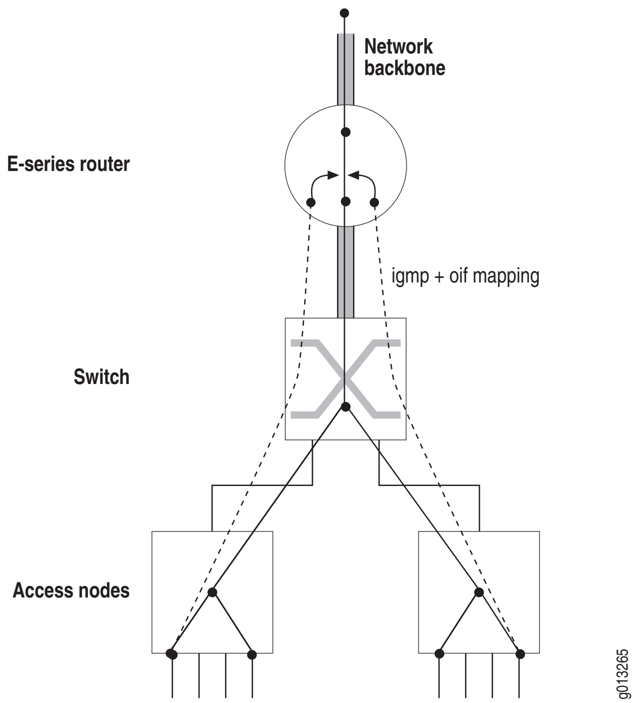
NOTE: For additional information about QoS adjustment, see *JUNOSe Quality of Service Configuration Guide, Chapter 26, Configuring IP Multicast Bandwidth Adjustment with QoS Parameters*.

Multicast OIF Mapping Case

Multicast OIF mapping enables the router to decrease the inefficiencies associated with replicating streams of multicast traffic. Using OIF maps, IGMP joins that the router receives on a subscriber interface can be mapped to a special interface for forwarding. This special interface can be on a different physical port or line module from that of the join interface.

Using this mapping function, the router can send a single copy of each multicast stream over the special interface and the access nodes are configured to perform any final replication to the subscribers and merge unicast and multicast data flows onto the subscriber interfaces as necessary. See Figure 1.

Figure 1: Multicast OIF Mapping



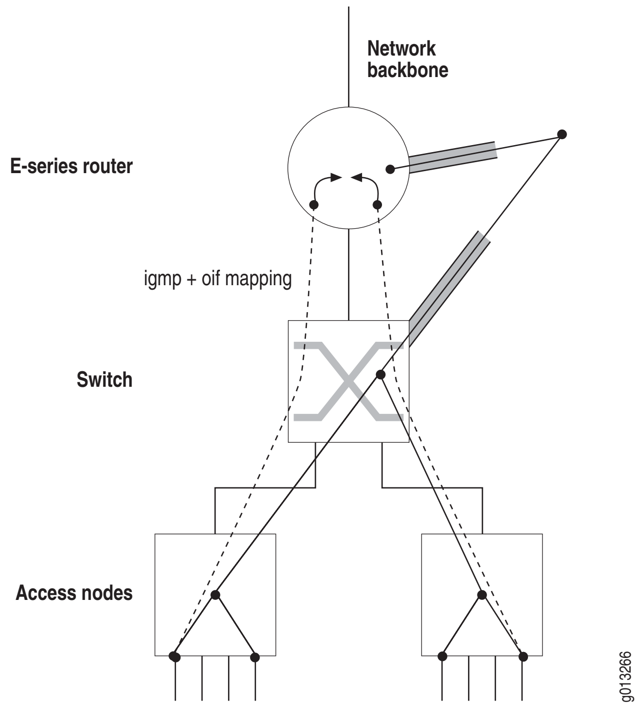
One disadvantage to using multicast OIF mapping is that the multicast traffic bypasses any QoS treatment that is applied to subscriber interfaces. Configuring QoS adjustment resolves this problem. (See *JUNOSe Quality of Service Configuration Guide, Chapter 24, Configuring a QoS Parameter* for additional information about configuring QoS adjustment.) With QoS adjustment configured, when a subscriber requests to receive a multicast stream (or, more appropriately, when an OIF is added to the mroute), the router reduces the unicast QoS bandwidth applied to the subscriber interface (that is, the join interface) by the amount of bandwidth for that multicast stream.

Multicast Traffic Receipt Without Forwarding

In this case, the router is not given the responsibility of forwarding multicast streams. Instead, the service provider arranges for the router to receive the multicast streams so the router can detect the flow and perform QoS adjustment. An OIF map is installed that maps the traffic streams to a loopback interface configured for IGMP version passive. This means that when the traffic is received, a null mroute is installed (that is, an mroute with an empty OIF list) and the router applies the QoS adjustment to the join interface. See Figure 2.

NOTE: Ensure that PIM-SM (or any other upstream multicast protocol) is informed of the group (or source-group) interest.

Figure 2: Multicast Traffic Receipt Without Forwarding



Activating Multicast QoS Adjustment Functions

The **ip multicast-routing bandwidth-map** command activates the specified bandwidth map. By activating the bandwidth map, this command also activates the multicast QoS adjustment function contained in the bandwidth map.

CAUTION: To activate multicast QoS adjustment, you must first create a bandwidth map. See *Defining a Multicast Bandwidth Map* on page 31 for details.

ip multicast-routing bandwidth-map

- Use to activate the QoS adjust function on the router.
- Example

  host1(config)#**ip multicast-routing bandwidth-map mcast-bandwidths**

- Use the **no** version to disable the multicast QoS adjustment function on the router.

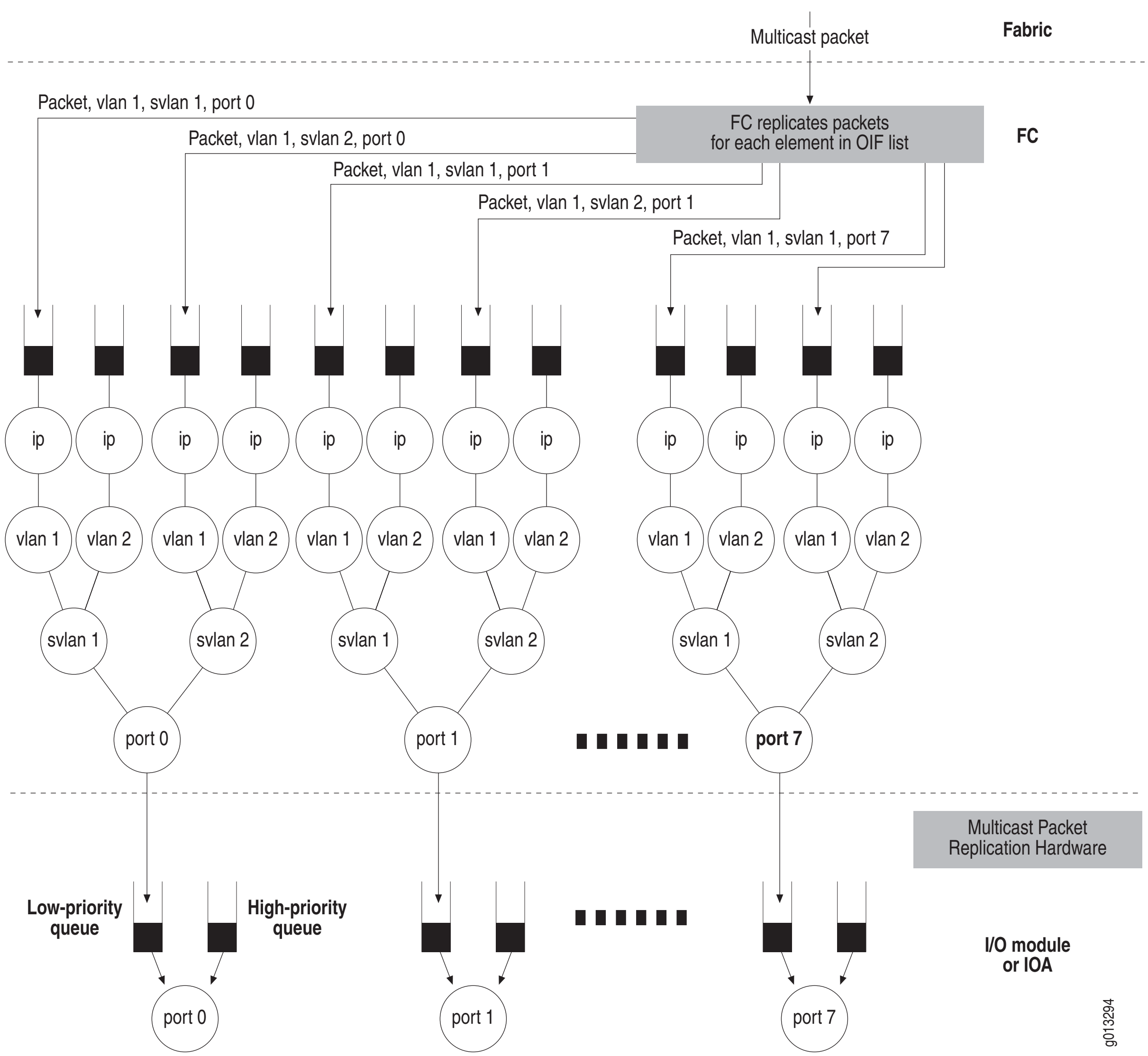
Configuring Hardware Multicast Packet Replication

You can configure IPv4 multicast to replicate packets to optimized hardware on a logical port instead of using the forwarding controller (FC) on the router.

The bandwidth between the line module and the I/O module or IOA on the E-series router is limited. A high-density Ethernet module provides eight physical ports that can consume the bandwidth between the line module and the I/O module or IOA before providing enough traffic to support egress line rate for all of these ports.

Figure 3 on page 38 displays how multicast traffic is typically replicated on the line module. Each of these replicated packets is transmitted from the line module to the I/O module or IOA.

Figure 3: Packet Flow Without Hardware Multicast Packet Replication



The hardware multicast packet replication feature enables you to configure multicast traffic for a VLAN or S-VLAN to be replicated on the I/O module or IOA so that only one copy of the packet is transmitted from the line module to the I/O module or IOA. Replication for each of the ports is performed on the I/O module or IOA.

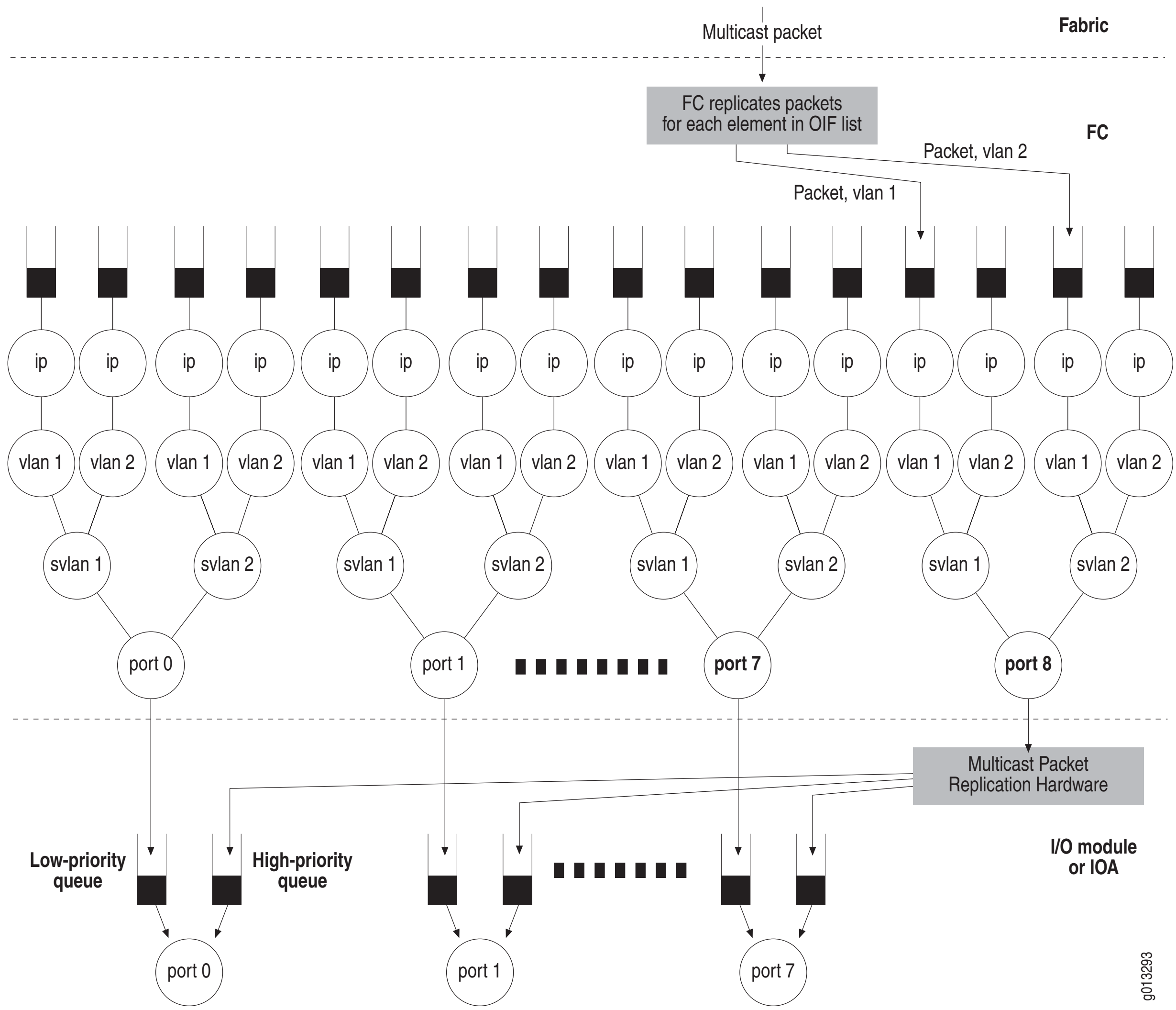
Configuring hardware multicast packet replication for high-density Ethernet is useful when you want to provide the same multicast stream out of some or all of the ports, such as for IP television (IPTV). Configuring hardware multicast packet replication enables you to:

- Reduce the number of packets sent from the FC to the module.
- Reduce the CPU consumed by the FC processing each elaboration of the packet.

You can use the additional bandwidth to increase the bandwidth of multicast traffic out of each of the Gigabit Ethernet ports.

Figure 4 displays the flow of a multicast packet using the hardware multicast packet feature.

Figure 4: Packet Flow with Hardware Multicast Packet Replication



Each high-density Ethernet module has eight physical ports, numbered 0–7. A logical port is available for the hardware multicast packet replication feature, numbered port 8.

JUNOSe tracks the OIFs in an mroute that have been redirected to use the hardware multicast packet replication hardware. The system accepts only egress multicast traffic to traverse the interface stack on the enabled port. The system drops unicast traffic that is routed to this port.

Each port on the I/O module or IOA displayed in Figure 4 has two queues. These queues are further down the egress path than the queues found on the line module and populated by the FC.

The low-priority queue is dedicated to packets that are received from the line module queues that are dedicated to the physical ports. This queue blocks when full and provides backpressure to the line module. This queue services unicast and multicast traffic that is not using the hardware multicast packet replication feature.

The high-priority queue is dedicated to packets that are received from the line module queue for port 8. This queue is serviced at a higher priority than the first queue, and drops packets when full.

For more information about high-density Ethernet, see *JUNOSe Physical Layer Configuration Guide, Chapter 5, Configuring Ethernet Interfaces*.

Supported Modules and Encapsulations

You can enable hardware multicast packet replication on port 8 of the following high-density Ethernet modules:

- GE-8 I/O module (pairs with the GE-HDE line module)
- ES2-S1 GE-8 IOA (pairs with the ES2 4G LM and the ES2 10G LM)

When enabled, the hardware multicast packet replication feature defines the encapsulation of the egress multicast packet. The following encapsulations are supported:

- IPv4 over Gigabit Ethernet
- IPv4 over VLAN
- IPv4 over S-VLAN

NOTE: 802.3ad link aggregation group (LAG) bundles do not support hardware multicast packet replication.

The hardware multicast packet replication feature also provides an interface over which you can configure the following:

- IP MTU
- Ethernet MTU
- Egress IP policy
- Egress VLAN policy
- QoS

Relationship with OIF Mapping

Multicast OIF mapping enables the router to decrease the inefficiencies associated with replicating streams of multicast traffic. Using OIF maps, IGMP joins that the router receives on a subscriber interface can be mapped to a dedicated multicast VLAN.

The hardware multicast packet replication feature enables you to redirect each of the IP interfaces on a line module over a dedicated multicast VLAN to a single IP interface over port 8. The FC is only required to send a single packet per dedicated multicast VLAN to the I/O module or IOA. The module then replicates this packet to the appropriate ports.

For more information about configuring OIF mapping, see *Configuring Group Outgoing Interface Mapping* in *Chapter 6, Configuring IGMP*.

Hardware Multicast Packet Replication Considerations

When configuring hardware multicast packet replication, the following considerations apply.

- Do not configure or transmit routing protocols over port 8. The FC drops traffic routed to an IP interface stacked over port 8.
- We recommend that you configure the IP address of the IP interface over port 8 to be unnumbered.
- We recommend that you configure an IP interface over a VLAN over one of the physical ports to reference the IP interface over the same VLAN over port 8.

  You cannot create the following configurations:

  - When two IP interfaces configured over a port reference the same IP interface over port 8. The system does not accept this configuration attempt because you typically configure the hardware multicast packet replication feature to redirect multicast traffic over one VLAN, then redirect it to the same VLAN on port 8.
  - When the IP interface configured with the hardware multicast packet replication attribute is not installed on a line module that supports hardware multicast packet replication.
  - When the IP interface designated by the hardware multicast packet replication attribute is not installed on a line module that supports hardware multicast packet replication.
  - When the IP interface designated by the hardware multicast packet replication attribute is not on the same line module as the IP interface configured with this attribute.
- When you configure a unique source MAC address for VLANs on port 8, the hardware multicast packet replication hardware stamps the source MAC address on the VLAN, overwriting any MAC address that you configured. For more information, see *JUNOSe Physical Layer Configuration Guide, Chapter 5, Configuring Ethernet Interfaces*.

- The regular multicast implementation utilizes interface stacking that provides a unique IP attachment point for each elaboration of the egress multicast packet.

  For the hardware multicast packet replication feature, you must attach policies to an interface stack over port 8 that defines the encapsulation of the egress multicast traffic. The system supports policies over port 8 just as it is above any of the other ports on this line module.

  Policies applied to the interface stack over port 8 affect the packets traversing this stack whether or not the packet is destined for one port or all of the physical ports. Therefore, you cannot apply different egress policies to multicast traffic for the interfaces stacked above different ports, or rate limit on an individual interface over a port. You also cannot monitor policy statistics on individual interfaces over a port.

  Instead, you can apply egress policy to an interface stacked over port 8. The system applies the policy before the packet has been elaborated for each of the ports.

- The JUNOSe QoS component provides hierarchical egress scheduling and shaping on Gigabit Ethernet ports 0–7. The regular multicast implementation replicates packets on the FC, with each replicated packet placed on a line module queue destined for a single physical port. The line module queue can also receive QoS behavior specific to that queue.

  For the hardware multicast packet replication feature, the FC does not replicate the packet for each of the individual ports. Instead, it places the packet on a special queue destined for port 8.

  You can configure QoS on the packets flowing through port 8, but this has limited value because each packet passed through this port can be transmitted through one of more of the physical ports. Therefore, the packets placed on this special queue might not receive the same QoS behavior as ports 0–7.

  We recommend that you configure the network so the I/O or IOA queues are not oversubscribed. The traffic transmitted by the physical port is a combination of packets from the two I/O or IOA queues. When the sum of the packets in these queues is greater than line rate, the system can drop traffic that is not using hardware multicast packet replication.

  When you configure a traffic shaper on a physical port and configure hardware multicast packet replication, the packets created using the feature avoid the traffic shaper for that port. To control this, you can use traffic shaper on the physical port and port 8. The sum of the traffic shapers must be less than or equal to the line rate of the port.

  A traffic shaper on port 8 can result in the overall utilization of egress bandwidth for any one port being less the line rate because the packets being replicated might not be transmitted to every port. Packets destined to some of the ports contribute to the traffic shaping for all of the ports on the I/O module or IOA.

Configuring Hardware Multicast Packet Replication

To configure hardware multicast packet replication:

1. Configure port 8 on a high-density Ethernet module to accept redirected egress multicast traffic.

    a. Specify the Gigabit Ethernet interface on port 8.

    b. Create a VLAN major interface.

    c. Create a VLAN subinterface.

    d. Assign a VLAN ID.

    e. Configure an unnumbered IP interface.

    f. Enable IGMP on the interface with only multicast-data-forwarding capability.

    host1(config)#**interface gigabitEthernet 2/8**
    host1(config-if)#**encapsulation vlan**
    host1(config-if)#**interface gigabitEthernet 2/8.1**
    host1(config-if)#**vlan id 1**
    host1(config-if)#**ip unnumbered loopback 0**
    host1(config-if)#**ip igmp version passive**

2. Configure an IP interface to redirect egress multicast traffic to port 8.

    a. Create a VLAN subinterface.

    b. Assign a VLAN ID.

    c. Assign an IP address.

    d. Configure the interface to redirect egress multicast traffic to port 8.

    host1(config)#**interface gigabitEthernet 2/0.101**
    host1(config-if)#**vlan id 1**
    host1(config-if)#**ip address 10.1.1.1 255.255.255.0**
    host1(config-if)#**ip multicast ioa-packet-replication gigabitEthernet 2/8.1**

encapsulation vlan

- Use to configure VLAN as the encapsulation method for the interface.
- Example

  host1(config-if)#**encapsulation vlan**

- Use the **no** version to disable VLAN on an interface.

ip igmp version

- Use to set the IGMP version (1, 2, or 3) for the interface or specify a passive interface with only multicast-data-forwarding capability (passive).
- Example

  host1:boston(config-if)#**ip igmp version passive**

- Use the **no** version to set the version to the default, IGMPv2.

ip multicast ioa-packet-replication

- Use to configure hardware multicast packet replication on port 8 of a high-density Ethernet module.
- Example

  host1(config-if)#**ip multicast ioa-packet-replication gigabitEthernet 3/8.1**

- Use the **no** version to disable hardware multicast packet replication.

ip unnumbered

- Use to configure an unnumbered IP interface.
- This command enables IP processing on an interface without assigning an explicit IP address to the interface.
- You must specify an interface location, which is the identifier of another interface on which the router has an assigned IP address. This interface cannot be another unnumbered interface.
- Example

  host1(config-if)#**ip unnumbered loopback 10**

- Use the **no** version to disable IP processing on the interface.

Monitoring Hardware Multicast Packet Replication

This section describes how to monitor hardware multicast packet replication.

Port Statistics

Use the **show interfaces gigabitEthernet** command to display port statistics for port 8. For port 8, queue statistics have no direct relationship to any of the 8 ports because each packet transmitting through the queue can be sent through 1 or more of the 8 physical ports. For more information, see *Monitoring Ethernet Interfaces* in *JUNOSe Physical Layer Configuration Guide, Chapter 5, Configuring Ethernet Interfaces*.

IP and VLAN Statistics

Use the **show vlan subinterface** command to display statistics for a VLAN interface configured over port 8. For more information, see *Monitoring Ethernet Interfaces* in *JUNOSe Physical Layer Configuration Guide, Chapter 5, Configuring Ethernet Interfaces*.

Use the **show ip interface** command to display statistics for an IP interface configured over port 8. For more information, see *Monitoring IP* in *JUNOSe IP, IPv6, and IGP Configuration Guide, Chapter 1, Configuring IP*.

Multicast traffic redirected by the hardware multicast packet replication feature is displayed in the statistics for the IP or VLAN interface over port 8, not the original IP or VLAN interface over the physical port.

The statistics for the IP or VLAN interface over port 8 reflect the number of packets that passed through this interface destined for the hardware multicast packet replication hardware. These statistics have no direct correlation to the number of packets being transmitted from any of the physical ports.

IGMP Statistics

Use the **show ip igmp interface** command to display statistics, including hardware multicast packet replication configuration, for an IP interface stacked over port 8. For more information, see *Monitoring IGMP* in *Chapter 6, Configuring IGMP*.

Blocking and Limiting Multicast Traffic

You can either block mroute creation, limit the multicast bandwidth admitted on an outgoing interface, or limit outgoing interface creation on a port.

Blocking Mroutes

By default, when an interface that is configured with one or more multicast protocols (for example, PIM or IGMP) receives multicast traffic, even when the scope of that traffic exceeds link-local, the virtual router creates an mroute. You can use the **ip block-multicast-sources** command to block all multicast traffic with a scope larger than link-local (for example, global) and prevent mroute creation under these conditions.

NOTE: Issuing this command does not affect reception of link-local multicast packets.

ip block-multicast-sources

- Use to prevent mroute creation by blocking multicast traffic that has a scope larger than link-local (for example, global).
- Example

  host1(config-if)#**ip block-multicast-sources**

- Use the **no** version to restore the default behavior of creating mroutes on received multicast packets.

Limiting Interface Admission Bandwidth

Interface-level multicast admission control is performed when an OIF on the interface is added to the mroute for a given (S,G) multicast data stream and the multicast bandwidth map contains a **set admission-bandwidth** action for that (S,G).

When enabled, the admission-bandwidth for a particular (S,G) is read from the multicast bandwidth map and recorded in the mroute when the (S,G) mroute is created. When an OIF is subsequently added to the mroute, the OIF is blocked from forwarding data if the additional bandwidth contributed by the (S,G) would exceed the admission-bandwidth limit for the interface.

CAUTION: Before you can limit interface-level admission bandwidth, you must first create a bandwidth map. See *Defining a Multicast Bandwidth Map* on page 31 for details.

Enabling Interface Admission Bandwidth Limitation

You can use the **ip multicast admission-bandwidth-limit** command to enable multicast admission control on interfaces (including dynamic IP interfaces) that are configured to run IGMP. You can also use this command on a PIM (sparse-mode, dense-mode, or sparse-dense-mode) interface if IGMP is configured on the interface (including the **ip igmp version passive** command).

ip multicast admission-bandwidth-limit

- Use to limit bandwidth for an interface that accepts IGMP groups.
- Example

  host1:boston(config-if)#**ip multicast admission-bandwidth-limit 2000000**

- Use the **no** version to remove the bandwidth limitation for the interface.

OIF Interface Reevaluation Example

If you change the admission bandwidth for an interface, all mroutes with that interface as an OIF are reevaluated as follows:

- If the bandwidth limit is increased, blocked OIFs may become unblocked. If the interface is a blocked OIF on multiple mroutes, the order in which the mroutes are visited, and which (S,G) streams become unblocked, is not specified.

- If the bandwidth limit is decreased, no currently admitted OIFs are blocked. However, no new OIFs are admitted until the total admitted bandwidth for the interface drops below the new limit.

- If the bandwidth is increased to the point that the bandwidth limit for an interface is now exceeded, no currently admitted OIFs for the affected mroutes are blocked. However, no new OIFs are admitted until the total admitted bandwidth drops below the configured limit.

NOTE: If the multicast bandwidth map that includes the **set admission-bandwidth command** is changed, all affected mroutes are reevaluated in the same manner described previously.

As an example of this function, if the interface has accepted a total bandwidth of 2000000 bps, and you set a limit of 1000000 bps on the interface, the router does not disconnect any already connected OIFs but prevents the interfaces from accepting any more groups. Over time, some groups leave the interfaces and, eventually, the interface limit of 1000000 bps is reached and maintained by the router.

If you set limits for both a port and interfaces on that port, the router uses the lower of the two limits when determining whether or not an interface can accept any new IGMP groups. For example, if you specify an admission bandwidth limit of 2000000 bps for the port and 3000000 bps groups for each interface, additional groups can only be accepted until the port limit of 2000000 bps is reached.

Creating Mroute Port Limits

When a multicast forwarding entry (that is, an mroute) is added with an outgoing interface (OIF) on a port, the OIF count for that port is incremented. If you configure a port limit, and the OIF count on the port exceeds that limit, no OIFs on that port are added to mroutes (that is, OIFs are blocked).

mroute port limit

- Use to configure a limit on the number of mroute OIFs that can be added across different virtual routers, on a port.
- Example

  host1(config)#**mroute port 3/0 limit 10**

- Use the **no** version to remove any OIF port limits.

Limiting Port Admission Bandwidth

Port-level multicast admission control is performed when an OIF on that port is added to the mroute for a given (S,G) multicast data stream and the multicast bandwidth map contains a **set admission-bandwidth** action for that (S,G).

When enabled, the admission-bandwidth for a particular (S,G) is read from the multicast bandwidth map and recorded in the mroute when the (S,G) mroute is created. If you configure a port limit and the OIF count on the port exceeds that limit, no OIFs on that port are added to mroutes (that is, OIFs are blocked).

When a multicast forwarding entry (an mroute) is added with an outgoing interface, OIF is blocked from forwarding data if the additional bandwidth contributed by the (S,G) would exceed the admission-bandwidth limit for the port on which the interface resides.

CAUTION: Before you can limit port-level admission bandwidth, you must first create a bandwidth map. See *Defining a Multicast Bandwidth Map* on page 31 for details.

Enabling Port Admission Bandwidth Control

You can use the **mroute port admission-bandwidth-limit** command to limit the total multicast bandwidth that can be admitted on a port. The admitted bandwidth is summed across all virtual routers with IPv4 and IPv6 mroutes that have OIFs on the port.

NOTE: Admission bandwidth values for a given (S,G) mroute are determined from the bandwidth map. See *Defining a Multicast Bandwidth Map* on page 31 for details.

Dynamic Port Admission Bandwidth Control

You can configure the system to dynamically limit the total multicast bandwidth that can be admitted on a port. The system performs dynamic port-level admission control when an OIF on that port is added to the mroute for a given <S, G> multicast stream.

After the priority bandwidth limit on the port is reached, OIFs on the prioritized <S, G> are only allowed to forward the traffic and unprioritized <S, G> streams are blocked from forwarding data on the OIF.

To enable a priority value for the <S, G> multicast stream, issue the **set priority** command in the multicast bandwidth map. A priority value of 0 indicates an unprioritized stream and any value other than 0 indicates a prioritized stream. Currently there is no support for classification of prioritized streams. For more information about the **set priority** command, see *Defining a Multicast Bandwidth Map* on page 31.

You can configure limits for the bandwidth that is dynamically admitted on the port. The priority bandwidth limit controls the priority bandwidth admitted on a port. The hysteresis limit sets the minimum priority bandwidth limit before the system evaluates mroutes and admits any blocked OIFs.

mroute port admission-bandwidth-limit

- Use to configure a limit on the total multicast bandwidth that can be admitted on a port.
- Use the **priority-bandwidth-limit** keyword to configure the priority bandwidth admitted on a port.
- Use the **hysteresis** keyword to configure the minimum priority bandwidth limit before the system evaluates mroutes and admits any blocked OIFs.
- Example

  host1(config)#**mroute port admission-bandwidth-limit 3000000**

- Use the **no** version to remove any OIF admission bandwidth limits.

OIF Port Reevaluation Example

If you change the admission bandwidth for a port, all mroutes with an OIF on that port are reevaluated as follows:

- If the bandwidth limit is increased, blocked OIFs can become unblocked. However, the order in which the mroutes are visited, and which (S,G) streams become unblocked, is not specified.
- If the bandwidth limit of a port is decreased, no currently admitted OIFs are blocked. However, no new OIFs are admitted until the total admitted bandwidth for the port drops below the new limit.
- If the bandwidth is increased to the point that the bandwidth limit for an interface is now exceeded, no currently admitted OIFs for the affected mroutes are blocked. However, no new OIFs are admitted until the total admitted bandwidth drops below the configured limit.

NOTE: If the multicast bandwidth map that includes the **set admission-bandwidth command** is changed, all affected mroutes are reevaluated in the same manner described previously.

As an example of this function, if the port has accepted a total bandwidth of 3000000 bps, and you set a limit of 2000000 bps on the port, the router does not disconnect any already connected OIFs but prevents the interfaces from accepting any more groups. Over time, some groups leave the interfaces and, eventually, the port limit of 2000000 bps is reached and maintained by the router.

If you set limits for both a port and interfaces on that port, the router uses the lower of the two limits when determining whether or not an interface can accept any new IGMP groups. For example, if you specify an admission bandwidth limit of 2000000 bps for the port and 3000000 bps groups for each interface, additional groups can only be accepted until the port limit of 2000000 bps is reached.

Deleting Multicast Forwarding Entries

You can clear one or more forwarding entries from the multicast routing table. However, if you do so, the entries might reappear in the routing table if they are rediscovered.

clear ip mroute

- Use to delete IPv4 multicast forwarding entries.
- If you specify an *, the router clears all IP multicast forwarding entries.
- If you specify the IPv4 address of a multicast group, the router clears all multicast forwarding entries for that group.
- If you specify the IPv4 address of a multicast group and the IPv4 address of a multicast source, the router clears the multicast forwarding entry that matches that group and source.
- Example

  host1:boston#**clear ip mroute ***

- There is no **no** version.

Monitoring IP Multicast Settings

To display general information about the IP multicast configuration on the router, use the following **show** commands.

show ip mroute

- Use to display information about all or specified multicast forwarding entries.
- Specify a multicast group IP address or both a multicast group IP address and a multicast source IP address to display information about particular multicast forwarding entries.
- Use the **summary** option to see a summary rather than a detailed description.
- Use the **count** option to display the number of multicast forwarding entries.
- Use the **statistics** option to display statistics for packets received through all multicast forwarding entries that the router has added to the multicast routing table and established on the appropriate line modules.
- Use the **active** option to display the active multicast routes with admission bandwidth greater than the specified bandwidth threshold. The default is 4000 bps.
- Field descriptions
  - (S, G)—IP addresses of the multicast source and the multicast group
  - Admission bandwidth—Admission bandwidth per mroute, in bps
  - QoS bandwidth—QoS bandwidth per mroute, in bps
  - Uptime—Length of time that the (S,G) pair has been active, in *days hours:minutes:seconds* format
  - Data Rate—Flow rate for the threshold entry, in Kbps

- SPT Threshold—SPT threshold value for the entry, in Kbps
- Threshold—Threshold value for the entry, in Kpbs
- Expires—Length of time that the (S,G) pair can be active, in *days hours:minutes:seconds* format or *never*
- RPF route—IP address and subnetwork mask of the RPF route
- incoming interface—Type and specifier of the incoming interface for the RPF route
- neighbor address—IP address of the neighbor
- State/Owner—Owner of the route
  - Local—Route belonging to the local interface
  - Static—Static route
  - Other protocols—Route established by a protocol such as RIP or OSPF
- Incoming interface list—List of incoming interfaces on the router. Details include:
  - Type of interface and its specifier
  - Action that the interface takes with packets: Accept or Discard
  - Multicast protocol that owns the interface
- Outgoing interface list—List of outgoing interfaces on the router. Details include:
  - Type of interface and its specifier
  - Action that the interface takes with packets: Forward or Blocked (port-limit)
  - Protocol running on the interface: PIM, DVMRP, or IGMP
  - Amount of time that the interface has been active in this multicast forwarding entry, in *days hours:minutes:seconds* format
  - Length of time that the interface can remain active in this multicast forwarding entry, in *days hours:minutes:seconds* format or *never*
- Counts—Number of types of source group mappings
  - (S, G)—Number of (S, G) entries
  - (*, G)—Number of (*, G) entries

- Example 1—Constant bandwidth bit rate

```
host1#show ip mroute
IP Multicast Routing Table

(S, G) uptime d h:m:s
  [Data rate: Kbps]  [SPT Threshold: Kbps]  [Threshold: Kbps]
  [Admission bandwidth: bps]
  [QoS bandwidth: bps]
  RPF route: addr/mask, incoming interface
             neighbor address, owner route-owner
  Incoming interface list:
      Interface (addr/mask), State/Owner [(RPF IIF)]
  Outgoing interface list:
      Interface (addr/mask), State/Owner, Uptime/Expires
```

```
(10.0.10.1, 225.1.1.1) uptime 0 00:10:31
  Data rate: 2132 Kbps, Threshold 500 Kbps
  Admission bandwidth: 2000000 bps
  RPF route: 10.0.10.0/24, incoming interface atm5/3.1010
             neighbor 10.0.10.8, owner Local
  Incoming interface list:
      atm5/3.1010 (10.0.10.8/24), Accept/Pim (RPF IIF)
  Outgoing interface list:
      atm5/1.108 (108.0.8.5/8), Forward/Pim, 0 00:02:52/never
      atm5/1.109 (107.0.8.4/8), Forward/Pim, 0 00:10:07/never

(1.1.1.1, 225.1.1.1) uptime 0 00:00:34, never expires
RPF route: 1.0.0.0/8, incoming interface ATM5/1.200
             neighbor 2.2.2.2, owner Netmgmt
  Incoming interface list:
      ATM5/1.200 (2.1.1.1/8), Accept/Igmp (RPF IIF)
  Outgoing interface list:
      ATM5/1.300 (3.1.1.1/8), Forward/Igmp, 0 00:00:34/never

Counts:     2 (S, G) entries
            0 (*, G) entries
```

NOTE: The (S,G) entry (1.1.1.1, 225.1.1.1) is the permanent mroute.

- Example 2—Adaptive bandwidths enabled

```
Host1#show ip mroute
                  IP Multicast Routing Table

(S, G) uptime d h:m:s[, expires d h:m:s]
  [Admission bandwidth: bps]
  [QoS bandwidth: bps]
  RPF route: addr/mask, incoming interface
             neighbor address, owner route-owner
  Incoming interface list:
      Interface (addr/mask), State/Owner [(RPF IIF)]
  Outgoing interface list:
      Interface (addr/mask), State/Owner, Uptime/Expires

 (10.0.1.9, 225.1.1.1) uptime 0 00:00:23
  Admission bandwidth: 1998000 bps (adaptive)
  QoS bandwidth: 1998000 bps (adaptive)
  RPF route: 10.0.0.0/8, incoming interface ATM2/1.200
             neighbor 21.1.1.1, owner Netmgmt
  Incoming interface list:
      ATM2/1.200 (21.2.2.2/8), Accept/Pim (RPF IIF)
  Outgoing interface list:
      ATM2/1.300 (31.2.2.2/8), Blocked (port-adm-limit)/Pim, 0
00:00:23/never

Counts: 1 (S, G) entries
        0 (*, G) entries
```

show ip mroute active

- Use to display the active multicast routes with admission bandwidth greater than the specified bandwidth threshold.
- The default is 4000 bps.
- Field descriptions
  - See the **show ip mroute** command and the **show ip mroute summary** command for descriptions of all fields.
- Example 1—Displays active multicast routes with bandwidth above 10000 bps

```
host1#show ip mroute active 10000
              Active IP Multicast Routes >=10000 bps

(S, G) uptime d h:m:s[, expires d h:m:s]
  [Admission bandwidth: bps]
  [QoS bandwidth: bps]
  RPF route: addr/mask, incoming interface
             neighbor address, owner route-owner
  Incoming interface list:
      Interface (addr/mask), State/Owner [(RPF IIF)]
  Outgoing interface list:
      Interface (addr/mask), State/Owner, Uptime/Expires

(52.0.0.1, 232.0.0.1) uptime 0 00:01:07
  Admission bandwidth: 47000 bps (adaptive)
  QoS bandwidth: 47000 bps (adaptive)
  RPF route: 52.0.0.0/24, incoming interface ATM2/1.17
      neighbor 17.0.0.2, owner NetmgmtRpf
  Incoming interface list:
      ATM2/1.17 (17.0.0.2/24), Accept/Igmp (RPF IIF)
  Outgoing interface list:
      NULL

Counts: 1 (S, G) entries
        0 (*, G) entries
```

- Example 2—Displays the summary of active multicast routes

```
host1#show ip mroute summary active
              Active IP Multicast Routes >=4000 bps

Group Address   Source Address  RPF route          RPF Iif         #Oifs
--------------- --------------- ------------------ --------------- -----
232.0.0.1       51.0.0.1        51.0.0.0/24        ATM3/1.17       0
232.0.0.2       51.0.0.1        51.0.0.0/24        ATM3/1.17       0
232.0.0.3       51.0.0.1        51.0.0.0/24        ATM3/1.17       0
Counts: 3 (S, G) entries
        0 (*, G) entries
```

show ip mroute count

- Use to display information about the number of groups and sources.
- Specify a multicast group address or both a multicast group address and a multicast source address to display information about a particular multicast forwarding entry.
- Field descriptions
  - Counts—Number of types of source group mappings
    - (S, G)—Number of (S,G) entries
    - (*, G)—Number of (*,G) entries
- Example

```
host1#show ip mroute count
                 IP Multicast Routing Table

Counts:     2 (S, G) entries
            0 (*, G) entries
```

show ip mroute statistics

- Use to display statistics for packets received through multicast routes that the router has added to the multicast routing table and established on the appropriate line modules.
- Specify a multicast group IP address or both a multicast group IP address and a multicast source IP address to display information about a particular multicast forwarding entry.
- Field descriptions
  - See the **show ip mroute** command for descriptions of all fields except the Statistics field.
  - Statistics

NOTE: The display shows statistics after the VR has added the multicast route to the multicast routing table and established the route on the appropriate line module. Statistics for interactions that take place before the route is established on the line module are not displayed.

    - Received—Number of packets and bytes that the VR received for this multicast route
    - Forwarded—Number of packets and bytes that the VR has forwarded for this multicast route
    - Rcvd on OIF—Number of packets that the VR has received on the outgoing interface (OIF) for this multicast route
- Example

```
host1#show ip mroute statistics
IP Multicast Routing Table

(S, G) uptime d h:m:s[, expires d h:m:s]
  [Admission bandwidth: bps]
  [QoS bandwidth: bps]
  RPF route: addr/mask, incoming interface
             neighbor address, owner route-owner
```

```
  Incoming interface list:
      Interface (addr/mask), State/Owner [(RPF IIF)]
  Outgoing interface list:
      Interface (addr/mask), State/Owner, Uptime/Expires
(10.0.1.9, 225.1.1.1) uptime 0 00:00:23
  Admission bandwidth: 2000000 bps
  QoS bandwidth: 2000000 bps
  RPF route: 10.0.0.0/8, incoming interface ATM2/1.200
             neighbor 21.1.1.1, owner Netmgmt
  Incoming interface list:
      ATM2/1.200 (21.2.2.2/8), Accept/Pim (RPF IIF)
  Outgoing interface list:
      ATM2/1.300 (31.2.2.2/8), Blocked (port-adm-limit)/Pim, 0
00:00:23/never
  Statistics:
      Received   : 23 pkts, 1472 bytes
      Forwarded  : 0 pkts, 0 bytes
      Rcvd on OIF: 0 pkts

Counts: 1 (S, G) entries
        0 (*, G) entries
```

show ip mroute summary

- Use to display a summary of all or specified multicast routes.
- Specify a multicast group IP address or both a multicast group IP address and a multicast source IP address to display information about a particular multicast forwarding entry.
- Field descriptions
  - Group Address—IP address of the multicast group
  - Source Address—IP address of the multicast source
  - RPF route—IP address and network mask of the RPF route
  - RPF Iif —Type and identifier for the incoming interface for the RPF route
  - #Oifs—Number of outgoing interfaces
  - Counts—Numbers of types of (S,G) pairs
    - (S,G)—Number of (S,G) entries
    - (*,G)—Number of (*,G) entries
- Example

```
host1#show ip mroute summary
                  IP Multicast Routing Table

Group Address   Source Address  RPF route    RPF Iif        #Oifs
--------------- --------------- ---------    -------------  ----
224.0.1.39      52.1.1.1        51.1.1.1/32  Register IIF   0
224.0.1.40      51.1.1.1        51.1.1.1/32  loopback1      1

Counts:     2 (S, G) entries
            0 (*, G) entries
```

show ip multicast protocols

- Use to display information about multicast protocols enabled on the router.
- Use the **brief** option to display a summary of information rather than a detailed description.
- Field descriptions
  - Multicast Protocols—Multicast protocols on this router
  - Protocol—Name of the multicast protocol
  - Type—Mode of the multicast protocol
    - For DVMRP—Dense
    - For PIM—Sparse, Dense, or Sparse-Dense
    - For IGMP—Local
  - Interfaces
    - registered—Number of interfaces on which the protocol is configured
    - owned—Number of interfaces that a protocol owns. If you configure only IGMP on an interface, IGMP owns the interface. However, if you configure IGMP and either PIM or DVMRP on the same interface, PIM or DVMRP owns the interface.
  - Registered interfaces—Information about interfaces on which the protocol is configured:
    - Types and specifiers of interfaces. For details about interface types and specifiers, see *JUNOSe Command Reference Guide, About This Guide*.
    - Protocols configured on the interface and the protocol that owns the interface. If you configure only IGMP on an interface, IGMP owns the interface. However, if you configure IGMP and PIM or DVMRP on the same interface, PIM or DVMRP owns the interface.
- Admission-bandwidth—Actual admission bandwidth/configured admission bandwidth (in bps)
- QoS Adjust—Bandwidth of QoS adjustment, in bps
  - Count—Number of multicast protocols on the VR
  - Active <S,G> count—Number of active S,G data streams on the interface
  - Blocked <S,G> count—Number of blocked S,G data streams on the interface
- Example

```
host1#show ip multicast protocols
Multicast protocols:

Protocol Pim
    Type: Sparse
    Interfaces: 1 registered, 1 owned
    Registered interfaces:
        ATM2/1.103 (103.0.0.2/24) owner Pim

Protocol Igmp
    Type: Local
    Interfaces: 1000 registered, 1000 owned
```

```
    Registered interfaces:
        ATM2/0.131 (13.0.0.1/24) local Igmp owner Igmp
            Admission-bandwidth 2000000/10000000 bps
            QoS Adjust 2000000 bps
        Active <S,G> count   15
        Blocked <S,G> count  10

        ATM2/0.132 (13.0.0.2/24) local Igmp owner Igmp
            Admission-bandwidth 0/10000000 bps
            QoS Adjust 0 bps
        Active <S,G> count   25
        Blocked <S,G> count  10

        ATM2/0.133 (13.0.0.3/24) local Igmp owner Igmp
            Admission-bandwidth 8000000/10000000 bps
            QoS Adjust 0 bps
...
Count: 2  protocols
```

show ip multicast protocols brief

- Use to display a summary of information about multicast protocols enabled on the router.
- Field descriptions
  - Protocol—Name of the multicast protocol
  - Registered Interfaces—Number of interfaces on which the protocol is configured
  - Owned Interfaces—Number of interfaces that a protocol owns. If you configure only IGMP on an interface, IGMP owns the interface. However, if you configure IGMP and either PIM or DVMRP on the same interface, PIM or DVMRP owns the interface.
  - Type—Mode of the multicast protocol
    - For DVMRP—Dense
    - For PIM—Sparse, dense, or sparse-dense
    - For IGMP—Local
  - Count—Number of multicast protocols on the VR
- Example

```
host1#show ip multicast protocols brief

Protocol  Registered  Owned       Type
          Interfaces  Interfaces
--------- ----------  ----------  -------------------
Pim       2           2           Sparse Dense
Igmp      1           0           Local

Count: 2 protocols
```

show ip multicast routing

- Use to display information about the status of IP multicast on the VR.
- Example

```
host1#show ip multicast routing
Multicast forwarding is enabled on this router
Multicast graceful restart is complete (timer 0 seconds) on this router
Multicast cache-miss processing is enabled on this router
```

show mroute port count

- Use to display the mroute port outgoing interface, limits, counts, bandwidth settings, and bandwidth accepted.

NOTE: This command displays information for mroutes on a port across all virtual routers.

- Field descriptions
  - Port—Slot/port value on the router
  - Limit—Port limit value defined for the specified port; -l indicates that no mrout port limits have been configured for the port
  - Count—Number of mroute outgoing interfaces on the specified port
  - BW bps—Bandwidth limit, in bits per second
  - Priority BW bps—Priority bandwidth limit, in bits per second
  - Admitted—Bandwidth admitted on the port, in bits per second
- Example

```
host1#show mroute port count

BW     Priority
Port    Limit   Count    bps     BW bps    Hysteresis   Admitted
-----   -----   -----   -----   --------   ----------   --------
1/1/0   None    1       None    None       85           0
1/1/1   None    2       15000   10000      85           2000
```

Support for Multicast Router Information

When you enable multicast routing on a virtual router, the router acts as a multicast router information (mrinfo) server. This feature enables the router to respond to mrinfo requests from other network hosts. Specifically, E-series virtual routers respond to DVMRP ask neighbors and DVMRP ask neighbors2 requests.

Each virtual router responds to mrinfo requests with a list of multicast interfaces and their IP addresses. If appropriate, the virtual router also supplies the following information for each interface:

- Current functional status of the interface (for example, if the interface is down).
- Information as to whether the interface is disabled and the reason for the interface being disabled—either because IP is not configured on the interface or because the interface has been disabled through the software.
- Whether the interface is performing the IGMP queries for this subnet.
- Information about PIM neighbors:

  If PIM is configured on the interface, the virtual router supplies a list of the interface's PIM neighbors and indicates which neighbors are leaf neighbors.
- Information about DVMRP and GRE tunnels:

  If the interface is an endpoint of a tunnel, the virtual router specifies the IP address of the endpoint of the tunnel.

BGP Multicasting

BGP multicasting (MBGP) is an extension of the BGP unicast routing protocol. Many of the functions available for BGP unicasting are also available for MBGP.

The MBGP extensions specify that BGP can exchange information within different types of *address families*. The address families available are unicast IPv4, multicast IPv4, and VPN-IPv4. When you enable BGP, the router employs unicast IPv4 addresses by default.

We recommend you be thoroughly familiar with BGP before configuring MBGP. See *JUNOSe BGP and MPLS Configuration Guide, Chapter 1, Configuring BGP Routing,* for detailed information about BGP and MBGP.

Investigating Multicast Routes

You can use the **mtrace** command to trace the path that multicast packets take from a source to a destination through a multicast group address. This command is similar to the **traceroute** command for investigating unicast routes.

mtrace

- Use to trace the path that multicast packets take to a destination.
- Specify the unicast IP address of the source for the packets.
- To direct the packets to a particular destination, specify the unicast address for that destination. If you do not specify a destination, the router traces the route from the device on which you issue the command.
- To direct the packets through a particular multicast group address, specify that multicast group address. If you do not specify a multicast group address, the router traces the route through the MBone audio multicast group.
- To send the trace to a particular device, specify the IP address of that device. If you do not specify a response address, the router sends the trace to an IP address on the router.
- To investigate a problem at a particular point in the route, specify the maximum number of hops for the trace. The default number of hops is 64.
- The trace starts at the destination and works back to the source.
- Field descriptions
  - Tracing multicast route from *a.a.a.a* to *b.b.b.b* for group *c.c.c.c* using response address *d.d.d.d*—A description of the trace is as follows:
    - *a.a.a.a*—IP address of the source
    - *b.b.b.b*—IP address of the destination
    - *c.c.c.c*—IP address of the multicast group
    - *d.d.d.d*—IP address of the router to which the router sends the trace
  - Received mtrace response packet of length *n*—Length of the response packet, in bytes
  - Each line of the trace has the following format: *hops. ip-address Protocol: protocol FwdingCode:forwarding code*
    - *hops*—Number of hops from the destination to this intermediate router
    - *ip-address*—IP address of the intermediate router
    - *protocol*—Multicast protocol running on the intermediate router. A value of 12 indicates IGMP; other values comply with *A “traceroute” Facility for IP Multicast – draft-ietf-idmr-traceroute-ipm-07.txt*.
    - *FwdingCode*—Forwarding information or error associated with this hop. For example, RPF iif indicates that the request arrived on the expected RPF interface for this source group. For more information about the forwarding information or error codes, see *A “traceroute” Facility for IP Multicast – draft-ietf-idmr-traceroute-ipm-07.txt*.

- Example

```
host1#mtrace 100.4.4.4 40.1.1.1 232.1.1.1
Tracing multicast route from 100.4.4.4 to 40.1.1.1 for group 232.1.1.1 using
response address 10.6.129.56
(Press ^c to stop.)
 Received mtrace response packet of length 88
   1. 40.1.1.1 Protocol: PIM(3) FwdingCode: RPF iif(9)
   2. 21.2.2.2 Protocol: PIM(3) FwdingCode: Reached RP(8)
```

- There is no **no** version.