Chapter 3
IP Multicast Overview

The JUNOS Internet software implements the following protocols to support IP multicast routing:

- Internet Group Management Protocol (IGMP), Versions 1 and 2—Used to learn whether group members are present, for IPv4 routers.
- Multicast Listener Discovery (MLD), versions 1 and 2—Used to learn whether group members are present, for IPv6 routers.
- Distance Vector Multicast Routing Protocol (DVMRP)—Dense-mode multicast routing protocol.
- Protocol-Independent Multicast (PIM)—Multicast routing protocol that routes to multicast groups that might span wide-area and interdomain internetworks. Both dense mode and sparse mode are supported.
- Multicast Source Discovery Protocol (MSDP)—Multicast routing protocol that discovers active sources of multicast messages. PIM sparse mode uses these sources.
- Session Announcement Protocol (SAP) and Session Description Protocol (SDP)—Handle conference session announcements.

This chapter discusses the following topics:

IP Multicast Standards

The protocols related to IP multicast are defined in the following documents:

- RFC 1112, *Host Extensions for IP Multicasting* (defines IGMP Version 1)
- RFC 2236, *Internet Group Management Protocol, Version 2*
- RFC 2327, *SDP: Session Description Protocol*
- RFC 2362, *Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification*

RFC 2365, *Administratively Scoped IP Multicast*

RFC 2547, *BGP/MPLS VPNs*

RFC 2710, *Multicast Listener Discovery (MLD) for IPv6*

RFC 2858, *Multiprotocol Extensions for BGP-4*

RFC 3376, *Internet Group Management Protocol, Version 3* (SSM include mode only)

Anycast Rendezvous Point (RP) Mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP), Internet draft draft-ietf-mboned-anycast-rp-08.txt

Bootstrap Router (BSR) Mechanism for PIM Sparse Mode, Internet draft draft-ietf-pim-sm-bsr-03.txt

Distance Vector Multicast Routing Protocol, Internet draft draft-ietf-idmr-dvmrp-v3-10.txt

Multicast in MPLS/BGP VPNs, Internet draft draft-rosen-vpn-mcast-05.txt

Multicast Source Discovery Protocol (MSDP), Internet draft draft-ietf-msdp-spec-13.txt

Protocol Independent Multicast—Sparse Mode (PIM-SM): Protocol Specification (Revised), Internet draft draft-ietf-pim-sm-v2-new-06.txt

Protocol Independent Multicast Version 2 Dense Mode Specification, Internet draft draft-ietf-pim-dm-new-v2-03.txt

SAP: Session Announcement Protocol, Internet draft draft-ietf-mmusic-sap-00.txt

Source Address Selection for Multicast Listener Discovery Protocol, Internet draft draft-ietf-magma-mld-source-05.txt (SSM include mode only)

An Overview of Source-Specific Multicast (SSM) Deployment, Internet draft draft-ietf-ssm-overview-02.txt

Source-Specific Multicast for IP, Internet draft draft-holbrook-ssm-arch-02.txt

Source-Specific Protocol Independent Multicast in 232/8, Internet draft draft-ietf-mboned-ssm232-02.txt

Using IGMPv3 and MLDv2 for Source-Specific Multicast, Internet draft draft-holbrook-idmr-igmpv3-ssm-04.txt

To access Internet RFCs and drafts, go to the IETF Web site at http://www.ietf.org.

Multicast Overview

IP Version 4 (IPv4) has three fundamental types of addresses: unicast, broadcast, and multicast. A *unicast address* is used to send a packet to a single destination. A *broadcast address* is used to send a datagram to an entire subnetwork. A *multicast address* is used to send a datagram to a set of hosts that can be on different subnetworks and that are configured as members of a multicast group.

A multicast datagram is delivered to destination group members with the same best-effort reliability as a standard unicast IP datagram. This means that multicast datagrams are not guaranteed to reach all members of a group or to arrive in the same order in which they were transmitted. The only difference between a multicast IP packet and a unicast IP packet is the presence of a group address in the IP header destination address field. Multicast addresses use the Class D address format.

Individual hosts can join or leave a multicast group at any time. There are no restrictions on the physical location or the number of members in a multicast group. A host can be a member of more than one multicast group at any time and does not have to belong to a group to send packets to members of a group.

Routers use a group membership protocol to learn about the presence of group members on directly attached subnetworks. When a host joins a multicast group, it transmits a group membership protocol message for the group or groups that it wants to receive and sets its IP process and network interface card to receive frames addressed to the multicast group.

The Internet multicast backbone (MBone) is an interconnected set of subnetworks and routers that support the delivery of IP multicast traffic. The MBone is a virtual network that is layered on top of sections of the physical Internet. The MBone is composed of islands of multicast routing capability that are connected to other islands by virtual point-to-point links called tunnels. The tunnels allow multicast traffic to pass undisturbed through the parts of the Internet that are not multicast-capable. Because the MBone and the Internet have different topologies, multicast routers execute a separate routing protocol to decide how to forward multicast packets.

Multicast Addresses

Multicast host group addresses are defined to be the IP addresses whose high-order four bits are 1110, giving an address range from 224.0.0.0 through 239.255.255.255, or simply 224.0.0.0/4. (These addresses also are referred to as Class D addresses.)

The Internet Assigned Numbers Authority (IANA) maintains a list of registered IP multicast groups. The base address 224.0.0.0 is reserved and cannot be assigned to any group. The block of multicast addresses from 224.0.0.1 through 224.0.0.255 is reserved for local wire use. Groups in this range are assigned for various uses, including routing protocols and local discovery mechanisms.

The range 239.0.0.0 through 239.255.255.255 is reserved for administratively scoped addresses. Because packets addressed to administratively scoped multicast addresses do not cross configured administrative boundaries, and because administratively scoped multicast addresses are locally assigned, these addresses do not need to be unique across administrative boundaries.