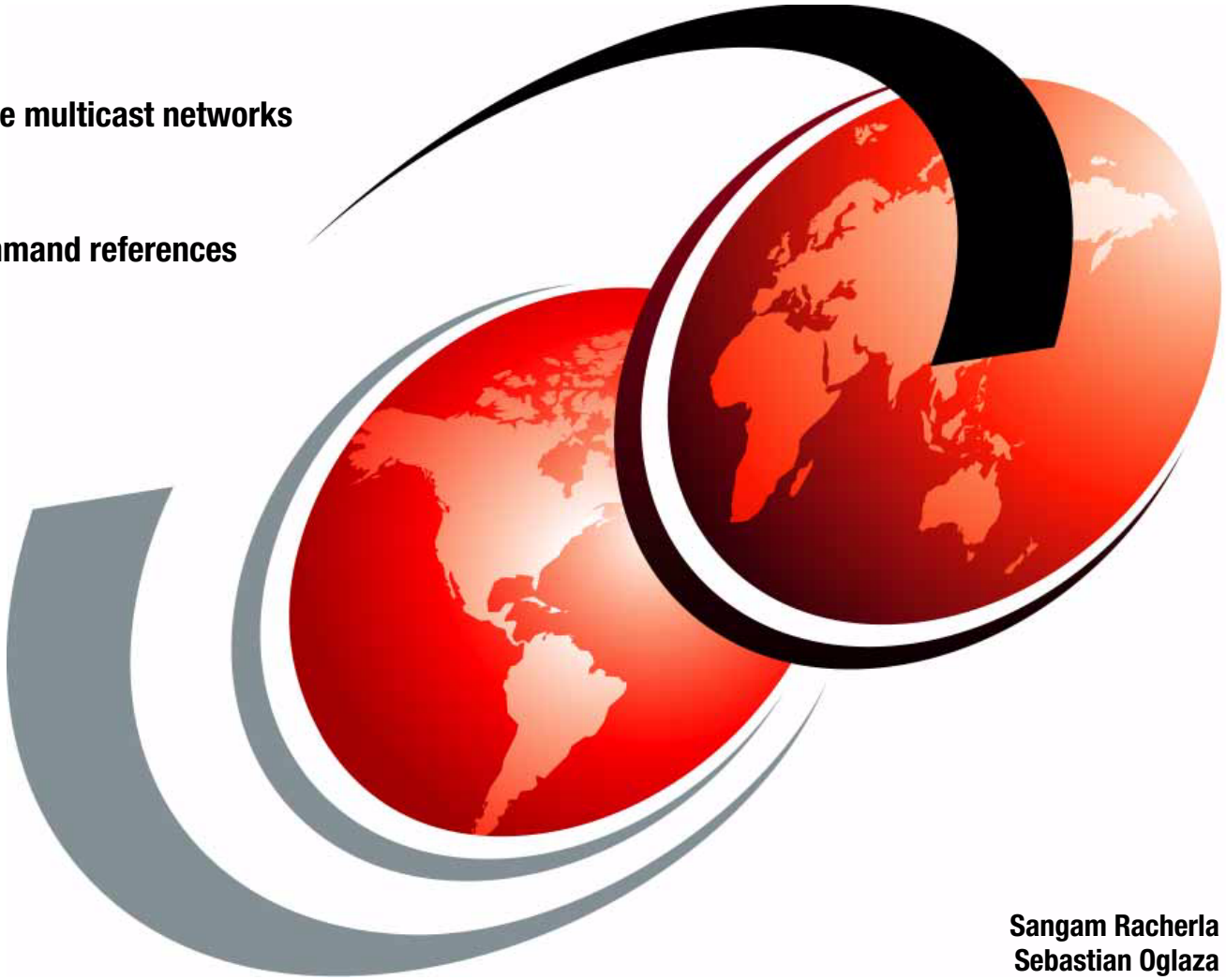
IBM

IP Multicast Protocol Configuration

- Learn the basics of IP Multicast
- See sample multicast networks
- Learn command references



Sangam Racherla
Sebastian Oglaza

Redpaper

ibm.com/redbooks

International Technical Support Organization

IP Multicast Protocol Configuration

April 2012

REDP-4777-00

Note: Before using this information and the product it supports, read the information in “Notices” on page v.

First Edition (April 2012)

This edition applies to IP Multicast configuration on the IBM System Networking 10 Gb Ethernet switches.

Contents

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. These and other IBM trademarked terms are marked on their first occurrence in this information with the appropriate symbol (® or ™), indicating US registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at http://www.ibm.com/legal/copytrade.shtml

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

AIX®	Redbooks®	System p®
Global Technology Services®	Redpapers™	System x®
IBM®	Redbooks (logo)  ®	

The following terms are trademarks of other companies:

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Other company, product, or service names may be trademarks or service marks of others.

Preface

The most common transmission scheme used in networks today is unicast, which represents “one-to-one” transmission with one sender and one receiver.

Sometimes there is a need for one host to send packets that are received by multiple hosts. The problem with implementing this kind of transmission using unicast is that the stream of packets must be replicated as many times as there are receivers. IP Multicast addresses the problem by intelligently sending only one stream of packets and then replicating the stream when it reaches the target domain that includes multiple receivers or reaches a necessary bifurcation point leading to different receiver domains.

In this IBM® Redpapers™ publication, we introduce principles of IP Multicast and describe the IPv4 addressing used for multicast. We discuss the protocols that are used to implement multicast in an IP network and then provide the general IP Multicast configuration procedures and then presents IP Multicast configuration in a sample network using IBM System Networking Ethernet Switches. We conclude this paper with command references that include all commands and their parameters for configuration of multicast protocols and features.

After understanding the basics of how to configure IP Multicast for the networking scenario described in this paper, IT network professionals will be able replicate a similar design and configuration to suit their network infrastructure.

The team who wrote this paper

This paper was produced by a team of specialists from around the world working at the International Technical Support Organization, San Jose Center.

Sangam Racherla is an IT Specialist and Project Leader working at the ITSO in San Jose, CA. He has 12 years of experience in the IT field and has been with the ITSO for the past eight years. Sangam has extensive experience in installing and supporting the ITSO lab equipment for various IBM Redbooks® projects. He has expertise in working with Microsoft Windows, Linux, IBM AIX®, IBM System x®, IBM System p® servers, and various SAN and storage products. Sangam holds a degree in electronics and communication engineering.

Sebastian Oglaza joined IBM Global Technology Services® in 2006. Since then, he has been working as a Network Specialist in the Integrated Communications Services group. During this time, he participated in numerous projects in both design and implementation roles. He is an expert in data and voice networking and holds CCIE certification in Routing and Switching.

Thanks to the following people for their contributions to this project:

Ann Lund, Jon Tate, David Watts
International Technical Support Organization, San Jose Center

Tim Shaughnessy, Jeffery M. Jaurigui, Pushkar B. Patil, Kam-Yee (Johnny) Chung, Nghiem V. Chu, Tuan A. Nguyen, Lan T. Nguyen, Harry W. Lafnear, William V. (Bill) Rogers, David Iles, Hector Sanchez, Rakesh Saha, David Faircloth, Michael Easterly, Selvaraj Venkatesan
IBM System Networking Team, San Jose

Now you can become a published author, too!

Here's an opportunity to spotlight your skills, grow your career, and become a published author—all at the same time! Join an ITSO residency project and help write a book in your area of expertise, while honing your experience using leading-edge technologies. Your efforts will help to increase product acceptance and customer satisfaction, as you expand your network of technical contacts and relationships. Residencies run from two to six weeks in length, and you can participate either in person or as a remote resident working from your home base.

Find out more about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

We want our papers to be as helpful as possible. Send us your comments about this paper or other IBM Redbooks publications in one of the following ways:

- Use the online **Contact us** review Redbooks form found at:

  ibm.com/redbooks
- Send your comments in an email to:

  redbooks@us.ibm.com
- Mail your comments to:

  IBM Corporation, International Technical Support Organization
  Dept. HYTD Mail Station P099
  2455 South Road
  Poughkeepsie, NY 12601-5400

Stay connected to IBM Redbooks

- Find us on Facebook:

  http://www.facebook.com/IBMRedbooks
- Follow us on Twitter:

  http://twitter.com/ibmredbooks
- Look for us on LinkedIn:

  http://www.linkedin.com/groups?home=&gid=2130806
- Explore new Redbooks publications, residencies, and workshops with the IBM Redbooks weekly newsletter:

  https://www.redbooks.ibm.com/Redbooks.nsf/subscribe?OpenForm
- Stay current on recent Redbooks publications with RSS Feeds:

  http://www.redbooks.ibm.com/rss.html

1

Introduction to IP Multicast

The purpose of this paper is to present IP Multicast protocol configuration on IBM System Networking switches. For configuration guides on other IP functionality, refer to *10 Gigabit Ethernet Implementation with IBM System Networking Switches*, SG24-7960.

The most common transmission scheme used in networks today is *unicast*, which represents "one-to-one" transmission, with one sender and one receiver.

Sometimes, we need one host to send packets that are received by multiple hosts. The problem with implementing this kind of transmission using unicast is that the stream of packets must be replicated as many times as there are receivers. For example, a 10 Kbps stream of packets sent to five receivers results in 50 Kbps of used bandwidth.

IP Multicast addresses the problem by intelligently sending only one stream of packets and then replicating the stream when it reaches the target domain that includes multiple receivers or reaches a necessary bifurcation point leading to different receiver domains.

IP Multicast and UDP: IP Multicast uses UDP as a transport layer protocol because UDP is connection-less. TCP cannot be used in multicast applications because it requires a connection to be established, and connection cannot exist between more than two hosts.

1.1 IP Multicast addressing

Within the entire IP address space, class D addresses have been reserved for multicast purposes. Class D addresses begin with their binary representation with a sequence of *1110*, as shown in Figure 1-1.

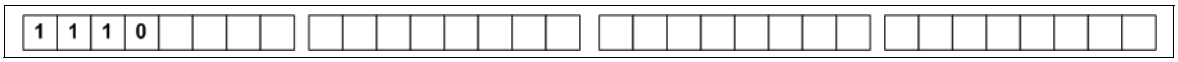


Figure 1-1 Multicast IP address binary representation

In decimal, this binary sequence translates into a 224.0.0.0 through 224.0.0.255 address range. Within the range, the number of multiblock of addresses are defined, as follows:

- Local subnetwork

  The local sub-network is made up of multicast addresses in the 224.0.0.0/24 block. Packets designated by these addresses are never forwarded by routers regardless of the Time-To-Live (TTL) field.

  A number of well-known IP addresses in that range are registered with the Internet Assigned Numbers Authority (IANA). This range includes IP addresses to which the routing protocols send their hello packets, for example, 224.0.0.5 for Open Shortest Path First (OSPF) protocol.

- The block 232.0.0.0/8 is reserved for *source-specific multicast,* described later on in this paper.

- GLOP addressing

  The 233.0.0.0/8 block is an experimental, public, statically assigned multicast address space for publishers and Internet service providers that want to source content in the Internet.

- Unicast prefix-based IPv4 multicast addresses

  The 234.0.0.0/8 range is assigned as a range of global IPv4 multicast address space provided to each organization that has /24 or larger globally-routed unicast address space allocated. A resulting advantage over GLOP is that the mechanisms in IPv4 and IPv6 become more similar.

- Administratively scoped addresses

  The 239.0.0.0/8 range is a locally administered address space with local or organizational scope. Anyone can use this address space for private multicast domains without concern for address collisions, similar to the private IP space, such as 10.0.0.0/8 for unicast networking

1.2 Reverse path forwarding

Multicast reverse path forwarding (RPF) ensures loop-free forwarding of multicast packets. In multicast routing, the decision to forward traffic is based upon source address and not on destination address, as with unicast routing. RPF ensures loop-free forwarding using either a dedicated multicast routing table or the router's native unicast routing table.

When a multicast packet enters a router's interface, it looks up the list of networks reachable through that input interface, that is, it checks the reverse path of the packet. If the router finds a matching routing entry for the source IP of the multicast packet, the RPF check passes and the packet is forwarded to all other interfaces that are participating in multicast for this multicast group. If the RPF check fails, the packet is dropped. As a result, the forwarding of the packet is decided based upon the reverse path of the packet rather than the forward path. RPF routers only forward packets that come into the interface holding the routing entry for the source of the packet, thus breaking any loop.

This functionality is critically important in redundant multicast topologies. Because the same multicast packet can reach the same router through multiple interfaces, RPF checking is integral in the decision to forward packets or not. If the router forwards all packets that move from interface A to interface B, forwards all packets coming in interface B to interface A, and both interfaces receive the same packet, a classic routing loop is created. In this loop, packets are forwarded in both directions until their IP times to live (TTL) expire. Even considering TTL expiration, all types of routing loops are best avoided as they involve at least temporary network degradation.

1.3 Multicast protocols

There are two protocols used in every multicast network:

- Internet Group Management Protocol (IGMP)

  IGMP is used for *host-to-router* signalling. Its purpose is to signal a router that hosts on the router's segment are interested in receiving multicast traffic destined for a particular multicast group or multicast address.

- Protocol Independent Multicast (PIM)

  PIM is used for *router-to-router* signalling. The main purpose of PIM is to provide loop-free multicast delivery using RPF.

1.3.1 Internet Group Management Protocol

Internet Group Management Protocol (IGMP) is used by IPv4 multicast routers to discover the existence of host group members on their directly attached subnet (see RFC 2236). The IPv4 multicast routers get this information by broadcasting IGMP membership queries and listening for IPv4 hosts reporting their host group memberships. This process is used to set up a client/server relationship between an IPv4 multicast router, which provides the data streams on behalf of the multicast sender and the clients that want to receive the data.

IBM switches connect to static multicast routers (Mrouters) and perform IGMP snooping. IBM switches can act as a querier and participate in the IGMP querier election process.

IBM switches support IGMP version 1, 2, and 3.

Internet Group Management Protocol snooping

IGMP makes it possible for the switch to forward multicast traffic only to those ports that request it. IGMP snooping prevents multicast traffic from being flooded to all ports. The switch detects which server hosts are interested in receiving multicast traffic and forwards this information only to ports connected to those servers. In this way, other ports are not burdened with unwanted multicast traffic.

The switch can sense IGMP Membership Reports from attached clients and acts as a proxy to set up a dedicated path between the requesting host and a local IPv4 multicast router. After the pathway is established, the switch blocks the IPv4 multicast stream from flowing through any port that does not connect to a host member, conserving bandwidth.

The client-server path is set up as follows:

1. An IPv4 multicast router (Mrouter) sends membership queries and switch forwards them to all ports in a given VLAN.
2. Hosts that want to receive the multicast data stream send membership reports and switch sends a proxy membership report to the Mrouter.
3. The switch sets up a path between the Mrouter and the host and blocks all other ports from receiving the multicast.
4. Periodically, the Mrouter sends membership queries to ensure that the host wants to continue receiving the multicast. If a host fails to respond with a membership report, the Mrouter stops sending the multicast to that path.
5. The host can send a leave report to the switch, which in turn sends a proxy leave report to the Mrouter. The multicast path is terminated immediately.

IGMP entries

IGMP entries are allocated for each unique join request, based on the virtual local area network (VLAN) and IGMP group address. If hosts on multiple ports join the same IGMP group using the same VLAN, only a single IGMP entry is used.

FastLeave

In normal IGMP operation, when the switch receives an IGMPv2 leave message, it sends a group-specific query to determine if any other devices in the same group (and on the same port) are still interested in the specified multicast group traffic. The switch removes the affiliated port from that particular group if the following conditions apply:

- The switch does not receive an IGMP membership report within the query-response-interval.
- The switch detects no multicast routers on that port.

With FastLeave enabled on the VLAN, a port can be removed immediately from the port list of the group entry when the IGMP leave message is received unless a multicast router was detected on the port.

IGMP v3 snooping

IGMPv3 includes new membership report messages to extend IGMP functionality. The switch provides snooping capability for all types of IGMP version 3 (IGMPv3) membership reports. IGMPv3 supports source-specific multicasts (SSMs). SSM identifies session traffic using both source and group addresses.

The IGMPv3 implementation keeps records on the multicast hosts present in the network. If a host is already registered, when it receives a new report from same host, the switch makes the correct transition to new (port-host-group) registration based on the IGMPv3 RFC. The registrations of other hosts for the same group on the same port are not changed.

Static multicast router

A static multicast router (Mrouter) can be configured for a particular port on a particular VLAN. A static Mrouter does not have to be detected though IGMP snooping. Any data port can accept a static Mrouter. When you configure a static Mrouter on a VLAN, it replaces any dynamic Mrouters detetected through IGMP snooping.

IGMP querier

The IGMP querier enables the switch to perform the multicast router (Mrouter) role and provide Mrouter discovery on the broadcast network or VLAN.

When IGMP querier is enabled on a VLAN, the switch acts as an IGMP querier in a Layer 2 network environment. The IGMP querier periodically broadcasts IGMP queries and listens for hosts to respond with IGMP reports indicating their IGMP group memberships. If multiple Mrouters exist on a given network, the Mrouters elect one as the querier, which performs all periodic membership queries. The election process can be based on IPv4 address or Media Access Control (MAC) address.

IGMP Relay

The IBM switch can act as an IGMP Relay (or IGMP proxy) device that relays IGMP multicast messages and traffic between an Mrouter and end stations. An IGMP Relay makes it possible for a switch to participate in network multicasts with no configuration of the various multicast routing protocols, so you can deploy it in the network with minimal effort.

To an IGMP host connected to IBM switch, the IGMP Relay appears to be an IGMP Mrouter. The IGMP Relay sends membership queries to hosts, which respond by sending an IGMP response message. A host can also send an unsolicited join message to the IGMP Relay.

To a multicast router, the IGMP Relay appears as a host. The Mrouter sends IGMP host queries to the IGMP Relay, and the IGMP Relay responds by forwarding IGMP host reports and unsolicited join messages from its attached hosts. The IGMP Relay also forwards multicast traffic between the Mrouter and end stations.

You can configure up to two Mrouters to use with an IGMP Relay. One Mrouter acts as the primary Mrouter, and one is the backup Mrouter. The switch uses health checks to select the primary Mrouter.

IGMP filtering

With IGMP filtering, you can allow or deny a port to send and receive multicast traffic to certain multicast groups. Unauthorized users are restricted from streaming multicast traffic across the network.

If access to a multicast group is denied, IGMP membership reports from the port are dropped, and the port no longer receives IPv4 multicast traffic from that group. If access to the multicast group is allowed, membership reports from the port are forwarded for normal processing.

To configure IGMP filtering, you must globally enable IGMP filtering, define an IGMP filter, assign the filter to a port, and enable IGMP filtering on the port. To define an IGMP filter, you must configure a range of IPv4 multicast groups, choose whether the filter will allow or deny multicast traffic for groups within the range, and enable the filter.

1.3.2 Protocol-Independent Multicast

Protocol-Independent Multicast (PIM) is designed for routing of multicast traffic across one or more IPv4 domains. This design benefits applications such as IP television, collaboration, education, and software delivery, where a single source must deliver content (a multicast) to a group of receivers that span both wide-area and inter-domain networks.

Instead of sending a separate copy of content to each receiver, a multicast efficiently sends only a single copy of content toward its intended receivers. This single copy is duplicated only when it reaches the target domain that includes multiple receivers, or when it reaches a necessary bifurcation point leading to different receiver domains.

PIM is used by multicast source stations, client receivers, and intermediary routers and switches, to build and maintain efficient multicast routing trees. PIM is protocol independent; It collects routing information using the existing unicast routing functions underlying the IPv4 network but does not rely on any particular unicast protocol. For PIM to function, a Layer 3 routing protocol , such as Border Gateway Protocol (BGP), Open Shortest Path First (OSPF), Router Information Protocol (RIP), or static routes, must first be configured on the switch.

PIM-SM (PIM sparse mode, described in “PIM sparse mode” on page 7) is a reverse-path routing mechanism. Client receiver stations advertise their willingness to join a multicast group. The local routing and switching devices collect multicast routing information and forward the request toward the station that will provide the multicast content. When the join requests reach the sending station, the multicast data is sent to the receivers, flowing in the opposite direction of the original join requests.

Some routing and switching devices perform special PIM-SM functions. Within each receiver segment, one router is elected as the designated router (DR) for handling multicasts for the segment. DRs forward information to a device *rendezvous point (RP)*, which holds the root tree for the particular multicast group.

Receiver join requests and sender multicast content initially converge at the RP, which generates and distributes multicast routing data for the DRs along the delivery path. As the multicast content flows, DRs use the routing tree information obtained from the RP to optimize the paths both to and from send and receive stations, bypassing the RP for the remainder of content transactions if a more efficient route is available.

DRs continue to share routing information with the RP, modifying the multicast routing tree when new receivers join, or pruning the tree when all the receivers in any particular domain are no longer part of the multicast group.

Supported PIM modes and features

For each interface attached to a PIM network component, PIM can be configured to operate either in PIM sparse mode (PIM-SM) or PIM dense mode (PIM-DM):

- PIM-SM is used in networks where multicast senders and receivers comprise a relatively small (sparse) portion of the overall network. PIM-SM uses a more complex process than PIM-DM for collecting and optimizing multicast routes but minimizes impact on other IP services and is more commonly used.
- PIM-DM is used where multicast devices are a relatively large (dense) portion of the network, with very frequent (or constant) multicast traffic. PIM-DM requires less configuration on the switch than PIM-SM, but uses broadcasts that can consume more bandwidth in establishing and optimizing routes.

PIM dense mode

PIM dense mode, which is not very commonly used today, is intended for densly-populated networks with many receivers. PIM dense mode uses *flood-prune* behavior, which means traffic is by default flooded to each network segment. It is up to the router on the segment to send *prune* message towards the source, signalling that there are no receivers interested in the multicast traffic flooded.

PIM sparse mode

Behavior of PIM sparse mode is opposite to that of sparse mode. Its default behavior is not to flood the multicast traffic unless the downstream routers signal otherwise by sending a *PIM Join* message, which indicates that receivers on their directly connected networks are interested in receiving the multicast traffic.

In PIM sparse mode, one of the switches must be designated as the rendezvous point (RP). The rendezvous point is a supplementary role for a device that holds the root tree for the particular multicast group.

RP can be configured in two ways:

- Statically

  Each PIM router must be configured with the static address of the RP for each group address. The group mask address can be used to specify the static RP address for a number of multicast groups.

- Dynamically, with use of Bootstrap Router (BSR) protocol.

  In BSR there are two roles:

  – RP candidate, a router that advertises itself as a RP for specific group(s)

  – Bootstrap Router (BSR), a PIM-capable router that hosts the election of the RP from available RP candidate routers.

  After the RP candidate and the Bootstrap Router are configured, all multicast routers learn RP assignments for specific groups from BSR protocol messages carried by PIM.

2

IP Multicast configuration

In Chapter 1, “Introduction to IP Multicast” on page 1, we described concepts of IP Multicast. This chapter focuses on commands required to implement multicast protocols on IBM System Networking switches. For the full list of IP Multicast industry standard command-line interface (ISCLI) configuration commands, see Appendix A, “IP Multicast command reference” on page 39.

2.1 Internet Group Management Protocol configuration

As far as Internet Group Management Protocol (IGMP) is concerned, IBM switches have the following capabilities:

- IGMP snooping
- IGMP version 1, 2 and 3
- IGMP static multicast router
- IGMP Querier
- IGMP Relay
- IGMP filtering

In the following sections, we show syntax for configuration of different IGMP features.

2.1.1 Internet Group Management Protocol snooping

IGMP snooping makes it possible for you to forward multicast traffic only out of ports that are interested in receiving it. It work by keeping track of IGMP message exchange between hosts (multicast receivers) and the multicast router.

Configuring FastLeave

You can enable FastLeave only on VLANs that have only one host connected to each physical port. To enable FastLeave, run the following command:

```
RS8264(config)# ip igmp snoop <VLAN number> fast-leave
```

Configuring Internet Group Management Protocol v3 snooping

By default, the switch snoops the first eight sources listed in the IGMPv3 Group Record. Run the following command to change the number of snooping sources:

```
RS8264(config)# ip igmp snoop igmpv3 sources <1-64>
```

IGMPv3 snooping is compatible with IGMPv1 and IGMPv2 snooping. You can disable snooping on version 1 and version 2 reports using the following command:

```
RS8264(config)# no ip igmp snoop igmpv3 v1v2
```

The switch supports the following IGMPv3 Filter modes:

- INCLUDE mode

  The host requests membership to a multicast group and provides a list of IPv4 addresses from which it wants to receive traffic.

- EXCLUDE mode

  The host requests membership to a multicast group and provides a list of IPv4 addresses from which it does not want to receive traffic. This indicates that the host wants to receive traffic only from sources that are not part of the Exclude list. To disable snooping on EXCLUDE mode reports, run the following command:

  ```
  RS8264(config)# no ip igmp snoop igmpv3 exclude
  ```

Configuring Internet Group Management Protocol snooping

This section provides steps to configure IGMP snooping on the switch.

1. Configure port and VLAN membership on the switch.
2. Add VLANs to IGMP snooping by running the following command:

   ```
   RS8264(config)# ip igmp snoop vlan 1
   ```

3. Enable IGMPv3 snooping (optional) by running the following command:

   ```
   RS8264(config)# ip igmp snoop igmpv3 enable
   ```

4. Enable the IGMP feature by running the following command:

   ```
   RS8264(config)# ip igmp enable
   ```

5. View dynamic IGMP information by running the following commands:

   - **RS8264# show ip igmp groups**
   - **RS8264# show ip igmp mrouter**

Configuring the static multicast router

1. For each Mrouter, configure a port (1-64), VLAN (1-4094), and version (1-3) by running the following command:

   ```
   RS8264(config)# ip igmp mrouter 5 1 2
   ```

   The syntax for the command is:

   ip igmp mrouter port *<port alias or number>* *<VLAN number>* *<version (1-3)>*

2. Verify the configuration by running the following command:

   ```
   RS8264# show ip igmp mrouter
   ```

2.1.2 Configuring the Internet Group Management Protocol Querier

Follow this procedure to configure IGMP Querier.

1. Enable IGMP and configure the source IPv4 address for IGMP Querier on a VLAN by running the following commands:

   - **RS8264(config)# ip igmp enable**
   - **RS8264(config)# ip igmp querier vlan 2 source-ip 10.10.10.1**

2. Enable IGMP Querier on the VLAN by running the following command:

   ```
   RS8264(config)# ip igmp querier vlan 2 enable
   ```

3. Configure the Querier election type and define the address by running the following command:

   ```
   RS8264(config)# ip igmp querier vlan 2 election-type ipv4
   ```

4. Verify the configuration by running the following command:

   ```
   RS8264# show ip igmp querier vlan 2
   ```

2.1.3 Configuring the Internet Group Management Protocol Relay

Consider the following guidelines when you configure IGMP Relay:

- IGMP Relay and IGMP snooping are mutually exclusive. If you enable the IGMP Relay, you must turn off IGMP snooping.
- Add the upstream Mrouter VLAN to the IGMP Relay list, using the following command:

  `RS8264(config)# ip igmp relay vlan <VLAN number>`

Use the following procedure to configure IGMP Relay:

1. Configure IP interfaces with IPv4 addresses, and assign VLANs by running the following commands:

   ```
   – RS8264(config)# interface ip 2
   – RS8264(config-ip-if)# ip address 10.10.1.1
   – RS8264(config-ip-if)# ip netmask 255.255.255.0
   – RS8264(config-ip-if)# vlan 2
   – RS8264(config-ip-if)# enable
   – RS8264(config-ip-if)# exit
   – RS8264(config)# interface ip 3
   – RS8264(config-ip-if)# ip address 10.10.2.1
   – RS8264(config-ip-if)# ip netmask 255.255.255.0
   – RS8264(config-ip-if)# vlan 3
   – RS8264(config-ip-if)# enable
   – RS8264(config-ip-if)# exit
   ```

2. Turn IGMP on by running the following command:

   `RS8264(config)# ip igmp enable`

3. Enable the the IGMP Relay and add VLANs to the downstream network by running the following commands:

   ```
   – RS8264(config)# ip igmp relay enable
   – RS8264(config)# ip igmp relay vlan 2
   – RS8264(config)# ip igmp relay vlan 3
   ```

4. Configure the upstream Mrouters with IPv4 addresses by running the following commands:

   ```
   – RS8264(config)# ip igmp relay mrouter 1 address 100.0.1.2
   – RS8264(config)# ip igmp relay mrouter 1 enable
   – RS8264(config)# ip igmp relay mrouter 2 address 100.0.2.4
   – RS8264(config)# ip igmp relay mrouter 2 enable
   ```

2.1.4 Configuring Internet Group Management Protocol filtering

Use the following procedure to configure IGMP filtering:

1. Enable IGMP filtering on the switch by running the following command:

   `RS8264(config)# ip igmp filtering`

2. Define an IGMP filter with IPv4 information by running the following commands:

   ```
   – RS8264(config)# ip igmp profile 1 range 224.0.0.0 226.0.0.0
   – RS8264(config)# ip igmp profile 1 action deny
   – RS8264(config)# ip igmp profile 1 enable
   ```

3. Assign the IGMP filter to a port by running the following command:
   - **RS8264(config)# interface port 3**
   - **RS8264(config-if)# ip igmp profile 1**
   - **RS8264(config-if)# ip igmp filtering**

2.2 PIM configuration

PIM is a multicast protocol between multicast routers. The main purpose of PIM is to provide loop-free multicast delivery using RPF.

2.2.1 Basic PIM settings

To use PIM, the following are required:

- The PIM feature must be enabled globally on the switch.
- PIM network components and PIM modes must be defined.
- IP interfaces must be configured for each PIM component.
- PIM neighbor filters may be defined (optional).
- If PIM-SM is used, define additional parameters:
  - Rendezvous point
  - Designated router preferences (optional)
  - Bootstrap router preferences (optional)

Each of these tasks is covered in the following sections.

2.2.2 Globally enabling or disabling the PIM feature

By default, PIM is disabled on the switch. PIM can be globally enabled or disabled using the following command:

```
RS8264(config)# [no] ip pim enable
```

2.2.3 Defining a PIM network component

The IBM RackSwitch G8264 can be attached to a maximum of two independent PIM network components. Each component represents a different PIM network and can be defined for either PIM-SM or PIM-DM operation. Basic PIM component configuration is performed using the following commands:

- **RS8264(config)# ip pim component <1-2>**
- **RS8264(config-ip-pim-comp)# mode {sparse|dense}**
- **RS8264(config-ip-pim-comp)# exit**

The **sparse** option will place the component in sparse mode (PIM-SM). The **dense** option will place the component in dense mode (PIM-DM). By default, PIM component 1 is configured for sparse mode. PIM component 2 is unconfigured by default.

2.2.4 Defining an IP interface for PIM use

Each network attached to an IP interface on the switch can be assigned one of the available PIM components. The same PIM component can be assigned to multiple IP interfaces. The interfaces may belong to the same VLAN, and they may also belong to different VLANs as long as their member IP addresses do not overlap.

To define an IP interface for use with PIM, first configure the interface with an IPv4 address and VLAN by running the following commands:

- **RS8264(config)# interface ip <Interface number>**
- **RS8264(config-ip-if)# ip address <IPv4 address> <IPv4 mask>**
- **RS8264(config-ip-if)# vlan <VLAN number>**
- **RS8264(config-ip-if)# enable**

PIM support for VLAN: The PIM feature currently supports only one VLAN for each IP interface. Configurations where different interfaces on different VLANs share IP addresses are not supported.

Next, PIM must be enabled on the interface, and the PIM network component ID must be specified by running the following commands:

- **RS8264(config-ip-if)# ip pim enable**
- **RS8264(config-ip-if)# ip pim component <1-2>**
- **RS8264(config-ip-if)# exit**

By default, PIM component 1 is automatically assigned when PIM is enabled on the IP interface.

PIM prevents VLAN change: While PIM is enabled on the interface, the interface VLAN cannot be changed. To change the VLAN, first disable PIM on the interface.

2.2.5 Using PIM neighbor filters

IBM RackSwitch G8264 accepts connection to up to 72 PIM interfaces. By default, the switch accepts all PIM neighbors attached to the PIM-enabled interfaces, up to the maximum number. Once the maximum is reached, the switch will deny further PIM neighbors.

To ensure that only the appropriate PIM neighbors are accepted by the switch, the administrator can use PIM neighbor filters to specify which PIM neighbors may be accepted or denied on a per-interface basis.

To turn PIM neighbor filtering on or off for a particular IP interface, use the following commands:

- **RS8264(config)# interface ip <Interface number>**
- **RS8264(config-ip-if)# [no] ip pim neighbor-filter**

When filtering is enabled, all PIM neighbor requests on the specified IP interface will be denied by default. To allow a specific PIM neighbor, run the following command:

RS8264(config-ip-if)# **ip pim neighbor-addr *<neighbor IPv4 address>* allow**

To remove a PIM neighbor from the accepted list, run the following commands:

- **RS8264(config-ip-if)# ip pim neighbor-addr <neighbor IPv4 address> deny**
- **RS8264(config-ip-if)# exit**

You can view configured PIM neighbor filters globally or for a specific IP interface by running the following commands:

- **RS8264# show ip pim neighbor-filters**
- **RS8264# show ip pim interface <Interface number> neighbor-filters**

2.2.6 Additional sparse mode settings

For sparse mode, a number of both mandatory and optional settings must be configured, for example, IP address of rendezvous point (either static, manual, or BSR).

Specifying the rendezvous point

Using PIM-SM, at least one PIM-capable router must be a candidate for use as a Rendezvous Point (RP) for any given multicast group. If desired, the switch can act as an RP candidate. To assign a configured switch IP interface as a candidate, use the following procedure.

1. Select the PIM component that will represent the RP candidate by running the following command:

   RS8264(config)# **ip pim component *<1-2>***

2. Configure the IPv4 address of the switch interface which will be advertised as a candidate RP for the specified multicast group by running the following command:

   RS8264(config-ip-pim-comp)# **rp-candidate rp-address *<group address>*** <group address mask> <candidate IPv4 address>

The switch interface will participate in the election of the RP that occurs on the bootstrap router (BSR).

Alternately, if no election is desired, the switch can provide a static RP, which is specified by running the following command:

RS8264(config-ip-pim-comp)# **rp-static rp-address <group address> <group address mask> <candidate IPv4 address>**

3. If using dynamic RP candidates, configure the amount of time that the elected interface will remain the RP for the group before a re-election is performed by running the following commands:
   - **RS8264(config-ip-pim-comp)# rp-candidate holdtime <1-255>**
   - **RS8264(config-ip-pim-comp)# exit**

Influencing the designated router selection

Using PIM-SM, All PIM-enabled IP interfaces are considered as potential designate routers (DR) for their domain. By default, the interface with the highest IP address on the domain is selected.

However, if an interface is configured with a DR priority value, it overrides the IP address selection process. If more than one interface on a domain is configured with a DR priority, the one with the highest number is selected.

Run the following commands to configure the DR priority value (interface IP mode):

- **RS8264(config)# interface ip <Interface number>**
- **RS8264(config-ip-if)# ip pim dr-priority <value (0-4294967294)>**
- **RS8264(config-ip-if)# exit**

DR zero value: A value of 0 (zero) specifies that the G8264 will not act as the DR. This setting requires the switch to be connected to a peer that has a DR priority setting of 1 or higher in order to ensure that a DR will be present in the network.

Specifying a bootstrap router

Using PIM-SM, a bootstrap router (BSR) is a PIM-capable router that hosts the election of the RP from available candidate routers. For each PIM-enabled IP interface, the administrator can set the preference level for which the local interface becomes the BSR by running the following commands:

- **RS8264(config)# interface ip <Interface number>**
- **RS8264(config-ip-if)# ip pim cbsr-preference <-1 to 255>**
- **RS8264(config-ip-if)# exit**

A value of 255 highly prefers the local interface as a BSR. A value of -1 indicates that the local interface should not act as a BSR.

2.2.7 Using PIM with other features

PIM works with conjuction with other protocols (Unicast Routing Protocol for RPF checks and IGMP for determining where the receivers are located) and features For example, you can use ACLs or VLAN Maps (VMAPs) to filter PIM neighbors or multicast groups or RP addresses.)

PIM with ACLs or VMAPs

If using ACLs or VMAPs, be sure to permit traffic for local hosts and routers.

PIM with IGMP

If using IGMP:

- IGMP static Joins can be configured with a PIM-SM or PIM-DM multicast group IPv4 address by running the following command

  RS8264(config)# **ip mroute *<multicast group IPv4 address> <VLAN> <port>***

- IGMP Query is disabled by default. If IGMP Querier is needed with PIM, be sure to enable the IGMP Query feature globally, and on each VLAN where it is needed.

If the switch is connected to multicast receivers and/or hosts, be sure to enable IGMP snooping globally, as well as on each VLAN where PIM receivers are attached.

3

IP Multicast configuration example

In Chapter 2, “IP Multicast configuration” on page 9, we described commands required to implement multicast protocols on IBM System Networking switches. In this chapter, we use those commands to implement sample multicast network.

3.1 Sample IP Multicast network

In this section, we present a sample network that we can use for IP Multicast implementation. The architecture resembles one you might find in typical Data Center network based on IBM System Networking switches. You can easily incorporate the configuration presented here in your network for implementation of multicast protocols.

For the IP Multicast configuration example, we use the network topology shown in Figure 3-1.

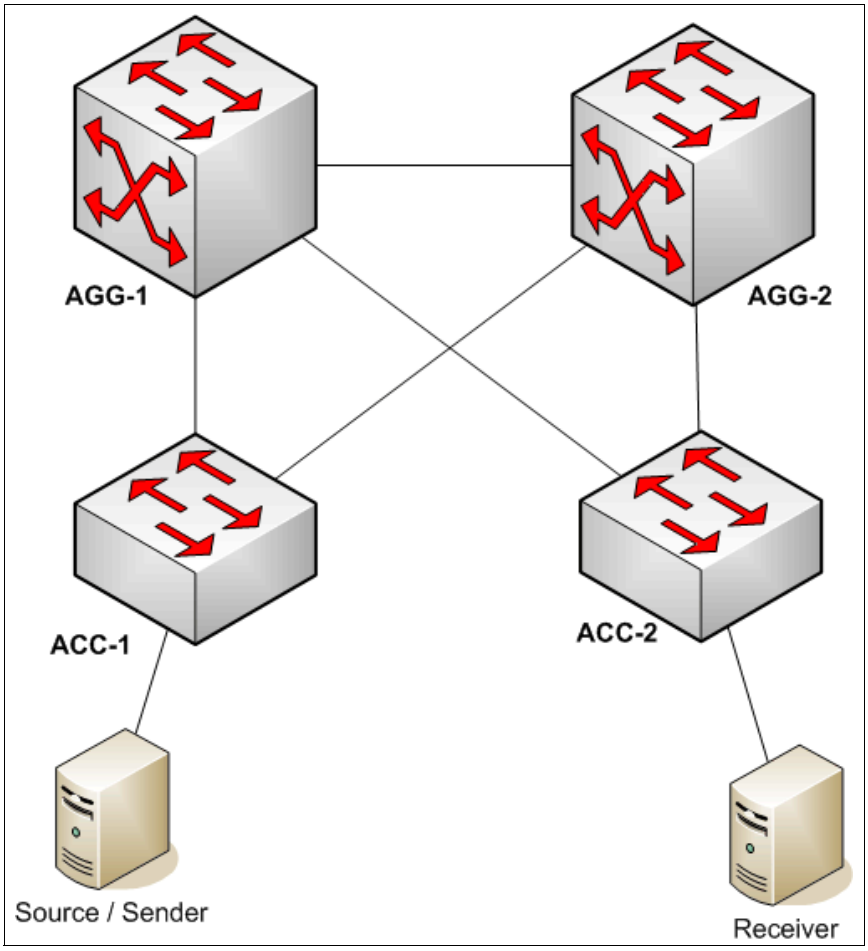


Figure 3-1 Multicast network example

3.1.1 Layer 1 architecture

Layer 1 of the sample multicast network is shown in Figure 3-2.

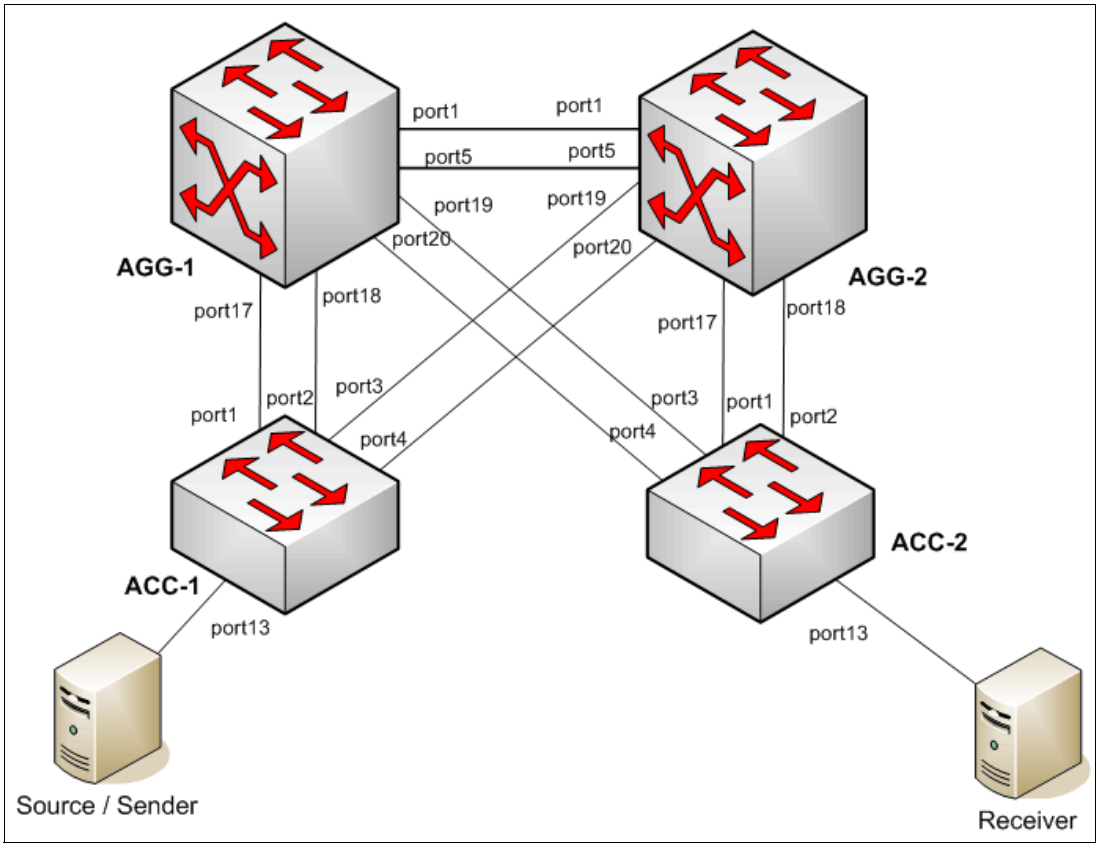


Figure 3-2 Layer 1 architecture of the example multicast network

3.1.2 Layer 2 architecture

A number of VLANs are used in the topology. Table 3-1 shows the VLANs and member ports.

Table 3-1 VLANs in example topology

VLAN	Member ports
50	ACC-1, port13 (untagged)
60	ACC-2, port13 (untagged)
100	AGG-1, port1 (untagged) AGG-1, port5 (untagged) AGG-2, port1 (untagged) AGG-2, port5 (untagged)
101	ACC-1, port1 (untagged) ACC-1, port2 (untagged) AGG-1, port17 (untagged) AGG-1, port18 (untagged)

VLAN	Member ports
102	ACC-1, port3 (untagged) ACC-1, port4 (untagged) AGG-2, port19 (untagged) AGG-2, port20 (untagged)
103	ACC-2, port3 (untagged) ACC-2, port4 (untagged) AGG-1, port19 (untagged) AGG-1, port20 (untagged)
104	ACC-2, port1 (untagged) ACC-2, port2 (untagged) AGG-2, port17 (untagged) AGG-2, port18 (untagged)

The physical links are aggregated into trunks, as shown in Table 3-2.

Table 3-2 Trunks in example topology

Switch	Trunk	Trunk members	Static or LACP
ACC-1	portchannel1	port1, port2	static
ACC-1	portchannel2	port3, port4	static
ACC-2	portchannel1	port1, port2	static
ACC-2	portchannel2	port3, port4	static
AGG-1	portchannel1	port17, port18	static
AGG-1	portchannel2	port19, port20	static
AGG-1	portchannel3	port1, port5	static
AGG-2	portchannel1	port17, port18	static
AGG-2	portchannel2	port19, port20	static
AGG-2	portchannel3	port1, port5	static

3.1.3 Layer 3 architecture

Table 3-3 shows the VLANs used in the topology and their addresses.

Table 3-3 VLANs in example topology

VLAN	Subnet	Description
VLAN 50	10.0.50.0/24	VLAN50, Sender VLAN
VLAN 60	10.0.60.0/24	VLAN60, Receiver VLAN

VLAN	Subnet	Description
VLAN101	10.0.101.0/30	Point-to-point link subnet between ACC-1 and AGG-1
VLAN102	10.0.102.0/30	Point-to-point link subnet between ACC-1 and AGG-2
VLAN103	10.0.103.0/30	Point-to-point link subnet between ACC-2 and AGG-1
VLAN104	10.0.104.0/30	Point-to-point link subnet between ACC-2 and AGG-2
VLAN100	10.0.100.0/30	Point-to-point link subnet between AGG-1 and AGG-2

The layer 3 architecture of the example multicast network is shown in Figure 3-3.

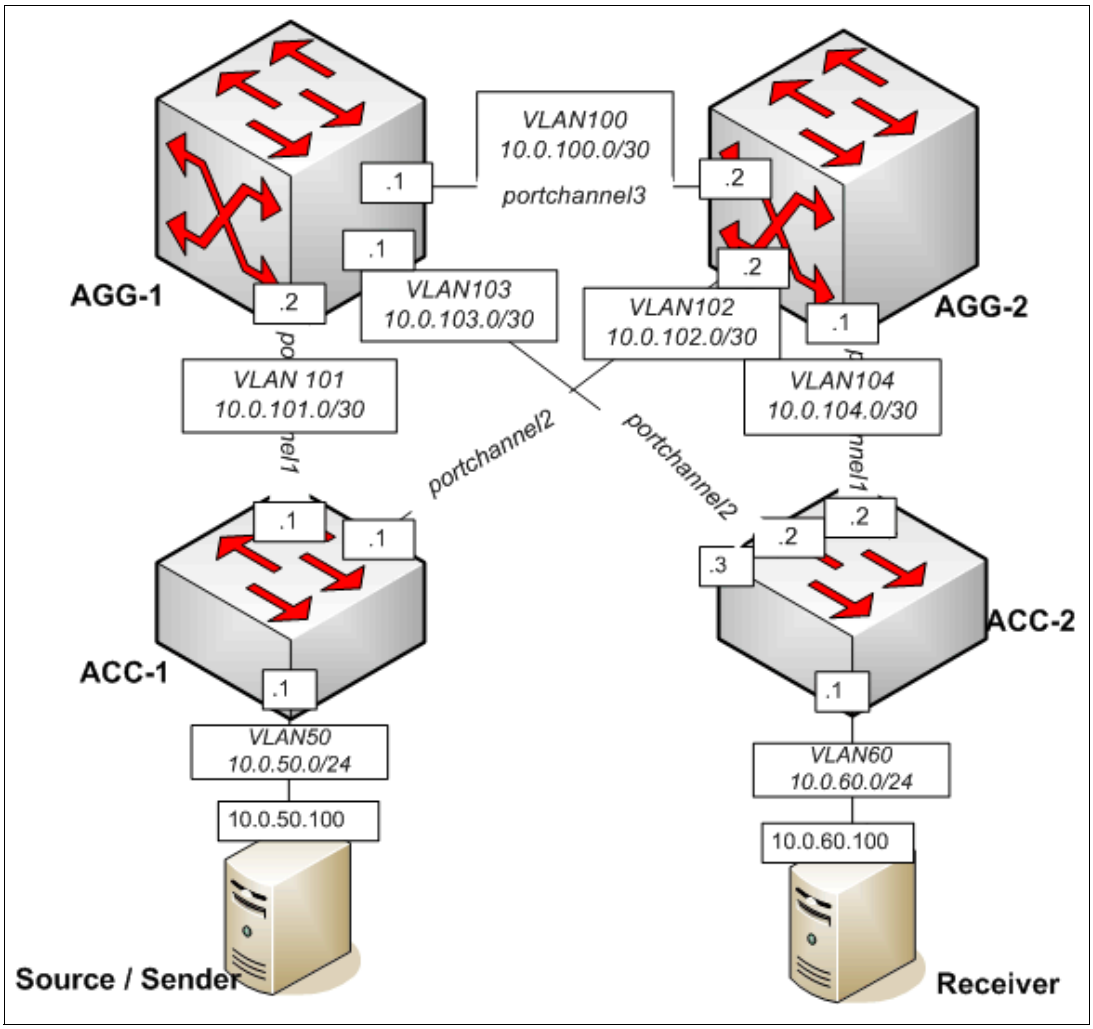


Figure 3-3 Layer 3 architecture of multicast network

3.2 Implementing Internet Group Management Protocol

In our example, the host with the IP address of 10.0.60.100, located in virtual local area network (VLAN) 60, is a receiver of multicast groups 239.0.0.20 and 239.0.0.30. The host signals its interest in receiving traffic directed for that group by sending Internet Group Management Protocol (IGMP) messages.

3.2.1 Enabling Internet Group Management Protocol

This section describes how to enable IGMP in our example.

Implementation

For ACC-2, which is the first-hop router for the receiver, run the following command to enable IGMP:

```
ACC-2(config)#ip igmp enable
```

Verification

To verify the IGMP has been turned on, use the command shown in Example 3-1.

Example 3-1 Verifying IGMP status

```
ACC-2#show ip igmp
Current IGMP settings: ON

Current IGMP snooping settings:
snoop dis, timeout 10, aggr ena,
  mrto timeout 255
  qintrval 125
  robust 2
  srcip 255.255.255.255
  Send IGMP Messages with Router Alert option: dis
  Snooping enabled VLANs:  empty
  Fastleave processing enabled VLANs:  empty


IGMP filtering disabled
Current IGMPv3 Snooping settings:
  sources 8, igmpv3 disabled, v1v2 enabled, exclude enabled
Current IGMP Querier settings:
IGMP querier: dis
```

From the output, you can see that IGMP has been enabled.

3.2.2 Enabling Internet Group Management Protocol snooping

This section describes how to enable IGMP snooping in our example.

Implementation

We want to make sure that multicast traffic will not be forwarded from the ports of the ACC-2 switch, which are not interested in receiving the traffic. To accomplish this task, complete the following steps:

1. Enable IGMP snooping for VLAN60 by running the following command:

   ```
   ACC-2(config)#ip igmp snoop vlan 60
   ```

2. Enable IGMP snooping globally by running the following command:

   ```
   ACC-2(config)#ip igmp snoop enable
   ```

Verification

To verify the IGMP snoop setting, run the command shown in Example 3-2.

Example 3-2 Verifying IGMP snoop status

```
ACC-2#show ip igmp snoop
Current IGMP snooping settings:
snoop ena, timeout 10, aggr ena,
  mrto timeout 255
  qintrval 125
  robust 2
  srcip 255.255.255.255
  Send IGMP Messages with Router Alert option: dis
```

```
  Snooping enabled VLANs: 60
  Fastleave processing enabled VLANs:  empty
```

From the output, we can see that IGMP snooping is enabled.

3.2.3 Enabling FastLeave

We must enable the FastLeave feature for VLAN60 in our example so that receivers can use IGMP to signal that they are not interested in receiving multicast traffic anymore and the multicast router can process IGMP messages and prune sending traffic to those hosts immediately.

Implementation

Enable FastLeave for the example topology using the following command:

```
ACC-2(config)#ip igmp snoop vlan 60 fast-leave
```

Verification

To verify the FastLeave status, run the command shown in Example 3-2 on page 23.

Example 3-3 Verifying FastLeave setting

```
ACC-2#show ip igmp snoop
   Current IGMP snooping settings:
   snoop ena, timeout 10, aggr ena,
     mrto timeout 255
     qintrval 125
     robust 2
     srcip 255.255.255.255
     Send IGMP Messages with Router Alert option: dis
     Snooping enabled VLANs: 60
     Fastleave processing enabled VLANs: 60
```

From the output, you can see that FastLeave is enabled for VLAN 20.

3.2.4 Internet Group Management Protocol filtering

This section describes how to enable filtering for our example topology.

Implementation

In our scenario, ensure that the receiver host, connected to port13 of switch ACC-2, is not able to join multicast groups in range 239.100.100.100 through 239.100.100.200. To accomplish this task, configure IGMP filtering using the following procedure:

1. Configure an IGMP group range for the filtering profile by running the following command:

   ```
   ACC-2(config)#ip igmp profile 1 range
   ```

2. Configure the action of the IGMP filtering profile by running the following command:

   ```
   ACC-2(config)#ip igmp profile 1 action deny
   ```

3. Enable the IGMP filtering profile by running the following command:

   ```
   ACC-2(config)#ip igmp profile 1 enable
   ```

4. Enable IGMP filtering by running the following command:

   ```
   ACC-2(config)#ip igmp filtering
   ```

   When filter 1 is created, verify its configuration, as shown in Example 3-4.

Example 3-4 Verifying the configuration of Filter

```
ACC-2#show ip igmp profile 1
Current profile 1:
enabled, range 239.100.100.100 - 239.100.100.200, action deny
```

5. Assign the profile to port13, as shown in Example 3-5.

Example 3-5 Adding the profile to the port

```
ACC-2(config)#int port 13
ACC-2(config-if)#ip igmp profile 1
ACC-2(config-if)#ip igmp filtering
```

Verification

Verify that IGMP filtering is turned on, as shown in Example 3-6.

Example 3-6 Verifying IGMP filtering

```
ACC-2#show ip igmp filtering

IGMP filtering enabled
Filter 1:
   enabled, range 239.100.100.100 - 239.100.100.200, action deny
Port 13:
     filt  enabled, filters: 1
```

You can see that filter 1 has been enabled on Port13.

3.2.5 Verifying overall IGMP configuration

To verify that the IGMP configuration performed on the switch is correct, use a traffic generator sending IGMP group reports for multicast groups 239.0.0.20, 239.0.0.30, 239.100.100.120, and 239.100.100.130. Verify the configuration as shown in Example 3-7.

Example 3-7 Verifying the IGMP configuration

```
ACC-2#show ip igmp groups
Total entries: 2  Total IGMP groups: 2
Note: The <Total IGMP groups> number is computed as
      the number of unique (Group, Vlan) entries!
Note: Local groups (224.0.0.x) are not snooped and will not appear.
      Source           Group       VLAN   Port   Version    Mode  Expires   Fwd
 ---------------- --------------- ------ ------- ---------   ---- ---------- ---
       *           239.0.0.20      60     13      V2         -       4:18     Yes
       *           239.0.0.30      60     13      V2         -       4:19     Yes
```

Only the entries for groups 239.0.0.20 and 239.0.30 are created because groups 239.100.100.120 and 239.100.100.130 fall in the range in the group list denied by IGMP Filter.

3.3 PIM implementation

If the multicast traffic is confined within the topology, we can use PIM dense mode for multicast traffic delivery because the topology is not large. In larger networks, PIM sparse mode is the recommended PIM configuration. In this section, we show examples of how to configure both PIM modes.

3.3.1 Using PIM dense mode

This section describes how to implement PIM in dense mode.

Implementation

To configure PIM dense mode in the example network, perform the following steps:

1. Globally enable PIM on all the switches (ACC-1, ACC-2, AGG-,1 and AGG-2). Here we show the configuration on the AGG-1 switch by running the following command:

   ```
   AGG-1(config)#ip pim enable
   ```

2. You can attach a switch to a maximum of two independent PIM network components. Each component represents a different PIM network and can be defined for either PIM-SM or PIM-DM operation. The default mode for the component is sparse. Here, use PIM component number 1 for dense mode by changing the mode from sparse to dense, as shown in Example 3-8.

   Example 3-8 Changing from sparse mode to dense mode

   ```
   AGG-1(config)#ip pim component 1
   AGG-1(config-ip-pim-comp)#mode dense
   Mode changed from SPARSE to DENSE. Clearing all Sparse mode specific
   configurations
   ```

3. Enable PIM and configure PIM component 1 on the interfaces in Table 3-4.

   Table 3-4 PIM dense mode interfaces

Switch	PIM Interface
ACC-1	IP 101
ACC-1	IP 102
ACC-2	IP 103
ACC-2	IP 104
AGG-1	IP 100
AGG-1	IP 101
AGG-1	IP 103
AGG-2	IP 100
AGG-2	IP 102
AGG-2	IP 104
ACC-1	IP 50
ACC-2	IP 60

Enabling PIM in multiple places: Remember that PIM must also be enabled on IP interfaces for VLANs that are source and receiver (IP 50 for VLAN50 and IP60 for VLAN60 in our scenario).

4. Enable IP PIM on the example interface with the commands shown in Example 3-9.

Example 3-9 Enabling PIM on interface

```
AGG-1(config)#interface ip 100
AGG-1(config-ip-if)#ip pim enable
```

By default, PIM component 1 is assigned after the PIM is enabled on the interface, so we do not need to do any configuration besides changing mode of PIM component 1 to dense and enabling PIM on the interfaces. However, to explicitly configure a specific component on the interface in our example, use the commands shown in Example 3-10.

Example 3-10 Configuring a component on the interface

```
AGG-1(config)#interface ip 100
AGG-1(config-ip-if)#ip pim component 1
```

Verification

After you enable PIM on the device, change the mode of PIM component 1 to dense, and enable PIM on all interfaces from Table 3-4 on page 26, you can verify PIM configuration.

To display the interfaces where the PIM is enabled, run the following command:

```
show ip pim interface
```

The output of the command from the switches in your network is shown in Example 3-11.

Example 3-11 Showing PIM Interface output

```
ACC-1#show ip pim interface

Address         IfName/IfId Ver/Mode  Nbr   Qry          DR-Address   DR-Prio
                                      Count Interval
-------         ----------- --------  ----- --------     ----------   -------
10.0.50.1       net50/50    2/ Dense  0     30           10.0.50.1       1

10.0.101.1      net101/101   2/ Dense  1     30           10.0.101.2      1

10.0.102.1      net102/102   2/ Dense  1     30            10.0.102.2      1


ACC-2#show ip pim interface

Address         IfName/IfId Ver/Mode  Nbr   Qry          DR-Address   DR-Prio
                                      Count Interval
-------         ----------- --------  ----- --------     ----------   -------
10.0.60.1       net60/60    2/ Dense  0     30           10.0.60.1       1

10.0.103.2      net103/103   2/ Dense  1     30           10.0.103.2      1

10.0.104.2      net104/104   2/ Dense  1     30            10.0.104.2      1
```

```
AGG-1#show ip pim interface

Address         IfName/IfId Ver/Mode  Nbr   Qry           DR-Address   DR-Prio
                                      Count Interval
-------         ----------- --------  ----- --------      ----------   -------
10.0.100.1      net100/100   2/ Dense  1     30           10.0.100.2      1

10.0.101.2      net101/101   2/ Dense  1     30           10.0.101.2      1

10.0.103.1      net103/103   2/ Dense  1     30            10.0.103.2      1

AGG-2#show ip pim interface

Address         IfName/IfId Ver/Mode  Nbr   Qry           DR-Address   DR-Prio
                                      Count Interval
-------         ----------- --------  ----- --------      ----------   -------
10.0.100.2      net100/100   2/ Dense  1     30           10.0.100.2      1

10.0.102.2      net102/102   2/ Dense  1     30           10.0.102.2      1

10.0.104.1      net104/104   2/ Dense  1     30            10.0.104.2      1
```

From the output, you can see that PIM dense was enabled on the desired interfaces. You can also see the address of the designated router and the number of PIM neighbors on the interface (`NbrCount`).

To display the PIM neighbors of the switch, run the following command:

```
show ip pim neighbor
```

The output of the command from the switches in our network is shown in Example 3-12.

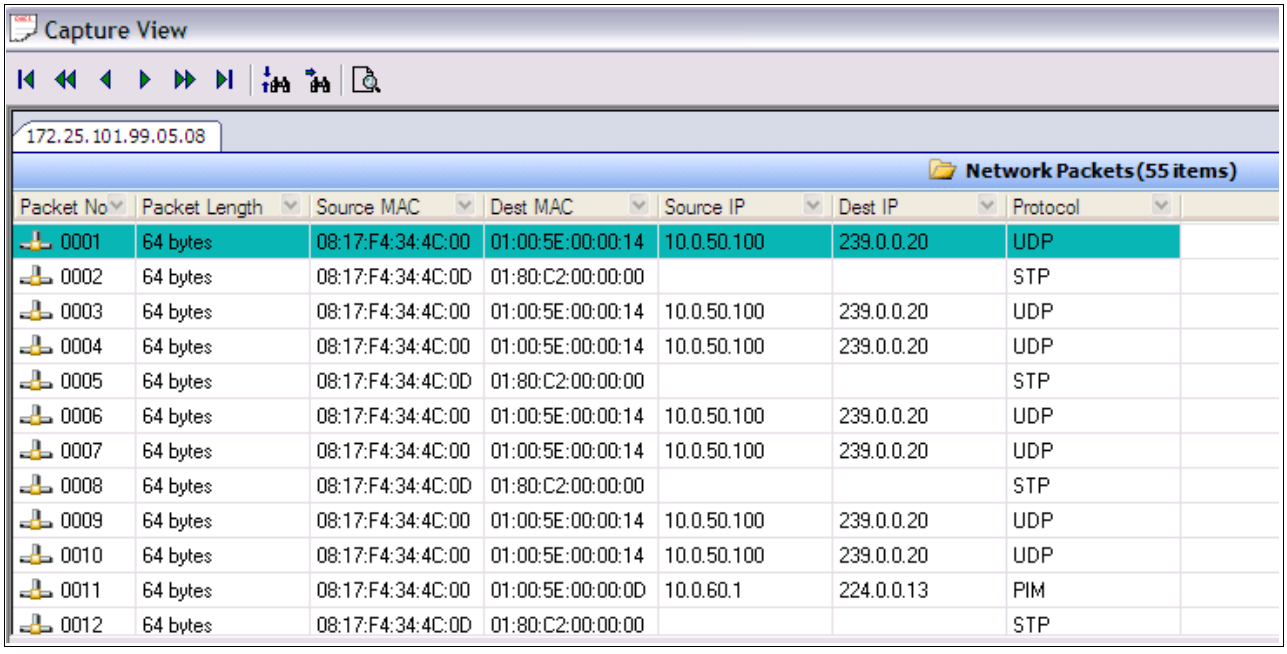
Example 3-12 PIM neighbors output

```
ACC-1#show ip pim neighbor

Neighbour      IfName/Idx Uptime/Expiry Ver DRPri/Mode CompId Override   Lan
Address                                                    Interval   Delay
---------      ---------- ------------- --- ---------- ------ --------  ------
10.0.101.2     net101/101  00:15:16/82    v2     1/D         1        0       0

10.0.102.2     net102/102  00:09:28/76    v2     1/D         1        0       0

ACC-2#show ip pim neighbor

Neighbour      IfName/Idx Uptime/Expiry Ver DRPri/Mode CompId Override   Lan
Address                                                    Interval   Delay
---------      ---------- ------------- --- ---------- ------ --------  ------
10.0.103.1     net103/103  00:11:06/95    v2     1/D         1        0       0

10.0.104.1     net104/104  00:09:33/99    v2     1/D         1        0       0


AGG-1#show ip pim neighbor
```

```
Neighbour       IfName/Idx Uptime/Expiry Ver DRPri/Mode CompId Override   Lan
Address                                                        Interval   Delay
---------       ---------- ------------ --- ---------- ------ --------  ------
10.0.100.2      net100/100  00:09:33/91    v2     1/D         1        0       0

10.0.101.1      net101/101  00:15:17/87    v2     1/D         1        0       0

10.0.103.2      net103/103  00:11:03/79    v2     1/D         1        0       0


AGG-2#show ip pim neighbor

Neighbour       IfName/Idx Uptime/Expiry Ver DRPri/Mode CompId Override   Lan
Address                                                        Interval   Delay
---------       ---------- ------------ --- ---------- ------ --------  ------
10.0.100.1      net100/100  00:09:36/87    v2     1/D         1        0       0

10.0.102.1      net102/102  00:09:35/81    v2     1/D         1        0       0

10.0.104.2      net104/104  00:09:37/79    v2     1/D         1        0       0
```

In our setup, we generate multicast traffic (UDP stream) directed to 239.0.0.20 from the receiver connected to port 13 in VLAN50 on ACC-1. From the aggregation switches running PIM dense mode, we expect to see the stream delivered to the receiver connected to port13 in VLAN60 on ACC-2 switch.

To verify that packets are delivered correctly, run a packet capture application on the receiver host. Figure 3-4 shows the output of such an application.



Packet No	Packet Length	Source MAC	Dest MAC	Source IP	Dest IP	Protocol
0001	64 bytes	08:17:F4:34:4C:00	01:00:5E:00:00:14	10.0.50.100	239.0.0.20	UDP
0002	64 bytes	08:17:F4:34:4C:0D	01:80:C2:00:00:00			STP
0003	64 bytes	08:17:F4:34:4C:00	01:00:5E:00:00:14	10.0.50.100	239.0.0.20	UDP
0004	64 bytes	08:17:F4:34:4C:00	01:00:5E:00:00:14	10.0.50.100	239.0.0.20	UDP
0005	64 bytes	08:17:F4:34:4C:0D	01:80:C2:00:00:00			STP
0006	64 bytes	08:17:F4:34:4C:00	01:00:5E:00:00:14	10.0.50.100	239.0.0.20	UDP
0007	64 bytes	08:17:F4:34:4C:00	01:00:5E:00:00:14	10.0.50.100	239.0.0.20	UDP
0008	64 bytes	08:17:F4:34:4C:0D	01:80:C2:00:00:00			STP
0009	64 bytes	08:17:F4:34:4C:00	01:00:5E:00:00:14	10.0.50.100	239.0.0.20	UDP
0010	64 bytes	08:17:F4:34:4C:00	01:00:5E:00:00:14	10.0.50.100	239.0.0.20	UDP
0011	64 bytes	08:17:F4:34:4C:00	01:00:5E:00:00:0D	10.0.60.1	224.0.0.13	PIM
0012	64 bytes	08:17:F4:34:4C:0D	01:80:C2:00:00:00			STP

Figure 3-4 Capture of multicast packets delivered to the receiver

You can see that, among other packets, the UDP stream from the sender 10.0.50.100 directed to the multicast address of 239.0.20 is successfully delivered over the multicast network to the receiver.

3.3.2 Using PIM sparse mode

In order to configure PIM sparse mode in the example network, complete the following steps:

1. Globally enable PIM on all the switches (ACC-1, ACC-2, AGG-1 and AGG-2). Here we show the configuration of the example AGG-1 switch by running the following command:

   ```
   AGG-1(config)#ip pim enable
   ```

2. A switch can be attached to a maximum of two independent PIM network components. Each component represents a different PIM network and can be defined for either PIM PIM-SM or PIM-DM operation. The default mode for the component is sparse. We use PIM component number 1 for sparse mode, and thus we do not have to modify the default mode for the component. Component 1 is always configured on the switch, so you do not need to do any configuration.

   To verify the component settings, run the following command:

   ```
   show ip pim component
   ```

   An example output is shown in Example 3-13.

   Example 3-13 Example output of the show ip pim component command

   ```
   AGG-1#show ip pim component 1

   PIM Component Information
   --------------------------
   Component-Id: 1
     PIM Mode: sparse,   PIM Version: 2
     Elected BSR: 0.0.0.0
     Candidate RP Holdtime: 0
   ```

3. Enable PIM on the interfaces, as shown in Table 3-5.

   Table 3-5 PIM sparse mode interfaces

Switch	PIM Interface
ACC-1	IP 101
ACC-1	IP 102
ACC-2	IP 103
ACC-2	IP 104
AGG-1	IP 100
AGG-1	IP 101
AGG-1	IP 103
AGG-2	IP 100
AGG-2	IP 102
AGG-2	IP 104

Switch	PIM Interface
ACC-1	IP 50
ACC-2	IP 60

Enabling PIM on IP interfaces: PIM must also be enabled on IP interfaces for VLANs that are source and receiver (IP 50 for VLAN50 and IP60 for VLAN60 in our scenario).

PIM sparse mode needs a rendezvous point (RP), as described in 1.3.2, “Protocol-Independent Multicast” on page 6.

We can use either a static RP or use BSR protocol to propagate group-to-RP mapping to all multicast routers in the network. The following sections describe configurations for both scenarios.

Static rendezvous point

This section describes how to statically configure RP addresses for groups.

For redundancy, it is a preferred practice to use loopback addresses instead of IP addresses assigned to VLANs. This practice mitigates situations where the VLAN IP interface is down but the switch is still up.

The loopback addresses for aggregation switches are shown in Table 3-6.

Table 3-6 Loopback addresses

Switch	Loopback address /mask
AGG-1	1.1.1.1 / 32
AGG-2	1.1.1.2 / 32

PM sparse mode and RP: It is important that PIM sparse mode is enabled on the interfaces that are used as RP (Loopback1 on AGG-1 and AGG-2 in our scenario).

Static RP configuration maps specific groups (239.0.0.20 and 239.0.0.30) to the corresponding IP address of the RP, as shown in Table 3-7.

Table 3-7 Group-to-RP mappings

Group	Group Mask	RP	RP address
239.0.0.20	255.255.255.255	AGG-1	1.1.1.1
239.0.0.30	255.255.255.255	AGG-2	1.1.1.2

Implementation

To map the RPs to groups, complete these steps:

1. Configure all the static RP addresses as shown in Example 3-14.

Example 3-14 Configuring RP addresses for groups

```
Switch(config)#ip pim component 1
Switch(config-ip-pim-comp)#rp-static rp-address 239.0.0.20 255.255.255.255 1.1.1.1
Switch(config-ip-pim-comp)#rp-static rp-address 239.0.0.30 255.255.255.255 1.1.1.2
```

2. Enable static RP configuration globally using the following command. Again, static RP addresses must be configured on all multicast routers).

```
Switch(config)#ip pim static-rp enable
```

Verification

To verify that PIM sparse mode has been enabled on all required interfaces and that PIM neighborship has been established on these interfaces, perform the following steps:

1. Use the **show ip pim interface** command shown in Example 3-15 and check the output.

Verification for one switch: In the section, we show output of the verification commands from one switch only.

Example 3-15 Verifying PIM sparse mode

```
ACC-1#show ip pim interface

Address         IfName/IfId Ver/Mode  Nbr   Qry           DR-Address   DR-Prio
                                      Count Interval
-------         ----------- --------  ----- --------      ----------   -------
10.0.50.1       net50/50    2/Sparse  0     30           10.0.50.1       1

10.0.101.1      net101/101   2/Sparse  1     30           10.0.101.2      1

10.0.102.1      net102/102   2/Sparse  1     30           10.0.102.2      1


ACC-1#show ip pim neighbor

Neighbour       IfName/Idx Uptime/Expiry Ver DRPri/Mode CompId Override   Lan
Address                                                      Interval   Delay
---------       ---------- ------------- --- ---------- ------ --------  ------
10.0.101.2      net101/101  02:38:30/101   v2     1/S         1        0       0

10.0.102.2      net102/102  02:38:40/90    v2     1/S         1        0       0
```

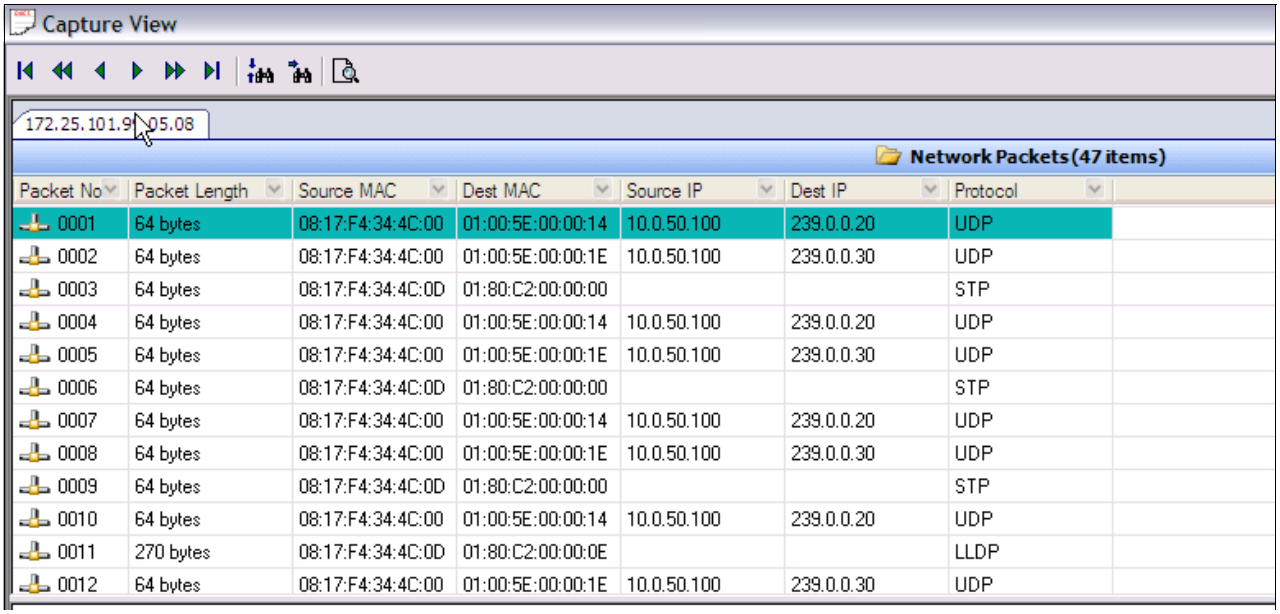
2. Then, we verify that static RP configuration is correct by running the show ip pim rp-static command, as shown in Example 3-16.

Example 3-16 Verifying the static RP configuration

```
ACC-1#show ip pim rp-static

Static-RP Enabled

CompId    GroupAddress      Group Mask       RPAddress
```

```
------    ------------      ----------       ---------
     1      239.0.0.20 255.255.255.255         1.1.1.1

     1      239.0.0.30 255.255.255.255         1.1.1.2
```

3. Generate some multicast traffic, and capture it on the receiver. From the capture at the receiver (Figure 3-5), you can see that the UDP traffic generated from source 10.0.50.100 and directed to multicast groups 239.0.0.20 and 239.0.0.30 is successfully delivered to the receiver.



Packet No	Packet Length	Source MAC	Dest MAC	Source IP	Dest IP	Protocol
0001	64 bytes	08:17:F4:34:4C:00	01:00:5E:00:00:14	10.0.50.100	239.0.0.20	UDP
0002	64 bytes	08:17:F4:34:4C:00	01:00:5E:00:00:1E	10.0.50.100	239.0.0.30	UDP
0003	64 bytes	08:17:F4:34:4C:0D	01:80:C2:00:00:00			STP
0004	64 bytes	08:17:F4:34:4C:00	01:00:5E:00:00:14	10.0.50.100	239.0.0.20	UDP
0005	64 bytes	08:17:F4:34:4C:00	01:00:5E:00:00:1E	10.0.50.100	239.0.0.30	UDP
0006	64 bytes	08:17:F4:34:4C:0D	01:80:C2:00:00:00			STP
0007	64 bytes	08:17:F4:34:4C:00	01:00:5E:00:00:14	10.0.50.100	239.0.0.20	UDP
0008	64 bytes	08:17:F4:34:4C:00	01:00:5E:00:00:1E	10.0.50.100	239.0.0.30	UDP
0009	64 bytes	08:17:F4:34:4C:0D	01:80:C2:00:00:00			STP
0010	64 bytes	08:17:F4:34:4C:00	01:00:5E:00:00:14	10.0.50.100	239.0.0.20	UDP
0011	270 bytes	08:17:F4:34:4C:0D	01:80:C2:00:00:0E			LLDP
0012	64 bytes	08:17:F4:34:4C:00	01:00:5E:00:00:1E	10.0.50.100	239.0.0.30	UDP

Figure 3-5 Capture of multicast streams delivered to the receiver

Bootstrap router

We use a bootstrap router (BSR) to propagate RP information to multicast routers in the network. As described in “PIM sparse mode” on page 7,BSR protocol requires two roles: a candidate RP and the BSR itself.

We assign those roles to aggregation switches, as shown in Table 3-8.

Table 3-8 BSR roles

Switch	Roles
AGG-1, 1.1.1.1	- Candidate RP for 239.0.0.20 group - Candidate RP for all multicast groups - BSR, priority 200
AGG-2, 1.1.1.2	- Candidate RP for 239.0.0.30 - Candidate RP for all multicast groups - BSR, priority 100

Multicast group addresses: Group address 224.0.0.0 with subnet mask 240.0.0.0 matches all multicast group addresses.

Implementation

To configure the switch as the RP component (as shown in Table 3-8 on page 33), complete the following steps:

1. Issue the **ip pim component** command for IP PIM component 1, as shown in Example 3-17:

   Example 3-17

```
AGG-1(conf)#ip pim component 1
AGG-1(config-ip-pim-comp)rp-candidate rp-address 239.0.0.20 255.255.255.255
1.1.1.1
AGG-1(config-ip-pim-comp)rp-candidate rp-address 224.0.0.0 240.0.0.0 1.1.1.1
```

2. Configure `holdtime`, the amount of time that the elected interface will retain the RP for the group before a re-election is performed, as shown in Example 3-18.

   Example 3-18 Configuring RP holdtime for AAG-1

```
AGG-1(config-ip-pim-comp)rp-candidate holdtime 100
```

   Configuration of the candidate RP on AGG-2 is similar (Example 3-19).

   Example 3-19 Configuring RP for AAG-2

```
AGG-2(config)#ip pim component 1
AGG-2(config-ip-pim-comp)#rp-candidate rp-address 239.0.0.30 255.255.255.255
1.1.1.2
AGG-2(config-ip-pim-comp)#rp-candidate rp-address 224.0.0.0 240.0.0.0 1.1.1.2
AGG-2(config-ip-pim-comp)#rp-candidate holdtime 100
```

3. Merge the text. To verify candidate RP configuration, run the **show ip pim rp-candidate** command, as shown in Example 3-20.

   Example 3-20 Showing candidate RP status

```
AGG-2#show ip pim rp-candidate

CompId    GroupAddress      Group Mask       RPAddress/Priority
------    ------------      ----------       ---------- -------
     1       224.0.0.0       240.0.0.0         1.1.1.2/192

     1      239.0.0.30 255.255.255.255         1.1.1.2/192
```

4. Configure Loopback1 interfaces as BSR on aggregation switches. BSR priority for AGG-1 is 200, making it preferred over AGG-2, which has a priority of 100.
   - On AGG-1, run the following commands:
     - **AGG-1(config)#int loopback1**
     - **AGG-1(config-ip-loopback)#ip pim cbsr-preference 200**
   - On AGG-2, run the following commands:
     - **AGG-2(config)#int loopback1**
     - **AGG-2(config-ip-loopback)#ip pim cbsr-preference 100**

   Perform this configuration only on switches having candidate RP and BSR roles. The configuration propagates to all other switches in the network, so we can verify it there.

Example 3-21 shows the bootstrap configuration on the ACC-1 switch.

Example 3-21 Bootstrap configuration on ACC-1

```
ACC-1#show ip pim bsr

PIMv2 Bootstrap Configuration For Component 1
---------------------------------------------
Elected BSR for Component  1
  BSR Address : 1.1.1.1
  BSR Priority : 200, Hash Mask Length : 30

PIMv2 Bootstrap Configuration For Component 2
---------------------------------------------
Elected BSR for Component  2
  BSR Address : 0.0.0.0
  BSR Priority : 0, Hash Mask Length : 30
```

From the output, you can see that for PIM component 1, the BSR address is 1.1.1.1 with a priority of 200.

You can see group-to-RP mappings on all switches, as shown in Example 3-22.

Example 3-22 Group-to-RP mappings

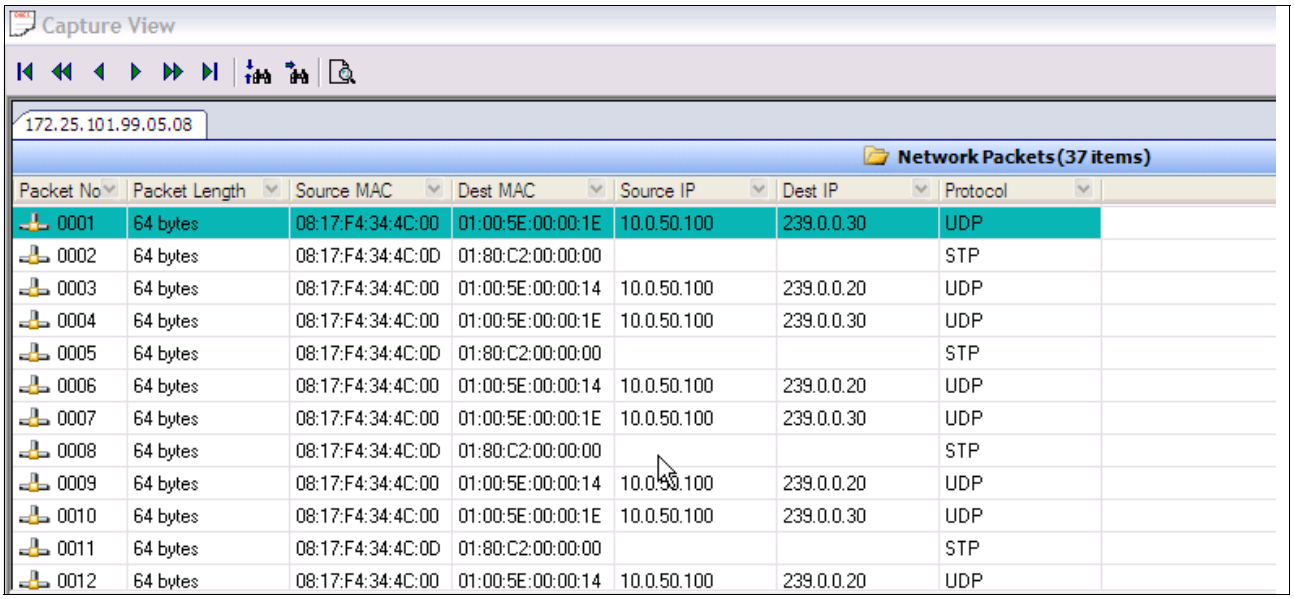
```
ACC-1#show ip pim rp-set

PIM Group-to-RP mappings
------------------------
Group Address : 224.0.0.0 Group Mask : 240.0.0.0
   RP: 1.1.1.2
  Component-Id : 1
    Hold Time : 100, Expiry Time : 00:00:44

Group Address : 224.0.0.0 Group Mask : 240.0.0.0
   RP: 1.1.1.1
  Component-Id : 1
    Hold Time : 100, Expiry Time : 00:00:44

Group Address : 239.0.0.20 Group Mask : 255.255.255.255
   RP: 1.1.1.1
  Component-Id : 1
    Hold Time : 100, Expiry Time : 00:00:44

Group Address : 239.0.0.30 Group Mask : 255.255.255.255
   RP: 1.1.1.2
  Component-Id : 1
    Hold Time : 100, Expiry Time : 00:00:44
```

From the output, we can see that all configured mappings are there.

Verification

Verify the overall PIM sparse mode configuration by sending some real multicast traffic. We use 10.0.50.100 sender to send traffic destined to 239.0.0.20 and 239.0.0.30 groups and observe if the traffic is delivered to the receiver of 10.0.60.100.

In Figure 3-6 we can see that multicast packets are successfully delivered to the receiver.



Packet No	Packet Length	Source MAC	Dest MAC	Source IP	Dest IP	Protocol
0001	64 bytes	08:17:F4:34:4C:00	01:00:5E:00:00:1E	10.0.50.100	239.0.0.30	UDP
0002	64 bytes	08:17:F4:34:4C:0D	01:80:C2:00:00:00			STP
0003	64 bytes	08:17:F4:34:4C:00	01:00:5E:00:00:14	10.0.50.100	239.0.0.20	UDP
0004	64 bytes	08:17:F4:34:4C:00	01:00:5E:00:00:1E	10.0.50.100	239.0.0.30	UDP
0005	64 bytes	08:17:F4:34:4C:0D	01:80:C2:00:00:00			STP
0006	64 bytes	08:17:F4:34:4C:00	01:00:5E:00:00:14	10.0.50.100	239.0.0.20	UDP
0007	64 bytes	08:17:F4:34:4C:00	01:00:5E:00:00:1E	10.0.50.100	239.0.0.30	UDP
0008	64 bytes	08:17:F4:34:4C:0D	01:80:C2:00:00:00			STP
0009	64 bytes	08:17:F4:34:4C:00	01:00:5E:00:00:14	10.0.50.100	239.0.0.20	UDP
0010	64 bytes	08:17:F4:34:4C:00	01:00:5E:00:00:1E	10.0.50.100	239.0.0.30	UDP
0011	64 bytes	08:17:F4:34:4C:0D	01:80:C2:00:00:00			STP
0012	64 bytes	08:17:F4:34:4C:00	01:00:5E:00:00:14	10.0.50.100	239.0.0.20	UDP

Figure 3-6 Capture of multicast packets delivered to the receiver

Failover verification

To test a failover scenario, shut down the AGG-1 interface to simulate its failure and see how it affects multicast forwarding. After BSR and mapping entries time out, you can see that BSR information has been updated and now point to AGG-2 (1.1.1.2), as shown in Example 3-23.

Example 3-23 Failover testing

```
ACC-1#show ip pim bsr

PIMv2 Bootstrap Configuration For Component 1
------------------------------------------------
Elected BSR for Component  1
  BSR Address : 1.1.1.2
  BSR Priority : 100, Hash Mask Length : 30

PIMv2 Bootstrap Configuration For Component 2
------------------------------------------------
Elected BSR for Component  2
  BSR Address : 0.0.0.0
  BSR Priority : 0, Hash Mask Length : 30
```

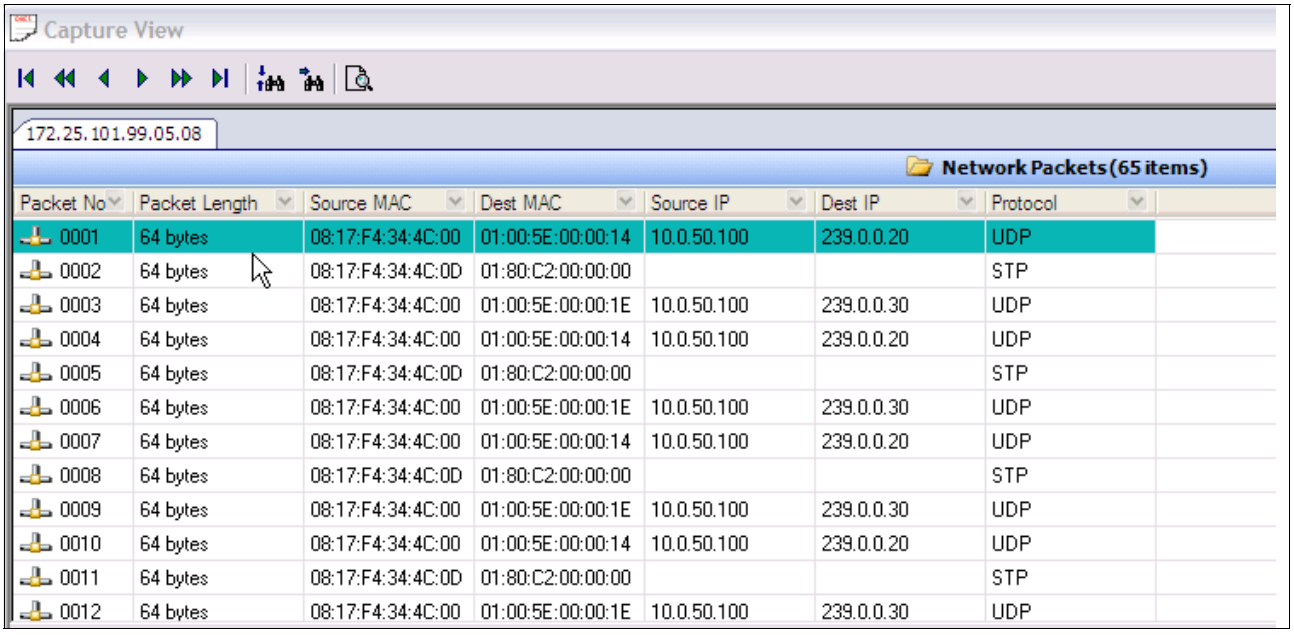
Also, mapping entries have been updated, as shown in Example 3-24.

Example 3-24 Updated mapping entries

```
ACC-1#show ip pim rp-set

PIM Group-to-RP mappings
------------------------
Group Address : 224.0.0.0 Group Mask : 240.0.0.0
   RP: 1.1.1.2
  Component-Id : 1
    Hold Time : 100, Expiry Time : 00:01:35
```

```
Group Address : 239.0.0.30 Group Mask : 255.255.255.255
   RP: 1.1.1.2
  Component-Id : 1
    Hold Time : 100, Expiry Time : 00:01:35
```

When the new settings take place, the multicast streams are successfully delivered to the receiver, as shown in Figure 3-7.



Packet No	Packet Length	Source MAC	Dest MAC	Source IP	Dest IP	Protocol
0001	64 bytes	08:17:F4:34:4C:00	01:00:5E:00:00:14	10.0.50.100	239.0.0.20	UDP
0002	64 bytes	08:17:F4:34:4C:0D	01:80:C2:00:00:00			STP
0003	64 bytes	08:17:F4:34:4C:00	01:00:5E:00:00:1E	10.0.50.100	239.0.0.30	UDP
0004	64 bytes	08:17:F4:34:4C:00	01:00:5E:00:00:14	10.0.50.100	239.0.0.20	UDP
0005	64 bytes	08:17:F4:34:4C:0D	01:80:C2:00:00:00			STP
0006	64 bytes	08:17:F4:34:4C:00	01:00:5E:00:00:1E	10.0.50.100	239.0.0.30	UDP
0007	64 bytes	08:17:F4:34:4C:00	01:00:5E:00:00:14	10.0.50.100	239.0.0.20	UDP
0008	64 bytes	08:17:F4:34:4C:0D	01:80:C2:00:00:00			STP
0009	64 bytes	08:17:F4:34:4C:00	01:00:5E:00:00:1E	10.0.50.100	239.0.0.30	UDP
0010	64 bytes	08:17:F4:34:4C:00	01:00:5E:00:00:14	10.0.50.100	239.0.0.20	UDP
0011	64 bytes	08:17:F4:34:4C:0D	01:80:C2:00:00:00			STP
0012	64 bytes	08:17:F4:34:4C:00	01:00:5E:00:00:1E	10.0.50.100	239.0.0.30	UDP

Figure 3-7 Capture of multicast packets delivered to the receiver

3.3.3 Conclusions

PIM is a signalling protocol that facilitates carrying multicast traffic over Layer 3 network, that is, routing the traffic if the sender and receiver are in different IP submits.

PIM dense mode is a plug-and-play multicast protocol with a simple configuration: you just need to configure it on multicast interfaces in the network. However, PIM dense mode uses Flood-Prune behavior, assuming everyone is interested in the traffic. Because this approach can lead to unnecessary use of bandwidth, PIM dense mode is suitable only for small networks or environment with a large number of receivers.

PIM sparse mode is generally standard for multicast transmission used in today's network. Sparse mode requires some additional configuration, but the advantage is that multicast traffic is only delivered to the hosts that explicitly signal the interest in receiving the multicast traffic. PIM sparse mode defined a new multicast router role, the rendezvous point (RP). There are two options for configuring RP: static and BSR.

Although a static RP might seem like a simple solution, it has its drawbacks:

- It must be configured on every multicast router.
- It does not provide redundancy. If a static RP for a specific group fails, no configuration provides backup.[1]

[1] It is valid for the current release of IBM Networking Operating System version 6.8. Future releases will have this capability.

Bootstrap Router (BSR) is a protocol that facilitates distribution of group-to-RP mappings in the network. It also allows for redundancy for both RP or BSR failure.

A

IP Multicast command reference

This appendix contains commands used to configure different IP Multicast features on IBM System Networking switches. For a complete list of commands for IBM Networking Operating System version 6.8, see “Related publications” on page 49.

Internet Group Management Protocol commands

This section presents commands used for basic and advances configuration of Internet Group Management Protocol (IGMP) protocol.

Internet Group Management Protocol snooping

Table A-1 lists IGMP snooping commands and descriptions.

Table A-1 IGMP snooping commands

Command	Command mode	Description
ip igmp snoop mrouter-timeout *<1-600>*	Global configuration	Configures the timeout value for IGMP membership queries (querying is done by the Mrouter). When the timeout value is reached, if the proper conditions are met, the switch removes the multicast router from its IGMP table. The range is 1 to 600 seconds. The default is 255 seconds.
[no] ip igmp snoop aggregate	Global configuration	Enables or disables IGMP Membership Report aggregation.
ip igmp snoop source-ip *<IP address>*	Global configuration	Configures the source IP address used as a proxy for IGMP group-specific queries.
ip igmp snoop vlan *<VLAN number>*	Global configuration	Adds the selected VLAN(s) to IGMP snooping.
no ip igmp snoop vlan *<VLAN number>*	Global configuration	Removes the selected VLAN(s) from IGMP snooping.
no ip igmp snoop vlan all	Global configuration	Removes all VLANs from IGMP snooping.
ip igmp snoop enable	Global configuration	Enables IGMP snooping.
no ip igmp snoop enable	Global configuration	Disables IGMP snooping.
default ip igmp snoop	Global configuration	Resets IGMP snooping parameters to their default values.
show ip igmp snoop	All	Displays the current IGMP snooping parameters.

Internet Group Management Protocol v3 configuration

Table A-2 lists the IGMPv3 configuration commands and the description.

Table A-2 IGMPv3 configuration commands

Command	Command mode	Description
ip igmp snoop igmpv3 sources <*1-64*>	Global configuration	Configures the maximum number of IGMP multicast sources to snoop from within the group record. Use this command to limit the number of IGMP sources to provide more refined control. The default value is 8.
[no] ip igmp snoop igmpv3 v1v2	Global configuration	Enables or disables snooping on IGMP version 1 and version 2 reports. When disabled, the switch drops IGMPv1 and IGMPv2 reports. The default value is enabled.
[no] ip igmp snoop igmpv3 exclude	Global configuration	Enables or disables snooping on IGMPv3 Exclude Reports. When disabled, the switch ignores Exclude Reports. The default value is enabled.
ip igmp snoop igmpv3 enable	Global configuration	Enables IGMP version 3. The default value is disabled.
no ip igmp snoop igmpv3 enable	Global configuration	Disables IGMP version 3.
show ip igmp snoop igmpv3	All except User EXEC	Displays the current IGMP v3 snooping configuration.

Internet Group Management Protocol Relay configuration

When you configure an IGMP Relay, also configure the IGMP Relay multicast routers. Table A-3 lists IGMP Relay configuration commands and their description.

Table A-3 IGMP Relay configuration commands

Command	Command mode	Description
ip igmp relay enable	Global configuration	Enables IGMP Relay.
no ip igmp relay enable	Global configuration	Disables IGMP Relay.
ip igmp relay vlan <*VLAN number*>	Global configuration	Adds the VLAN to the list of IGMP Relay VLANs.
no ip igmp relay vlan <*VLAN number*>	Global configuration	Removes the VLAN from the list of IGMP Relay VLANs.
ip igmp relay report <*0-150*>	Global configuration	Configures the interval between unsolicited Join reports sent by the switch, in seconds. The default value is 10.
show ip igmp relay	All	Displays the current IGMP Relay configuration.

Internet Group Management Protocol Relay multicast router configuration

Table A-4 describes the commands used to configure multicast routers for the IGMP Relay.

Table A-4 IGMP Relay multicast router configuration commands

Command	Command mode	Description
ip igmp relay mrouter <*1-2*> address <*IP address*>	Global configuration	Configures the IP address of the IGMP multicast router used for IGMP Relay.
ip igmp relay mrouter <*1-2*> interval <*1-60*>	Global configuration	Configures the time interval between ping attempts to the upstream Mrouters, in seconds. The default value is 2.
ip igmp relay mrouter <*1-2*> retry <*1-120*>	Global configuration	Configures the number of failed ping attempts required before the switch declares this Mrouter is down. The default value is 4.
ip igmp relay mrouter <*1-2*> attempt <*1-128*>	Global configuration	Configures the number of successful ping attempts required before the switch declares this Mrouter is up. The default value is 5.
ip igmp relay mrouter <*1-2*> version <*1-2*>	Global configuration	Configures the IGMP version (1 or 2) of the multicast router.
ip igmp relay mrouter <*1-2*> enable	Global configuration	Enables the multicast router.
no ip igmp relay mrouter <*1-2*> enable	Global configuration	Disables the multicast router.
no ip igmp relay mrouter <*1-2*>	Global configuration	Deletes the multicast router from IGMP Relay.

Internet Group Management Protocol static multicast router configuration

Table A-5 describes the commands used to configure a static multicast router.

Dynamic Mrouters: When static Mrouters are used, the switch continues discovering dynamic Mrouters through IGMP snooping. However, dynamic Mrouters cannot replace static Mrouters. If a dynamic Mrouter has the same port and VLAN combination as a static Mrouter, the dynamic Mrouter is not learned.

Table A-5 IGMP static multicast router configuration commands

Command	Command mode	Description
ip igmp mrouter <*port alias or number*> <*VLAN number*> <*version (1-3)*>	Global configuration	Selects a port/VLAN combination on which the static multicast router is connected, and configures the IGMP version of the multicast router.
no ip igmp mrouter <*port alias or number*> <*VLAN number*> <*version (1-3)*>	Global configuration	Removes a static multicast router from the selected port/VLAN combination.
no ip igmp mrouter all	Global configuration	Removes all static multicast routers.
clear ip igmp mrouter	Global configuration	Clears the multicast router port table.

Command	Command mode	Description
show ip igmp mrouter	All except User EXEC	Displays the current IGMP static multicast router parameters.

Internet Group Management Protocol filtering configuration

Table A-6 describes the commands used to configure an IGMP Filter.

Table A-6 IGMP filtering configuration commands

Command	Command mode	Description
ip igmp profile <*1-16*>	Global configuration	Configures the IGMP Filter.
ip igmp filtering	Global configuration	Enables IGMP filtering globally.
no ip igmp filtering	Global configuration	Disables IGMP filtering globally.
show ip igmp filtering	All	Displays the current IGMP filtering parameters.
ip igmp profile <*1-16*> range <*IP address 1*> <*IP address 2*>	Global configuration	Configures the range of IP Multicast addresses for the designated filter.
ip igmp profile <*1-16*> action {allow|deny}	Global configuration	Allows or denies multicast traffic for the IP Multicast addresses specified. The default action is `deny`.
ip igmp profile <*1-16*> enable	Global configuration	Enables this IGMP Filter.
no ip igmp profile <*1-16*> enable	Global configuration	Disables this IGMP Filter.
no ip igmp profile <*1-16*>	Global configuration	Deletes this parameter definitions for the IGMP Filter.
show ip igmp profile <*1-16*>	All	Displays the current IGMP Filter.
[no] ip igmp filtering	Interface port	Enables or disables IGMP filtering on this port.
ip igmp profile <*1-16*>	Interface port	Adds an IGMP Filter to the designated port.

Internet Group Management Protocol advanced configuration

Table A-7 describes the commands used to configure advanced IGMP parameters.

Table A-7 IGMP advanced configuration commands

Command	Command mode	Description
no ip igmp profile <*1-16*>	Interface port	Removes an IGMP Filter from the designated port.
show interface port <*port alias or number*> igmp-filtering	All except User EXEC	Displays the current IGMP Filter parameters for the designated port.
ip igmp query-interval <*1-600*>	Global configuration	Sets the IGMP router query interval, in seconds. The default value is `125`.

Command	Command mode	Description
ip igmp robust *<2-10>*	Global configuration	Configures the IGMP Robustness variable, which allows you to tune the switch for expected packet loss on the subnet. If the subnet is expected to be lossy (having a high rate of packet loss), increase the value. The default value is 2.
ip igmp timeout *<1-255>*	Global configuration	Configures the timeout value for IGMP Membership Reports (host). When the timeout value is reached, the switch removes the host from its IGMP table. The range is from 1 to 255 seconds. The default is 10 seconds.
[no] ip igmp fastleave *<VLAN number>*	Global configuration	Enables or disables FastLeave processing. FastLeave allows the switch to immediately remove a port from the IGMP port list if the host sends a Leave message and the proper conditions are met. This command is disabled by default.
[no] ip igmp flood	Global configuration	Configures the switch to flood unregistered IP Multicast traffic to all ports. The default setting is enabled.[a]
[no] ip igmp cpu	Global configuration	Configures the switch to forward unregistered IP Multicast traffic to the Management Processor, which adds an entry in the IPMC table, with the following conditional results: ► If no Mrouter is present, drop subsequent packets with same IPMC. ► If an Mrouter is present, forward subsequent packets to the Mrouter(s) on the ingress VLAN. The default setting is enabled.[b]
[no] ip igmp snoop rtralert	Global configuration	Enables or disables the Router Alert option in IGMP messages.

a. If none of the IGMP hosts reside on the VLAN of the streaming server for a IPMC group, you must disable IGMP flooding to ensure that multicast data is forwarded across the VLANs for that IPMC group.

b. If both **flood** and **cpu** are disabled, then the switch drops all unregistered IPMC traffic.

Internet Group Management Protocol Querier configuration

Table A-8 describes the commands IGMP Querier configuration commands.

Table A-8 IGMP Querier configuration commands

Command	Command mode	Description
ip igmp querier vlan <*VLAN number*> source-ip <*IP address*>	Global configuration	Configures the IGMP source IP address for the selected VLAN.
ip igmp querier vlan <*VLAN number*> max-response <*1-256*>	Global configuration	Configures the maximum time, in tenths of a second, allowed before responding to a Membership Query message. The default value is 100. By varying the Query Response Interval, an administrator can tune the burstiness of IGMP messages on the subnet; larger values make the traffic less bursty as host responses are spread out over a larger interval.
ip igmp querier vlan <*VLAN number*> query-interval <*1-608*>	Global configuration	Configures the interval between IGMP Query broadcasts. The default value is 125 seconds.
ip igmp querier vlan <*VLAN number*> robustness <*2-10*>	Global configuration	Configures the IGMP **Robustness** variable, which is the number of times that the switch sends each IGMP message. The default value is 2.
ip igmp querier vlan <*VLAN number*> election-type *[ipv4|mac]*	Global configuration	Sets the IGMP Querier election criteria as IP address or Mac address. The default setting is IPv4.
ip igmp querier vlan <*VLAN number*> startup-interval <*1-608*>	Global configuration	Configures the Startup Query Interval, which is the interval between general queries sent out at startup.
ip igmp querier vlan <*VLAN number*> startup-count <*1-10*>	Global configuration	Configures the Startup Query Count, which is the number of IGMP queries sent out at startup. Each query is separated by the Startup Query Interval. The default value is 2.
ip igmp querier vlan <*VLAN number*> version [v1|v2|v3]	Global configuration	Configures the IGMP version. The default version is v3.
ip igmp querier enable	Global configuration	Enables IGMP Querier.
no ip igmp querier enable	Global configuration	Disables IGMP Querier.
show ip igmp querier vlan <*VLAN number*>	Global configuration	Displays IGMP Querier information for the selected VLAN.
show ip igmp querier	All	Displays the current IGMP Querier parameters.

PIM commands

Table A-9 describes PIM commands.

Table A-9 PIM commands

Command	Command mode	Description
ip pim component ***<1-2>***	Global configuration	Enter PIM component mode.
ip pim regstop-ratelimit-period ***<0-2147483647>***	Global configuration	Configures the register stop rate limit, in seconds. The default value is `5`.
[no] ip pim static-rp enable	Global configuration	Enables or disables static RP configuration. The default setting is `disabled`.
[no] ip pim pmbr enable	Global configuration	Enables or disables PIM border router. The default setting is `disabled`.
ip pim enable	Global configuration	Globally turns PIM on.
no ip pim enable	Global configuration	Globally turns PIM off.
clear ip pim mroute	Global configuration	Clears PIM multicast router entries.

PIM component configuration

Table A-10 describes the commands PIM component configuration commands.

Table A-10 PIM component configuration commands

Command	Command mode	Description
ip pim component <1-2>	Global configuration	Enter PIM component mode.
mode **{*dense*|*sparse*}**	PIM component	Configures the operational mode of the PIM router (`dense` or `sparse`).
show ip pim component [<*1-2*>]	All	Displays the current PIM component configuration settings.

Rendezvous point candidate configuration

Table A-11 describes the commands for rendezvous point (RP) candidate configuration.

Table A-11 RP Candidate configuration commands

Command	Command mode	Description
rp-candidate rp-address ***<group multicast address> <group subnet mask> <IP address>***	PIM Component	Adds an RP candidate.
no rp-candidate rp-address ***<group multicast address> <group subnet mask> <IP address>***	PIM Component	Removes the specified RP candidate.
rp-candidate holdtime ***<0-255>***	PIM Component	Configures the hold time of the RP candidate, in seconds.

Static rendezvous point configuration

Table A-10 on page 46 describes the commands for static RP configuration.

Table A-12 Static RP configuration commands

Command	Command mode	Description
rp-static rp-address *<group multicast address> <group subnet mask> <IP address>*	PIM Component	Adds a static RP.
no rp-static rp-address *<group multicast address> <group subnet mask> <IP address>*	PIM Component	Removes the specified static RP.

PIM Interface configuration

Table A-13 describes the commands for PIM Interface configuration.

Table A-13 PIM Interface configuration commands

Command	Command mode	Description
interface ip *<interface number>*	Global Configuration	Enter Interface IP mode.
ip pim hello-interval *<0-65535>*	Interface IP	Configures the time interval, in seconds, between PIM Hello packets. The default value is 30.
ip pim join-prune-interval *<0-65535>*	Interface IP	Configures the interval between Join Prune messages, in seconds. The default value is 60.
ip pim cbsr-preference *<-1-255>*	Interface IP	Configures the candidate bootstrap router preference.
ip pim component-id *<1-2>*	Interface IP	Defines the component ID for the interface.
ip pim hello-holdtime *<1-65535>*	Interface IP	Configures the time period for which a neighbor is to consider this switch to be operative (up). The default value is 105.
ip pim dr-priority *<0-4294967294>*	Interface IP	Configures the designated router priority. The default value is 1.
ip pim override-interval *<0-65535>*	Interface IP	Configures the override interval for the router interface, in seconds.
ip pim lan-delay *<0-32767>*	Interface IP	Configures the LAN delay value for the router interface, in seconds.
[no] ip pim border-bit	Interface IP	Enables or disables the interface as a border router. The default setting is disabled.
[no] ip pim lan-prune-delay	Interface IP	Enables or disables LAN delay advertisements on the interface. The default setting is disabled.

Command	Command mode	Description
ip pim neighbor-addr <*IP address*> allow|deny	Interface IP	Allows or denies PIM access to the specified neighbor. You can configure a list of up to 72 neighbors that bypass the neighbor filter. After you configure the interface to allow a neighbor, you can configure the interface to deny the neighbor.
[no] ip pim neighbor-filter	Interface IP	Enables or disables the PIM neighbor filter on the interface. When enabled, this interface does not accept any PIM neighbors unless specifically permitted using the following command: **ip pim neighbor-addr <*IP address*>**
ip pim enable	Interface IP	Enables PIM on the interface.
no ip pim enable	Interface IP	Disables PIM on the interface.
show ip pim neighbor-filters	All	Displays the configured PIM neighbor filters.
show ip pim interface [<*interface number*>|detail]	All	Displays the current PIM interface parameters.

Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this paper.

IBM Redbooks

The following IBM Redbooks publications provide additional information about the topic in this document. Note that some publications referenced in this list might be available in softcopy only.

- *10 Gigabit Ethernet Implementation with IBM System Networking Switches*, SG24-7960
- *IBM BladeCenter Products and Technology*, SG24-7523
- *BNT 1/10Gb Uplink Ethernet Switch Module for IBM BladeCenter*, TIPS0705
- *BNT Virtual Fabric 10Gb Switch Module for IBM BladeCenter*, TIPS0708
- *IBM System Networking RackSwitch G8052*, TIPS0813
- *IBM System Networking RackSwitch G8124*, TIPS0787
- *IBM System Networking RackSwitch G8264/G8264T*, TIPS0815

You can search for, view, download, or order these documents and other Redbooks, Redpapers, web docs, draft and additional materials, at the following website:

ibm.com/redbooks

Other publications

These publications are also relevant as further information sources:

- *IBM 1/10 Gb Uplink Ethernet Switch Module for IBM BladeCenter Application Guide*:

  http://www-947.ibm.com/systems/support/supportsite.wss/docdisplay?brandind=5000008&lndocid=MIGR-5076214

- *IBM 1/10 Gb Uplink Ethernet Switch Module for IBM BladeCenter BBI Quick Guide*:

  http://www-947.ibm.com/systems/support/supportsite.wss/docdisplay?brandind=5000008&lndocid=MIGR-5076219

- *IBM 1/10 Gb Uplink Ethernet Switch Module for IBM BladeCenter Command Reference*:

  http://www-947.ibm.com/systems/support/supportsite.wss/docdisplay?brandind=5000008&lndocid=MIGR-5076525

- *IBM 1/10 Gb Uplink Ethernet Switch Module for IBM BladeCenter Installation Guide*:

  ftp://ftp.software.ibm.com/systems/support/system_x_pdf/dw1gymst.pdf

- *IBM 1/10 Gb Uplink Ethernet Switch Module for IBM BladeCenter ISCLI Reference*:

  http://www-947.ibm.com/systems/support/supportsite.wss/docdisplay?brandind=5000008&lndocid=MIGR-5076215

- *IBM BNT 10-Port 10Gb Ethernet Switch Module for IBM BladeCenter Installation Guide*:
  http://download.boulder.ibm.com/ibmdl/pub/systems/support/system_x_pdf/46m1525.pdf
- *IBM BNT RackSwitch G8052 Application Guide*:
  http://www-01.ibm.com/support/docview.wss?uid=isg3T7000353
- *IBM BNT RackSwitch G8052 Browser-Based Interface Quick Guide*:
  http://www-01.ibm.com/support/docview.wss?uid=isg3T7000348
- *IBM BNT RackSwitch G8052 Installation Guide*:
  http://www-01.ibm.com/support/docview.wss?uid=isg3T7000287&aid=1
- *IBM BNT RackSwitch G8052 ISCLI Command Reference*:
  http://www-01.ibm.com/support/docview.wss?uid=isg3T7000344
- *IBM BNT RackSwitch G8052 Menu-Based Command Reference*:
  http://www-01.ibm.com/support/docview.wss?uid=isg3T7000347
- *IBM BNT RackSwitch G8124/G8124E Application Guide*:
  http://www-01.ibm.com/support/docview.wss?uid=isg3T7000388
- *IBM BNT RackSwitch G8124/G8124E Browser-Based Interface Quick Guide*:
  http://www-01.ibm.com/support/docview.wss?uid=isg3T7000389
- *IBM BNT RackSwitch G8124/G8124E ISCLI Command Reference Guide*:
  http://www-01.ibm.com/support/docview.wss?uid=isg3T7000390
- *IBM BNT RackSwitch G8124/G8124E Menu-Based CLI Reference Guide*:
  http://www-01.ibm.com/support/docview.wss?uid=isg3T700039
- *IBM BNT RackSwitch G8124 Installation Guide*:
  https://www-304.ibm.com/support/docview.wss?uid=isg3T7000299&aid=1
- *IBM BNT RackSwitch G8264 Application Guide*:
  http://www-01.ibm.com/support/docview.wss?uid=isg3T7000326
- *IBM BNT RackSwitch G8264 Browser-Based Interface Quick Guide*:
  http://www-01.ibm.com/support/docview.wss?uid=isg3T7000342
- *IBM BNT RackSwitch G8264 Installation Guide*:
  https://www-304.ibm.com/support/docview.wss?uid=isg3T7000294&aid=1
- *IBM RackSwitch G8264 ISCLI Command Reference*:
  http://www-01.ibm.com/support/docview.wss?uid=isg3T7000329
- *IBM RackSwitch G8264 Menu-Based Command Reference Guide*:
  http://www-01.ibm.com/support/docview.wss?uid=isg3T7000328
- *IBM Virtual Fabric 10Gb Switch Module for IBM BladeCenter Application Guide*:
  http://download.boulder.ibm.com/ibmdl/pub/systems/support/system_x_pdf/bmd00189.pdf
- *IBM Virtual Fabric 10Gb Switch Module for IBM BladeCenter BBI Quick Guide*:
  http://download.boulder.ibm.com/ibmdl/pub/systems/support/system_x_pdf/bmd00192.pdf

- *IBM Virtual Fabric 10Gb Switch Module for IBM BladeCenter Command Reference*:

  http://download.boulder.ibm.com/ibmdl/pub/systems/support/system_x_pdf/bmd00190.pdf

- *IBM Virtual Fabric 10Gb Switch Module for IBM BladeCenter ISCLI Reference*:

  http://download.boulder.ibm.com/ibmdl/pub/systems/support/system_x_pdf/bmd00191.pdf

Online resources

These websites are also relevant as further information sources:

- IBM 1/10 Gb Uplink Ethernet Switch Module Announcement Letter:

  http://www.ibm.com/common/ssi/rep_ca/5/872/ENUSAG08-0365/ENUSAG080365.PDF

- IBM BladeCenter Information Center - Installing the 8740 or 8750 BladeCenter unit:

  http://publib.boulder.ibm.com/infocenter/bladectr/documentation/topic/com.ibm.bladecenter.8750.doc/bc_8750_iug.html

- IBM BladeCenter Information Center - Troubleshooting the 8740 or 8750 BladeCenter unit:

  http://publib.boulder.ibm.com/infocenter/bladectr/documentation/topic/com.ibm.bladecenter.8750.doc/bc_8750_pdsg.html

- IBM BladeCenter Information Center - Installing the BladeCenter unit:

  http://publib.boulder.ibm.com/infocenter/bladectr/documentation/topic/com.ibm.bladecenter.8852.doc/bc_8852_iug.html

- IBM BladeCenter Information Center - Troubleshooting the BladeCenter unit:

  http://publib.boulder.ibm.com/infocenter/bladectr/documentation/topic/com.ibm.bladecenter.8852.doc/bc_8852_pdsg.html

- IBM RackSwitch G8052 and G8264 Announcement Letter:

  http://www.ibm.com/common/ssi/cgi-bin/ssialias?infotype=AN&subtype=CA&appname=gpateam&supplier=872&letternum=ENUSAG11-0005&pdf=yes

- IBM RackSwitch G8124 Announcement Letter:

  http://www.ibm.com/common/ssi/cgi-bin/ssialias?infotype=AN&subtype=CA&appname=gpateam&supplier=899&letternum=ENUSLG11-0096&pdf=yes

- IBM Virtual Fabric 10 Gb Ethernet Switch Module Announcement Letter:

  http://www.ibm.com/common/ssi/rep_ca/5/872/ENUSAG09-0245/ENUSAG09-0245.PDF

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services

IP Multicast Protocol Configuration

Learn the basics of IP Multicast

See sample multicast networks

Learn command references

The most common transmission scheme used in networks today is unicast, which represents “one-to-one” transmission with one sender and one receiver.

Sometimes there is a need for one host to send packets that are received by multiple hosts. The problem with implementing this kind of transmission using unicast is that the stream of packets must be replicated as many times as there are receivers. IP Multicast addresses the problem by intelligently sending only one stream of packets and then replicating the stream when it reaches the target domain that includes multiple receivers or reaches a necessary bifurcation point leading to different receiver domains.

In this IBM Redpapers publication, we introduce principles of IP Multicast and describe the IPv4 addressing used for multicast. We discuss the protocols that are used to implement multicast in an IP network and then provide the general IP Multicast configuration procedures and then presents IP Multicast configuration in a sample network using IBM System Networking Ethernet Switches. We conclude this paper with command references that include all commands and their parameters for configuration of multicast protocols and features.

After understanding the basics of how to configure IP Multicast for the networking scenario described in this paper, IT network professionals will be able replicate a similar design and configuration to suit their network infrastructure.

REDP-4777-00

INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION

BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

For more information:
ibm.com/redbooks