Part No. 314719-B Rev 00
May 2003

4655 Great America Parkway
Santa Clara, CA 95054

Configuring IP Multicast Routing Protocols

Passport 8000 Series
Software Release 3.5

NORTEL NETWORKS™

Copyright © 2003 Nortel Networks

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks Inc.

The software described in this document is furnished under a license agreement and may be used only in accordance with the terms of that license. The software license agreement is included in this document.

Trademarks

Nortel Networks, the Nortel Networks logo, the Globemark, Unified Networks, and PASSPORT are trademarks of Nortel Networks.

Adobe and Acrobat Reader are trademarks of Adobe Systems Incorporated.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation.

IPX is a trademark of Novell, Inc.

The asterisk after a name denotes a trademarked item.

Restricted rights legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of conditions

In the interest of improving internal design, operational function, and/or reliability, Nortel Networks Inc. reserves the right to make changes to the products described in this document without notice.

Nortel Networks Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product may be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Nortel Networks Inc. software license agreement

This Software License Agreement (“License Agreement”) is between you, the end-user (“Customer”) and Nortel Networks Corporation and its subsidiaries and affiliates (“Nortel Networks”). PLEASE READ THE FOLLOWING CAREFULLY. YOU MUST ACCEPT THESE LICENSE TERMS IN ORDER TO DOWNLOAD AND/OR USE THE SOFTWARE. USE OF THE SOFTWARE CONSTITUTES YOUR ACCEPTANCE OF THIS LICENSE AGREEMENT. If you do not accept these terms and conditions, return the Software, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

“Software” is owned or licensed by Nortel Networks, its parent or one of its subsidiaries or affiliates, and is copyrighted and licensed, not sold. Software consists of machine-readable instructions, its components, data, audio-visual content (such as images, text, recordings or pictures) and related licensed materials including all whole or partial copies. Nortel Networks grants you a license to use the Software only in the country where you acquired the Software. You obtain no rights other than those granted to you under this License Agreement. You are responsible for the selection of the Software and for the installation of, use of, and results obtained from the Software.

1. Licensed Use of Software. Nortel Networks grants Customer a nonexclusive license to use a copy of the Software on only one machine at any one time or to the extent of the activation or authorized usage level, whichever is applicable. To the extent Software is furnished for use with designated hardware or Customer furnished equipment (“CFE”), Customer is granted a nonexclusive license to use Software only on such hardware or CFE, as applicable. Software contains trade secrets and Customer agrees to treat Software as confidential information using the same care and discretion Customer uses with its own similar information that it does not wish to disclose, publish or disseminate. Customer will ensure that anyone who uses the Software does so only in compliance with the terms of this Agreement. Customer shall not a) use, copy, modify, transfer or distribute the Software except as expressly authorized; b) reverse assemble, reverse compile, reverse engineer or otherwise translate the Software; c) create derivative works or modifications unless expressly authorized; or d) sublicense, rent or lease the Software. Licensors of intellectual property to Nortel Networks are beneficiaries of this provision. Upon termination or breach of the license by Customer or in the event designated hardware or CFE is no longer in use, Customer will promptly return the Software to Nortel Networks or certify its destruction. Nortel Networks may audit by remote polling or other reasonable means to determine Customer’s Software activation or usage levels. If suppliers of third party software included in Software require Nortel Networks to include additional or different terms, Customer agrees to abide by such terms provided by Nortel Networks with respect to such third party software.

2. Warranty. Except as may be otherwise expressly agreed to in writing between Nortel Networks and Customer, Software is provided “AS IS” without any warranties (conditions) of any kind. NORTEL NETWORKS DISCLAIMS ALL WARRANTIES (CONDITIONS) FOR THE SOFTWARE, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OF NON-INFRINGEMENT. Nortel Networks is not obligated to provide support of any kind for the Software. Some jurisdictions do not allow exclusion of implied warranties, and, in such event, the above exclusions may not apply.

3. Limitation of Remedies. IN NO EVENT SHALL NORTEL NETWORKS OR ITS AGENTS OR SUPPLIERS BE LIABLE FOR ANY OF THE FOLLOWING: a) DAMAGES BASED ON ANY THIRD PARTY CLAIM; b) LOSS OF, OR DAMAGE TO, CUSTOMER’S RECORDS, FILES OR DATA; OR c) DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS OR SAVINGS), WHETHER IN CONTRACT, TORT OR OTHERWISE (INCLUDING NEGLIGENCE) ARISING OUT OF YOUR USE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS, ITS AGENTS OR SUPPLIERS HAVE BEEN ADVISED OF THEIR POSSIBILITY. The forgoing limitations of remedies also apply to any developer and/or supplier of the Software. Such developer and/or supplier is an intended beneficiary of this Section. Some jurisdictions do not allow these limitations or exclusions and, in such event, they may not apply.

4. General

a. If Customer is the United States Government, the following paragraph shall apply: All Nortel Networks Software available under this License Agreement is commercial computer software and commercial computer software documentation and, in the event Software is licensed for or on behalf of the United States Government, the respective rights to the software and software documentation are governed by Nortel Networks standard commercial license in accordance with U.S. Federal Regulations at 48 C.F.R. Sections 12.212 (for non-DoD entities) and 48 C.F.R. 227.7202 (for DoD entities).

b. Customer may terminate the license at any time. Nortel Networks may terminate the license if Customer fails to comply with the terms and conditions of this license. In either event, upon termination, Customer must either return the Software to Nortel Networks or certify its destruction.

c. Customer is responsible for payment of any taxes, including personal property taxes, resulting from Customer's use of the Software. Customer agrees to comply with all applicable laws including all applicable export and import laws and regulations.

d. Neither party may bring an action, regardless of form, more than two years after the cause of the action arose.

e. The terms and conditions of this License Agreement form the complete and exclusive agreement between Customer and Nortel Networks.

f. This License Agreement is governed by the laws of the country in which Customer acquires the Software. If the Software is acquired in the United States, then this License Agreement is governed by the laws of the state of New York.

Contents

Figures

Tables

Preface

This manual describes all the multicast protocols that the 8000 Series switches support. It provides information about using both the Device Manager graphical user interface (GUI) and the command line interface (CLI) to perform general network management operations on a Passport* switch.

An 8000 Series switch has one of two types of modules installed in it: Passport 8100 modules or Passport 8600 modules. The Passport 8100 modules offer high-performance, low-cost, high-density switching. The Passport 8600 modules provide very high-speed packet forwarding combined with the ability to route Internet Protocol (IP) and Internetwork Packet Exchange (IPX*) Protocol traffic.

Before you begin

This guide is intended for network administrators with the following background:

- Basic knowledge of networks, Ethernet bridging, and IP routing
- Familiarity with networking concepts and terminology
- Basic knowledge of network topologies
- Experience with windowing systems or GUIs

Text conventions

This guide uses the following text conventions:

angle brackets (< >)	Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: If the command syntax is `ping <ip_address>`, you enter `ping 192.32.10.12`
`bold Courier text`	Indicates command names and options and text that you need to enter. Example: Use the **`dinfo`** command. Example: Enter **`show ip`** {**`alerts`**|**`routes`**}.
braces ({})	Indicate required elements in syntax descriptions where there is more than one option. You must choose only one of the options. Do not type the braces when entering the command. Example: If the command syntax is `show ip {alerts|routes}`, you must enter either `show ip alerts` or `show ip routes`, but not both.
brackets ([ ])	Indicate optional elements in syntax descriptions. Do not type the brackets when entering the command. Example: If the command syntax is `show ip interfaces [-alerts]`, you can enter either `show ip interfaces` or `show ip interfaces -alerts`.
ellipsis points (. . .)	Indicate that you repeat the last element of the command as needed. Example: If the command syntax is `ethernet/2/1 [<parameter> <value>]...`, you enter `ethernet/2/1` and as many parameter-value pairs as needed.

italic text	Indicates new terms, book titles, and variables in command syntax descriptions. Where a variable is two or more words, the words are connected by an underscore. Example: If the command syntax is `show at <valid_route>`, `valid_route` is one variable and you substitute one value for it.
`plain Courier text`	Indicates command syntax and system output, for example, prompts and system messages. Example: `Set Trap Monitor Filters`
separator (>)	Shows menu paths. Example: Protocols > IP identifies the IP command on the Protocols menu.
vertical line (|)	Separates choices for command keywords and arguments. Enter only one of the choices. Do not type the vertical line when entering the command. Example: If the command syntax is `show ip {alerts|routes}`, you enter either `show ip alerts` or `show ip routes`, but not both.

Hard-copy technical manuals

You can print selected technical manuals and release notes free, directly from the Internet. Go to the www.nortelnetworks.com/documentation URL. Find the product for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Use Adobe* Acrobat Reader* to open the manuals and release notes, search for the sections you need, and print them on most standard printers. Go to Adobe Systems at the www.adobe.com URL to download a free copy of the Adobe Acrobat Reader.

Note: The list of related publications for this manual can be found in the release notes that came with your software.

How to get help

If you purchased a service contract for your Nortel Networks product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

If you purchased a Nortel Networks service program, contact Nortel Networks Technical Support. To obtain contact information online, go to the www.nortelnetworks.com/cgi-bin/comments/comments.cgi URL, then click on Technical Support.

From the Technical Support page, you can open a Customer Service Request online or find the telephone number for the nearest Technical Solutions Center. If you are not connected to the Internet, you can call 1-800-4NORTEL (1-800-466-7835) to learn the telephone number for the nearest Technical Solutions Center.

An Express Routing Code (ERC) is available for many Nortel Networks products and services. When you use an ERC, your call is routed to a technical support person who specializes in supporting that product or service. To locate an ERC for your product or service, go to the http://www.nortelnetworks.com/help/contact/erc/index.html URL.

Chapter 1
IP Multicast concepts

IP Multicast extends the benefits of layer 2 multicasting on LANs to WANs. Multicasting techniques are used on LANs primarily to help clients and servers to find each other. IP Multicast enables a source to send information to multiple destinations in a WAN with a single transmission. The source enjoys considerable efficiencies while a significant amount of bandwidth can be saved.

This chapter discusses the following topics and includes IP Multicast protocols that the 8000 Series switches support:

Overview of IP Multicast

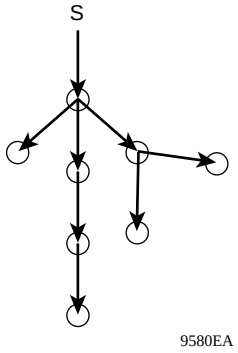
IP Multicast transmits messages to multiple recipients at the same time. This one-to-many delivery mechanism is similar to broadcasting, except multicasting transmits to specific groups and broadcasting transmits to everybody. Since multicast transmits only one stream of data to the network where it is replicated to many receivers, multicasting saves a considerable amount of bandwidth.

IP Multicast provides services such as the delivery of information to multiple destinations with a single transmission and the solicitation of servers by clients. IP Multicast services benefit applications such as video conferencing, dissemination of datagram information, and dissemination of mail or news to a large number of recipients.

Multicast protocols use different techniques to discover delivery paths.

A *Distribution Tree* is a set of multicast routers and subnetworks that allow the group's members to receive traffic from a source. The tree's source depends on the algorithm used by the multicast protocol. Figure 1 is an example of a simple distribution tree, where S is the multicast source and the arrows indicate the multicast broadcast procedure.

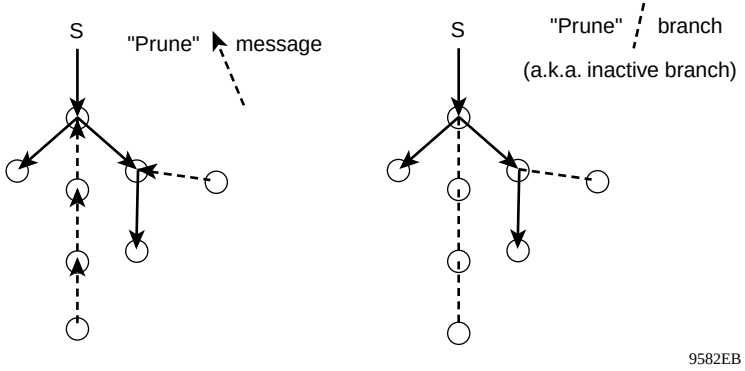
Figure 1 Multicast distribution tree and broadcasting



Broadcast and *prune* are methods to use multicast traffic to build the distribution tree. Periodically data is sent out or broadcast from the source to the extremities of the internetwork to search for active group members. If there are no local members of the group, the router sends a message to the host removing itself from the distribution tree, thus pruning the router.

Figure 2 illustrates how routers are pruned from the distribution tree. First a message is sent to the source, and then those routers do not receive multicast data.

Figure 2 Pruning routers from a distribution tree



Reverse path multicast is based on the concept that a multicast distribution tree should be built based on the shortest path from the source to each (sub) network containing active receivers. When a datagram arrives on an interface, the router determines the reverse path to the source of the datagram by examining the routing table of known network sources. If the datagram is not on the optimal delivery tree, it is discarded.

Multicast host groups and their group members enable the IP multicast router to transmit just to those groups interested in receiving the traffic. The Passport 8000 Series switches use the Internet Group Membership Protocol (IGMP) to learn the existence of host group members on their directly attached subnets. A router communicates with the hosts on a local network by sending IGMP queries. Hosts respond by issuing IGMP reports. For more information on host groups, see “Multicast host groups” on page 36 and “Multicast addresses” on page 37. For more information on IGMP, see “Internet Group Management Protocol (IGMP)” on page 39.

Multicast traffic forwarding transmits frames to all interfaces/subnets on which IGMP reports have been received for the multicast group indicated in the destination IP address. Multicast packets forwarded within the same VLAN remain unchanged. Packets are not forwarded to networks with no members of the multicast group indicated in the destination IP address.

Multicast host groups

IP Multicast is a method for addressing, routing, and delivering a datagram to a collection of receivers called a *host group*.

Host groups can be permanent or transient, with the following characteristics:

- A *permanent host group* has a well-known, administratively-assigned IP Multicast group address. This address is permanent and defines the group. A permanent host group can consist of zero or more members.
- A *transient host group* exists only as long as it has members that need its services. IP addresses in the multicast range that are not reserved for permanent groups are available for dynamic assignment to transient host groups.

Any host system on any IP network can send a message to a multicast group using the group's IP Multicast address. To receive a message addressed to a multicast group, however, the host must be a member of the group and must reside on a network where that group is registered with a local multicast router.

An IP Multicast host group can consist of zero or more members and places no restrictions on its membership. Host members can reside anywhere; they can join and leave the group at any time; and they can be members of more than one group at the same time.

In general, hosts that are members of the same group reside on different networks. However, a range of multicast addresses (224.0.0.*x*) is reserved for groups that are locally scoped. All message traffic for these hosts typically remains on the local network. Hosts that belong to a group in this address range and that reside in different networks do not receive each other's message traffic.

Note: In the 8000 Series switch, a special set of filters (global filters) can be applied to multicast packets. The user can create, deny or accept filters to configure which sources can receive and send data.

Multicast addresses

Each host group is assigned a unique multicast address. To reach all members of the group, a sender uses the multicast address as the destination address of the datagram.

An IP version 4 multicast address is a Class D address (the high-order bits are set to 1110) from 224.0.1.0 to 239.255.255.255. These addresses are assigned statically for use by permanent groups and dynamically for use by transient groups.

The block of addresses from 224.0.0.1 to 224.0.0.255 is reserved for routing protocols and other low-level protocols. Multicast routers do not forward datagrams with addresses in this range because the packet's Time to Live (TTL) is usually set to 1.

Multicast protocols

This chapter describes several protocols you can use to enable multicasting on an 8000 Series switch. These include:

- IP Multicast routers use Internet Group Management Protocol (IGMP) to learn the existence of host group members on directly attached subnets.
- Multicast Router Discovery Protocol (MRDP) discovers multicast routers in a layer 2 bridged domain configured for IGMP snooping.
- Distance Vector Multicast Routing Protocol (DVMRP) is a dense-mode protocol suitable for implementation in networks that are densely-populated by receivers.

- Protocol Independent Multicast (PIM)
  - — Sparse Mode (PIM-SM) protocol is suitable for implementation on networks that are sparsely populated by receivers.
  - — Source Specific Multicast (SSM) protocol uses a one-to-many model where members can only receive traffic from a single source. This is suitable for TV channels and other content-distribution applications.
- Pragmatic General Multicast (PGM) Protocol is suitable for multicast applications that require reliable, ordered, duplicate-free delivery of multicast traffic.

Static source groups

Static source groups (or static mroutes) enable you to configure **static** source-group entries in the DVMRP, PIM-SM or PIM-SSM multicast routing table. DVMRP and PIM cannot prune these entries from the distribution tree. In other words, even if there are no receivers for the group, the multicast stream for a static source-group entry stays active. Static forwarding entries are never pruned. When they are no longer needed, you should manually delete them.

To configure static source groups, you must first globally enable either DVMRP or PIM. If you disable DVMRP or PIM, the switch saves all of the configured static source-group entries and deactivates them. When you re-enable DVMRP or PIM, the switch re-activates the static source groups.

Static source groups ensure that the multicast route (mroute) records remain in the distribution tree. When receivers join the group, there is no delay in receiving multicast data because there is no need to graft onto the group or start a join process in the case of PIM. This is essential for applications where the multicast data must be sent to a receiver as soon as the receiver joins the group. For example, consider a case where a switch delivers TV channels to receivers. When the receiver turns the channel, which is equivalent to joining a group, the receiver should be able to view the channel immediately.

Static entries result in continuous traffic if the source is active, even when no receivers are present. However, traffic does not get forwarded by an 8000 Series switch with static entry if there are no receivers, but it gets forwarded continuously to the switch where the entry is programmed and crosses intermediate switches on the path.

Static source-group entries can be configured for a specific source or subnet. If several sources on the same subnet send traffic to the same group, traffic for all these sources will flow continuously when using the subnet configuration.

For information on configuring static source-groups using Device Manager, see "Configuring multicast static source groups" on page 240. For information on configuring static source-groups using the CLI, see "Configuring multicast static source groups" on page 467.

Internet Group Management Protocol (IGMP)

Internet Group Management Protocol (IGMP) has the following characteristics:

- IGMP allows a host to register group memberships with the local querier router to receive any datagrams sent to this router and targeted to a group with a specific IP Multicast address.
- IGMP allows a router to learn the existence of group members on networks to which it is directly attached. The router periodically sends a general query message to each of its local networks. Any host that is a member of any multicasting group identifies itself by sending a response.

IGMP is a protocol used by IP Multicast routers to learn the existence of host group members on their directly attached subnets. It allows hosts to communicate their desired group memberships to their local querier router, and to receive any datagrams sent to this router and targeted to a group with a specific IP Multicast address. A router communicates with the hosts on a local network by sending IGMP queries. Hosts respond by issuing IGMP reports.

IGMP queries

When there are multiple IGMP routers on a network, one router is elected to send queries. This elected querier periodically sends host membership queries (also known as general queries) to its attached local subnets. The 8000 Series switches support queries from all three versions of IGMP.

IGMP host reports

A host that receives a membership query from a local router can respond with a *host membership report*, one report for each joined multicast group. A host that receives a query delays its reply by a random interval and listens for a reply from any other host in the same host group. Consider a network that includes two host members — host A and host B — of the same multicast group. The router sends out a host membership query on the local network. Both host A and host B receive the query and listen on the network for a host membership report. Host B's delay timer expires first, so it responds to the query with a membership report. Hearing the response, host A does not send a report of its own for the same group.

Each query from a router to a host includes a Maximum Response Time field. IGMP inserts a value — *n* — into this field specifying the maximum time in tenths of a second within which the host must issue a reply. The host uses this value to calculate a random value between 0 and *n* tenths of a second for the period that it waits before sending a response.This is true for IGMP version 2 and version 3. For IGMP version 1, this field is set to 0 but defaults to a value of 100, that is, 10 seconds.

If at least one host on the local network specifies that it is a member of a given group the router will forward to that network all datagrams bearing the group's multicast address.

Upon initialization, the host may immediately issue a report for each of its supported multicast groups. The router accepts and processes these asynchronous reports the same way it accepts requested reports.

After hosts and routers are in a steady state, they communicate in a way that minimizes the exchange of queries and reports. The designated routers set up a path between the IP Multicast stream source and the end stations and periodically query the end stations about whether or not to continue participation. As long as any client continues to participate, all clients, including nonparticipating end stations on the switch port, receive the IP Multicast stream.

Host leave messages

When an IGMP version 2 host leaves a group and it was the host that issued the most recent report, it issues a *leave group message*. The multicast router on the network issues a group-specific query to determine whether there are other group members on the network. If no host responds to the query, the router assumes that no members belonging to that group exist on that interface.

Fast leave feature

The 8000 Series switches support a fast leave feature that is useful for multicast-based TV distribution applications. Fast leave relies on an alternative leave process in which the switch stops sending traffic for the group immediately after receiving a leave message, without issuing a query to check if other group members are present on the network. Fast leave alleviates the network from additional bandwidth demand when changing TV channels.

For information on configuring fast leave on an interface, port or VLAN, see "Configuring IGMP using Device Manager" on page 93 or "Configuring IGMP using the CLI" on page 265.

Fast leave mode

The Passport 8600 provides several fast leave processes for IP multicast:

- Immediate leave with one user per interface.
- Immediate leave with several users per interface.
- Standard IGMP leave based on a Last Member Query Interval (LMQI), which is configurable in tenths of seconds.

Fast leave modifies the IGMP leave processing mechanism on an IGMP interface. After receiving an IGMP leave on a fast leave-enabled interface, the switch does not send a group-specific query and will immediately stop sending traffic to the leaving member (IGMP host) port. Without fast leave, traffic will be forwarded until the group-specific query timed out. This wastes bandwidth if there is no receiver interested in the group traffic.

Fast leave mode provides two options of the fast leave mechanism - "single-user" mode and "multiple-users" mode.

- Single-user mode - In this mode, the port stops receiving traffic immediately after a group member on that port sends a leave. Nortel Networks recommends using the single-user mode when each switch interface port is connected to only one IGMP host
- Multiple-users mode - Use this mode if the switch interface port is connected to multiple IGMP hosts. In this case, the port stops receiving traffic after all members leave the IGMP group. The switch removes the leaving IGMP member and, if there are more group members on that port, the switch continues sending traffic to the port.

  When operating in multiple-users mode, the Passport 8600 switch must have the right membership information. To support this, multicast receivers on the same interface **cannot** use IGMP report suppression. If you have to use IGMP report suppression, Nortel Networks recommends not using this mode. Instead, you can use the LMQI (configurable in units of 1/10ths of seconds) to have a faster leave process while still sending group-specific queries after a leave message is received.

Fast leave mode applies to all fast leave-enabled IGMP interfaces.

Note: Fast leave mode applies only to fast-leave enabled IGMP interfaces. Although IGAP interfaces are always fast-leave enabled, they ignore this mode because they only operate in the multiple-user mode.

For information on configuring fast leave mode using Device Manager, see “Configuring fast leave mode” on page 97. For information on configuring fast leave mode using the CLI, see “Configuring fast leave mode” on page 282.

8000 Series implementation of IGMP

Multicast routing can be enabled and disabled on an interface basis. If multicast routing is disabled on an interface, IGMP queries are not generated. If the switch or interface is in IGMP router behavior mode i.e., DVMRP or PIM enabled, IGMP snooping is not configurable. The switch still learns the group membership and “snoops” multicast receivers on the switch vlan/ports.

IGMP snoop

The 8000 Series switch also provides IP multicast capability when used as a switch. Functioning as a switch, it supports all three versions of IGMP to prune group membership per port within a VLAN. This feature is called IGMP snoop.

Note: IGMP snoop can guarantee delivery only of local multicast data. In a VLAN with static IGMP receivers, multicast data from remote sources may not be delivered.

The IGMP snoop feature allows you to optimize the multicast data flow for a group within a VLAN to only those ports that are members of the group. The switch builds a database of group members by listening to IGMP reports from each port. It suppresses the reports heard by not forwarding them out to ports other than the one receiving the report, forcing the members to continuously send their own reports. The switch relays group membership from the hosts to the multicast routers. It forwards queries from multicast routers to all port members of the VLAN. Furthermore, it forwards multicast data only to the participating group members and to the multicast routers within the VLAN.

For information on configuring IGMP snoop using Device Manager, see "Enabling IGMP snooping on a VLAN" on page 101 and "Viewing IGMP snooping information" on page 108.

For information on configuring IGMP snoop using the CLI, see "Configuring IGMP on an interface" on page 275 or "Configuring IGMP on a VLAN" on page 307.

IGMP proxy

If an 8000 Series switch receives multiple reports for the same multicast group, it does not transmit each report to the multicast upstream router. Instead, the switch consolidates the reports into a single report and forwards it. If there is new information that another multicast group has been added or that a query has been received since the last report was transmitted upstream, then the report is forwarded onto the multicast router ports. This feature is known as IGMP proxy.

For information on configuring IGMP proxy using Device Manager, see "Configuring IGMP parameters on a VLAN" on page 98 and "Viewing IGMP snooping information" on page 108.

For information on configuring IGMP proxy using the CLI, see "Configuring IGMP on an interface" on page 275 or "Configuring IGMP on a VLAN" on page 307.

IGMP versions

The 8000 Series switches support IGMPv1, IGMPv2 and IGMPv2. The versions are backward compatible and they can all exist together on a multicast network. The following describes the main purpose for each version:

- IGMPv1 provides the support for IP multicast routing. IGMPv1 specifies the mechanism for communicating IP multicast group membership requests from a host to its locally attached routers. For more information, refer to RFC 1112.
- IGMPv2 extends the features in IGMPv1 by quickly reporting group membership termination to the routing protocol. This feature is important for multicast groups with highly volatile group membership. For more information, refer to RFC 2236.
- IGMPv3 supports the PIM Source-Specific Multicast (SSM) protocol. IGMPv3 provides the ability for a host to selectively request or filter traffic from individual sources within a multicast group. For more information, refer to IETF draft <draft-holbrook-idmr-igmpv3-ssm-02.txt>.

Multicast access control feature

Multicast access control is a set of features unique to the Passport 8600 and operate with standard existing multicast protocols. Multicast access control allows you to configure an IP multicast-enabled port or VLAN with an access control policy that consists of several IP multicast groups.

This feature is particularly useful when it is required to restrict access to certain multicast streams and protect multicast streams from spoofing (injecting data to the existing streams). For example, in a television distribution application, instead of applying a filter to each channel (multicast group), you apply a multicast access policy to a range of channels (groups), thereby reducing the total number of filters and allowing for a more simple, efficient and scalable configuration. Also, if you

want to add or remove television channels from a package, you modify the multicast access policy; you do not need to change filters for individual VLANs/ports. Multicast access policies contain an ID and a name (for example, PremiumChannels), the list of IP multicast addresses, and the subnet mask to be used.

It is important to note that multicast access control is not a regular filtering configuration and is specifically designed for multicast streams. It relies on handling multicast control and initial data to prevent hosts from sending or receiving specified multicast streams and it does not consume any filters. Also, multicast access control provides the ability to have a list of multicast groups in one configuration using the same routing policy prefix list configuration. For information about prefix lists, see *Configuring IP Routing Operations*. Multicast access control can be configured and changed dynamically in order to allow for the support of any changes in the configuration without having to restart any protocol. This allows you to change the access capabilities of a given user or service subscriber “on the fly.”

The following example describes a typical application:

Your local cable television company offers three packages; each one includes 35 channels (35 multicast groups). Each package is configured in an access control policy. That access policy is applied to a set of VLANs/ports to prevent users from viewing the channels on those VLANs. The same policy can be used to prevent users from sending traffic to those groups (also known as “spoofing”) by specifying the deny-tx option for that port. Once the packages are defined, you can use them for any access policy configuration. Also, you can easily change the package by changing the group range, without having to change all the port configurations.

The multicast access control functionality is applicable to any IP multicast application where controlling a user’s access is required. It can be used in financial-type applications and other enterprise applications, such as multicast-based videoconferencing.

Multicast access control policy types

There are six types of multicast access control policies:

- deny-tx
- deny-rx
- deny-both
- allow-only-tx
- allow-only rx
- allow-only-both

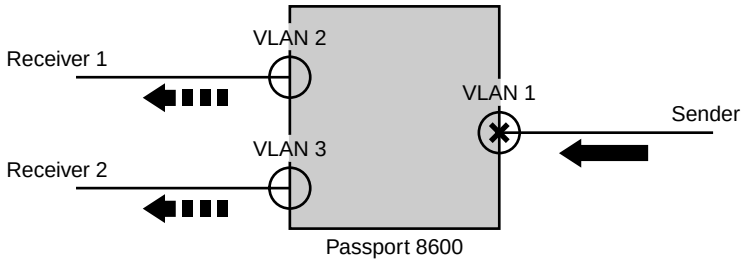
The “tx” policies control the sender and ingress interface for a group; the “rx” policies control the receivers and egress interface for a group

deny-tx

You use the deny-tx access policy to prevent a matching source from sending multicast traffic to the matching group on the interface where the deny-tx access policy is configured. You configure this policy on the ingress interface to the multicast source. The deny-tx access policy performs the opposite function of the allow-only-tx access policy. Therefore, the deny-tx access policy and the allow-only-tx access policy cannot exist on the same interface at the same time.

For example, in the following diagram, a deny-tx access policy is configured on VLAN 1 (the ingress VLAN to the Passport 8600). The deny-tx access policy prevents multicast traffic sent by Sender from being forwarded from VLAN 1 to any receiver, consequently preventing Receiver 1 and Receiver 2 from receiving data from the multicast group. The deny-tx policy allows you to create “receive only” VLANs, such as VLAN 1.

Figure 3 Data flow using deny-tx policy

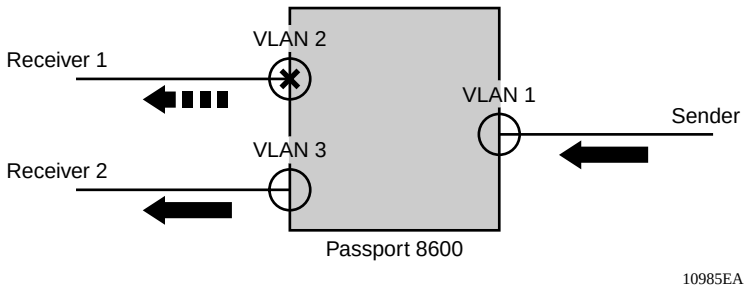


deny-rx

You use the deny-rx access policy to prevent a matching group from receiving IGMP reports from the matching receiver on the interface where the deny-rx access policy is configured. The deny-rx access policy performs the opposite function of the allow-only-rx access policy. Therefore, the deny-rx access policy and the allow-only-rx access policy cannot exist on the same interface at the same time.

For example, in the following diagram, a deny-rx access policy is configured on VLAN 2, preventing IGMP reports sent by Receiver 1 from being received on VLAN 2. The deny-rx policy allows you to deny a multicast group access to a specific VLAN or receiver.

Figure 4 Data flow using deny-rx policy

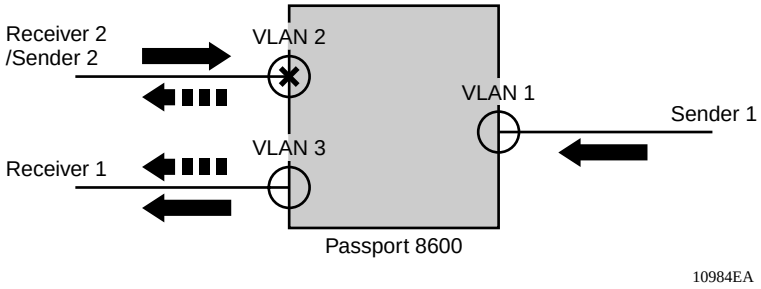


deny-both

You use the deny-both access policy to prevent a matching IP address from both sending multicast traffic to and receiving IGMP reports from a matching receiver on an interface where the deny-both policy is configured. This policy can be used to eliminate all multicast activity for a receiver or source in a specific multicast group. The deny-both access policy performs the opposite function of the allow-only-both access policy. Therefore, the deny-both access policy and the allow-only-both access policy cannot exist on the same interface at the same time.

For example, in the following diagram, a deny-both access policy is configured on VLAN 2, preventing IGMP reports sent by Receiver 2 from being received by VLAN 2, and preventing multicast traffic sent by Sender 2 from being forwarded from VLAN 2. The deny-both policy allows you to prevent certain VLANs from participating in any activity involving the specified multicast groups.

Figure 5 Data flow using deny-both policy



allow-only-tx

You use the allow-only-tx policy to allow only the matching source to send multicast traffic to the matching group on the interface where the allow-only-tx policy is configured. All other multicast data received on this interface is discarded. The allow-only-tx access policy performs the opposite function of the deny-tx access policy. Therefore, the allow-only-tx access policy and the deny-tx access policy cannot exist on the same interface at the same time.

allow-only-rx

You use the allow-only-rx policy to allow only the matching group to receive IGMP reports from the matching receiver on the interface where the allow-only-rx access policy is configured. All other multicast data received on this interface is discarded. The allow-only-rx access policy performs the opposite function of the deny-rx access policy. Therefore, the allow-only-rx access policy and the deny-rx access policy cannot exist on the same interface at the same time.

allow-only-both

You use the allow-only-both policy to allow only the matching IP address to both send multicast traffic to and receive IGMP reports from the matching receiver on an interface where the allow-only-both access policy is configured. All other multicast data and IGMP reports received on this interface are discarded. The allow-only-both access policy performs the opposite function of the deny-both access policy. Therefore, the allow-only-both access policy and the deny-both access policy cannot exist on the same interface at the same time.

Specifying host addresses and masks

When configuring multicast access policies, you must specify the host (IP) address and host (subnet) mask of the host that's being filtered (that is, the host that's sending multicast traffic).

You can use the host subnet mask to restrict access to a portion of the host's network. For example, when the host subnet mask is configured as 255.255.255.255, the full host address is used. To restrict access to a portion of the host's network, use a subnet mask such as 255.255.255.0. Access control is then applied to the specified subnet only.

For information on configuring multicast access control using Device Manager, see "Configuring multicast access control" on page 113. For information on configuring multicast access control using the CLI, see "Configuring multicast access control for an IGMP interface" on page 284.

Multicast stream limitation feature

The multicast stream limitation feature allows you to limit the number of multicast groups that can join a VLAN. By limiting the number of concurrent multicast streams, a service provider can, for example, protect the bandwidth on a specific interface and control access to multicast streams.

This feature can be used in any environment where users should not be getting more than a certain number of multicast streams simultaneously. For example, a TV service provider can limit the number of TV channels a user can watch at any given time. (To a TV service provider, a multicast stream is synonymous with a TV channel.) If a user has a service contract for two TV sets, the user can have two channels flowing at the same time, but is not allowed to get a third channel. This allows the service provider to control the bandwidth usage in addition to preventing users from watching more than the allowed number of channels at a given point in time.

There are several ways to enable the multicast stream limitation feature on the Passport 8600:

- per interface - This limitation controls the total number of streams for all clients on this interface.
- per interface port - This limitation controls the number of streams for all clients on this interface port.
- per Ethernet port - This limitation controls the number of streams for all clients on this Ethernet port.
- per VLAN - This limitation controls the total number of streams for all clients on this VLAN. This is equivalent to the interface stream limitation.
- per VLAN port - This limitation controls the number of streams for all clients on this VLAN port. This is equivalent to the per interface port stream limitation.

The maximum number of streams for each limit can be set independently. Once the stream limit is met, any additional join reports for new streams are dropped.

For information on configuring multicast stream limitation using Device Manager, see “Configuring multicast stream limitation” on page 124. For information on configuring multicast stream limitation using the CLI, see “Configuring multicast stream limitation” on page 319.

Multicast Router Discovery Protocol (MRDISC)

The Multicast Router Discovery Protocol (MRDISC) enables the automatic discovery of multicast capable routers. By listening to multicast router discovery messages, layer 2 devices can determine where to send multicast source data and IGMP host membership reports. This feature is useful in a layer 2 bridging domain that is configured for IGMP snooping.

IGMP multicast router discovery consists of three message types that discover multicast routers on the network. The three message types are:

- Multicast router advertisements are sent by routers to advertise that IP Multicast forwarding is enabled on an interface.
- Multicast router solicitations are sent by routers to solicit multicast router advertisements.
- Multicast router termination messages are sent when a router terminates its multicast routing functions.

Multicast routers send multicast router advertisements periodically on all interfaces on which multicast forwarding is enabled. Advertisements are also sent in response to multicast router solicitations which are sent to solicit a response of multicast router advertisements from all multicast routers on a subnet.

Multicast router solicitations are sent to the IGMP-MRDISC all-routers multicast group which has a multicast address of 224.0.0.2. Multicast router solicitations are sent whenever a router wishes to discover multicast routers on a directly attached subnet.

Multicast router termination messages are sent when a router terminates its multicast routing functions. Other non-IP forwarding devices, such as layer 2 switches, may send multicast router solicitations to solicit multicast router advertisements.

When you enable IGMP snooping on an 8000 Series switch, MRDISC is enabled by default.

Note: The Multicast Router Discovery protocol is not supported on brouter ports.

For information on configuring MRDISC using Device Manager, see "Viewing multicast router discovery information" on page 106. For information on configuring MRDISC using the CLI, see "Configuring IGMP multicast router discovery options" on page 288 and "Configuring IGMP multicast router discovery on a VLAN" on page 315.

Distance Vector Multicast Routing Protocol (DVMRP)

Distance Vector Multicast Routing Protocol (DVMRP) is a distance vector type of multicast routing protocol. It advertises shortest-path routes to multicasting *source networks* — that is, any network containing hosts that have the capability to issue multicast datagrams. In this respect, DVMRP is the opposite of RIP, which advertises all routes to destination networks. Coupled with IGMP, membership for a multicast stream is learned from both the routers and directly attached hosts.

DVMRP constructs a different distribution tree for each source and its destination host group. The distribution tree provides a shortest path between the source and each multicast receiver in the group, based on the number of hops in the path. A tree is constructed on demand, using a broadcast and prune technique, when a source begins to transmit messages to a multicast group.

DVMRP assumes that initially every host on the network is part of the multicast group. The designated router on the source subnet (the router that has been selected to handle routing for all hosts on the subnet) begins transmitting a multicast message to all adjacent routers. Each of these routers then selectively forwards the message to downstream routers until the message is eventually passed to all multicast group members.

This section discusses the following topics:

Reverse path forwarding

In the selective forwarding process during the formation of the multicast tree, when a router receives a multicast stream, it checks its DVMRP routing tables to determine the interface that provides the shortest path back to the source. If that was the interface over which the multicast stream arrived, the router enters state information to identify the multicast stream and its source in its internal tables and forwards the multicast message to all adjacent routers except to the ones that are on the same interface. If the interface was not the optimal one receiving the multicast stream, the stream is discarded. This mechanism, called reverse path forwarding, ensures that there are no loops in the tree and that the tree includes the shortest path from the source to all recipients.

Pruning and grafting

Pruning eliminates branches of the distribution tree that do not lead to any multicast group members. The IGMP running between hosts and their immediately neighboring multicast routers is used to maintain group membership data in the routers. When a router determines that no hosts beyond it belong to the multicast group, it sends a prune message to its upstream router. Routers update source and destination group state information in their tables to reflect which branches are eliminated from the tree, resulting in a minimum multicast tree. If a router later learns of new group memberships from the hosts or downstream routers, it sends a graft message upstream to retract the prune sent earlier.

After the multicast tree is constructed, it is used to transmit multicast messages from the source to multicast members. Each router in the path forwards messages over only those interfaces that lead to group members. Because new members can join the group at any time and these members may depend on one of the pruned branches to receive the transmission, DVMRP periodically re-initiates the construction of the multicast tree.

DVMRP concepts and terminology

DVMRP is a multicasting protocol that provides a mechanism for routers to propagate multicast datagrams in a manner that minimizes the number of excess copies sent to any particular network.

Neighbor connections

In a DVMRP environment, *neighbors* are multicasting routers that have an interface to the same network.

At startup, a DVMRP multicasting router performs the following tasks:

- Initializes its routing table with information on all of its local networks
- Learns the existence of its neighbors by sending a probe for all routes on each of its multicast interfaces
- Receives reports from its neighbors containing the routing information (including route costs)

Source route advertisements

A *source network* is any network containing hosts that have the capability to issue multicast datagrams. DVMRP advertises shortest-path routes to multicasting source networks. In this respect, DVMRP is the opposite of RIP, which advertises routes to destination networks.

Periodically, each multicasting router issues full or partial routing information on each DVMRP circuit using DVMRP report messages. This routing information represents the sending router's cost to reach the specified source network. The cost is the sum of the hop metrics along the shortest path to the given source network.

Upon receiving a DVMRP report from another router, DVMRP reexamines its routing table to determine whether the shortest path information needs updating. Specifically, DVMRP looks in the routing table for an entry describing a route to the same source network. If one exists, DVMRP compares the cost of the two routes and stores the route with the lower cost in its routing table.

A router does not send route reports on an interface until it knows (by means of received probes or reports) that it has a neighboring multicast router on that interface. The 8000 Series switch acknowledges implicit probes from neighboring multicast routers, and it sends probes periodically on an interface.

How DVMRP chooses a route

Each DVMRP interface is configured with a metric that indicates the cost of the hop. A router that receives multiple route reports for the same multicasting source network performs the following tasks:

- Compares the cost specified in each route report (based on the metric field)
- Stores information from the report with the lowest cost in its routing table

A route metric is the sum of all the interface (hop) metrics from a given route source to a given router. After a next-hop neighbor has been declared for a route, the route updates received from that neighbor for that route take precedence until either the route times out or another router advertises a better metric for that route.

Routing table

Table 1 shows the principal items in a routing table entry.

Table 1 Parts of a routing table entry

Item	Description
Source subnet address and mask	The network address and mask that identify the source for which this entry contains multicast routing information
Upstream neighbor	The address of the upstream neighbor from which multicast datagrams are received
Interface	The value of the interface index on which IP datagrams sent by these sources are received
Metric	The distance in hops to the source subnet
Expiration Time	The maximum amount of time (in time ticks) remaining before this entry will be aged out

Note that the source subnet and the previous-hop router in the DVMRP routing table are the opposite of the destination subnet and next-hop router in a RIP routing table.

Using this information, the router performs the following tasks:

- Receives a multicast datagram and determines whether the datagram has arrived on the interface that is on the shortest path to the source network
- Drops the datagram if it has not arrived on the shortest-path interface
- Floods the multicast stream to all active, non-pruned, downstream DVMRP neighbors

Shortest-path trees

Route information used by DVMRP is independent of any other routing information used by the router. The purpose of this routing information is to create a shortest-path tree entry in the routing table for the propagation of multicast datagrams.

The shortest-path tree entry indicates the interface that provides the shortest path to the network that is the source of the multicast datagram. A shortest-path tree also indicates those interfaces that are on the shortest path to that source network from a neighboring router.

In IGMP version 2, neighboring routers have the same metric to a given source network.The router with the lower IP address is responsible for propagating multicast traffic originating from that source network onto the network or tunnel that is common to these neighboring routers.

A network is considered a leaf network if it has no dependent downstream neighbors for a source.

DVMRP static source groups

Static source groups (or static mroutes) enable you to configure **static** source-group entries in the DVMRP multicast routing table. DVMRP cannot prune these entries from the distribution tree. For more information about static source groups, see “Static source groups” on page 38.

DVMRP routing policies

DVMRP routing policies allow you to improve the management of the DVMRP routing tables by providing control of how the routing table is populated and how the routes are exchanged between 8000 series switches. These routing policies, when enabled, can be applied to an interface that can be either a VLAN or a brouter port.

Default route policy

DVMRP uses a default route to summarize routes in the routing table in an effort to reduce the size of the routing table, which is particularly useful for the edge switches in your network. Default route policies allow DVMRP to:

- **Listen for a default route**—you can enable or disable a switch to listen for a default route; the 8000 series switch is configured by default to listen for the default route.
- **Advertise a default route**—you can enable or disable a switch to advertise a default route; the 8000 series switch is configured by default to advertise a default route if the route exists in the routing table.
- **Supply a default route**—you can configure an interface to supply a default route, where the default route is generated and advertised. In this case, the default route is not added to the routing table but used by a neighbor switch as a path from which all unknown source addresses are accepted.

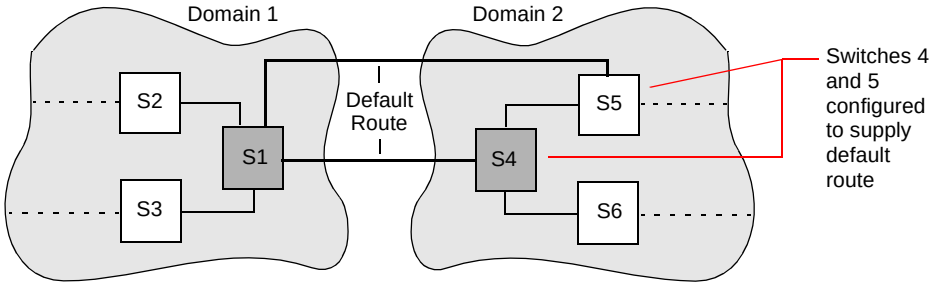
When supplying a default route, you must consider the following:

- You can set the Passport 8000 switch to advertise a default route only if that switch is not enabled to listen for the default route.
- When you configure an interface to supply a default route, it does not advertise any other route to neighbors.
- The Passport 8000 switch does not listen for default route on an interface that is configured to supply default route.

Configuration example

Figure 6 shows a network with two domains that include multiple switches. In this configuration, switch 1 (S1) is an edge switch that connects only to S4 and S5 in a different domain. S4 and S5 are configured to supply default routes to S1. The metrics for these switches are set as 1 hop for S1 and 2 hops for S5. S4 and S5 will not advertise any other route to S1 because they are configured to supply the default route. In this case, the default route is not added to the S4 and S5 routing tables because the default supply is enabled on the interface.

Figure 6 Default route configuration example



In this example, one default route only can be active at a time; therefore, there is no load sharing on the links. In addition, there may be cases where a non-optimal path is taken to reach S1 from a switch in the other domain. By default, the other switches in the domain that includes S1 will get the default route advertised by S1 as any other regular route and there are no exceptions as none of the switches are configured with a supply default route policy. These switches can be set to not accept the route, if required.

All the switches with a default route in their routing table will accept traffic on the interface where they learned the default route from any source that is unknown to them.

You can simplify the configuration shown in Figure 6. In the simplified configuration, S1 has only one link to domain 2 and S4 is configured to supply a default route to S1. In this configuration, S1 accepts all multicast traffic from domain 2 on that interface.

Refer to Figure 8 on page 61 and Figure 10 on page 63 for configuration examples that show the application of the DVMRP announce and accept policies to the same network configuration shown in Figure 6 on page 58.

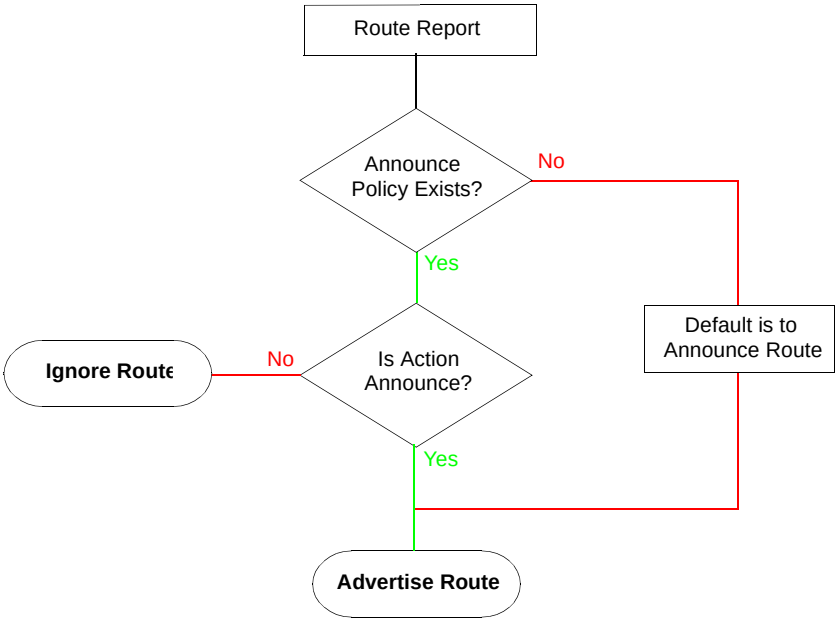
Announce policy

A DVMRP announce policy (out filter) governs the propagation of DVMRP routing information. Use DVMRP announce policies to control what routes are sent to neighboring routers to reduce the size of routing tables or provide a level of security for the network.

The announce policies are applied to the outgoing advertisements to the other neighbors/peers in the protocol domain. These policies determine whether or not to announce specific route information. Announce policies allow you to selectively announce routes. You can configure a policy to apply to any route. If there is no policy configured or no matching policy for a given route, then the default configuration enables the switch to accept the route. If there is no policy configured or no matching policy for a route, then the default behavior is to announce the route.

Figure 7 shows how an outgoing route is handled when a DVMRP announce policy does or does not exist on a switch.

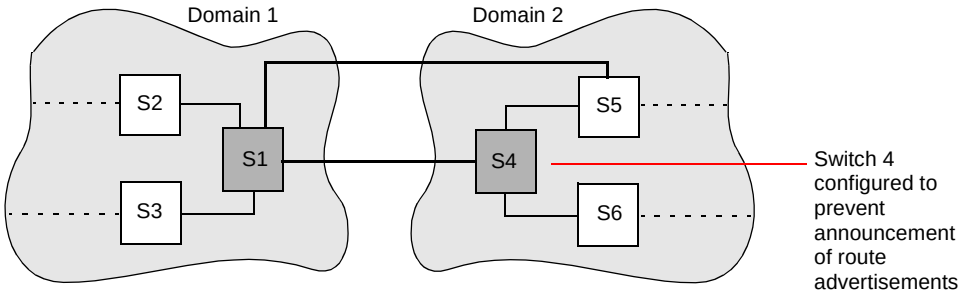
Figure 7 DVMRP announce policy logic



Configuration example

Figure 8 provides an example of an announce policy communication that takes place between two different domains that include multiple switches. In this example, S1 is an edge switch that connects only to S4 and S5, which are located in a different domain. S4 is configured so that it will not announce routing information. The result and benefit of this configuration is that the local switch (S4) will not send route advertisements to the other switches in the network; therefore, reducing the size of the routing stable and providing a level of security for the network

Figure 8 Announce policy configuration example



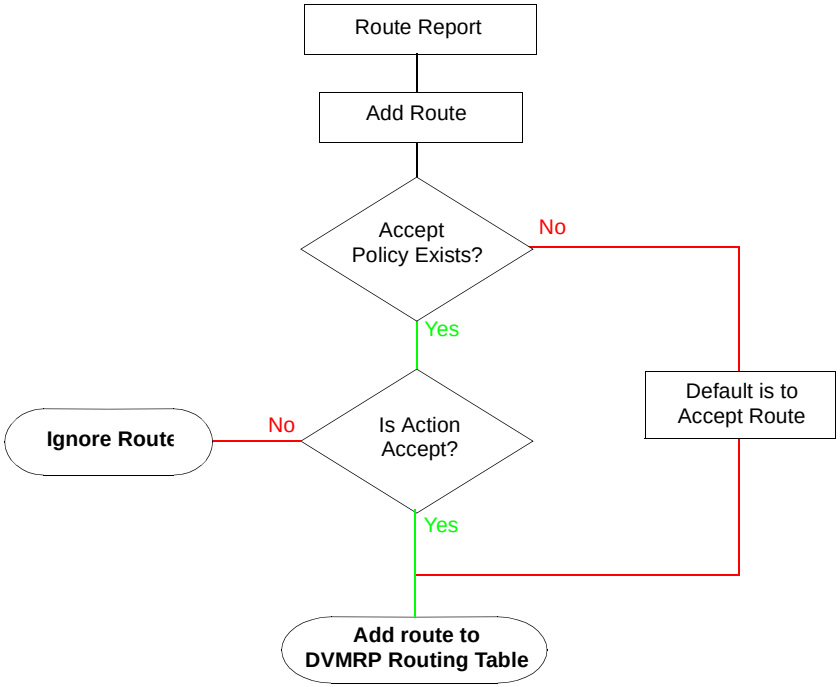
Accept policy

A DVMRP accept policy (in filter) is required to control the way DVMRP manages incoming routes advertisements. Accept policies apply to incoming advertisements and allow users to reduce the size of the DVMRP routing table. For example, an edge switch can be configured to use a default route and not to accept any route; therefore, reducing the size of its routing table (the routing table includes only the default and local routes). In this case, this switch can still advertise all of its routes to the rest of the network.

Accept policies allow injecting routes into the DVMRP routing table and can be applied to a single or all interfaces of a switch. These policies allow you to selectively accept routes and you can configure a policy to apply for any route. If there is no policy configured or no matching policy for a given route, then the default configuration enables the switch to accept the route.

Figure 9 shows how an incoming route is handled when a DVMRP accept policy is or is not enabled on your switch.

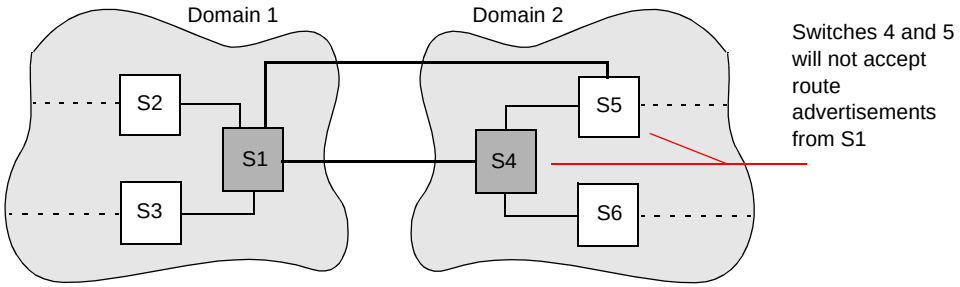
Figure 9 DVMRP accept Policy logic



Configuration example

Figure 10 provides an example of an accept policy communication that takes place between two different domains that include multiple switches. In this example, S1 is an edge switch that connects only to S4 and S5, which are located in a different domain. S4 and S5 are configured so that they will not accept routing information from S1. The result and benefit of this configuration is that the switches in domain 2 will not receive routing information from domain 1, therefore reducing the size of the their routing tables and providing a level of security for the network. S4 and S5 will however, advertise routing information to S1. Therefore, switches in domain 1 will receive the routing information from domain 2.

Figure 10 Accept policy configuration example



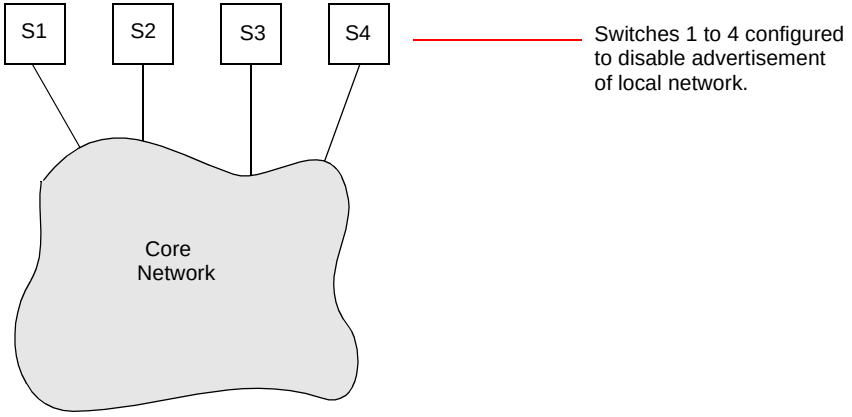
Advertisement of local networks policy

By default, DVMRP advertises its own local networks over an interface. With the advertisement of local networks policy, you can configure an interface to omit the advertisement of local routes to other switches in your network. This policy allows for the reduction of the size of routing table and provides a level of security where multicast traffic on interface will not get routed to other interfaces in the network; however, the interface will still receive multicast traffic from the other interfaces in the network.

Configuration example

Figure 11 provides an example of how the advertisement of a local networks policy is applied to switches communicating with a core network. In this example, there are four switches with several interfaces that contain receivers (such as a television) that communicate with devices in the core network. The switches are configured so that they disable the advertisement of their local network which means the switch will only receive (not supply) multicast traffic. The result and benefit of this configuration allow the switches to maintain smaller routing tables.

Figure 11 Advertisement of local networks policy configuration example



DVMRP passive interface policy

The DVMRP passive interface policy feature allows you to configure multiple DVMRP interfaces on an 8000 switch without affecting the performance of the switch. The DVMRP passive interface policy allows you to configure an interface as passive or active. When you configure an interface as passive, it drops all types of incoming DVMRP packets from neighbors and will not send out any probes or route reports to its neighbor switches. When you configure a DVMRP interface as passive, you can only change the interface type if the interface is disabled.

For information on configuring routing policies using Device Manager, see "Configuring DVMRP routing policies" on page 150. For information on configuring routing policies using the CLI, see "Configuring DVMRP routing policies" on page 348.

8000 Series implementation of DVMRP

DVMRP in 8000 Series switches fully supports multiaccess networks. The forwarding entries for the receivers on multiaccess networks are port based rather than network based. Therefore, on a multiaccess network, data will not be received by any ports other than the ones interested in the data. That is, IP Multicast routing is supported on ports with port-based or IP subnet-based VLANs enabled.

The DVMRP router listens to all IGMP host membership reports even if it is not the designated querier and keeps a local group database of every host membership reporter.

When a multicast stream of UDP packets first enters the switch, if DVMRP is enabled for the interface, then DVMRP processes this packet as necessary and creates a hardware cache entry to handle subsequent packets in the same stream for the same multicast destination. The packets are discarded if there are no members; otherwise they are forwarded.

The 8000 Series implementation does not support DVMRP tunneling.

Protocol Independent Multicast-Sparse Mode (PIM-SM)

Protocol Independent Multicast-Sparse Mode (PIM-SM), as defined in RFC 2362, was designed to support multicast groups spread out across large areas of a company or the Internet. Unlike dense mode protocols, such as DVMRP, that initially flood multicast traffic to all routers over an entire internetwork, PIM-SM sends multicast traffic only to routers that have specifically joined a multicast group. This technique reduces traffic flow over WAN links and overhead costs for processing unwanted multicast packets.

Dense-mode protocols use a “flood-and-prune” technique, which is efficient where receivers are densely populated. However, for sparsely populated networks, PIM-SM is more efficient because it sends multicast traffic only to those routers that belong to a specific multicast group and that choose to receive the traffic.

PIM-SM is independent of any specific unicast routing protocol, but it does require the presence of a unicast routing protocol, such as RIP or OSPF. PIM-SM uses the information from the unicast routing table to create and maintain multicast trees that enables PIM-enabled routers to communicate.

PIM-SM concepts and terminology

Typically, a PIM-SM network consists of several multipoint data streams, each targeted to a small number of LANs in the internetwork. For example, customers whose networks consist of multiple hosts on different LANs can use PIM-SM to simultaneously access a video data stream, such as a video teleconference, on a different subnet.

Note: In some cases, PIM stream initialization can take several seconds.

Hosts

A host can be a source, a receiver, or both.

- A *source*, also known as a *sender,* sends multicast data to a multicast group.
- A *receiver* receives multicast data from one or several sources sending data to a multicast group.

PIM-SM domain

PIM-SM operates in a domain of contiguous routers that have PIM-SM enabled. These routers are all configured to operate within a common boundary defined by PIM Multicast Border Routers (PMBRs).

Each PIM-SM domain requires the following routers:

- Designated router (DR)
- Rendezvous-point (RP) router
- Bootstrap router (BSR)

Although a PIM-SM domain can have only one active RP router and one active BSR, you can configure additional routers as candidate RP routers and as candidate BSRs. Candidate routers provide backup protection in case the primary RP or BSR router fails.

Designated router (DR)

The *designated router* (DR) is the router with the highest IP address on a LAN designated to perform the following tasks:

- Sends register messages to the rendezvous-point (RP) router on behalf of directly connected sources.
- Sends join/prune messages to the RP router on behalf of directly connected receivers.
- Maintains information about the status of the active RP router for local sources in each multicast group.

Note: The DR is not a required configuration and switches act automatically as such for directly attached sources and receivers.

Rendezvous-Point (RP) router

PIM-SM builds a shared multicast distribution tree within each domain, and the *rendezvous point* (RP) is at the root of this shared tree. Although the RP can be physically located anywhere on the network, it should be as close to the source as possible. There is only one active RP router for a multicast group.

The RP router is where receivers meet new sources. Sources use the RP to identify themselves to other routers on the network; receivers use the RP to learn about new sources.

The RP performs the following tasks:

- Registers a source that wants to announce itself and send data to group members
- Joins a receiver that wants to receive data for the group
- Forwards data to group

Candidate rendezvous-point router

You can configure a set of routers as candidate rendezvous-point (C-RP) routers that serve as backup to the RP router. If an RP fails, all the routers in the domain apply the same algorithm to elect a new RP from the group of C-RPs. To make sure that the routers have a complete list of C-RPs, the C-RP periodically sends unicast advertisement messages to the bootstrap router (BSR). The most common implementation is to configure a PIM-SM router as both a candidate RP and a candidate BSR.

Note: Although you can configure a candidate RP on a DVMRP interface, there is no functionality tied to this configuration.

Static rendezvous point router

Static RP enables you to configure a static entry for a rendezvous point (RP). This feature avoids the process of selecting an active RP from the list of candidate RPs and dynamically learning about RPs through the BSR mechanism. Static RP-enabled switches cannot learn about RPs through the BSR because the switch loses all dynamically-learned BSR information and ignores BSR messages. When you configure static RP entries, the switch adds them to the RP-set as if they were learned through the BSR.

Note: In a PIM domain with both static and dynamic RP switches, the static RP switches cannot have one of their (local) interfaces configured as RP.

Static RP-enabled 8000 Series switches can communicate with switches from other vendors that do not use the BSR mechanism. Some vendors use either early implementations of PIM-SM v1 that do not support the BSR or proprietary mechanisms like the Cisco Auto-RP. For a network to work properly with static RP, you must have all the switches in the network (including switches from other vendors) map to the same RP or RPs, if several RPs are present in the network.

To avoid a single point of failure, you can also configure redundant static RPs for those RPs that are configured as redundant.

The static RP feature can also be used when dynamic learning mode is not needed, typically in small networks or for security reasons, where RPs have to be forced to some devices in the network so that they will not learn other RPs.

Bootstrap router

The BSR receives RP router advertisement messages from the candidate RPs. The BSR adds the RP router with its group prefix to the RP set. Only one BSR exists for each PIM-SM domain.

The BSR periodically sends bootstrap messages containing the complete RP set to all routers in the domain. The BSR ensures that all PIM-SM routers learn to which RP router to send join/prune and register packets.

Candidate bootstrap router

Within a PIM-SM domain, you can configure a small set of routers as candidate BSRs (C-BSRs). The candidate BSR with the highest configured priority becomes the BSR for the domain. If two candidate BSRs have equal priority, the candidate with the higher IP address becomes the BSR. If you add a new candidate BSR with a higher priority to the domain, it automatically becomes the new BSR.

For information on configuring a candidate BSR using Device Manager, see "Configuring a candidate bootstrap router (C-BSR)" on page 194. For information on configuring a candidate BSR using the CLI, see "Configuring a candidate BSR on an interface" on page 400, "Configuring a candidate BSR on an Ethernet port" on page 413 or "Configuring a candidate BSR on a VLAN" on page 418.

Join/prune messages

The DR sends *join/prune* messages from a receiver toward a group's RP to either join the shared tree or remove (prune) a branch from it. A single message contains both a join and a prune list. This list includes a set of source addresses indicating the shortest-path trees or the shared trees that the host wants to join. The DR sends join and prune messages hop by hop to each PIM router on the path to the source or the RP.

Register and register-stop messages

The DR sends *register* messages to the RP for a directly connected source. The register message informs the RP of a new source, causing the RP to send join/prune messages back toward the source's DR and forwards the data down the RP tree after it gets the data natively. When the receiver DR gets the first packet, it switches to the shortest-path tree (SPT) and continues receiving data through the SPT path.

The DR stops sending encapsulated packets to the RP after receiving a *register-stop* message. This traffic stops without any delay because the RP sends a register-stop message immediately after receiving the first multicast data packet, and joins the shortest-path tree.

Shared trees and shortest-path trees

In a PIM-SM domain, shared trees and shortest-path trees are used to deliver data packets to group members. This section describes both trees.

Shared trees

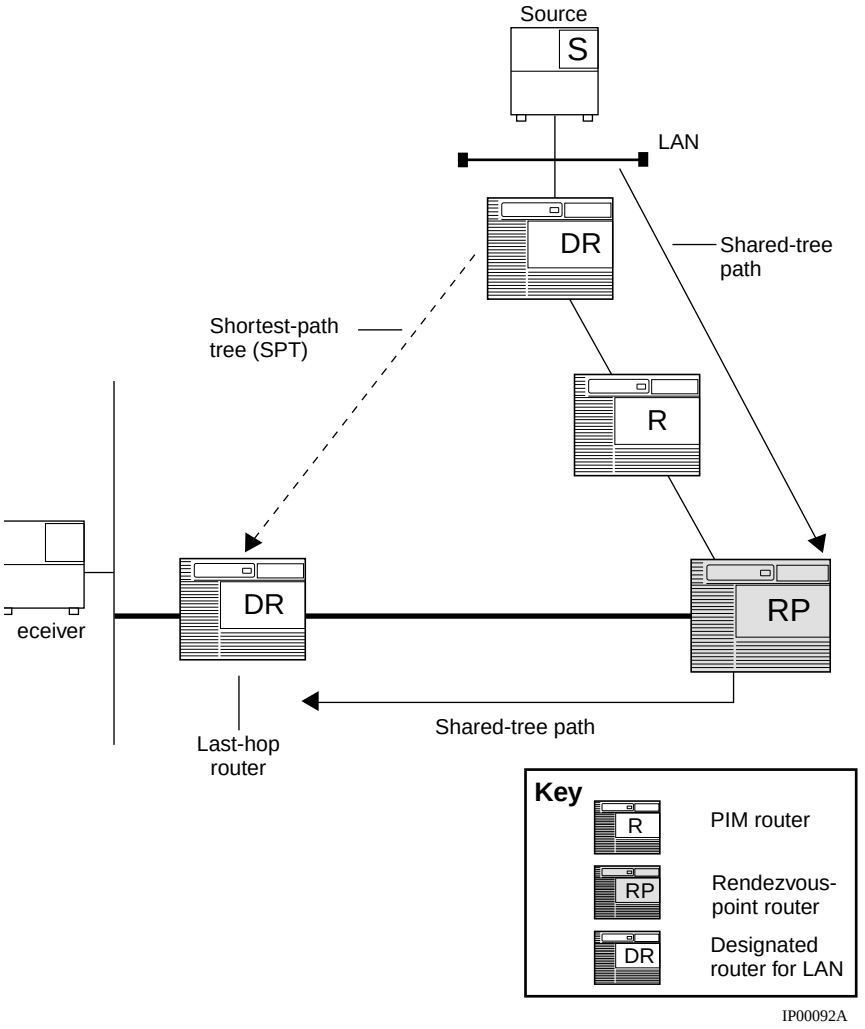
Group members in a PIM-SM domain receive the first packet of data from sources across a shared tree. A *shared tree* consists of a set of paths that connect all members of a multicast group to the RP. PIM creates a shared tree when sources and receivers send messages toward the RP.

Shortest-path trees

After receiving a certain number of packets from the RP, the DR switches from a shared tree to a *shortest-path tree* (SPT). Switching to a shortest-path tree creates a direct route between the receiver and the source. The 8000 Series implementation switches to the SPT when it receives the first packet from the RP.

Figure 12 shows a shared tree and a shortest-path tree.

Figure 12 Shared tree and shortest-path tree



Receiver joining group

The following steps describe how a receiver joins a multicast group:

1. A receiver multicasts an IGMP host membership message to the group that it wants to join.
2. When the DR (normally the PIM router with the highest IP address for that VLAN) receives the IGMP message for a new group, the DR looks up the associated active RP.
3. After determining the RP router for the group, the DR creates a (*,G) route entry in the multicast forwarding table and sends a (*,G) join to the RP. When the DR receives data packets from the RP, the DR switches to shortest path, creates an (S,G) entry in the multicast forwarding table and sends (S,G) join to the source.
4. All intermediate routers along the path to the source create the (S,G) entry.
5. The DR receives data from the data source using the SPT.

Receiver leaving group

Before it leaves a multicast group, a receiver sends an IGMP leave message to the DR. If all directly connected members of a multicast group leave or time out and no downstream members remain, the DR sends a prune message upstream and PIM-SM deletes the route entry after that entry times out.

Source sending packets to group

The following steps describe how a source sends multicast packets to a group:

1. A source directly attached to a VLAN bridges the multicast data to the DR. The DR for the VLAN (the router with the highest IP address) encapsulates each packet in a register message and sends a unicast message directly to the RP router to distribute to the multicast group.
2. If a downstream group member chooses to receive multicast traffic, the RP router sends a join/prune message towards the source DR and forwards the data down the RP tree after it gets the data natively.

3. When the receiver DR gets the first packet, it switches to the shortest-path tree (SPT) and continues receiving data through the SPT path.
4. If no downstream members want to receive multicast traffic, the RP router sends a register-stop message to the DR for the source.

   The DR starts the register suppression timer upon receiving the first register-stop message. During the register suppression timeout period (the default is 60 seconds), the following events occur:

   - The source's DR sends a probe packet to the RP router before the register suppression timer expires. The probe packet prompts the RP router to determine whether any new downstream receivers have joined the group.
   - If no new receivers have joined the group, the RP router sends another register-stop message to the source's DR, and its register suppression timer restarts.
   - When the RP router no longer responds with a register-stop message to the source DR probe message, the register suppression timer expires and the DR sends encapsulated multicast packets to the RP router. The RP router uses this method to tell the DR that new members have joined the group.

The RP sends a register-stop message to the DR immediately after receiving the first multicast data packet

Required elements for PIM-SM operation

For PIM-SM to operate, a number of elements must be present in the PIM-SM domain including the following:

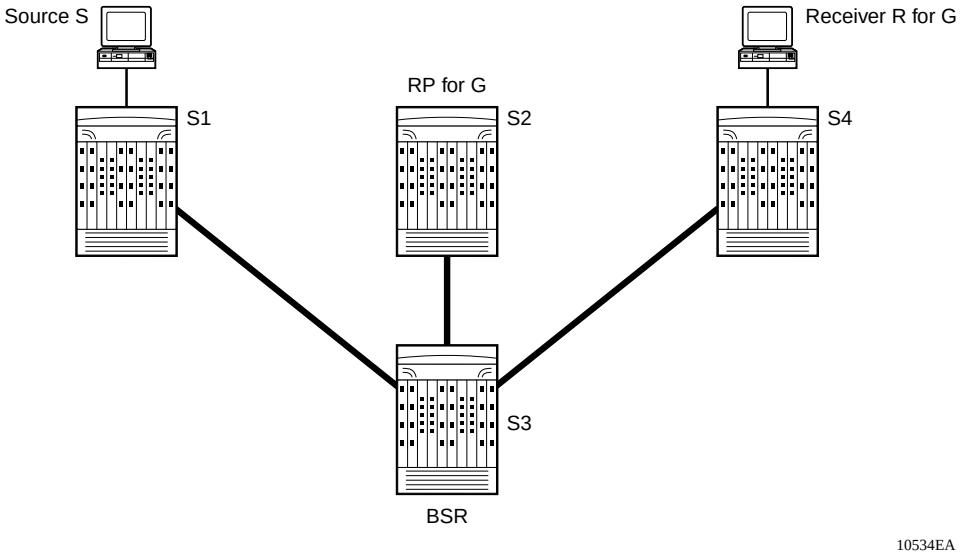
- An underlying unicast routing protocol must be enabled for the switch to provide routing table information to PIM-SM
- In a PIM-SM domain, an active BSR must be in place to send bootstrap messages to all PIM-V2 configured switches and routers to enable them to learn group-to-RP mapping. If several BSRs are configured in a network, an active BSR is elected based on priority and IP address (if priority is equal, the BSR with the higher IP address is elected).

- An RP must be in place in the PIM-SM domain to perform the following tasks:
  - To manage one or several IP Multicast groups
  - To become the root for the shared tree to these groups
  - To accept join messages from receiver switches for groups that it manages
  - If there is more than one RP that have groups in common, the RPs “elect” an active RP based on priority and IP address (if priority is equal, the RP with the higher IP address is elected)

PIM-SM simplified example

Figure 13 shows a simplified example of a PIM-SM configuration.

Figure 13 PIM-SM simplified example



In the sample configuration, the following events occur:

1. The BSR distributes RP information to all switches in the network
2. R sends a report to S4.
3. Acting on this report, S4 sends (*,G) join to RP

4 S starts sending data to G

5 The DR (S1 in this example) encapsulates the data which it unicasts to RP (S2) in register messages

6 S2 de-capsulates the data which it forwards to S4

7 S4 forwards the data to R

8 S4 joins S1 because it now knows the source

9 S1 starts forwarding to S4. When S4 receives data from S1, it prunes the stream from the RP.

Note: Figure 13 is a simplified example and is not the best design for a network if the source and receiver are placed as shown. In general, RPs are placed as close to sources as possible.

PIM-SM static source groups

Static source groups (or static mroutes) enable you to configure **static** source-group entries in the PIM-SM multicast routing table. PIM-SM cannot prune these entries from the distribution tree. For more information about static source groups, see "Static source groups" on page 38."

PIM-SSM (Source Specific Multicast)

Source Specific Multicast (SSM) optimizes PIM-SM by simplifying the many-to-many model. Since most multicast applications distribute content to a group in one direction, SSM uses a one-to-many model that only uses a subset of the PIM-SM features. This model is more efficient and puts less of a load on multicast routing devices.

SSM only builds source-based shortest path trees. Where PIM-SM always joins a shared tree first and then switches to the source tree, SSM eliminates the need for starting with a shared tree by immediately joining a source through the shortest path tree. This method enables SSM to avoid using a rendezvous point (RP) and RP-based shared trees, which can be a potential bottleneck.

Belonging to an SSM group means that its members can only receive from a single source. This is ideal for applications like TV channel distribution and other content-distribution businesses. Banking and trade applications can also use SSM because it provides more control over the hosts receiving data and sending data into their networks.

SSM applications use IP addresses reserved by the Internet Assigned Numbers Authority (IANA) in the 232/8 range (232.0.0.0 to 232.255.255.255). SSM recognizes packets in this range and controls the behavior of multicast routing devices and hosts that use these addresses. When a source (S) transmits IP datagrams to an SSM destination address G, a receiver can receive these datagrams by subscribing to the (S,G) channel.

A channel is a source-group (S,G) pair where S is the source sending to the multicast group and G is an SSM group address. SSM defines channels on a per-source basis, which enforces the one-to-many concept of SSM applications. In an SSM channel, each group is associated with one and only one source. However, another SSM channel can associate the same multicast group with a different source, which allows an efficient use of the SSM address range. For example, channel (192.1.3.4, 232.1.2.3) is different from channel (141.251.186.13, 232.1.2.3)

SSM features

SSM only uses a subset of the PIM-SM features such as the shortest path tree, designated router (DR) and some messages (Hello, Join/Prune and Assert). However, there are also some features that are unique to SSM. These features, which are described in the following sections, are extensions to the IGMP and PIM protocols.

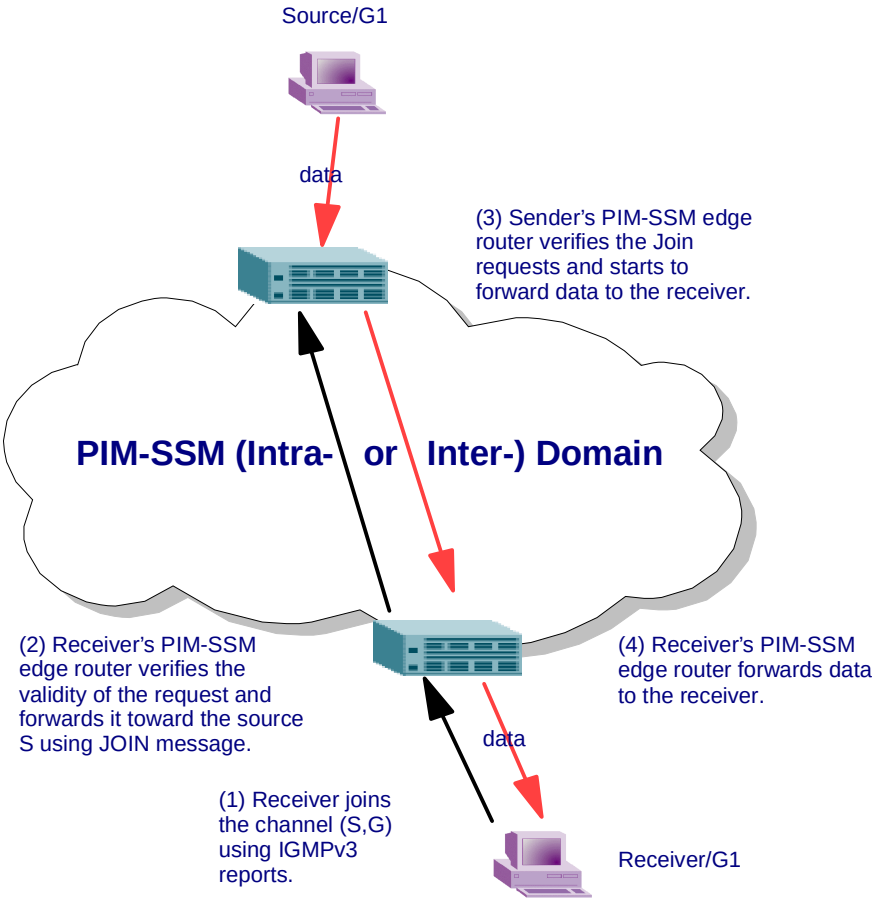
PIM-SSM architecture

Figure 14 illustrates how the PIM-SSM architecture requires routers to:

- Support IGMPv3 source-specific host membership reports and queries at the edge routers.
- Initiate PIM-SSM (S,G) joins directly and immediately after receiving an IGMPv3 join report from the designated router.

- Restrict forwarding to shortest-path trees within the SSM address range by all PIM-SSM routers.

Figure 14 PIM-SSM Architecture



The following rules apply to layer 3 devices with SSM enabled:

- Receive IGMPv3 membership join reports in the SSM range and, if there is no entry (S,G) in the SSM channel table, create one.
- Receive IGMPv2 membership join reports, but only for groups that already have a static (S,G) entry in the SSM channel table.
- Send periodic join messages to maintain a steady SSM tree state.
- Use standard PIM-SM SPT procedures for unicast routing changes, but ignore any rules associated with the SPT-bit for the (S,G) route entry.
- Receive prune messages and use standard PIM-SM procedures to remove interfaces from the source tree.
- Forward data packets to interfaces from which downstream neighbors have sent an SSM join or to interfaces with locally attached SSM group members.
- Drop data packets that do not have an exact-match lookup in its forwarding database for S and G.

8000 Series implementation of SSM and IGMP

The following sections describe how PIM-SSM and IGMP are implemented in the 8000 Series.

SSM range

The standard SSM range is 232/8, but the 8000 Series implementation of SSM allows you to extend the range to include any IP multicast address. Although you can configure the SSM range, configuring it for all multicast groups (224/4 or 224.0.0.0/240.0.0.0 or 224.0.0.0/255.0.0.0) is not allowed.

Extending the SSM range enables you to configure existing applications without having to change their group configurations. This flexibility allows applications to take immediate advantage of SSM.

For information on configuring the SSM range using Device Manager, see “Configuring the SSM range and global parameters” on page 119. For information on configuring the SSM range using the CLI, see “Configuring SSM dynamic learning and range group” on page 293.

SSM channel table

The SSM channel table gives you the flexibility to manually configure S,G entries that map existing groups to their sending source. These table entries apply to the whole switch, not per interface, and both IGMPv2 and IGMPv3 hosts use the SSM channel table.

The following rules apply to an SSM channel table for an individual switch:

- You can map one source to multiple groups.
- You can map one group to one source only, that is, you cannot map the same group more than once in a given table.

Note: Different switches can have different mappings for groups to sources i.e., different channels, even if they are on the same network.

For information on configuring the SSM channel table using Device Manager, see "Configuring the SSM channel table" on page 122. For information on configuring the SSM channel table using the CLI, see "Configuring the SSM channel table" on page 296.

SSM and IGMPv2

SSM-configured switches can accept reports from IGMPv2 hosts on IGMPv2 interfaces if the group has an SSM channel table entry. However, the IGMPv2 host groups **must** be in the SSM range defined on the switch, which is 232/8 by default.

- When the SSM switch receives an IGMPv2 report for a group that is in the SSM channel table, it joins the specified source immediately.

- When the SSM switch receives an IGMPv2 report for a group that has an enabled static SSM channel table entry, it triggers PIM-SSM processing as if it received an equivalent IGMPv3 report.

- When the SSM switch receives an IGMPv2 report for a group out of the SSM range, it processes the report as if it was in PIM-SM mode.

SSM and IGMPv3

The 8000 Series supports IGMPv3 for SSM. IGMPv3 enables a host to selectively request or filter traffic from sources within the multicast group. IGMPv3 is an interface-level configuration.

Note: IGMPv3 works only with PIM-SSM or SSM snoop enabled on the interface.

The following rules apply to IGMPv3-enabled interfaces:

- Send only IGMPv3 (source-specific) reports for addresses in the SSM range.
- Accept IGMPv3 reports.
- Drop IGMPv2 reports.

  Note that the IGMPv2 report mentioned in the "SSM and IGMPv2" section was processed because it was an IGMPv2 report received on an IGMPv2 interface. If it was an IGMPv3 report received on an IGMPv2 interface, it would have been dropped even if PIM-SSM was enabled and the entry was in the SSM channel table. The rule is — the IGMP version must match first.

- Discard any IGMP packets with a group address out of the SSM range.

The IGMPv3 implementation on the 8000 Series can operate in one of two modes: dynamic and static.

- In dynamic mode, the switch learns about new (S,G) pairs from IGMPv3 reports and adds them to the SSM channel table. If dynamic mode is not enabled and an IGMPv3-enabled interface receives a report that includes a group not listed in the SSM channel table, it will ignore the report.
- In static mode, you can statically configure (Source,Group) entries in the SSM channel table. If an IGMPv3-enabled interface receives a report that includes a group not listed in the SSM channel table, it will ignore the report. It will also ignore the report if the group is in the table, but the source/mask does not match what is in the table.

Note: When IGMPv3 is enabled, changes to the query interval and robustness values on the querier switch are propagated to other switches on the same VLAN through IGMP query.

Both IGMPv2 and IGMPv3 hosts use the SSM channel table.

- For an IGMP v2 host (with an IGMPv2 VLAN), it must have an existing SSM channel entry if the group is in SSM range.
- For an IGMP v3 host, if dynamic learning is enabled, then the SSM channel will automatically learn the group. Otherwise, it also needs a static entry.

Table 2 summarizes how a switch in PIM-SSM mode works with IGMP.

Table 2 Summary of how PIM-SSM interacts with IGMPv2 and v3[1]

Host	VLAN	SSM Range	Action
IGMPv2 host	IGMPv3 VLAN	In or Out of range	Drop report.
IGMPv3 host	IGMPv2 VLAN	In or Out of range	Drop report.
IGMPv2 host	IGMPv2 VLAN	In SSM range	If the report matches an existing static SSM channel entry, create (S,G). If the report does not match any existing static SSM channel entry, drop it.
IGMPv2 host	IGMPv2 VLAN	Out of SSM range	Ignore the SSM channel table and process the report as if it was in PIM-SM mode.
IGMPv3 host	IGMPv3 VLAN	Out of SSM range	Drop report.
IGMPv3 host	IGMPv3 VLAN	In SSM range	Dynamic enabled. Create (S,G).
IGMPv3 host	IGMPv3 VLAN	In SSM range	Dynamic disabled and matches an existing SSM channel entry, create (S,G).
IGMPv3 host	IGMPv3 VLAN	In SSM range	Dynamic disabled and does not match an existing SSM channel entry, drop it.

1 References to any matching static SSM channel entry assumes that the entry is enabled. If an entry is disabled, it will treated the same as if it was disallowed.

When an IGMPv3 interface receives an IGMPv2 or v1 query, the interface backs down to IGMPv2 or v1. As a result, all senders and receivers on this interface will be flushed.

PIM-SSM static source groups

Static source groups (or static mroutes) enable you to configure **static** source-group entries in the PIM-SSM multicast routing table. PIM-SSM cannot prune these entries from the distribution tree. For more information about static source groups, see "Static source groups" on page 38."

Configuration limitations

Nortel Networks recommends running PIM-SSM on either all the switches in the domain or only on the edge routers. If there is a mix of PIM-SSM and PIM-SM switches in the domain, run PIM-SSM on all the edge routers and PIM-SM on all the core routers.

Note: A PIM domain with edge routers running PIM-SM and core routers running PIM-SSM will not work properly.

Nortel Networks does not support SSM interoperability with DVMRP. However, the MBR functionality works properly for non-SSM groups because SSM-enabled interfaces use PIM-SM behavior for groups outside the SSM range.

SSM switches running IGMPv3 will drop any reports that it receives that are out of the SSM range. It will not forward them to a PIM-SM switch.

Static source groups cannot conflict with SSM channels and vice versa. When you configure a static source group or an SSM channel, the switch performs a consistency check to make sure there are no conflicts. You cannot map one group (G) to different sources for both a static source group and an SSM channel.

PIM passive interfaces

You can specify whether you want a PIM interface to be active or passive. The default is active. An active interface allows PIM control traffic to be transmitted and received. A passive interface drops all PIM control traffic, thereby reducing the load on the system. This feature is useful when you have a high number of PIM interfaces and these interfaces are connected to end-users, not to other switches.

A PIM interface that is configured as passive will not transmit and will drop any messages of the following type:

- Hello
- Join/Prune
- Register (see Note below)
- Register-Stop (see Note below)
- Assert
- Candidate-RP-Advertisement
- Bootstrap

If a PIM passive interface receives any of these types of messages, the interface drops those messages and the switch logs a message, detailing the type of protocol message that was received and the IP address of the sending device. These log messages help to identify the device that is performing routing on the interface, which is useful if you must disable a device that is not operating correctly.

Note: A device may send Register and Register-Stop messages to a PIM passive interface, but these messages cannot be sent out of that interface.

The PIM passive interface maintains information about hosts, through the IGMP protocol, that are related to senders and receivers, but the interface does not maintain information about any PIM neighbors. You can configure a bootstrap router (BSR) or a rendezvous point (RP) on a PIM passive interface.

The PIM passive interface feature can also be used as a security measure to prevent routing devices from being attached and participating in the multicast routing of the network.

Note: Before you change the state (active or passive) of a PIM interface, you must first disable PIM on that interface. This prevents any instability in the PIM operations, especially when neighbors are present or when streams are received.

For information on configuring PIM passive interfaces using Device Manager, see "Viewing and editing PIM interface parameters" on page 198. For information on configuring PIM passive interfaces using the CLI, see "Changing the interface type" on page 397, "Changing the port interface type" on page 413 or "Changing the VLAN interface type" on page 416.

Pragmatic General Multicast (PGM)

Pragmatic General Multicast (PGM) is a standard transport-level protocol that addresses the disadvantages inherent to other multicasting protocols such as unreliable packet delivery, packet duplication, and network congestion. PGM addresses these limitations with techniques that enable it to provide reliable, duplicate-free delivery of data packets while reducing network congestion.

PGM sources multicast data packets (ODATA, original data) in an ordered sequence. If there is a missing packet in the sequence, the receiver detects the missing sequence number and unicasts a negative acknowledgement to the source. The source responds by sending a NAK confirmation (NCF) and either the source itself or a designated local repairer (DLR) retransmits the missing packet (RDATA, retransmitted data).

PGM is defined by the IETF <draft-speakman-pgm-spec-06.txt>.

PGM requires a host implementation as well as a network element (layer 3 device) implementation.

The 8000 Series switches implement the network element aspect of PGM, but they do not implement the DLR which requires a high amount of buffering and is usually implemented by end systems.

PGM concepts and terminology

The following sections describe PGM terms and how they are used within a PGM network.

Transport session identifiers (TSIs)

PGM runs over IP Multicast, and delivers data from a source to one or several receivers. The key distinction between PGM and other multicast protocols is that data must be delivered within a transmit window time frame. Each multicast session has a transport session identifier (TSI). PGM supports any number of sources within a multicast group, but each has its own TSI and all sources operate independently.

Source path messages (SPMs)

Source path messages (SPMs) establish the source path state for the TSI. The source sends out SPMs to maintain up-to-date PGM neighbor information for the distribution tree from source to receivers. PGM receivers also use this information to address negative acknowledgements (NAKs) to the source.

Negative acknowledgements (NAKs)

PGM uses NAKs to ensure reliable packet delivery. When a receiver detects a missing packet, it repeats this NAK until it receives a NAK confirmation. In this way, PGM guarantees that receivers either receive all data packets from transmissions and retransmissions, or can detect unrecoverable data packet loss.

PGM also uses NAKs to reduce congestion. Instead of sending a positive acknowledgement (ACK) every time a packet is received, which adds to network overhead, PGM issues a negative acknowledgement (NAK) only when a packet is *not* received.

NAK confirmations (NCFs)

NAK confirmations (NCFs) further reduce congestion by suppressing redundant NAKs. When a receiver detects a missing packet, it unicasts a NAK to the next-hop upstream PGM router. This router then multicasts an NCF to the subnet so other receivers will not send additional NAKs. The router also stores the group's address so that it forwards retransmissions only to those segments containing receivers that require the packet.

Designated local repairers (DLRs)

Designated local repairers (DLRs) are local hosts that retransmit missing data packets for a number of multicast groups. DLRs multicast the missing data to receivers below it in the distribution tree. This technique reduces the load on the network due to retransmissions and reduces the time for receivers to recover missing packets.

Note: The 8000 Series switches cannot serve as a DLR because DLRs require a large amount of buffering. Therefore, the null negative acknowledgement (NNAK) parameters in Device Manager and the CLI are not supported.

PGM network element

You can configure an 8000 Series switch as the network element of a PGM network. The network element performs several PGM tasks as follows:

- Sources periodically interleave Source Path Messages (SPMs) with data frames. SPM frames allow the network element (an 8000 Series switch with PGM enabled), to learn the path to the source and to maintain information on the PGM session.
- Because data frames are numbered, hosts can detect missing data and issue Negative Acknowledgement messages (NAKs) if data goes missing. The network element forwards NAKs to the source and stores information about the NAK to forward retransmitted data.

- Hosts continue to send NAK messages until they receive a NAK Confirmation (NCF) from the network element. To reduce traffic on the network, the network element does not forward all received NAKs, because NAKs can be transmitted from several receivers for the same lost packet.
- The source retransmits the requested frame which is forwarded by the network element to the interface(s) which sent the NAK.

For information on configuring PGM, see "Configuring PGM using Device Manager" on page 211 or "Configuring PGM using the CLI" on page 435.

Multicast flow distribution over MLT

MultiLink Trunking (MLT) provides a mechanism for distributing multicast streams over an MLT. It does so based on source-subnet and group addresses and in the process provides you with the ability to choose the address and the bytes in the address for the distribution algorithm. As a result, you can now distribute the load on different ports of the MLT and aim (whenever possible) to achieve an even distribution of the streams. In applications like TV distribution, multicast traffic distribution is particularly important since the bandwidth requirements can be substantial when a large number of TV streams are employed.

Note: The multicast flow distribution over MLT feature is supported only on 8000 Series E-modules. As a result, all the cards that have ports in an MLT must be 8000 Series E-cards in order to enable multicast flow distribution over MLT.

Distribution algorithm

To determine the port for a particular Source, Group (S,G) pair, the number of active ports of the MLT is used to MOD the number generated by the XOR of each byte of the masked group address with the masked source address. By default, the group mask and source mask is 255.255.255.255. A byte with a value of 255 in the mask means that the corresponding byte in the group or source address is taken into account when the algorithm is applied.

For example, consider:

Group address G[0].G[1].G[2].G[3], Group Mask GM[0].GM[1].GM[2].GM[3], Source Subnet address S[0].S[1].S[2].S[3], Source Mask SM[0].SM[1].SM[2].SM[3]

Then, the Port =:

(((((G[0] AND GM[0]) xor (S[0] AND SM[0])) xor ((G[1] AND GM[0]) xor (S[1] AND SM[1]))) xor ((G[2] AND GM[2]) xor (S[2] AND SM[2]))) xor ((G[3] AND GM[3]) xor (S[3] AND SM[3]))) MOD (active ports of the MLT)

The algorithm used for traffic distribution causes the distribution to be sequential if the streams are similar to those in the example that follows. Assume that the MLT ports are 1/1-1/4, that mask configuration is 0.0.0.0 for the source mask and 0.0.0.255 for the group mask, and that source A.B.C.D sends to groups:

X.Y.Z.1

X.Y.Z.2

X.Y.Z.3

.....

X.Y.Z.10

The algorithm chooses link 1/1 for group X.Y.Z.1, then X.Y.Z.2 goes on 1/2, X.Y.Z.3 goes on 1/3. X.Y.Z.4 goes on 1/4, X.Y.Z.5 goes on 1/1 and so on.

In the following configuration example, only the first byte of the grp-mask, and the first two bytes of the src-subnet mask are considered when distributing the streams.

```
config sys mcast-mlt-distribution grp-mask 255.0.0.0

config sys mcast-mlt-distribution src-mask 255.255.0.0
```

```
config sys mcast-mlt-distribution enable

config sys mcast-mlt-distribution redistribution enable
```

Note: When configuring flow distribution over MLT, it is recommended that you choose source and group masks that result in the most even traffic distribution over the MLT links. For example, if you find in the network group addressing that group addresses change incrementally, while there are few sources always sending to different groups, you should use a source mask of 0.0.0.0 and a group mask of 255.255.255.255. In most cases, this will provide a sequential distribution of traffic on the links of the MLT.

Traffic redistribution

The overall goal of traffic redistribution is to achieve a distribution of the streams on the MLT links in the event of an MLT configuration change. For example, ports might be added or deleted. By default, redistribution is disabled. When a link is added or removed from the MLT, the active streams continue flowing on their original links if redistribution is disabled.

If redistribution is enabled, however, the active streams are redistributed according to the distribution algorithm on the links of the MLT. Note that this may cause minor traffic interruptions. To minimize the effect of redistribution of multicast traffic on the MLTs, the implementation does not move the streams to the appropriate links all at once. Instead, it redistributes a few streams at every time tick of the system.

To that end, when an MLT port becomes inactive and redistribution is disabled, only the affected streams are redistributed on the remaining active ports. If redistribution is enabled, all the streams are redistributed on the MLT ports based on the assignment provided by the distribution algorithm. For more information, see the previous section, “Distribution algorithm.”

When a new port becomes active in an MLT and redistribution is disabled, existing streams will remain on their original links. If you need to redistribute the streams dynamically to split the load on all the links of the MLT, you should enable redistribution. This will result in a few streams being redistributed every system time tick.

Configuring multicast MLT distribution

You configure multicast flow distribution over MLT using either the command line interface (CLI), or Device Manager (DM). Using the CLI, you enable multicast flow distribution over MLT globally by entering the following command:

```
config sys mcast-mlt-distribution enable
```

You then enable multicast distribution per MLT by entering:

```
config mlt <mltid> mcast-distribution enable
```

For a more detailed description of these commands, see “Configuring multicast flow distribution over MLT using the CLI” on page 481.”

Using DM, you enable multicast flow distribution over MLT globally by:

➔ Selecting Edit > Chassis> Mcast MLT Distribution

You then enable multicast distribution per MLT by:

➔ Selecting VLAN > MLT > McastDistribution <Enable | Disable>

For a more detailed description of these commands, see “Configuring multicast flow distribution over MLT using Device Manager” on page 253.”

For more information on MLT, see *Configuring Layer 2 Operations: VLANs, Spanning Tree, MultiLink Trunking*.

Multicast MAC filtering

Some network applications rely on a Layer 2 multicast MAC mechanism to send a frame to multiple hosts for processing. For example, mirroring is one such application. With release 3.3 of the 8000 Series software, the multicast MAC filtering feature allows you to direct MAC multicast flooding to a specific set of ports.

Note: You can configure multicast MAC filtering only for local addresses to a switch. You cannot use this feature as a means to route traffic between switches (i.e., configure it to forward for interfaces that are not local).

Basically, the multicast MAC is defined as any MAC address in which the least significant bit of the most significant byte is set to 1. The multicast MAC filtering feature is available for Layer 2. Because it is also effective for IP routed traffic, however, Layer 3 functionality is available as well. (This filtering does not apply to BPDUs).

In Layer 2, a multicast MAC address generally floods to all ports in the VLAN. With multicast MAC filtering, you can now define a separate flooding domain for a given multicast MAC address, which is a subset of the ports on a VLAN. The maximum number of multicast MAC addresses that you can configure is 100. Depending upon the overall configuration of your switch, note that you may be limited to fewer addresses, however.

In Layer 3, you should configure an ARP entry for routed traffic that maps the unicast IP to the multicast MAC address and lists the ports where data destined for that IP/multicast MAC should be delivered.

To perform multicast MAC filtering, you create the VLAN normally and then manually define a flooding domain (that is, MAC address and port list) for a specific multicast address. When specifying the multicast MAC flooding domain, you should indicate which ports or Multilink Trunks (MLTs) should be considered for multicast traffic. The actual flooding will then be based on whether the specified ports are active members in the VLAN.

Configuration example

You can configure multicast MAC filtering on a VLAN through either the CLI or Device Manager (DM). To configure multicast MAC filtering for Layer 2, use the **`config vlan static-mcastmac`** command. For Layer 3 configuration, use the **`config ip arp static-mcastmac`** command.

For a more detailed description of these commands, see “Configuring multicast MAC filtering using the CLI” on page 487.”

To configure multicast MAC filtering for Layer 2 using the DM:

➔ Select VLANs > Bridge > Multicast

To configure multicast MAC filtering for Layer 3 using the DM:

➔ Choose IP Routing > IP > Multicast ARP

For a more detailed description of these commands, see “Configuring multicast MAC filtering using Device Manager” on page 259.”

Chapter 2
Configuring IGMP using Device Manager

IGMP is used by hosts to report their multicast group memberships to neighbor multicast routers. For more information about IGMP concepts and terminology, refer to Chapter 1, "IP Multicast concepts."

This chapter describes the following topics:

Configuration prerequisites and notes

Before you can configure IGMP, you must prepare the router as follows:

1. Configure an IP interface. For information, refer to *Configuring IP Routing Operations*.
2. Configure IGMP on a L2 interface by enabling IGMP snooping
   or
   Configure IGMP on a L3 interface by enabling multicast routing, i.e., DVMRP, PIM-SM or PIM-SSM.
   - To enable IGMP snooping, refer to "Enabling IGMP snooping on a VLAN."
   - To enable DVMRP or PIM-SM on an IP interface, first enable them globally. (PIM-SSM is a global configuration; you cannot enable it per interface.)
     — To enable DVMRP globally, see "Enabling DVMRP globally."
     — To enable PIM-SM globally, see "Enabling PIM-SM globally."
     — To enable PIM-SSM globally, see "Enabling Source Specific Multicast (SSM) globally."

Note: To drop IGMPv2 control packets that do not have the router alert option set, click IP Routing > IGMP and open the Interface tab. Change the RouterAlertEnable field to enable.

Configuring IGMP parameters on a brouter port

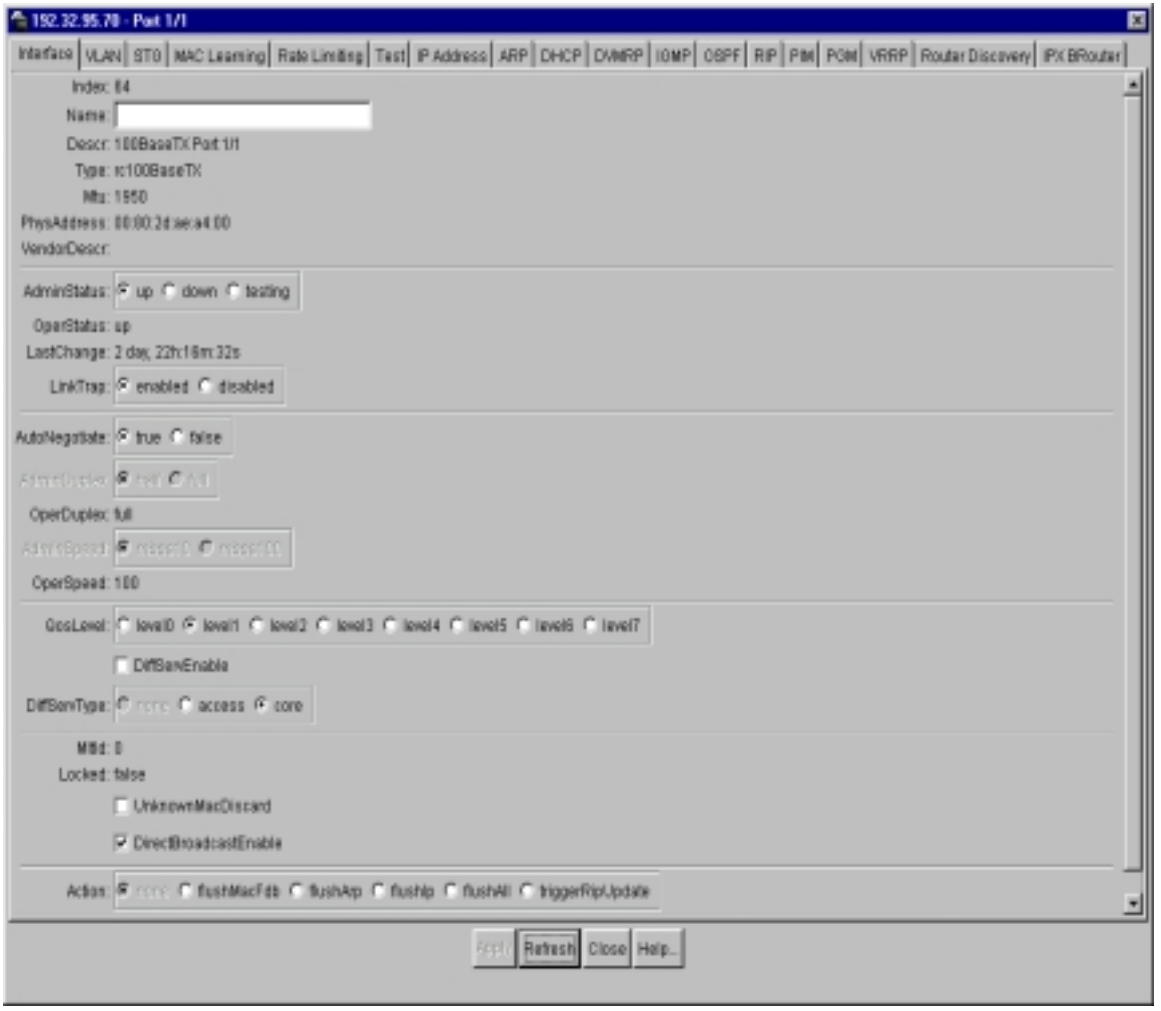
In order for IGMP parameters to take effect, DVMRP or PIM must be enabled globally on the particular interface.

To configure IGMP parameters on a brouter port:

1. On the Device Manager, select a port.
2. From the Device Manager menu bar, choose Edit > Port.

   The Port dialog box opens with the Interface tab displayed (Figure 15).

Figure 15 Port dialog box—Interface tab



3 Click the IGMP tab.

The IGMP tab opens (Figure 16).

Figure 16 Port dialog box—IGMP tab

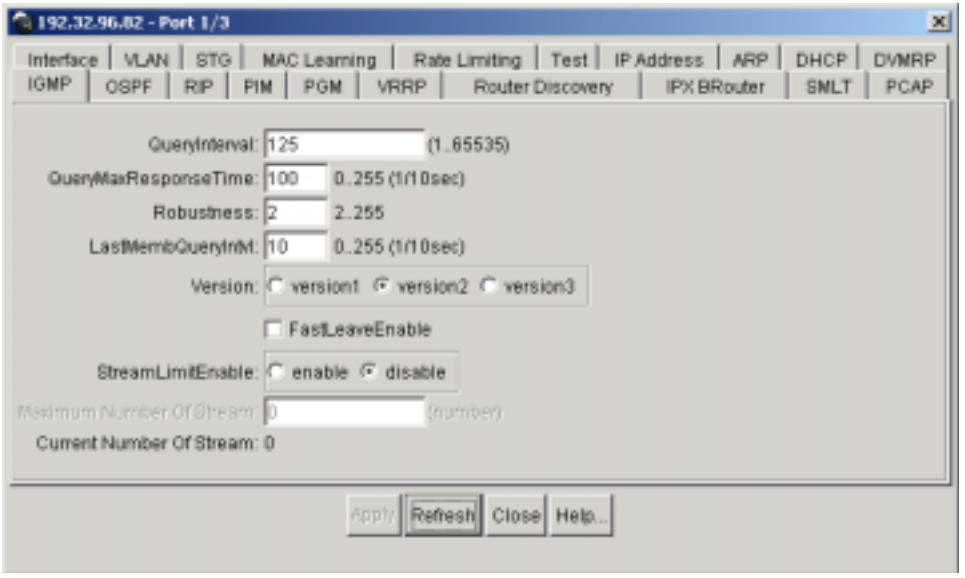


Table 3 describes the fields on the IGMP tab.

Table 3 IGMP tab fields

Field	Description
QueryInterval	The frequency (in seconds) at which IGMP host query packets are transmitted on the interface. The range is from 1 to 65535, and the default is 125.
QueryMaxResponseTime	The maximum response time (in 1/10 seconds) advertised in IGMPv2 general queries on this interface. This value is not configurable for IGMPv1. Smaller values allow a router to prune groups faster. The range is from 0 to 255, and the default is 100 tenth seconds (equal to 10 seconds). **Note:** This value must be less than the QueryInterval.
Robustness	This parameter allows tuning for the expected packet loss of a network. This value is equal to the number of expected query packet losses per serial query interval, plus 1. If a network is expected to lose query packets, the robustness value should be increased. The range is from 2 to 255, and the default is 2. The default value of 2 means that one query per query interval may be dropped without the querier aging out.

Table 3 IGMP tab fields (continued)

Field	Description
LastMembQueryIntvl	The maximum response time (in 1/10 seconds) that is inserted into group-specific queries sent in response to leave group messages. It is also the time between group-specific query messages. This value is not configurable for IGMPv1. Decreasing the value reduces the time to detect the loss of the last member of a group. The range is from 0 to 255, and the default is 10 tenth seconds. Nortel Networks recommends configuring this parameter to values higher than 3. If a fast leave process is not required, Nortel recommends values above 10. (The value 3 is equal to 0.3 of a second and 10 is equal to 1.0 second).
Version	The version of IGMP (1, 2 or 3) that you want to configure on this interface. For IGMP to function correctly, all routers on a LAN must use the same version. The default is version 2.
FastLeaveEnable	Enables fast leave on the interface.
StreamLimitEnable	Enables or disables stream limitation on this port.
Maximum Number Of Stream	Sets the maximum number of streams allowed on this port. The range is from 0 to 65535, and the default is 4.
Current Number Of Stream	Displays the current number of streams. This is a read-only value.

Configuring fast leave mode

Fast leave mode provides one command that controls all IGMP fast-leave enabled interfaces. Using this global parameter, you can alter the leave processing on fast-leave enabled IGMPv2, IGMPv3, and IGMP snoop interfaces.

Note: Fast leave mode applies only to fast-leave enabled IGMP interfaces. It does not apply to IGAP interfaces, which ignore this mode.

To configure the fast leave mode:

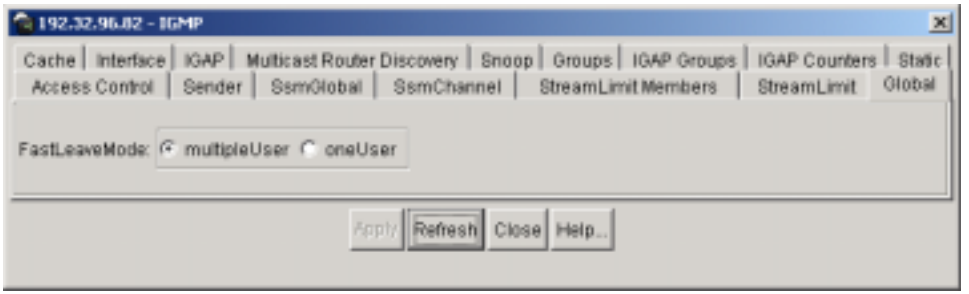
1 From the Device Manager menu bar, choose IP Routing > IGMP.

The IGMP dialog box opens with the Cache tab displayed.

2 Click the Global tab.

The Global tab opens (Figure 17).

Figure 17 IGMP dialog box— Global tab



3 Click on the mode you want, if not already selected.

4 Click Apply.

Table 4 describes the Global tab fields.

Table 4 Global tab fields

Field	Description
multipleUser	Removes from the group *only* the IGMP member who sent the Leave message. Traffic is not stopped if there are other receivers on the interface port. This is the default.
oneUser	Removes all group members on a fast-leave enabled interface port upon receiving the first Leave message from a member. This behavior is the same as the conventional fast leave process.

Configuring IGMP parameters on a VLAN

In order for IGMP parameters to take effect, DVMRP or PIM-SM must be enabled globally and on the particular interface.

To configure IGMP on a VLAN:

1. From the Device Manager menu bar, choose VLAN > VLANs.

   The VLAN dialog box opens, with the Basic tab displayed.

2. Select a VLAN.

3. Click IP.

   The IP, VLAN dialog box opens with the IP Address tab displayed.

4. Select IGMP.

   The IGMP tab opens (Figure 18).

Figure 18 IP, VLAN dialog box—IGMP tab

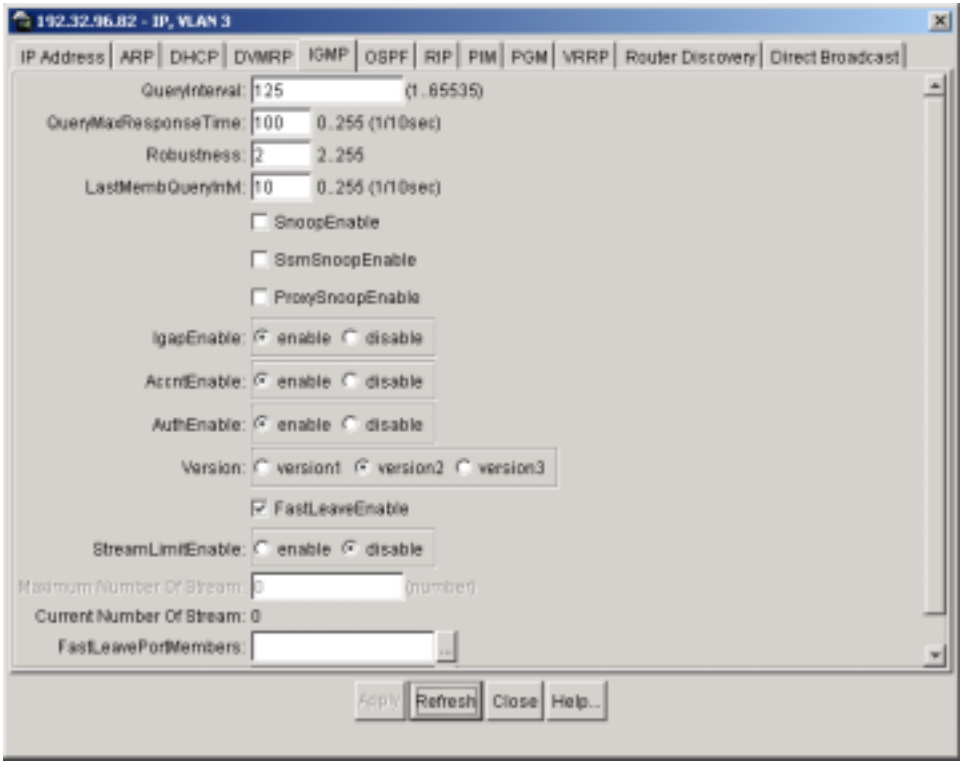


Table 5 describes the fields in the IGMP tab.

Table 5 IGMP tab fields

Field	Description
QueryInterval	The frequency (in seconds) at which IGMP host query packets are transmitted on the interface. The range is from 1 to 65535, and the default is 125.
QueryMaxResponseTime	The maximum response time (in 1/10 seconds) advertised in IGMPv2 general queries on this interface. This value is not configurable for IGMPv1. Smaller values allow a router to prune groups faster. The range is from 0 to 255, and the default is 100 tenth seconds (equal to 10 seconds). **Note:** This value must be less than the QueryInterval.

Table 5 IGMP tab fields (continued)

Field	Description
Robustness	This parameter allows tuning for the expected packet loss of a network. This value is equal to the number of expected query packet losses per serial query interval, plus 1. If a network is expected to lose query packets, the robustness value should be increased. The range is from 2 to 255, and the default is 2. The default value of 2 means that one query per query interval may be dropped without the querier aging out.
LastMembQueryIntvl	The maximum response time (in 1/10 seconds) that is inserted into group-specific queries sent in response to leave group messages. It is also the time between group-specific query messages. This value is not configurable for IGMPv1. Decreasing the value reduces the time to detect the loss of the last member of a group. The range is from 0 to 255, and the default is 10 tenth seconds. Nortel Networks recommends configuring this parameter to values higher than 3. If a fast leave process is not required, Nortel recommends values above 10. (The value 3 is equal to 0.3 of a second and 10 is equal to 1.0 second).
SnoopEnable	Enables snoop.
SsmSnoopEnable	Enables or disables support for PIM source-specific multicast (SSM) on the snooping interface.
ProxySnoopEnable	Enables proxy snoop.
IgapEnable	Enables or disables IGAP on this interface.
AccntEnable	Enables or disables IGAP Accounting on this interface.
AuthEnable	Enables or disables IGAP Authentication on this interface.
Version	The version of IGMP (1, 2 or 3) that you want to configure on this interface. For IGMP to function correctly, all routers on a LAN must use the same version. The default is version 2.
FastLeaveEnable	Enables fast leave on the interface.
StreamLimitEnable	Enables or disables stream limitation on this VLAN.
Maximum Number Of Stream	Sets the maximum number of streams allowed on this VLAN. The range is from 0 to 65535, and the default is 4.
Current Number Of Stream	Displays the current number of streams. This is a read-only value.

Table 5 IGMP tab fields (continued)

Field	Description
FastLeavePortMembers	The set of ports that are enabled for fast leave.
SnoopMRouterPorts	The set of ports in this interface that provide connectivity to an IP Multicast router.

Enabling IGMP snooping on a VLAN

The 8000 Series switch provides IP Multicast capability when used as a switch. As a switch, it supports Internet Group Management Protocols IGMPv1, IGMPv2, and IGMPv3 to prune group membership per port within a VLAN by reporting multicast group memberships to neighbor multicast routers. This feature is called IGMP snooping.

The IGMP snooping feature allows you to optimize the multicast data flow for a group within a VLAN only to those that are members of the group. The switch listens to group reports from each port and builds a database of multicast group members per port. It suppresses the reports heard by not forwarding them out to other hosts, forcing the members to continuously send their own reports. The switch relays group membership from the hosts to the multicast routers. It forwards queries from multicast routers to all port members of the VLAN. Furthermore, it multicasts data only to the participating group members and to the multicast routers within the VLAN.

To enable IGMP snooping:

1. From the Device Manager menu bar, choose VLAN > VLANs.

   The VLAN dialog box opens with the Basic tab displayed.
2. Select a VLAN.
3. Click IP.

   The IP, VLAN dialog box opens with the IP Address tab displayed.
4. Click IGMP.

   The IGMP tab opens (Figure 18).
5. Click SnoopEnable.

6 Click ProxySnoopEnable.

7 Click Apply.

Viewing IGMP cache information

To view IGMP cache information:

➔ From the Device Manager menu bar, choose IP Routing > IGMP.

The IGMP dialog box opens with the Cache tab displayed (Figure 19).

Figure 19 IGMP dialog box—Cache tab

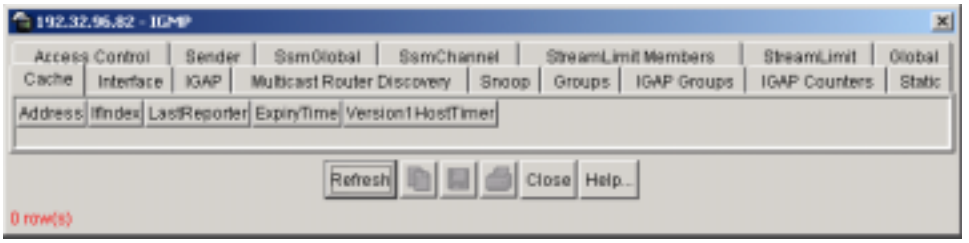


Table 6 describes the Cache tab fields.

Table 6 Cache tab fields

Field	Description
Address	The IP Multicast group address for which this entry contains information.
IfIndex	The interface from which the corresponding multicast group address is heard.
LastReporter	The IP address of the source of the last membership report received for this IP Multicast group address on this interface. If no membership report has been received, the object has the value 0.0.0.0.

Table 6 Cache tab fields (continued)

Field	Description
ExpiryTime	The amount of time (in seconds) remaining before this entry will be aged out.
Version1Host Timer	The time remaining until the local router will assume that there are no longer any IGMP version 1 members on the IP subnet attached to the interface. Upon hearing any IGMPv1 membership report, this value is reset to the group membership timer. When the time remaining is nonzero, the local router ignores any IGMPv2 Leave messages for this group that it receives on this interface.

Viewing and editing the IGMP interface table

Use the Interface tab to view or edit the IGMP interface table. When a particular interface does not have an IP address, its entry will not appear in the IGMP table. When an interface has an IP address, but DVMRP or PIM-SM is not enabled, it is shown as “notInService” in the Status field.

To view or edit the IGMP interface table:

1. From the Device Manager menu bar, choose IP Routing > IGMP.

   The IGMP dialog box opens with the Cache tab displayed.

2. Click the Interface tab.

   The Interface tab opens (Figure 20).

Figure 20 IGMP dialog box—Interface tab

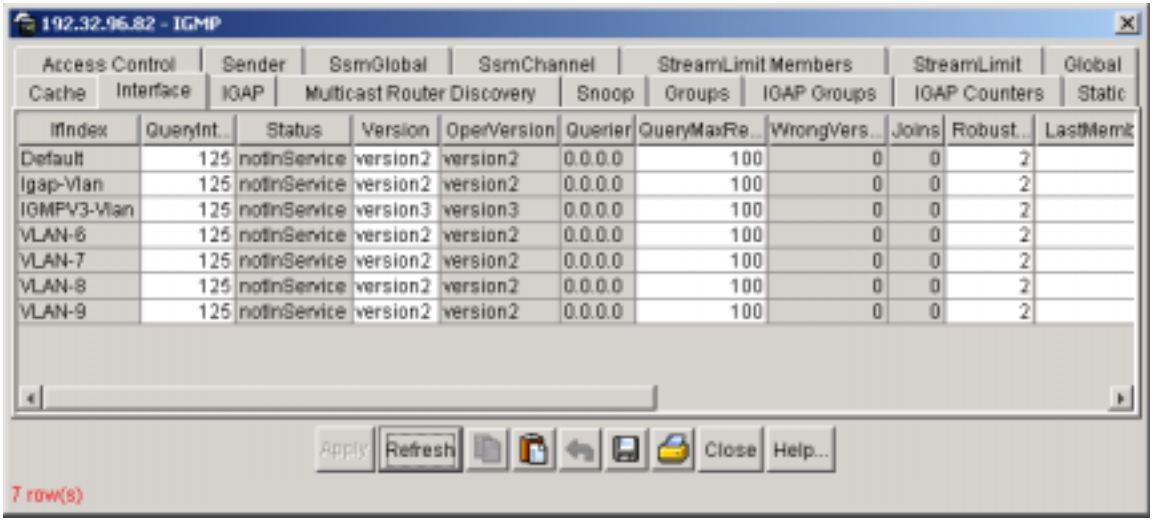


Table 7 describes the Interface tab fields.

Table 7 IGMP dialog box—Interface tab fields

Field	Description
IfIndex	The interface on which IGMP is enabled.
QueryInterval	The frequency (in seconds) at which IGMP host query packets are transmitted on the interface. The range is from 1 to 65535, and the default is 125.
Status	The IGMP row status. When an interface has an IP address and DVMRP or PIM-SM is enabled, status is shown as active. Otherwise, it will be shown as notInService.
Version	The version of IGMP (1, 2 or 3) that you want to configure on this interface. For IGMP to function correctly, all routers on a LAN must use the same version. The default is version 2.
OperVersion	The version of IGMP currently running on this interface.
Querier	The address of the IGMP querier on the IP subnet to which this interface is attached.

Table 7 IGMP dialog box—Interface tab fields (continued)

Field	Description
QueryMaxResponseTime	The maximum response time (in 1/10 seconds) advertised in IGMPv2 general queries on this interface. This value is not configurable for IGMPv1. Smaller values allow a router to prune groups faster. The range is from 0 to 255, and the default is 100 tenth seconds (equal to 10 seconds). **Note:** This value must be less than the QueryInterval.
WrongVersionQueries	The number of queries received with an IGMP version that does not match the interface. IGMP requires that all routers on a LAN be configured to run the same version of IGMP. If any queries are received with the wrong version, it indicates a version mismatch.
Joins	The number of times a group membership has been added on this interface; that is, the number of times an entry for this interface has been added to the cache table. This number gives an indication of the amount of IGMP activity over time.
Robustness	This parameter allows tuning for the expected packet loss of a network. This value is equal to the number of expected query packet losses per serial query interval, plus 1. If a network is expected to lose query packets, the robustness value should be increased. The range is from 2 to 255, and the default is 2. The default value of 2 means that one query per query interval may be dropped without the querier aging out.
LastMembQueryIntvl	The maximum response time (in 1/10 seconds) that is inserted into group-specific queries sent in response to leave group messages. It is also the time between group-specific query messages. This value is not configurable for IGMPv1. Decreasing the value reduces the time to detect the loss of the last member of a group. The range is from 0 to 255, and the default is 10 tenth seconds. Nortel Networks recommends configuring this parameter to values higher than 3. If a fast leave process is not required, Nortel recommends values above 10. (The value 3 is equal to 0.3 of a second and 10 is equal to 1.0 second).
OtherQuerierPresent Timeout	The length of time that must pass before a multicast router decides that there is no other router that should be the querier. If the local router is the querier, the value is 0.

Table 7 IGMP dialog box—Interface tab fields (continued)

Field	Description
FlushAction	• none • flushGrpMem • flushMrouter • flushSender
RouterAlertEnable	When enabled, this parameter instructs the router to process packets not directly addressed to it. **Note:** To maximize your network performance, Nortel Networks recommends that you set this parameter according to the version of IGMP currently in use. • IGMPv1 - Disable • IGMPv2 - Enable • IGMPv3 - Enable

Viewing multicast router discovery information

To view multicast router discovery information:

1. From the Device Manager menu bar, choose IP Routing > IGMP.

   The IGMP dialog box opens with the Cache tab displayed.

2. Click the Multicast Router Discovery tab.

   The Multicast Router Discovery tab opens (Figure 21).

Figure 21 IGMP dialog box—Multicast Router Discovery tab

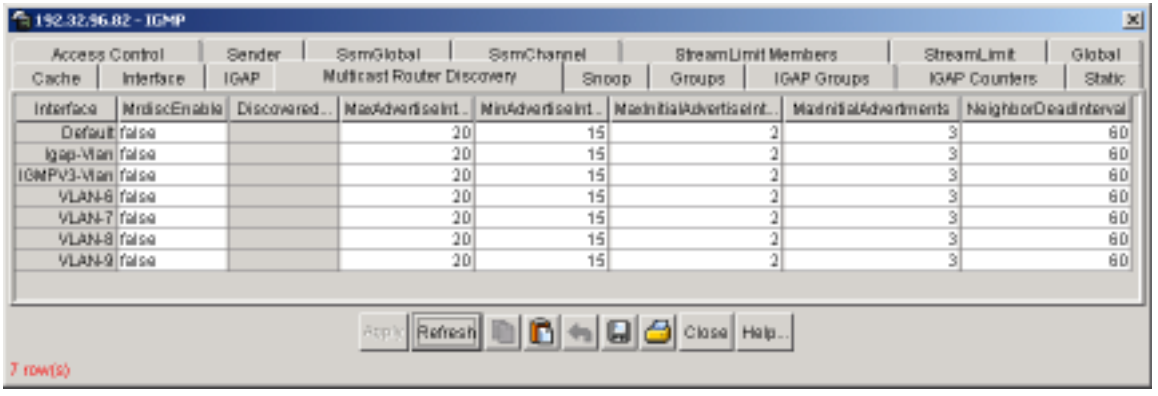


Table 8 describes the Multicast Router Discovery tab fields.

Table 8 Multicast Router Discovery tab fields

Field	Description
Interface	The interface on which IGMP is enabled.
MrdiscEnable	Enables or disables the router interface to listen for multicast router discovery messages to determine where to send multicast source data and IGMPv2 reports. Whenever snooping is enabled, multicast router discovery is automatically enabled.
DiscoveredRouterPorts	List of ports that were discovered by IGMP Multicast router discovery (MRDISC) protocol. **Note:** The Multicast Router Discovery protocol is not supported on brouter ports.
MaxAdvertiseInterval	The maximum time allowed between sending router advertisements from the interface, in seconds, between 2 and 180 seconds. Default is 20 seconds.
MinAdvertiseInterval	The minimum time allowed between sending unsolicited router advertisements from the interface, in seconds. Must be more than 3 seconds but no greater than the value assigned to the MaxAdvertiseInterval value.
MaxInitialAdvertiseInterval	Used to set the maximum number (in seconds) of multicast advertisement intervals that can be configured on the switch.
MaxInitialAdvertisements	Used to set the maximum number of initial multicast advertisements that can be configured on the switch.
NeighborDeadInterval	The time interval (in seconds) before the router interface drops traffic when a user leaves the multicast group.

Viewing IGMP snooping information

To view information about IGMP snooping:

1. From the Device Manager menu bar, choose IP Routing > IGMP.

   The IGMP dialog box opens with the Cache tab displayed.

2. Click the Snoop tab.

   The Snoop tab opens (Figure 22).

Figure 22 IGMP dialog box—Snoop tab

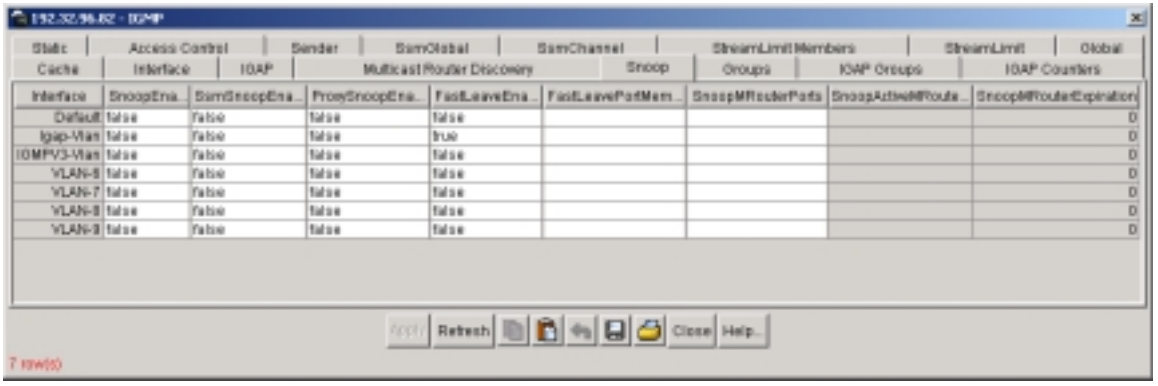


Table 9 describes the Snoop tab fields.

Table 9 Snoop tab fields

Field	Description
IInterface	The VLAN ID for the VLAN.
SnoopEnable	Enables (true) or disables (false) IGMP snooping. IGMP snooping works only when a multicast router exists in the VLAN.
ProxySnoopEnable	Indicates whether or not the IGMP report proxy feature is enabled. When this feature is enabled, reports are forwarded from hosts to the multicast router once per group per query interval or when there is new group information. When this feature is disabled, all reports from different hosts are forwarded to multicast routers, and more than one group report may be forwarded for the same multicast group per query interval. The default is enabled.

Table 9 Snoop tab fields (continued)

Field	Description
FastLeaveEnable	Enable or disable FastLeave for this port.
FastLeavePortMembers	The set of ports that are enabled for FastLeave.
SnoopMRouterPorts	Ports that have been configured as multicast router ports. Such ports are directly attached to a multicast router so the multicast data and group reports will be forwarded to the router. **Caution**: Configure this field only when there are multiple multicast routers that are not directly attached to one another but are directly attached to the VLAN (technically an invalid configuration). If multicast routers have a route between them (the valid configuration) and this field is configured, a multicast loop will form.
SnoopActiveMRouter Ports	Active multicast router ports are ports directly attached to a multicast router. These ports include the Querier port and all ports in the forwarding state that were configured by the user as well as those that were dynamically learned via receiving queries.
SnoopMRouterExpiration	Time remaining before the multicast router is aged out. If the switch does not receive any queries before this time expires, it flushes out all group memberships known to the VLAN. The Query Max Response Interval (obtained from the queries received) is used as the timer resolution.

Viewing IGMP group information

To view information about IGMP groups:

1. From the Device Manager menu bar, choose IP Routing > IGMP.

   The IGMP dialog box opens with the Cache tab displayed.

2. Click the Groups tab.

   The Groups tab opens (Figure 23).

Figure 23 IGMP dialog box—Groups tab

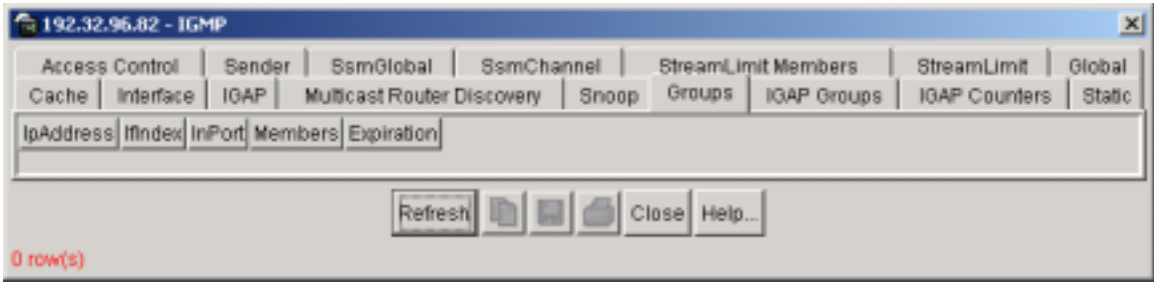


Table 10 describes the Groups tab fields.

Table 10 Group tab fields

Field	Description
IpAddress	Multicast group Address (Class D) that members can join. A group address can be the same for many incoming ports.
IfIndex	A unique value that identifies a physical interface or a logical interface (VLAN), which has received Group reports from various sources.
InPort	A unique value to identify a brouter interface or a logical interface (VLAN) that has received Group reports from various members.
Members	IP address of a member that has issued a group report for this group.
Expiration	Time left before the group report expires on this port. This variable is updated upon receiving a group report.

Creating and viewing IGMP static information

Some sources do not join a multicast group before transmitting a multicast stream. When this is the case and if there are no other group members joined in the VLAN, the data is flooded to all port members of the VLAN. You can create a static entry to forward multicast data streams to a particular set of ports within the VLAN. When the entry is created, multicast data streams are always forwarded to the multicast router within the VLAN in addition to the ports configured for this static entry.

Note: IGMP snoop can guarantee delivery only of local multicast data, but it does not guarantee delivery of remote multicast data. You cannot configure a port as a static receiver in an IGMP snoop-enabled VLAN that does not contain at least one dynamic receiver port and have multicast data forwarded.

To add members to the IGMP snoop group:

1. From the Device Manager menu bar, choose IP Routing > IGMP.

   The IGMP dialog box opens with the Cache tab displayed.

2. Click the Static tab.

   The Static tab opens (Figure 24).

3. In the Static tab, click Insert.

   The IGMP, Insert Static dialog box opens (Figure 24).

4. Enter the appropriate data, and click Insert.

Figure 24 IGMP and IGMP, Insert Static dialog boxes

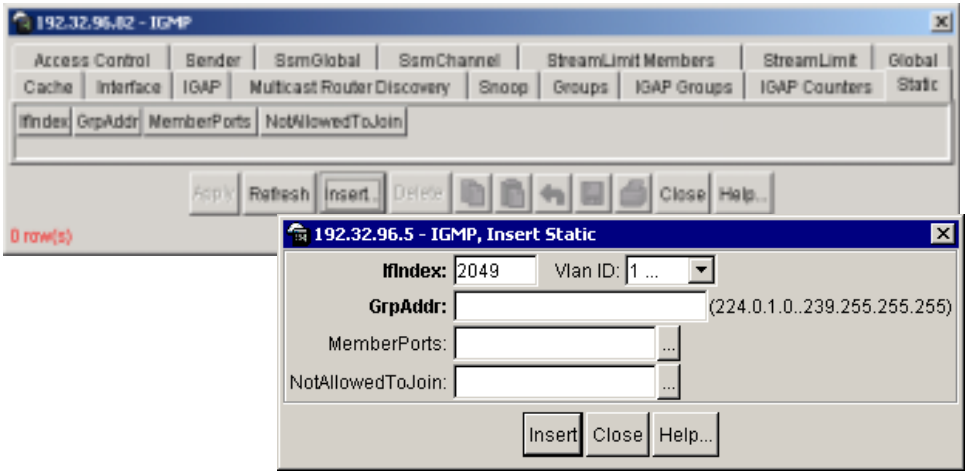


Table 11 describes the fields in the IGMP, Insert Static dialog box.

Table 11 IGMP, Insert Static dialog box fields

Field	Description
Ifndex	The interface on which IGMP entry is enabled.
GrpAddr	Enter the multicast group address of the multicast stream. Within the indicated valid range (224.0.1.0 to 239.255.255.255), the following are invalid addresses: 244.0.0.x and the corresponding 31 multicast addresses that map to the IP MAC addresses. If you try to select them, you will receive an invalid message.
MemberPorts	The ports to which you want to redirect the multicast stream for this multicast group. The ports must be member ports of the VLAN.
NotAllowedToJoin	The ports that will not receive the multicast stream for this multicast group.

Configuring multicast access control

Before you can configure multicast access control, you must first configure one or more prefix lists. Prefix lists are lists of routes that can be applied to one or more route policies. They contain a set of contiguous or non-contiguous routes. Prefix lists are referenced by name from within the routing policies. For more information about prefix lists, see *Configuring IP Routing Operations*.

This section contains the following topics:

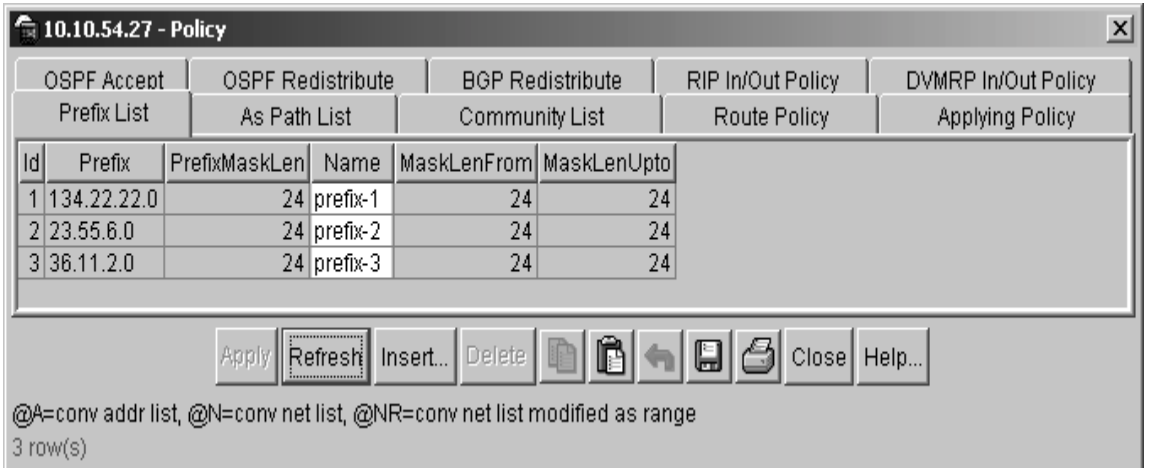
Configuring a prefix list

To set up a route policy prefix list:

1 From the Device Manager menu bar, choose IP Routing > Policy.

The Policy dialog box opens with the Prefix List tab displayed (Figure 25).

Figure 25 Policy dialog box—Prefix List tab



2 Click Insert.

The Policy, Insert Prefix List dialog box opens (Figure 26).

3 Click Insert.

Figure 26 Policy, Insert Prefix List dialog box

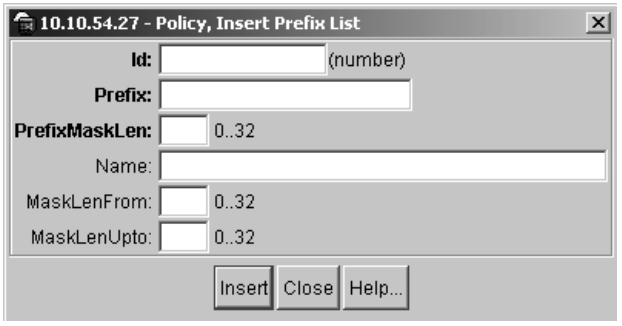


Table 12 describes the Policy, Insert Prefix List dialog box fields.

Table 12 Policy, Insert Prefix List dialog box fields

Field	Description
ID	The list identifier.
Prefix	The IP address.
PrefixMaskLen	This is the specified length of the prefix mask. **Note:** You must enter the full 32-bit mask in order to exact a full match of a specific IP address (for example, such as when creating a policy to match on next-hop).
Name	The name command is used to name a specified prefix list during the creation process or to rename the specified prefix list. The name length can be from 1 to 64 characters.
MaskLenFrom	The lower bound of the mask length. The default is the mask length.
MaskLenUpto	The higher bound mask length. The default is the mask length.
Note: Lower bound and higher bound mask lengths together can define a range of networks.	

Configuring multicast access control for an interface

To configure multicast access control for a selected IGMP interface or a VLAN:

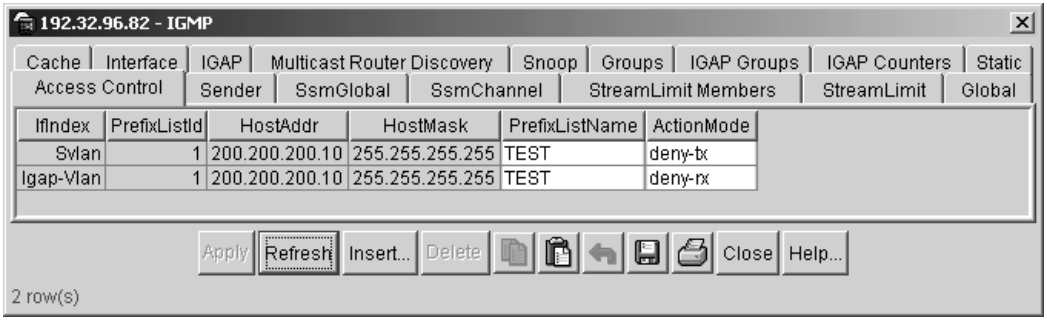
1 From the Device Manager menu bar, choose IP Routing > IGMP.

The IGMP dialog box opens with the Cache tab displayed.

2 Click the Access Control tab.

The Access Control tab opens (Figure 27).

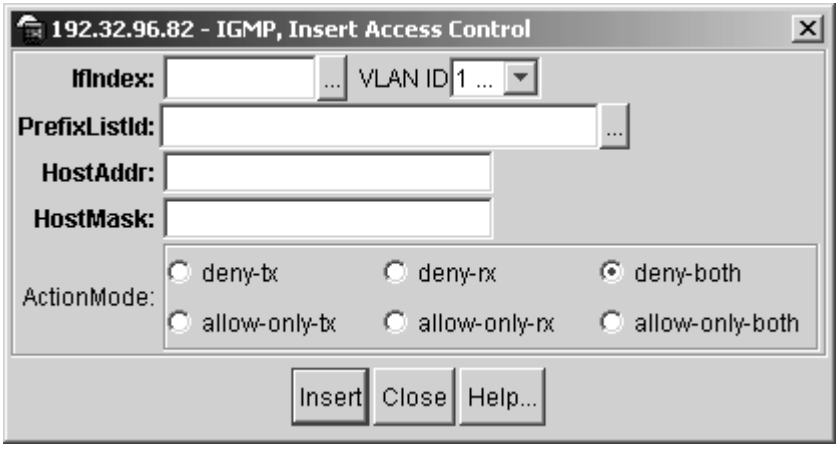
Figure 27 IGMP dialog box —Access Control tab



3 Click Insert.

The IGMP, Insert Access Control dialog box opens (Table 28).

Figure 28 IGMP, Insert Access Control dialog box



4 If you're configuring multicast access control for an IGMP interface, click the ellipsis button (...) next to IfIndex (Figure 29). Select the interface on which the IGMP entry is enabled.

If you're configuring multicast access control for a VLAN, click the down arrow button next to VLAN ID (Figure 30). Select the ID (1 through 8). The IfIndex defaults to a value between 2049 to 2056, inclusive. The value depends on the VLAN ID that you selected (for example, VLAN ID 1 = IfIndex 2049, VLAN ID 2 = IfIndex 2050, VLAN ID 3 = IfIndex 2051, and so forth).

Figure 29 IgmpNewAccessIfIndex dialog box

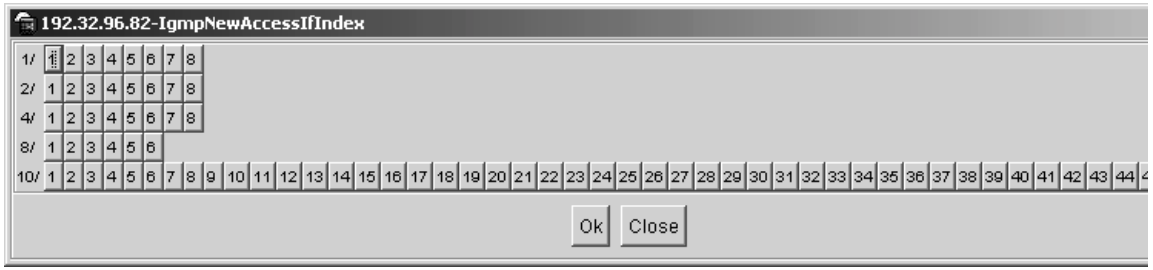
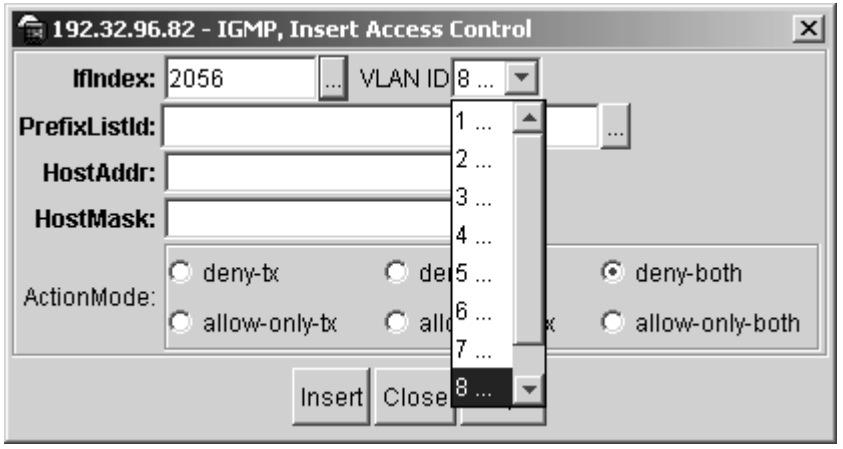


Figure 30 IGMP, Insert Access dialog box with VLAN ID



5. Click the down arrow button next to PrefixListId. Select the prefix list ID/ name that you want.
6. Enter the host address and host mask.
7. Select the action mode that you want for the specified host.
8. Click Insert.
9. Click Close.

Table 13 describes the Access Control tab fields.

Table 13 Access Control tab fields

Field	Description
IfIndex	The interface on which the IGMP entry is enabled.
VLAN ID	Identifies the VLAN on which you want to configure multicast access control.
PrefixListId	A numeric string that identifies the prefix list. See “Configuring a prefix list” on page 114 for more information about prefix lists.
HostAddr	The IP address of the host. See “Specifying host addresses and masks” for more information.
HostMask	The subnet mask used to determine the host or hosts covered by this configuration. You can use the host subnet mask to restrict access to a portion of the host’s network. See “Specifying host addresses and masks” for more information.
PrefixListName	The name of the prefix list. See “Configuring a prefix list” on page 114 for more information about prefix lists.
ActionMode	Used to specify whether the host identified by HostAddr should be: • Denied IP multicast transmitted traffic (deny-tx). • Denied IP multicast received traffic (deny-rx). • Denied both IP multicast transmitted and received traffic (deny-both). • Allowed IP multicast transmitted traffic (allow-only-tx). • Allowed IP multicast received traffic (allow-only-rx). • Allowed both IP multicast transmitted and received traffic (allow-only-both).

Configuring IGMP sender entries

To configure IGMP sender entries:

1. From the Device Manager menu bar, choose IP Routing > IGMP.

   The IGMP dialog box opens with the Cache tab displayed.

2. Click the Sender tab.

   The Sender tab opens (Figure 28).

Figure 31 IGMP dialog box —Sender tab

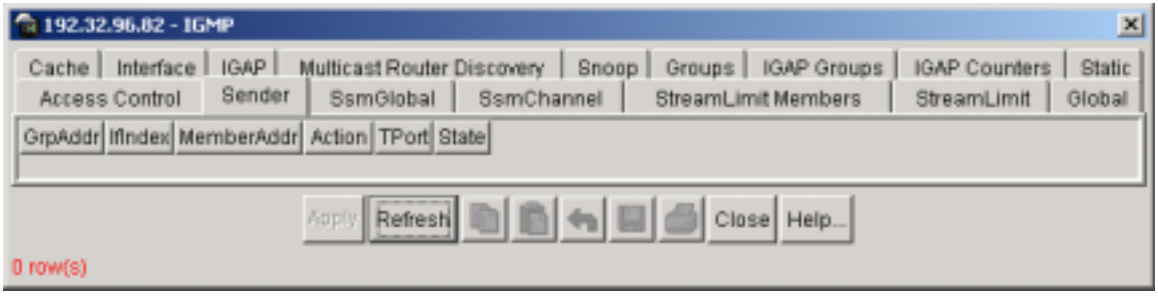


Table 14 describes the Sender tab fields.

Table 14 Sender tab fields

Field	Description
GrpAddr	Enter the Multicast group address of the multicast stream. Within the indicated valid range (224.0.1.0 to 239.255.255.255), the following are invalid addresses: 244.0.0.x and the corresponding 31 multicast addresses that map to the IP MAC addresses. If you try to select them, you will receive an invalid message.
IfIndex	The interface on which IGMP entry is enabled.
MemberAddr	The IP address of a host for which this entry contains information.
Action	Used to flush an entry or a group.

Table 14 Sender tab fields

Field	Description
TPort	Identifies the T Port.
State	Indicates whether or not a sender exists because of an IGMP access filter. The options are: filtered and not filtered.

Configuring the SSM range and global parameters

The SSM range parameter allows you to extend the default SSM range of 232/8 to include any IP multicast address. This feature enables you to configure existing applications without having to change their group configurations.

The other global parameters in this dialog box enable the IGMPv3 dynamic learning feature and set the admin state for all the entries in the SSM channel table.

To configure the SSM range and other global parameters:

1. From the Device Manager menu bar, choose IP Routing > IGMP.

   The IGMP dialog box opens with the Cache tab displayed.

2. Click the SsmGlobal tab.

   The SsmGlobal tab opens (Figure 32).

Figure 32 IGMP dialog box—SsmGlobal tab

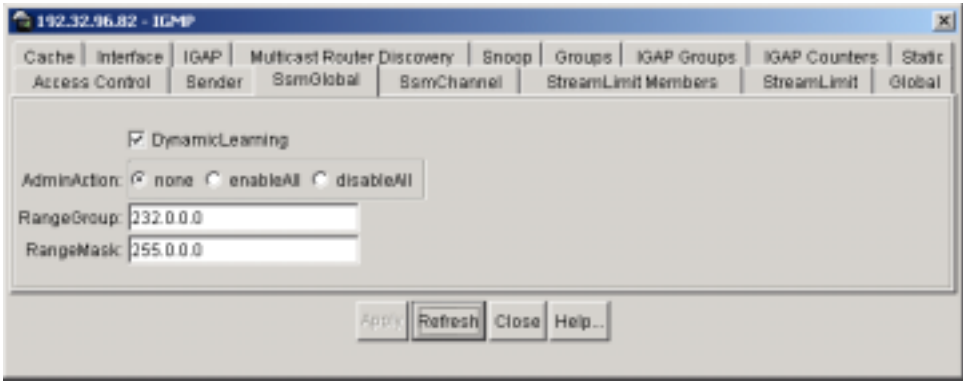


Table 15 describes the SsmGlobal tab fields.

Table 15 IGMP dialog box—SsmGlobal tab fields

Field	Description
DynamicLearning	Enables the dynamic learning of SSM channel (S,G) pairs from IGMPv3 reports. As new SSM channels are learned, they appear in the SSM channel table, see "Configuring the SSM channel table."
AdminAction	Sets the admin state, which determines whether or not the switch uses the table entries. • none (default) - Does not set the admin state globally so that you can set it for individual SSM channel table entries. • enableAll - Globally activates all the static entries in the SSM channel table. This setting does not affect the dynamically learned entries. • disableAll - Globally inactivates all the static entries in the SSM channel table. This setting does not affect the dynamically learned entries. For information on how this setting affects the switch's behavior, see "Configuring the SSM channel table."
RangeGroup	Sets the IP multicast group address. The lowest group address is 224.0.1.0 and the highest is 239.255.255.255. The default is 232.0.0.0. **Note:** Before changing this setting, see "Changing the SSM range group."
RangeMask	Sets the address mask of the multicast group. The default is 255.0.0.0.

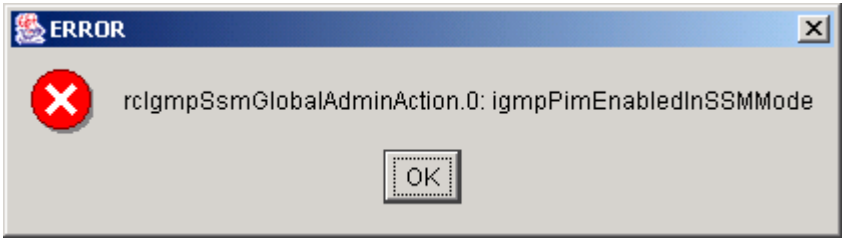
Changing the SSM range group

Note: This procedure re-initializes PIM and temporarily stops all PIM traffic. For those multicast groups out of SSM range (i.e. under PIM-SM behavior), it also causes an RP relearn delay of up to 60 seconds. This delay can be longer if the BSR is local.

To change the SSM range group address, you have to perform the following steps:

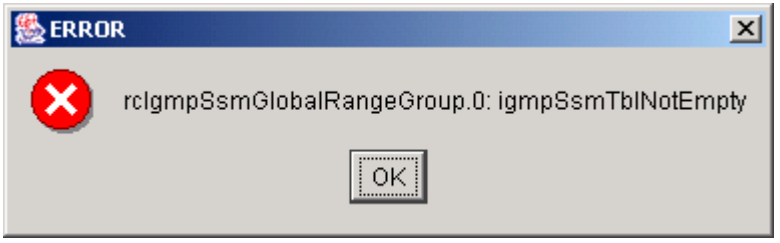
1. Disable PIM.

   If you forget to disable PIM, the following error message opens.



2. Open the SsmChannel tab and delete all of the entries in the SSM channel table.

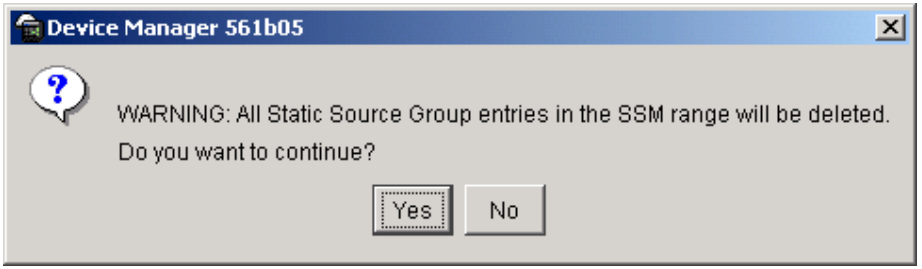
   If you forget to delete the SSM channels, the following error message opens.



3 Enter the new IP multicast group address in the RangeGroup field.

4 Click Apply.

The following message opens to warn you that every static mroute entry that falls into the new SSM range will be deleted.



5 Click Yes.

6 Enable PIM.

Configuring the SSM channel table

The SSM channel table consists of entries that map groups to their sending source. SSM channels cannot conflict with static source groups and vice versa. When you configure an SSM channel or a static source group, the switch performs a consistency check to make sure there are no conflicts. You cannot map one group (G) to different sources for both a static source group and an SSM channel.

The consistency check mentioned above applies to all SSM channel entries, even if they are disabled. Disabling an entry means that it becomes inactive. It does not delete the entry, and you can re-enable it at any time.

When you disable an SSM channel, the Passport 8600 stops any multicast traffic from the specified source to the specified group. If desired, you can use this static setting as a security feature to block traffic from a certain source to a specific group.

For more information, refer to "Configuring multicast static source groups" on page 240.

To create a new or modify an existing SSM channel table entry:

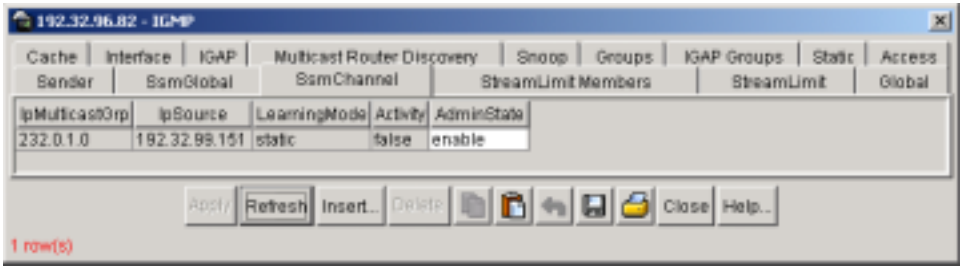
1 From the Device Manager menu bar, choose IP Routing > IGMP.

The IGMP dialog box opens with the Cache tab displayed.

2 Click the SsmChannel tab.

The SsmChannel tab opens (Figure 33).

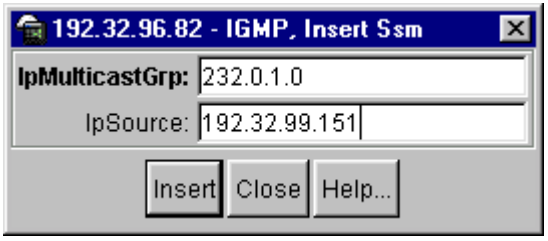
Figure 33 IGMP dialog box—SsmChannel tab



3 Click Insert.

The IGMP, Insert SsmChannel dialog box opens (Figure 34).

Figure 34 IGMP, Insert SsmChannel dialog box



4 Enter the IP address for the multicast group and source.

5 Click Insert.

The SsmChannel tab opens with the entry you just created in the table (Figure 35). You can change the default status of an SSM channel from enable to disable by clicking in the AdminState field.

Figure 35 IGMP dialog box—SsmChannel tab

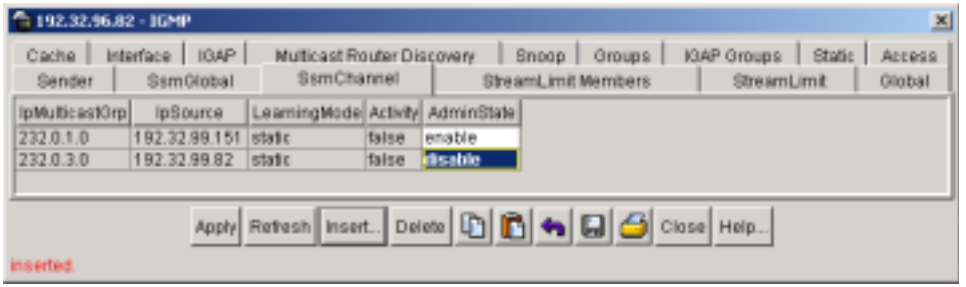


Table 16 describes the SsmChannel table entry fields.

Table 16 IGMP dialog box—SsmChannel tab fields

Field	Description
IpMulticastGrp	Any IP multicast address that is within the SSM range.
IpSource	The source's IP address that will be sending traffic to the group.
LearningMode	Displays whether the entry is statically configured (Static) or a dynamically-learned entry from IGMPv3 (Dynamic). This a read-only field.
Activity	Displays the current activity of the selected (S,G) entry. **True** indicates that traffic is flowing to the switch, otherwise it should display **false**. This a read-only field for the Passport 8600. It does not apply to the Passport 8100.
AdminState	The admin state for the selected static entry. This state determines whether or not the switch uses the static entries. Set this field to **enable** (default) to use the entry or **disable** to save for future use.

Configuring multicast stream limitation

Multicast stream limitation enables providers to limit the number of multicast groups that can join a VLAN. By limiting the number of concurrent multicast streams, providers can protect the bandwidth on a specific interface and control access to multicast streams.

The maximum number of streams can be set independently. Once the stream limit is met, any additional join reports for new streams are dropped. This allows you to control the overall bandwidth usage in addition to restricting users from receiving more than a set limit of multicast streams on a given interface.

This section includes the following topics:

Configuring multicast stream limitation on an interface

To configure stream limitation on a specific interface:

1. From the Device Manager menu bar, choose IP Routing > IGMP.

   The IGMP dialog box opens with the Cache tab displayed.

2. Click the StreamLimit tab.

   The StreamLimit tab opens and displays a list of interfaces (Figure 36).

   To change the status of an interface, double click on the StreamLimitEnable field for the selected interface and select enable or disable from the drop down menu. If the interface is enabled, you can edit the Maximum Number of Stream field.

Figure 36 IGMP dialog box—StreamLimit tab

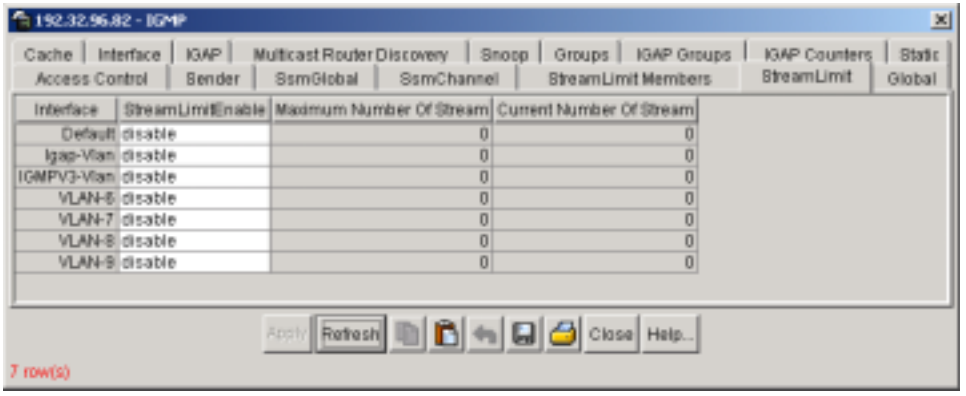


Table 17 describes the StreamLimit tab fields.

Table 17 IGMP dialog box—StreamLimit tab fields

Field	Description
Interface	Displays the slot/port number or VLAN ID for this interface.
Stream Limit Enable	Enables or disables stream limitation on this interface.
Maximum Number Of Stream	Sets the maximum number of streams allowed on this interface. The range is from 0 to 65535, and the default is 4.
Current Number Of Stream	Displays the current number of streams received on this interface. This is a read-only value.

Configuring multicast stream limitation members

To configure multicast stream limitation on ports of the specified interface:

1 From the Device Manager menu bar, choose IP Routing > IGMP.

The IGMP dialog box opens with the Cache tab displayed.

2 Click the StreamLimit Members tab.

The StreamLimit Members tab opens (Figure 32).

Figure 37 IGMP dialog box—StreamLimit Members tab

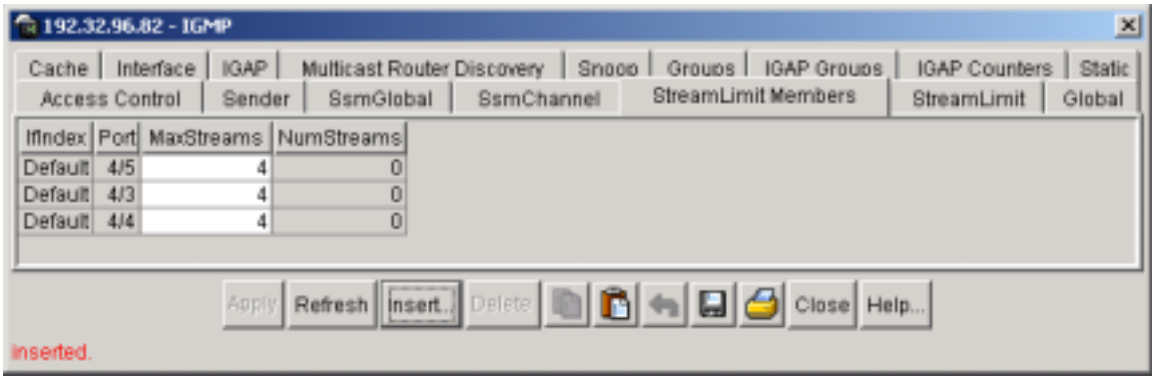


Table 18 describes the StreamLimit Members tab fields.

Table 18 IGMP dialog box—StreamLimit Members tab fields

Field	Description
IfIndex	Displays the name of the VLAN.
Port	Lists each slot/port number for this interface that has stream limitation enabled.
MaxStreams	Sets the maximum number of allowed streams for this specific port. The number of allowed streams cannot exceed the maximum number for the interface. The range is from 0 to 65535, and the default is 4.
NumStreams	Displays the current number of streams received on this interface. This is a read-only value.

Adding a multicast stream limitation member

To add a multicast stream limitation member to an interface:

1. From the Device Manager menu bar, choose IP Routing > IGMP.

   The IGMP dialog box opens with the Cache tab displayed.

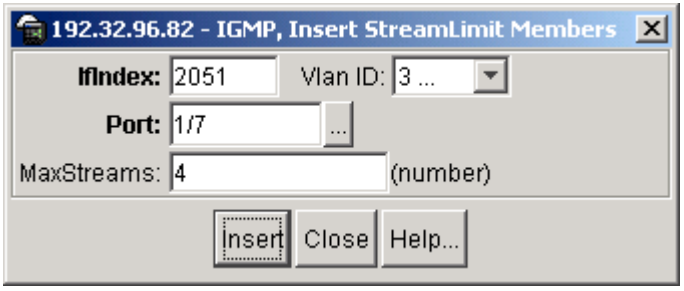
2. Click the StreamLimit Members tab.

   The StreamLimit Members tab opens.

3. Click Insert.

   The Insert StreamLimit Members dialog box opens (Figure 38).

Figure 38 IGMP, Insert StreamLimit Members dialog box



4. Enter the number of the VLAN that you want to add a member to or select one from the Vlan ID drop-down list.

5. Enter the number of the slot/port that you want to add as a member or click on the ellipsis (...) and select one from the graphic display.

Note: The port you select in this step must be one of the ports in the VLAN that you selected in step 4.

6. Enter a maximum number of streams or accept the default of 4.

7. Click Insert.

Deleting a multicast stream limitation member

To delete a multicast stream limitation member from an interface:

1. From the Device Manager menu bar, choose IP Routing > IGMP.

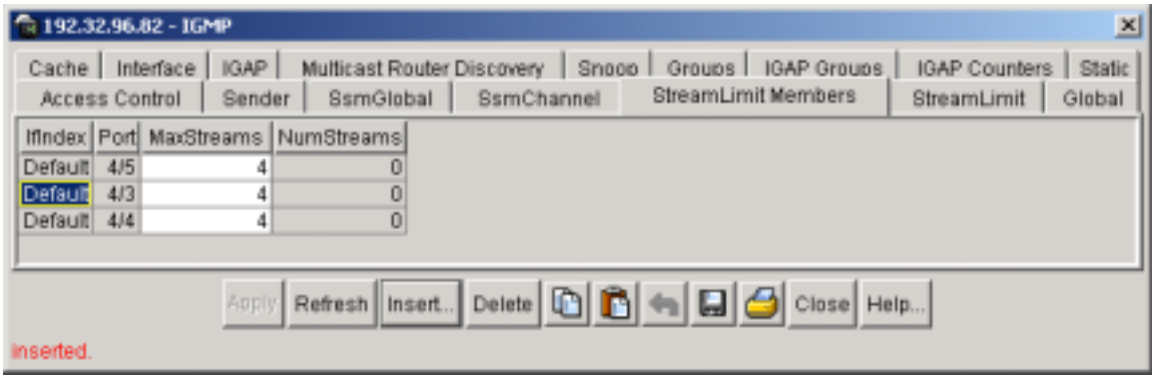
   The IGMP dialog box opens with the Cache tab displayed.

2. Click the StreamLimit Members tab.

   The StreamLimit Members tab opens (Figure 39).

3. Click on the row that lists the member you want to delete.

Figure 39 IGMP dialog box—StreamLimit Members tab



4. Click Delete.

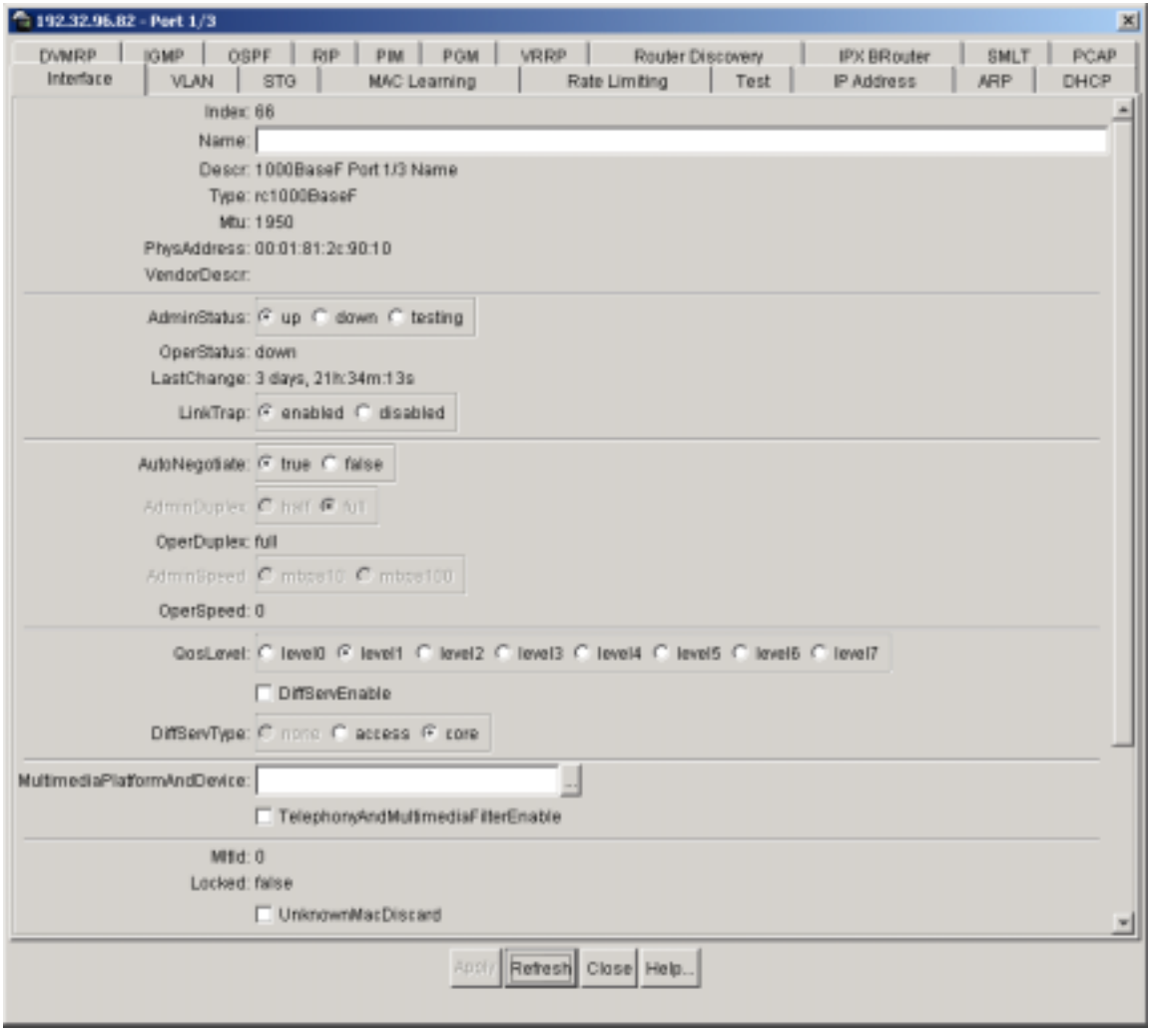
Configuring multicast stream limitation on an Ethernet port

To configure multicast stream limitation on an Ethernet port:

1. On the Device Manager, select a port.
2. From the Device Manager menu bar, choose Edit > Port.

   The Port dialog box opens with the Interface tab displayed (Figure 15).

Figure 40 Port dialog box—Interface tab



3 Click the IGMP tab.

The IGMP tab opens (Figure 16).

Figure 41 Port dialog box—IGMP tab

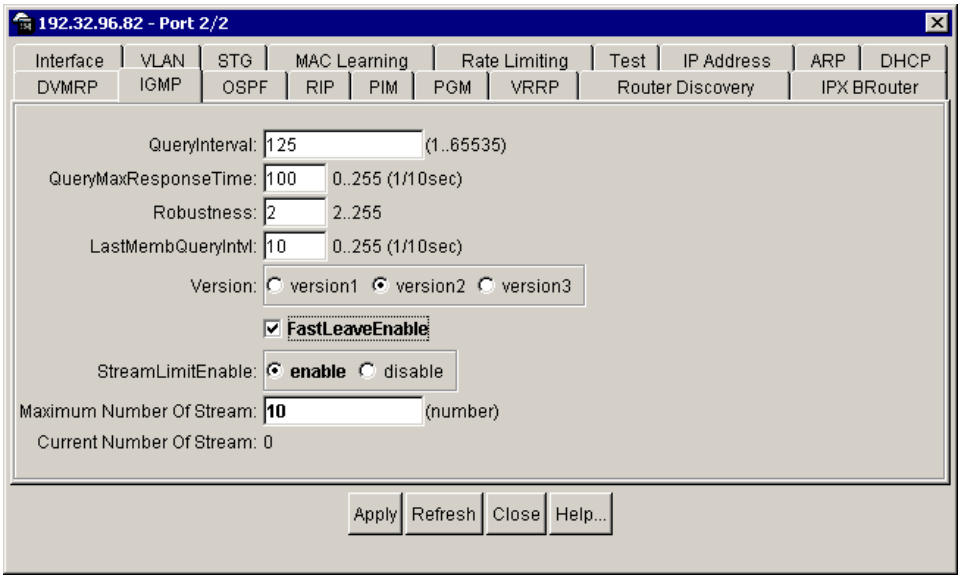


Table 19 describes the stream limitation fields on the port IGMP tab. For information on the other fields on this dialog box, refer to "Configuring IGMP parameters on a brouter port."

Table 19 Port stream limitation fields

Field	Description
StreamLimitEnable	Enables or disables stream limitation on this port.
Maximum Number Of Stream	Sets the maximum number of streams allowed on this port. The range is from 0 to 65535, and the default is 4.
Current Number Of Stream	Displays the current number of streams. This is a read-only value.

Configuring multicast stream limitation on a VLAN

To configure multicast stream limitation on a specific VLAN:

1 From the Device Manager menu bar, choose VLAN > VLANs.

The VLAN dialog box opens, with the Basic tab displayed.

2 Select a VLAN.

3 Click IP.

The IP, VLAN dialog box opens with the IP Address tab displayed.

4 Select IGMP.

The IGMP tab opens (Figure 18).

Figure 42 IP, VLAN dialog box—IGMP tab

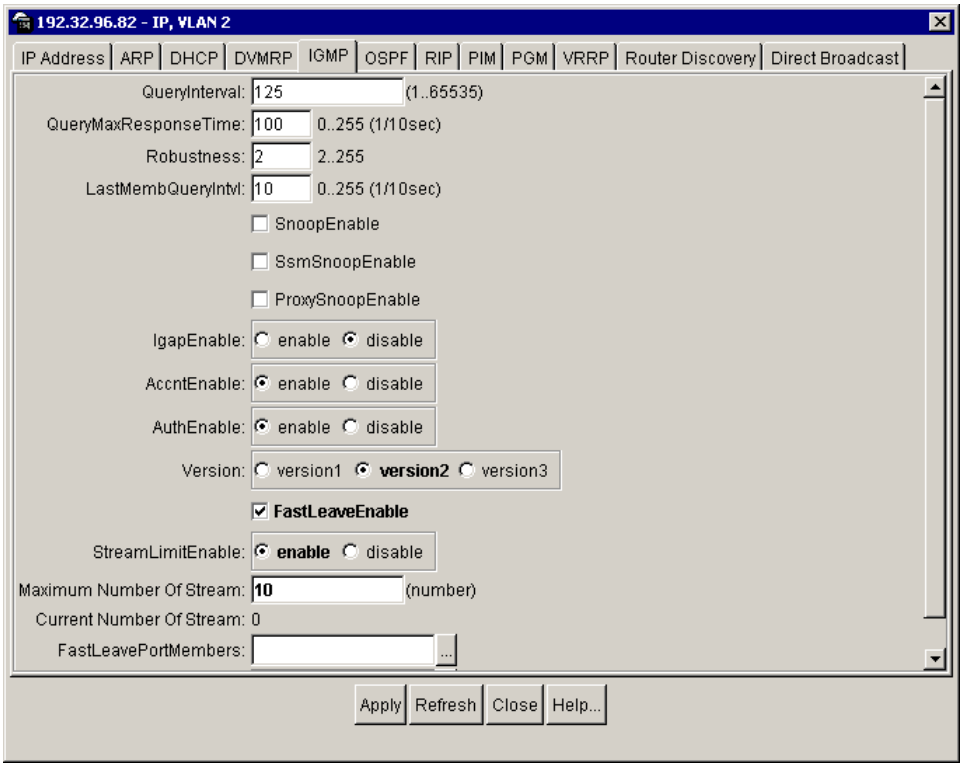


Table 20 describes the stream limitation fields on the IGMP tab. For information on the other fields on this dialog box, refer to "Configuring IGMP parameters on a VLAN."

Table 20 VLAN stream limitation fields

Field	Description
StreamLimitEnable	Enables or disables stream limitation on this VLAN.
Maximum Number Of Stream	Sets the maximum number of streams allowed on this VLAN. The range is from 0 to 65535, and the default is 4.
Current Number Of Stream	Displays the current number of streams. This is a read-only value.

Chapter 3
Configuring DVMRP using Device Manager

DVMRP is used between routers to exchange multicast routing information. For more information about DVMRP concepts and terminology, refer to Chapter 1, "IP Multicast concepts."

For instructions on how to configure DVMRP static source groups, refer to Chapter 6, "Viewing and editing multicast routes using Device Manager."

This chapter describes the following topics:

Configuration prerequisites

Before you can configure DVMRP, you must prepare the router as follows:

1. Configure an IP interface. For information, refer to *Configuring IP Routing Operations*.
2. Disable PIM-SM from the interface on which you want to configure DVMRP because you cannot configure PIM-SM and DVMRP on the same interface.

Note: Changing the configuration from PIM to DVMRP, or from DVMRP to PIM, is not recommended while multicast traffic is flowing on the network.

For information on disabling PIM-SM, refer to Chapter 4, "Configuring PIM using Device Manager."

   a. A *switch* can have a mix of DVMRP and PIM-SM interfaces if it is configured as an multicast border router (MBR).

   b. An *interface* can only be configured with one multicast routing protocol at a time (DVMRP or PIM-SM).

3. Enable DVMRP globally.

   To enable DVMRP globally, see "Enabling DVMRP globally."

Enabling DVMRP globally

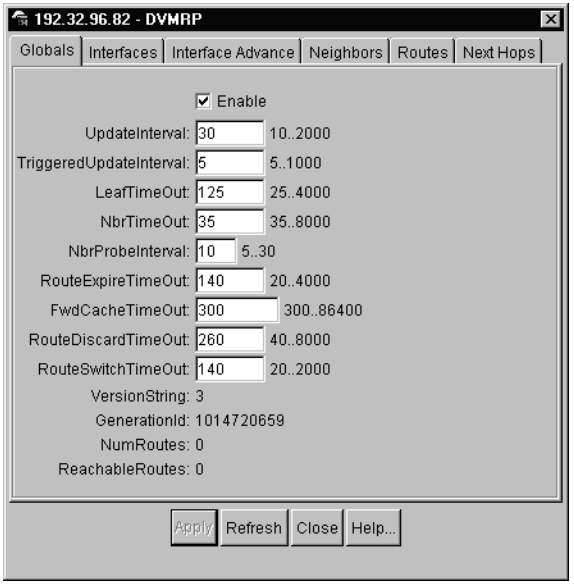
When you enable DVMRP globally and on a particular interface, the IGMP parameters automatically take effect.

To enable DVMRP globally:

1 From the Device Manager menu bar, choose IP Routing > DVMRP.

The DVMRP dialog box opens with the Globals tab displayed (Figure 43).

Figure 43 DVMRP dialog box—Globals tab



2 Click Enable.

3 Click Apply.

Table 21 describes the Globals tab fields.

Table 21 Globals tab fields

Field	Description
Enable	Enables (true) or disables (false) DRMRP on the routing switch. You must globally enable DVMRP before you can enable port or VLAN IGMP or DVMRP.
UpdateInterval	Periodically each multicast router advertises routing information on each DVMRP interface, using the DVMRP export message. You can specify the time interval (in seconds) between DMVRP updates. The range is from 10 to 2000 with a default of 60.
TriggeredUpdateInterval	Triggered updates are sent when routing information changes. This value is the amount of time (in seconds) between triggered update messages. The range is from 5 to 1000 with a default value of 5.
LeafTimeOut	When DVMRP advertises a route on an interface, it waits a period of time for a DVMRP neighbor to respond positively. If no neighbor responds in the given time, the router considers the network attached to the interface a leaf network. The leaf timer allows you to specify how long (in seconds) the router waits for a response from a neighbor. The range is from 25 to 4000 with a default value of 200.
NbrTimeOut	The neighbor report timer specifies how long (in seconds) the router waits to receive a report from a neighbor before considering the connection inactive. The range is from 35 to 8000 with a default of 140.
NbrProbeInterval	Specifies how often the DVMRP router sends probe messages on its interfaces. The range is 5 to 30 seconds with a default of 10.
RouteExpireTimeOut	Defines the route expiration time-out value. The range is 20 to 4000 seconds with a default value of 140 seconds.
FwdCacheTimeOut	Defines forward cache time-out value, which is used is aging prune entries. The range is 300 to 86,400 seconds with a default value of 300 seconds.
RouteDiscardTimeOut	Defines the time to garbage collect route. The range is 40 to 8000 seconds with a default value of 260 seconds.
RouteSwitchTimeOut	Defines the route discard time-out value. The range is 20 to 2000 seconds with a default value of 140 seconds.
VersionString	The router’s DVMRP version information.

Table 21 Globals tab fields (continued)

Field	Description
GenerationId	Used by neighboring routers to detect whether a reset or disable/enable DVMRP action has occurred to the switch or to a particular interface. If so, the router should resend the entire multicast routing table to its neighbor immediately instead of waiting for the next scheduled update.
NumRoutes	The number of entries in the routing table. Use this information to monitor the routing table size to detect illegal advertisements of multicast routes.
ReachableRoutes	The number of entries in the routing table with noninfinite metrics. Use this number to detect network partitions by observing the ratio of reachable routes to total routes.

Enabling DVMRP on a brouter port

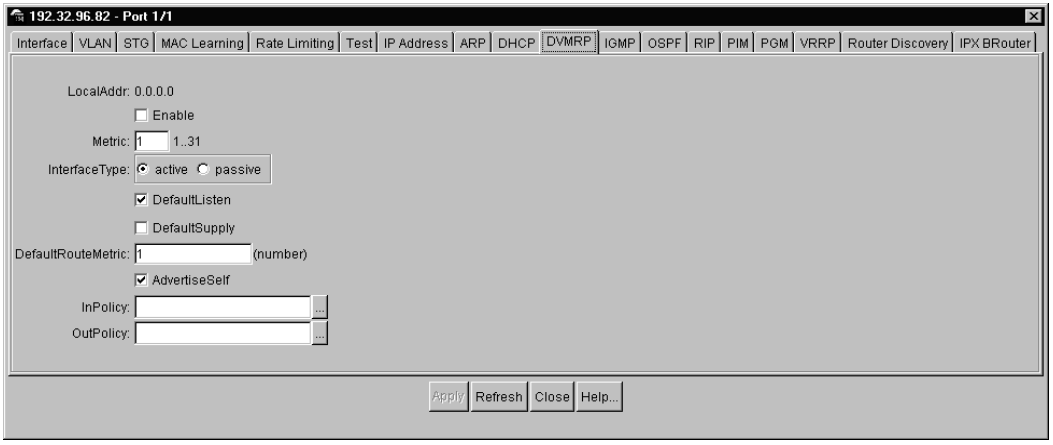
To configure DVMRP on a brouter port:

1. On the Device Manager, select a port.
2. From the Device Manager menu bar, choose Edit > Port.

   The Port dialog box opens with the Interface tab displayed.
3. Click the DVMRP tab.

   The Port dialog box opens with the DVMRP tab displayed (Figure 44).

Figure 44 Port dialog box—DVMRP tab



4 Click the Enable check box to select DVMRP on the port, or click to clear the check box.

5 Enter a metric (cost) in maximum number of hops for DVMRP; the range is 1 to 31. A default value of 1 means local delivery only. You can use the metric value to control the scope of the DVMRP routes.

Table 22 describes the Globals tab fields.

Table 22 Port dialog box—DVMRP tab fields

Field	Description
LocalAddress	Provides the IP address of the DVMRP router interface.
Enable	Enables (checkbox selected) or disables (checkbox not selected) DRMRP on the port.
Metric	Specifies the distance metric for this port, used to calculate distance vectors. The range is 1 to 31 hops.
InterfaceType	Sets the port type as passive or active.
DefaultListen	Sets the port to listen (checkbox selected) or not listen (checkbox not selected) for the default route.
DefaultSupply	Sets the port to supply (checkbox selected) or not supply (checkbox not selected) only the default route.
DefaultRouteMetric	Sets the metric (number of hops for DVMRP) of the default route. The range is 1 to 31 hops.
AdvertiseSelf	Sets the port to advertise (checkbox selected) or not advertise (checkbox not selected) local routes to neighbors.
InPolicy	Selects the name of the DVMRP accept policy applied to the port.
OutPolicy	Selects the name of the DVMRP announce policy applied to the port.

Enabling DVMRP on a VLAN

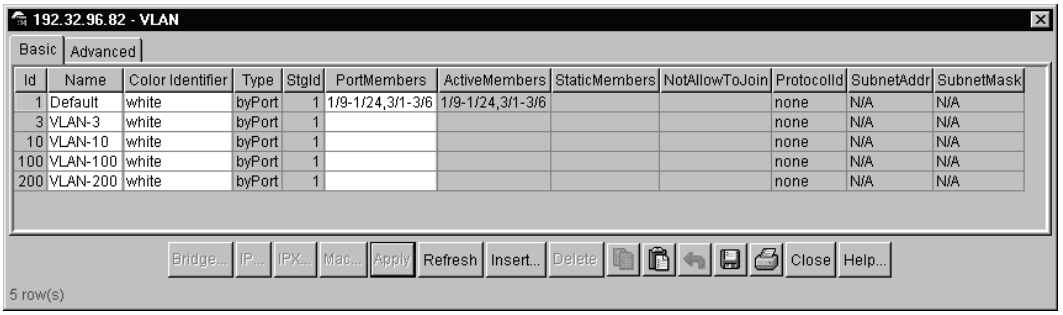
You must enable DVMRP on a VLAN before you configure IGMP on a VLAN.

To enable DVMRP on a VLAN:

1 From the Device Manager, choose VLAN > VLAN.

The VLAN dialog box opens with the Basic tab displayed (Figure 45).

Figure 45 VLAN dialog box—Basic tab

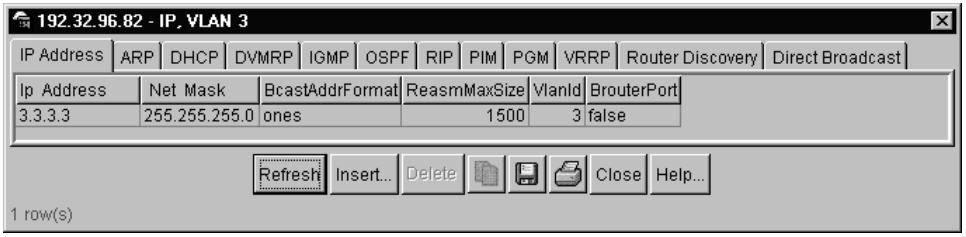


2 Select a VLAN.

3 Click IP.

The IP, VLAN dialog box opens with the IP Address tab displayed (Figure 46).

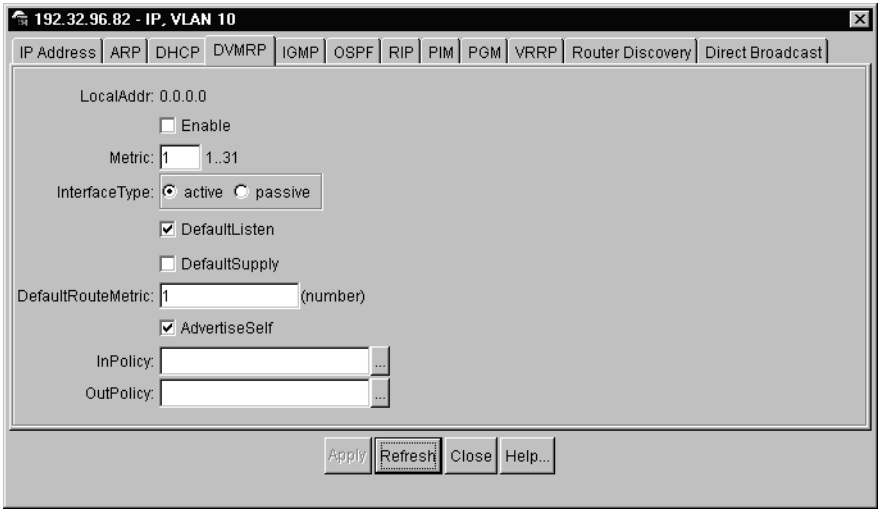
Figure 46 IP, VLAN dialog box—IP Address tab



4 Click the DVMRP tab.

The DVMRP tab opens (Figure 47).

Figure 47 IP, VLAN dialog box—DVMRP tab



5 Click the Enable check box to select DVMRP on the port, or click to clear the check box.

6 Enter a metric (cost) in maximum number of hops for DVMRP; the range is 1 to 31. A default value of 1 means local delivery only. You can use the metric value to control the scope of the DVMRP routes.

Table 23 describes the DVMRP tab fields

Table 23 DVMRP tab fields

Field	Description
LocalAddress	Provides the IP address of the DVMRP router interface.
Enable	Enables (checkbox selected) or disables (checkbox not selected) DRMRP on the VLAN.
Metric	Specifies the distance metric for this VLAN, used to calculate distance vectors. The range is 1 to 31 hops.
InterfaceType	Sets the VLAN type as passive or active.
DefaultListen	Sets the VLAN to listen (checkbox selected) or not listen (checkbox not selected) for the default route.
DefaultSupply	Sets the VLAN to supply (checkbox selected) or not supply (checkbox not selected) only the default route.
DefaultRouteMetric	Sets the metric (number of hops for DVMRP) of the default route. The range is 1 to 31 hops.
AdvertiseSelf	Sets the VLAN to advertise (checkbox selected) or not advertise (checkbox not selected) local routes to neighbors.
InPolicy	Selects the name of the DVMRP accept policy applied to the VLAN.
OutPolicy	Selects the name of the DVMRP announce policy applied to the VLAN.

Viewing and editing DVMRP interface parameters

To view or edit DVMRP interface parameters:

1. From the Device Manager menu bar, choose IP Routing > DVMRP.

   The DVMRP dialog box opens with the Globals tab displayed (Figure 43).

2. Click the Interfaces tab.

   The Interfaces tab opens (Figure 48).

Figure 48 DVMRP dialog box—Interfaces tab

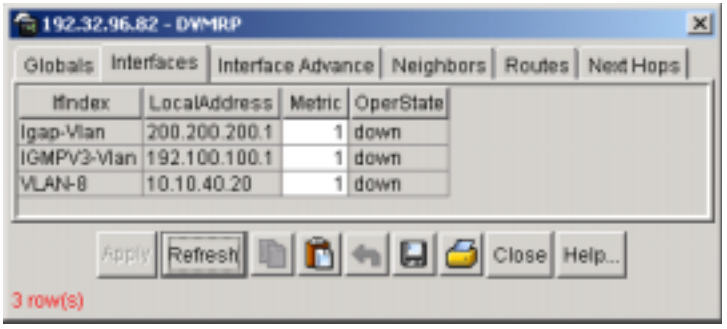


Table 24 describes the DVMRP Interfaces tab fields.

Table 24 DVMRP Interfaces tab fields

Field	Description
IfIndex	The DVMRP interface, slot/port number, or VLAN identification.
LocalAddress	The IP address of the DVMRP router interface.
Metric	The distance metric for this interface, used to calculate distance vectors. The range is 1 to 31. The default value is 1, which means local delivery only.
OperState	The current operational state of this DVMRP interface (up or down).

Viewing and editing DVMRP interface advance parameters

You can configure an interface to listen for a default route and/or supply a default route. You can also configure an interface to specify the metric (cost) of the default route, which will be advertised if the interface is configured to supply a default route.

To view or edit DVMRP interface advance parameters:

1. From the Device Manager menu bar, choose IP Routing > DVMRP.

   The DVMRP dialog box opens with the Globals tab displayed (Figure 43).

2. Click the Interface Advance tab.

   The DVMRP Interface Advance tab opens and displays the DVMRP configuration options (Figure 49). Table 25 provides a description of the fields in this dialog box.

Figure 49 DVMRP dialog box—Interface Advance tab

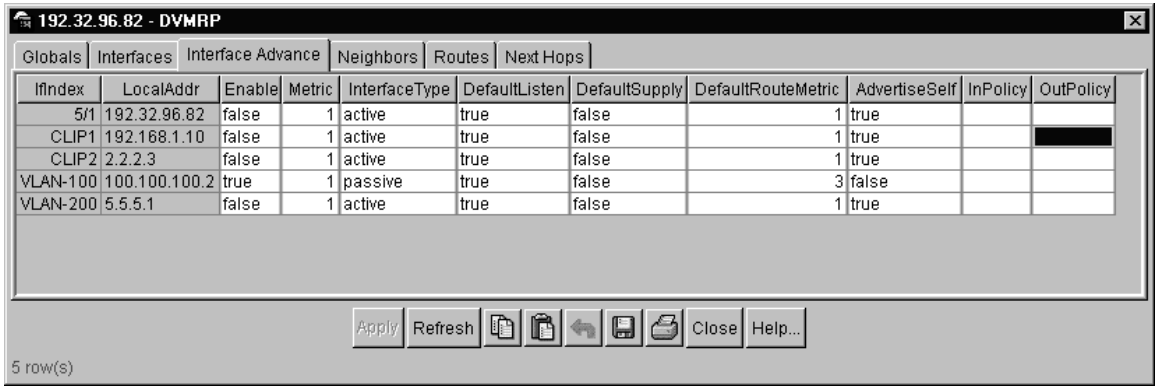


Table 25 describes the DVMRP Interface Advance tab fields.

Table 25 DVMRP dialog box—Interface Advance tab fields

Field	Description
IfIndex	Provides the DVMRP interface, VLAN, and/or slot/port number identification.
LocalAddress	Provides the IP address of the DVMRP router interface.
Enable	Enables (true) or disables (false) DRMRP on the interface.
Metric	Specifies the distance metric for this interface, used to calculate distance vectors. The range is 1 to 31 hops.
InterfaceType	Sets the interface type as passive or active.
DefaultListen	Sets the interface to listen (true) or not listen (false) for the default route. The default is true, which indicates that the interface will listen to the default route.
DefaultSupply	Sets the interface to supply (true) or not supply (false) only the default route. The default is false, which is not to supply a default route on that interface.
DefaultRouteMetric	Sets the metric (number of hops for DVMRP) of the default route. The range is 1 to 31 hops.
AdvertiseSelf	Sets the interface to advertise (true) or not advertise (false) its local route to neighbors. The default value is True.
InPolicy	Selects the name of the DVMRP accept policy applied to the interface.
OutPolicy	Selects the name of the DVMRP announce policy applied to the interface.

Viewing DVMRP neighbor parameters

To view the DVMRP neighbor parameters:

1 From the Device Manager menu bar, choose IP Routing > DVMRP.

The DVMRP dialog box opens with the Globals tab displayed (Figure 43).

2 Click the Neighbors tab.

The Neighbors tab opens (Figure 50).

Figure 50 DVMRP dialog box—Neighbors tab

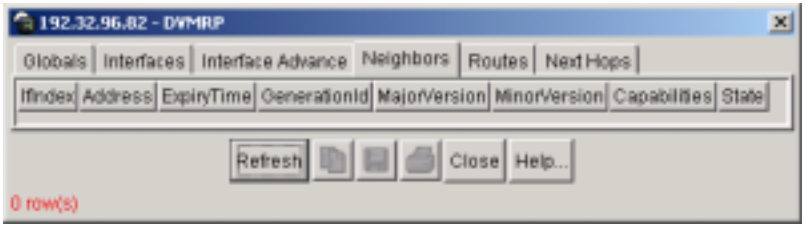


Table 26 describes the Neighbors tab fields.

Table 26 Neighbors tab fields

Field	Description
IfIndex	The DVMRP slot/port number or the virtual interface (VLAN) used to reach this DVMRP neighbor.
Address	The IP address of the DVMRP neighbor for which this entry contains information.
ExpiryTime	The time remaining before this DVMRP neighbor will be aged out.
GenerationId	The neighboring router's generation ID number.
MajorVersion	The neighboring router's major DVMRP version number.
MinorVersion	The neighboring router's minor DVMRP version number.

Table 26 Neighbors tab fields (continued)

Field	Description
Capabilities	The neighboring router's capabilities. The probe flag is 1 byte long with the lower 4 bits containing the following information: • The leaf bit (0) indicates that the neighbor has only one interface with neighbors. • The prune bit (1) indicates that the neighbor supports pruning. • The generationID bit (2) indicates that the neighbor sends its generation ID in probe messages. • The mtrace bit (3) indicates that the neighbor can handle mtrace requests.
State	The state of neighbor adjacency: • oneway—The switch sees a packet from the neighbor but no adjacency has been established. • active—Adjacency exists in both directions. • ignoring • down—The interface is not enabled.

Viewing DVMRP learned routes

To view the DVMRP learned routing table:

1. From the Device Manager menu bar, choose IP Routing > DVMRP.

   The DVMRP dialog box opens with the Globals tab displayed (Figure 43).

2. Click the Routes tab.

   The Routes tab opens (Figure 51).

Figure 51 DVMRP dialog box—Routes tab

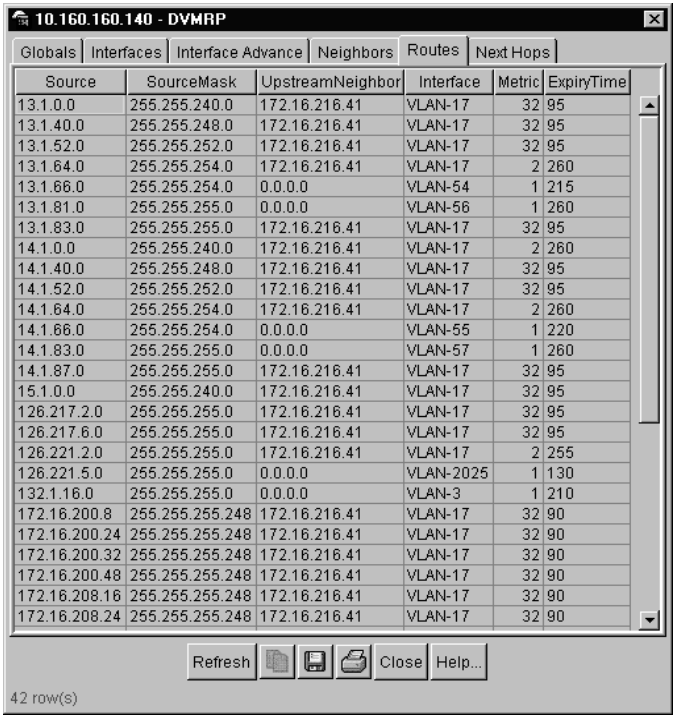


Table 27 describes the fields in the Routes tab.

Table 27 Routes tab fields

Field	Description
Source	The network address which, when combined with the corresponding route SourceMask value, identifies the sources for which this entry contains multicast routing information.
SourceMask	The network mask which, when combined with the corresponding route Source value, identifies the sources for which this entry contains multicast routing information.
UpstreamNeighbor	The address of the upstream neighbor (e.g., RPF neighbor) from which IP datagrams from these sources are received, or 0.0.0.0 if the network is local.
Interface	The DVMRP interface, slot/port number, or VLAN ID on which IP datagrams sent by these sources are received.

Table 27 Routes tab fields (continued)

Field	Description
Metric	The distance in hops to the source subnet. Range is 1 to 32.
ExpiryTime	The amount of time (in seconds) remaining before this entry will be aged out.

Viewing DVMRP next hop information

Note: Before you can show DVMRP next hops, you have to use the CLI to enable showing the next hop table. Enter the following command:
`config ip dvmrp show-next-hop-table enable`

Showing the next-hop table is disabled by default. This avoids using the large amount of memory required for these tables in a scaled multicast environment with a large number of VLANs.

For more information, see Chapter 10, “Configuring DVMRP using the CLI.

To view information about the DVMRP next hops on outgoing interfaces for routing IP multicast datagrams:

1. From the Device Manager menu bar, choose IP Routing > DVMRP.

   The DVMRP dialog box opens with the Globals tab displayed (Figure 43).

2. Click the Routes tab.

   The Next Hops tab opens (Figure 52).

Figure 52 DVMRP dialog box—Next Hops tab

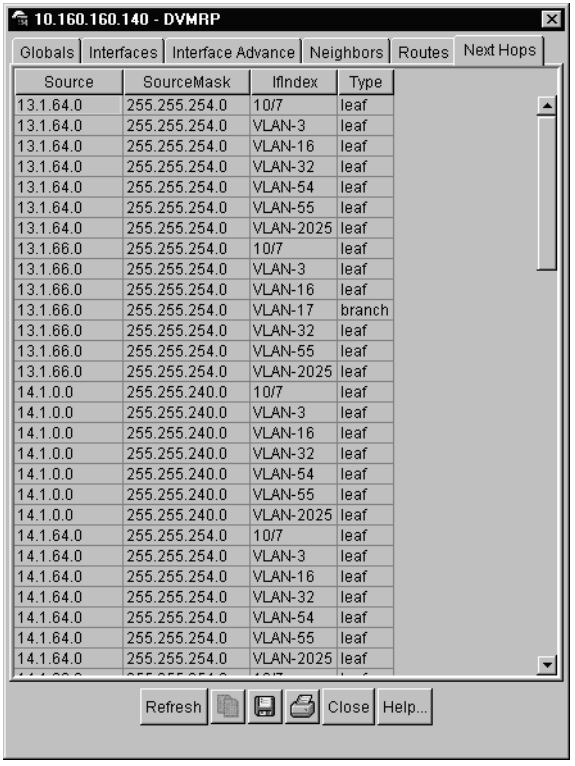


Table 28 describes the fields in the Next Hops tab.

Table 28 Next Hops tab fields

Field	Description
Source	The network address which, when combined with the corresponding next hop SourceMask value, identifies the source for which this entry specifies a next hop on an outgoing interface.
SourceMask	The network mask which, when combined with the corresponding next hop Source value, identifies the source for which this entry specifies a next hop on an outgoing interface.
IfIndex	The DVMRP interface, slot/port number, or VLAN ID for the outgoing interface for this next hop.
Type	Type is 0, or leaf, if no downstream dependent neighbors exist on the outgoing virtual interface. Otherwise, type is branch.

Configuring DVMRP routing policies

DVMRP routing policies allow you to improve the management of the DVMRP routing tables by providing control of how the routing table is populated and how the routes are exchanged between 8000 Series switches. These routing policies, when enabled, can be applied to an interface that can be either a VLAN or a brouter port.

This section includes the following topics:

Configuring default route policies

This section includes the following tasks that describe how to set up your default route configuration using Device Manager:

Before you apply the default route policy to the switch, you must perform the procedures provided in “Configuration prerequisites” on page 134.

You can apply a default route policy to an interface, VLAN or port. To display DVMRP default route configuration information for an interface, VLAN, or port, refer to “Displaying DVMRP routing policy information.”

Applying the default route policy to an interface

You can configure an interface to listen for a default route and/or supply a default route. You can also configure an interface to specify the metric (cost) of the default route, which will be advertised if the interface is configured to supply a default route.

To apply the default route policy to an interface:

1. From the Device Manager menu bar, choose IP Routing > DVMRP.

   The DVMRP dialog box opens with the Globals tab displayed.

2. Select the Interface Advance tab.

   The DVMRP Interface Advance tab opens and displays the DVMRP configuration options (Figure 49).

3. Configure the default route policy for a selected interface as follows:

   a. To set the interface to listen for a default route, set the DefaultListen field for the interface you want to modify to true.

      If you do not want the interface to listen for a default route, set the DefaultListen field to False.

   b. To set the interface to supply only a default route, set the DefaultSupply field for the interface you want to modify to true.

      If you do not want the interface to supply only a default route, set the DefaultSupply field to false.

   c. To set the metric (cost) of the default route to be used when this switch advertises this default route, enter the number of hops for DVMRP in the DefaultRouteMetric field; the range is 1 to 31.

4. Click Apply to save the new configuration.

Applying the default route policy to a VLAN

You can configure a VLAN to listen for a default route and/or supply a default route. You can also configure a VLAN to specify the metric (cost) of the default route, which will be advertised if the VLAN is configured to supply a default route.

To apply the default route policy to a VLAN:

1. From the Device Manager, choose VLAN > VLANs.

   The VLAN dialog box opens with the Basic tab displayed (Figure 45).

2. Select a VLAN ID that you want to configure.

   Several buttons at the bottom of the dialog box become active.

3. Click the IP button.

   The IP, VLAN dialog box opens with the IP Address tab displayed.

4. Click the DVMRP tab.

   The DVMRP tab opens and displays the DVMRP configuration options.

5. Configure the default route policy for the selected VLAN as follows:.

   a. To set the VLAN to listen for a default route, click the DefaultListen check box.

      If you do not want the VLAN to listen for a default route, make sure the DefaultListen check box is not selected.

   b. To set the VLAN to supply only the default route, click the DefaultSupply check box.

      If you do not want the VLAN to supply only the default route, make sure that you do not select the DefaultSupply check box.

   c. To set the metric (cost) of the default route to be used when this switch advertises this default route, enter the number of hops for DVMRP in the DefaultRouteMetric field; the range is 1 to 31.

6. Click Apply to save the new configuration.

Applying the default route policy to a port

You can configure a port to listen for a default route and/or supply a default route. You can also configure a port to specify the metric (cost) of the default route, which will be advertised if the port is configured to supply a default route.

To apply the default route policy to a port:

1. On the Device Manager, select a port.
2. From the Device Manager menu bar, choose Edit > Port.

   The Port dialog box opens with the Interface tab displayed.

3. Click the DVMRP tab.

   The DVMRP tab opens and displays the DVMRP configuration options.
4. Configure the default route policy for the selected port as follows:.
   a. To set the port to listen for a default route, click the DefaultListen check box.

      If you do not want the port to listen for a default route, make sure the DefaultListen check box is not selected.

   b. To set the port to supply only the default route, click the DefaultSupply check box.

      If you do not want the port to supply only the default route, make sure that you do not select the DefaultSupply check box.

   c. To set the metric (cost) of the default route to be used when this switch advertises this default route, enter the number of hops for DVMRP in the DefaultRouteMetric field; the range is 1 to 31.
5. Click Apply to save the new configuration.

Configuring DVMRP announce policies

This section includes the following tasks that describe how to set up your accept policy configuration using Device Manager:

Before you create and apply a DVMRP announce policy to the switch, you must perform the procedures provided in “Configuration prerequisites” on page 134.

Configuring a DVMRP announce policy involves creating a policy and then applying it. To display DVMRP announce policy configuration information for an interface, VLAN, or port, refer to “Displaying DVMRP routing policy information.”

Creating a DVMRP announce policy

Before you can apply an announce policy to an interface, VLAN, or port, you must first create the announce policy.

You can create one or more IP prefix lists and apply that list to any IP route policy. A prefix list with a 32 bit mask is equivalent to an address. A prefix list with a mask less than 32 bits can be used as a network. If you configure the MaskLenFrom field to be less than MaskLenUpto field, it can also be used as a range.

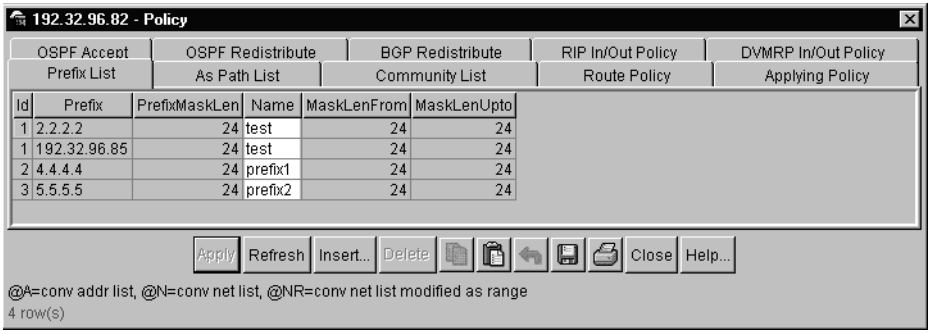
To create a DVMRP announce policy:

1 From the Device Manager menu bar, choose IP Routing > Policy.

The Policy dialog box opens with the Prefix List tab displayed (Figure 53).

The Policy dialog box opens with the Prefix List tab displayed.

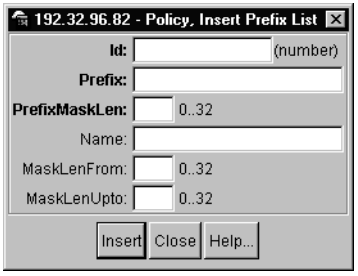
Figure 53 Policy dialog box—Prefix List tab



2 Click Insert.

The Policy, Insert Prefix List dialog box displays (Figure 54).

Figure 54 Prefix List tab—Policy, Insert Prefix List dialog box



3 Create a prefix list for the new policy by entering the following information in the Policy, Insert Prefix List dialog box. (Table 29 describes the information for the required fields in the dialog box.)

a An ID for the prefix list (unique number) in the Id field.

b An IP address in the Prefix field.

c The length of the prefix mask (range is 0 to 32) in the PrefixMaskLen field.

d A name for the prefix list in the Name field.

4 Click Insert.

Table 29 Policy, Insert Prefix List dialog box fields

Field	Description
ID	The list identifier.
Prefix	The IP address and mask.
PrefixMaskLen	This is the specified length of the prefix mask. The range is 0 to 32.
Name	Identifies a specific prefix list during the creation process. The name length can be have from 1 to 64 characters.
MaskLenFrom	A value that specifies the lower bound of mask length. The default is the mask length.
MaskLenUpto	A value that specifies the higher bound mask length. The default is the mask length.

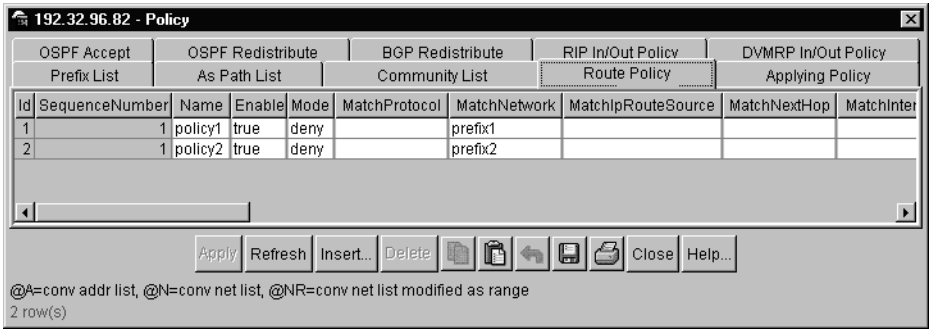
5 Repeat step 3 to include additional IP addresses for the prefix list you created.

You can also create additional prefix lists by repeating step 3.

6 From the Policy dialog box, click the Route Policy tab.

The Route Policy tab opens (Figure 55).

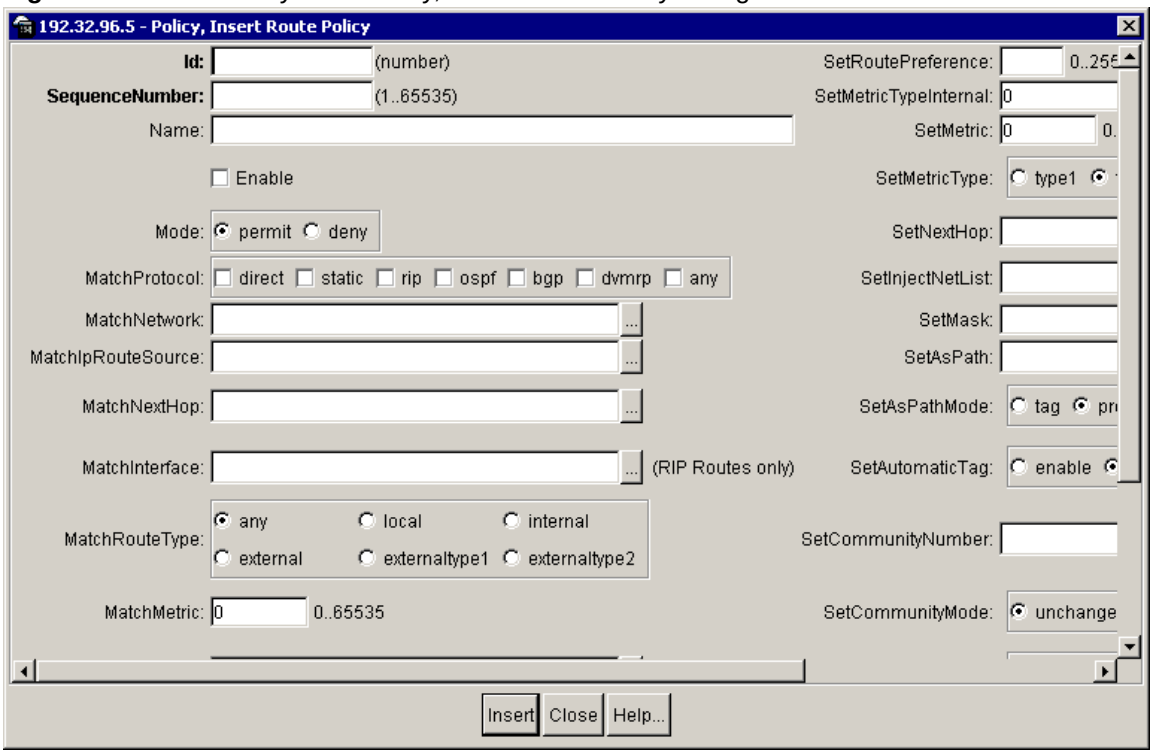
Figure 55 Policy dialog box—Route Policy tab



7 Click Insert.

The Policy, Insert Route Policy dialog box opens (Figure 56).

Figure 56 Route Policy tab—Policy, Insert Route Policy dialog box



8 Create the new policy by entering the following information in the Policy, Insert Route Policy dialog box:

Note: Not all the fields in the Policy, Insert Route Policy dialog box apply to the process of creating a DVMRP policy.

Table 30 describes the fields in the dialog box for which you must supply information to create the DVMRP policy. For information on the other fields in this dialog box, refer to *Configuring IP Routing Operations*.

a In the Id field, enter a number for the policy.

b In the SequenceNumber field, enter a policy sequence number (range is 1 to 65,535).

c In the Name field, specify the name of the policy.

d Select the DVMRP checkbox in the MatchProtocol field.

e Enter the applicable name(s) of the prefix lists you created in Steps 3 and 5 in the MatchNetwork, MatchIPRouteSource, and MatchNextHop fields.

You can enter a single or several prefix lists. You can select up to four lists. To enter the names of the prefix list(s), click the ellipse button to the right of the field, select the appropriate name(s) from the dialog box, and click OK. To select multiple names, use the CTRL key. To deselect an entry, use the ALT key.

f In the MatchMetric field, enter a value (range is 0 to 65,535)

g In the SetMetric field, enter a value (range is 0 to 65,535)

h Click Insert.

Table 30 Policy, Insert Route Policy dialog box

Field	Description
Id	The ID of an entry in the Prefix list table.
SequenceNumber	A second index used to identify a specific policy within a route policy group.
Name	The name of the route policy.
MatchProtocol	Selects the appropriate protocol. Matches the protocol through which the route is learned, if configured.
MatchNetwork	Matches the destination network against the contents of the specified prefix list, if configured.
MatchIpRouteSource	Matches the previous hop IP addresses for DVMRP routes against the contents of the specified prefix list, if configured. Click the ellipse button and choose from the list in the Match Route Source dialog box. You can select up to four entries. To deselect an entry, use the ALT key. Note: This field can also be changed in the Route Policy tab of the Policy dialog box.
MatchNextHop	Matches the previous hop IP address of the route against the contents for the specified prefix list. This field applies only to non-local routes, if configured. Click the ellipse button and choose from the list in the Match Next Hop dialog box. You can select up to four entries. To deselect an entry, use the ALT key.
MatchMetric	Matches the metric of the incoming advertisement or existing route against the specified value (1to 655535). If 0, then this field is ignored, if configured. The default is 0.

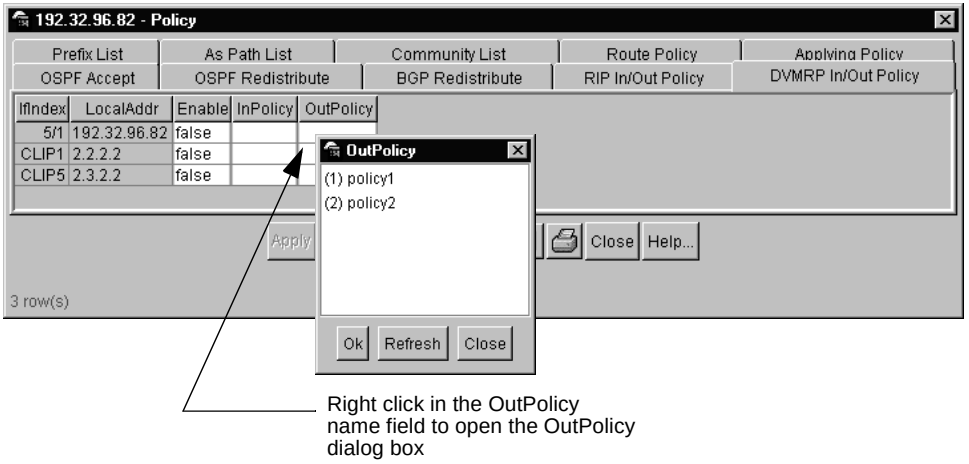
Table 30 Policy, Insert Route Policy dialog box (continued)

Field	Description
MatchInterface	If configured, the switch matches the IP address of the interface by which the RIP route was learned against the contents of the specified prefix list. This field is used only for RIP routes and ignored for all other type of route. (applies to RIP routes only.) Click the ellipse button and choose from the list in the Match Interface dialog box. You can select up to four entries. To deselect an entry, use the ALT key.
MatchRouteType	Sets a specific route-type to be matched (applies only to OSPF routes). Externaltype1, and Externaltype2 specify the OSPF routes of the specified type only. OSPF internal refers to intra and inter area routes.
MatchAsPath <as-list>	If configured, the switch matches the as-path attribute of the BGP routes against the contents of the specified as-lists. This field is used only for BGP routes and ignored for all other type of route. • *<as-list>* specifies the list id of up to four defined as-lists separated by a comma. • [clear] when presents, the as-list configured will be removed.

9 From the Policy dialog box, click the DVMRP In/Out Policy tab.

The DVMRP In/Out Policy tab opens (Figure 57). The Enable field indicates the current status (true is enabled; false is disabled).

Figure 57 Policy dialog box—DVMRP In/Out Policy tab



10 Right click in the OutPolicy name field of the DVMRP interface to which you want to apply the announce policy and select the appropriate policy name from the PolicyName dialog box.

11 Click Apply to save the new configuration.

Applying a DVMRP announce policy to an interface

To apply an announce policy to an interface:

1. From the Device Manager menu bar, choose IP Routing > DVMRP.

   The DVMRP dialog box opens with the Globals tab displayed.

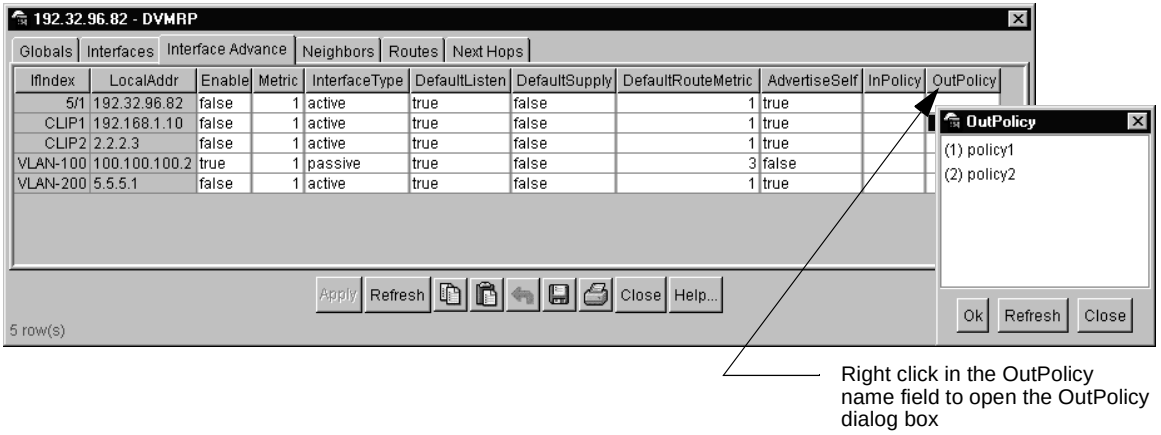
2. Select the Interface Advance tab.

   The DVMRP Interface Advance tab opens and displays the DVMRP configuration options (Figure 49).

3. Double-click the OutPolicy field for a selected interface.

   The OutPolicy dialog box opens and displays the list of policies you can apply to the interface (Figure 58).

Figure 58 DVMRP Interface tab—OutPolicy dialog box



4. Select a policy name and click OK.

5. Click Apply from the DVMRP Interface Advance tab.

Applying a DVMRP announce policy to a VLAN

To apply an announce policy to a VLAN:

1. From the Device Manager, choose VLAN > VLANs.

   The VLAN dialog box opens with the Basic tab displayed (Figure 45).

2. Select a VLAN and click IP.

   The IP, VLAN dialog box opens with the IP Address tab displayed.

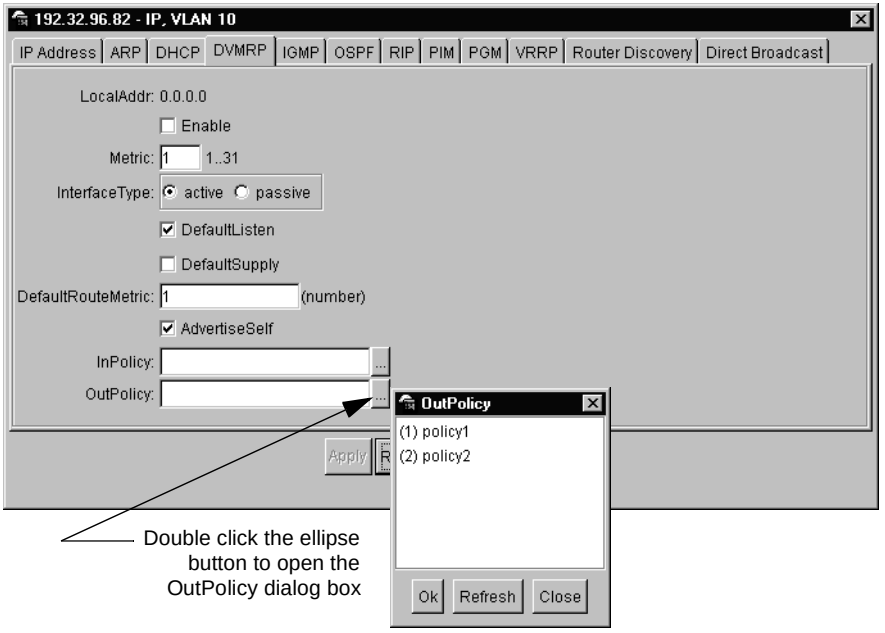
3. Click the DVMRP tab.

   The DVMRP tab opens and displays the DVMRP configuration options.

4. Double-click the button to the right of the OutPolicy field.

   The OutPolicy dialog box opens and displays the list of policies you can apply to the interface (Figure 59).

Figure 59 DVMRP VLAN tab—OutPolicy dialog box



5. Select a policy name and click OK.

6. Click Apply from the DVMRP port tab.

Applying a DVMRP announce policy to a port

To apply an announce policy to a port:

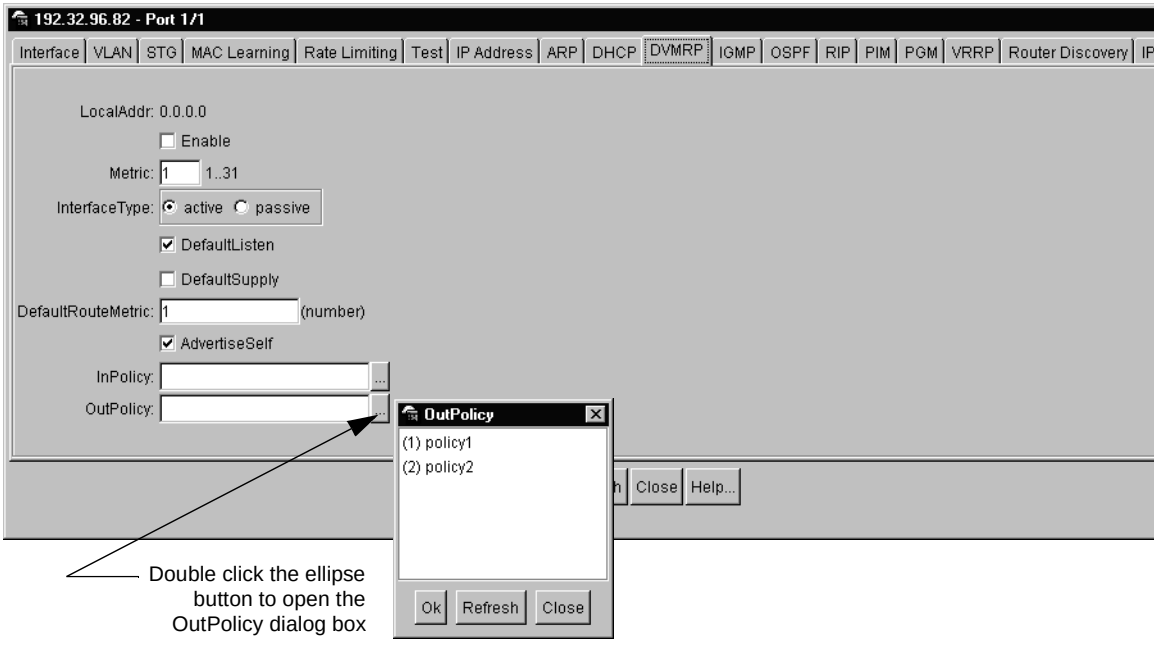
1. On the Device Manager, select a port.
2. From the Device Manager menu bar, choose Edit > Port.

   The Port dialog box opens with the Interface tab displayed.
3. Click the DVMRP tab.

   The DVMRP tab opens and displays the DVMRP configuration options.
4. Double-click the ellipse button to the right of the OutPolicy field.

   The OutPolicy dialog box opens and displays the list of policies you can apply to the interface (Figure 60).

Figure 60 DVMRP Port tab—OutPolicy dialog box



5. Select a policy name and click OK.
6. Click Apply from DVMRP tab.

Configuring DVMRP accept policies

This section includes the following tasks that describe how to set up your accept policy configuration using Device Manager:

Before you create and apply a DVMRP accept policy to the switch, you must perform the procedures provided in “Configuration prerequisites” on page 134.

Configuring a DVMRP accept policy involves creating a policy and then applying it. To display DVMRP accept policy configuration information for an interface, VLAN, or port, refer to “Displaying DVMRP routing policy information.”

Creating a DVMRP accept policy

Before you can apply an accept policy to an interface, VLAN, or port, you must first create the policy.

You can create one or more IP prefix lists and apply that list to any IP route policy. A prefix list with a 32 bit mask is equivalent to an address. A prefix list with a mask less than 32 bits can be used as a network. If you configure the MaskLenFrom field to be less than MaskLenUpto field, it can also be used as a range.

To create a DVMRP accept policy:

1. From the Device Manager menu bar, choose IP Routing > Policy.

   The Policy dialog box opens with the Prefix List tab displayed (Figure 53).

2. Click Insert.

   The Policy, Insert Prefix List dialog box displays (Figure 54).

3. Create a prefix list for the new policy by entering the following information in the Policy, Insert Prefix List dialog box. (Refer to Table 29 for a description of the information for the required fields in this dialog box):

   a. An ID for the prefix list (unique number) in the Id field.

   b. An IP address in the Prefix field.

   c. The length of the prefix mask (range is 0 to 32) in the PrefixMaskLen field.

   d. A name for the prefix list in the Name field.

   e. MaskLenFrom and MaskLenUpto are not required to create an accept policy. For information on these parameters, refer to Table 29.

   f. Click Insert.

4. Repeat step 3 to add additional IP addresses to the prefix list you created.

   You can also create additional prefix lists by repeating step 3.

5. From the Policy dialog box, click the Route Policy tab.

   The Route Policy tab opens (Figure 55).

6. Click Insert.

The Policy, Insert Route Policy dialog box displays (Figure 56).

7 Create the new policy by entering the following information in the Policy, Insert Route Policy dialog box:

Note: Not all the fields in the Policy, Insert Route Policy dialog box apply to the process of creating a DVMRP policy.

Table 30 describes the fields in the dialog box for which you must supply information to create the DVMRP policy. For information on the other fields in this dialog box, refer to *Configuring IP Routing Operations*.

a A number for the policy in the Id field.

b A number for the policy (range is 1 to 65,535) in the SequenceNumber field.

c A name for the policy in the Name field.

d Select DVMRP from the MatchProtocol field.

e Enter the applicable name(s) of the prefix lists you created in steps 3 and 4 in the MatchNetwork, MatchIPRouteSource, and MatchNextHop fields.

You can enter a single or several prefix lists. You can select up to four lists. To enter the names of the prefix list(s), click the ellipse button to the right of the field, select the appropriate name(s) from the dialog box, and click OK. To select multiple names, use the CTRL key. To deselect an entry, use the ALT key.

f Enter a value (range is 0 to 65,535) in the MatchMetric field.

g Enter a value (range is 0 to 65,535) in the SetMetric field.

h Click Insert.

8 From the Policy dialog box, click the DVMRP In/Out Policy tab.

The DVMRP In/Out Policy tab opens (Figure 57).

9 Right click in the InPolicy name field of the DVMRP interface to which you want to apply the accept policy and select the appropriate policy name from the PolicyName dialog box.

10 Click Apply to save the new configuration.

Applying a DVMRP accept policy to an interface

To apply an accept policy to an interface:

1. From the Device Manager menu bar, choose IP Routing > DVMRP.

   The DVMRP dialog box opens with the Globals tab displayed.

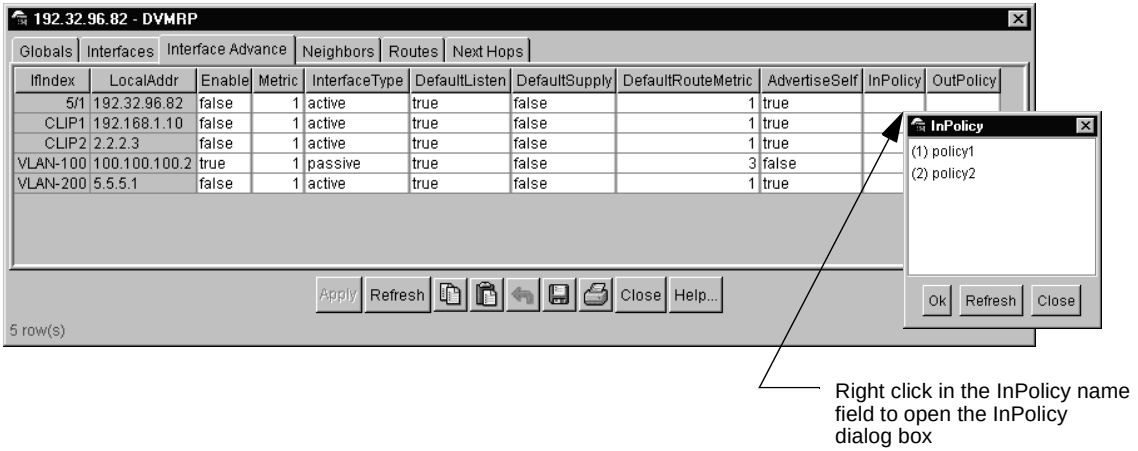
2. Select the Interface Advance tab.

   The DVMRP Interface Advance tab opens and displays the DVMRP configuration options.

3. Double-click the InPolicy field for a selected interface.

   The InPolicy dialog box opens and displays the list of policies you can apply to the interface (Figure 61).

Figure 61 DVMRP Interface tab—InPolicy dialog box



4. Select a policy name and click OK.
5. Click Apply from DVMRP Interface Advance tab.

Applying a DVMRP accept policy to a VLAN

To apply an accept policy to a VLAN:

1. From the Device Manager, choose VLAN > VLANs.

   The VLAN dialog box opens with the Basic tab displayed.

2. Select a VLAN and click IP.

   The IP, VLAN dialog box opens with the IP Address tab displayed.

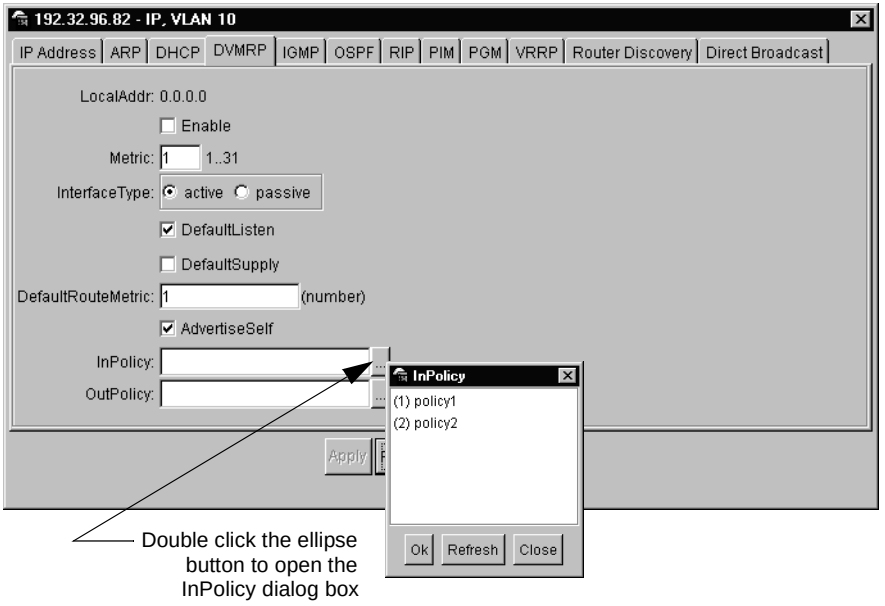
3. Click the DVMRP tab.

   The DVMRP tab opens and displays the DVMRP configuration options.

4. Double-click the tab to the right of the InPolicy field.

   The InPolicy dialog box opens and displays the list of policies you can apply to the interface (Figure 62).

Figure 62 DVMRP VLAN tab—InPolicy dialog box



5. Select a policy name and click OK.
6. Click Apply from DVMRP tab.

Applying a DVMRP accept policy to a port

To apply an accept policy to a port:

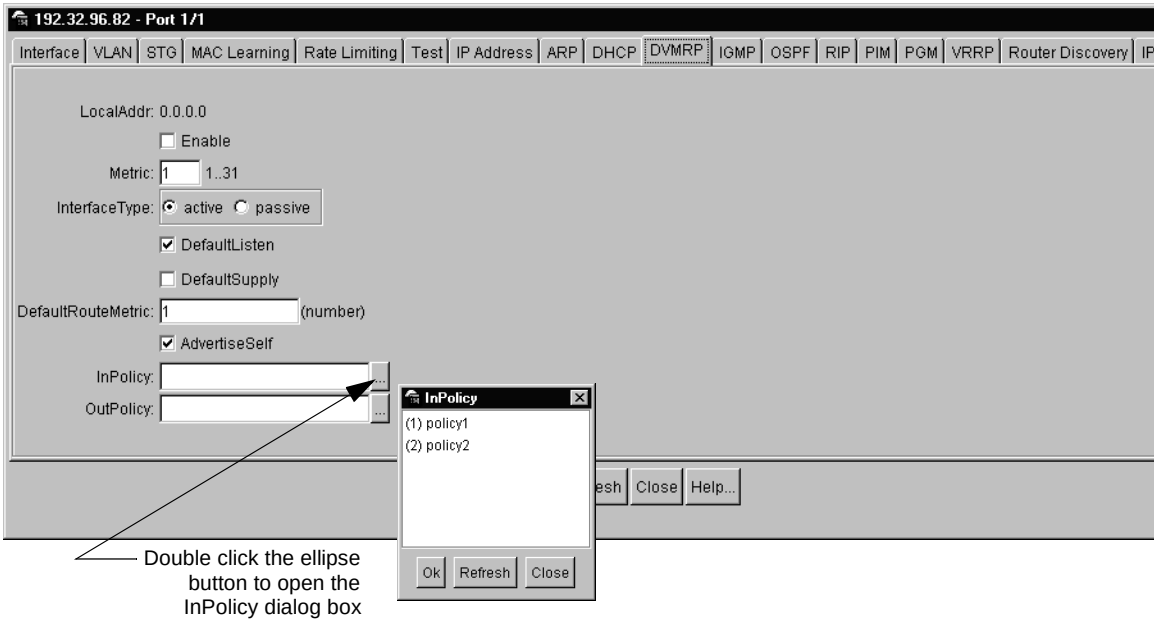
1. On the Device Manager, select a port.
2. From the Device Manager menu bar, choose Edit > Port.

   The Port dialog box opens with the Interface tab displayed.
3. Click the DVMRP tab.

   The DVMRP tab opens and displays the DVMRP configuration options.
4. Double-click the tab to the right of the InPolicy field.

   The InPolicy dialog box opens and displays the list of policies you can apply to the interface (Figure 63).

Figure 63 DVMRP Port tab—InPolicy dialog box



5. Select a policy name and click OK.
6. Click Apply from DVMRP tab.

Configuring the advertisement of local network policies

This section includes the following tasks that describe how configure the advertisement of local networks policy using Device Manager:

Task	Page
Apply the advertisement of local networks policy over an interface	171
Apply the advertisement of local networks policy over a VLAN	172
Apply the advertisement of local networks policy over a port	173

Before you apply the advertisement of local networks policy to the switch, you must perform the procedures provided in “Configuration prerequisites” on page 134.

You can apply the configuration for the advertisement of local networks policy to an interface, VLAN, or port. To display the advertisement policy configuration information, refer to “Displaying DVMRP routing policy information.”

Apply the advertisement of local networks policy over an interface

To enable the advertisement of local networks over an interface:

1. From the Device Manager menu bar, choose IP Routing > DVMRP.

   The DVMRP dialog box opens with the Globals tab displayed.

2. Select the Interface Advance tab.

   The DVMRP Interface Advance tab opens and displays the DVMRP configuration options.

3. Configure the advertisement of local networks policy for a selected interface as follows:

   a. To enable the policy, set the AdvertiseSelf field for the interface you want to modify to true.

   b. To disable the policy, set the AdvertiseSelf field for the interface you want to modify to false.

4. Click Apply to save the new configuration.

Apply the advertisement of local networks policy over a VLAN

To enable the advertisement of local networks over a VLAN:

1. From the Device Manager, choose VLAN > VLANs.

   The VLAN dialog box opens with the Basic tab displayed.

2. Select a VLAN and click IP.

   The IP, VLAN dialog box opens with the IP Address tab displayed.

3. Click the DVMRP tab.

   The DVMRP tab opens and displays the DVMRP configuration options.

4. Configure the advertisement of local networks policy for a selected VLAN as follows:

   a. To enable the VLAN to advertise its local networks, click the AdvertiseSelf check box.

   b. To disable the VLAN from advertising its local networks, deselect the AdvertiseSelf check box.

5. Click Apply to save the new configuration.

Apply the advertisement of local networks policy over a port

To enable the advertisement of local networks over a port:

1. On the Device Manager, select a port.
2. From the Device Manager menu bar, choose Edit > Port.

   The Port dialog box opens with the Interface tab displayed.
3. Click the DVMRP tab.

   The DVMRP tab opens and displays the DVMRP configuration options.
4. Configure the advertisement of local networks policy for a selected port as follows:
   a. To enable the port to advertise its local networks, click the AdvertiseSelf check box.
   b. To disable the port from advertising its local networks, deselect the AdvertiseSelf check box.
5. Click Apply to save the new configuration.

Configuring a DVMRP interface type

This section includes the following tasks that describe how to configure the interface type using Device Manager:

Task	Page
Configuring an active or passive interface type	175
Configuring an active or passive VLAN type	176
Configuring an active or passive port type	177

Before you apply the DVMRP passive interface policy to the switch, you must perform the procedures provided in “Configuration prerequisites” on page 134.

To display DVMRP interface type configuration information for an interface, VLAN, or port, refer to “Displaying DVMRP routing policy information.”

Configuring an active or passive interface type

You can configure an interface as active or passive when the interface is disabled.

To configure an active or passive interface type:

1. From the Device Manager menu bar, choose IP Routing > DVMRP.

   The DVMRP dialog box opens with the Globals tab displayed.

2. Select the Interface Advance tab.

   The DVMRP Interface Advance tab opens and displays the DVMRP configuration options.

3. To configure the interface type:, make sure the interface is disabled.

   The Enable field for the selected interface should be set to false. If the interface is enabled, disable the interface by selecting the false option from the Enable field.

   a. To set the interface to passive, select passive from the InterfaceType field for the selected interface.

   b. To set the interface to active, select active from the InterfaceType field for the selected interface

   c. If you had to disable the interface to change the interface type, re-enable the interface by selecting the true option from the Enable field.

4. Click Apply to save the new configuration.

Configuring an active or passive VLAN type

You can configure a VLAN as active or passive when the interface is disabled.

To configure an active or passive VLAN type:

1. From the Device Manager, choose VLAN > VLAN.

   The VLAN dialog box opens with the Basic tab displayed.

2. Select a VLAN and click IP.

   The IP, VLAN dialog box opens with the IP Address tab displayed.

3. Click the DVMRP tab.

   The DVMRP tab opens and displays the DVMRP configuration options.

4. Configure the interface type as follows:, make sure the interface is disabled.

   The Enable checkbox should not be selected. If the interface is enabled, disable the interface by deselecting the Enable checkbox.

   a. To set the interface to passive, select passive from the InterfaceType field.

   b. To set the interface to active, select active from the InterfaceType field.

   c. If you had to disable the interface to change the interface type, re-enable the interface by selecting the Enable checkbox.

5. Click Apply to save the new configuration.

Configuring an active or passive port type

You can configure a port as active or passive when the interface is disabled.

To configure an active or passive port type:

1. On the Device Manager, select a port.
2. From the Device Manager menu bar, choose Edit > Port.

   The Port dialog box opens with the Interface tab displayed.
3. Click the DVMRP tab.

   The DVMRP tab opens and displays the DVMRP configuration options.
4. Configure the interface type as follows, make sure the interface is disabled.

   The Enable checkbox should not be selected. If the interface is enabled, disable the interface by deselecting the Enable checkbox.

   a. To set the interface to passive, select passive from the InterfaceType field.

   b. To set the interface to active, select active from the InterfaceType field.

   c. If you had to disable the interface to change the interface type, re-enable the interface by selecting the Enable checkbox.
5. Click Apply to save the new configuration.

Displaying DVMRP routing policy information

This section describes the procedures for displaying DVMRP configuration information for an interface, VLAN, and port.

This section includes the following tasks:

You can display DVMRP routing policy information for an interface, VLAN, or port.

Displaying DVMRP routing policy information for an interface

To display DVMRP routing policy information for an interface:

1. From the Device Manager menu bar, choose IP Routing > DVMRP.

   The DVMRP dialog box opens with the Globals tab displayed.

2. Select the Interface Advance tab.

   The DVMRP Interface Advance tab opens and displays the DVMRP configuration settings.

Displaying DVMRP routing policy information for a VLAN

To display DVMRP routing policy information for a VLAN:

1. From the Device Manager, choose VLAN > VLAN.

   The VLAN dialog box opens with the Basic tab displayed.

2. Select a VLAN and click IP.

   The IP, VLAN dialog box opens with the IP Address tab displayed.

3. Click the DVMRP tab.

   The DVMRP tab opens and displays the DVMRP configuration settings.

Displaying DVMRP routing policy information for a port

To display DVMRP routing policy information for a port:

1. On the Device Manager, select a port.
2. From the Device Manager menu bar, choose Edit > Port.

   The Port dialog box opens with the Interface tab displayed.

3. Click the DVMRP tab.

   The DVMRP tab opens and displays the DVMRP configuration settings.

Chapter 4
Configuring PIM using Device Manager

The Passport 8600 supports two modes of Protocol Independent Multicast, sparse mode (SM) and source specific multicast (SSM). For information on PIM-SM, refer to the next section; for information on PIM-SSM, refer to "Configuring Source Specific Multicast (SSM)" on page 204.

Protocol Independent Multicast-Sparse Mode (PIM-SM) supports multicast groups spread out across large areas of a company or the Internet.

- What makes PIM-SM protocol-independent? — PIM-SM does not maintain its own or depend on a specific multicast protocol to maintain unicast routing tables. PIM-SM uses the routing table information from any underlying unicast routing protocol, such as RIP or OSPF.
- How does it multicast? — PIM-SM sends one stream of data to the network where it is replicated to all interested receivers.
- What is sparse mode? — Instead of using a "push" model. PIM-SM uses a "pull" model in which receivers pull down multicast traffic. For sparsely populated networks, PIM-SM is more efficient than dense-mode protocols because it sends multicast traffic only to those routers that belong to a specific multicast group and that choose to receive the traffic.

The 8000 Series switches support the following for PIM-SM:

- RP functionality
- Redundant RP configuration where several RPs can be configured for the same group(s)
- RP load sharing where several RPs can be configured in the same PIM domain

- BSR functionality
- Redundant BSR functionality
- MBR functionality to connect a PIM-SM domain to a DVMRP domain. When you configure an 8000 Series switch with MBR functionality, you can have some interfaces running PIM-SM and other interfaces running DVMRP to interconnect a PIM-SM domain to a DVMRP domain.

For more information about PIM-SM concepts and terminology, refer to Chapter 1, "IP Multicast concepts."

For instructions on how to configure PIM static source groups, refer to Chapter 6, "Viewing and editing multicast routes using Device Manager."

This chapter describes the following topics:

Configuration prerequisites

Before you can configure PIM-SM, you must prepare the router as follows:

1. Configure an IP interface. For information, refer to *Configuring IP Routing Operations*.
2. Disable DVMRP from the interface on which you want to configure PIM-SM because you cannot configure PIM-SM and DVMRP on the same interface.

Note: Changing the configuration from PIM to DVMRP, or from DVMRP to PIM, is not recommended while multicast traffic is flowing on the network.

For information on disabling DVMRP, refer to Chapter 3, "Configuring DVMRP using Device Manager."

   a. A *switch* can have a mix of DVMRP and PIM-SM interfaces if it is configured as an multicast border router (MBR).

   b. An *interface* can only be configured with one multicast routing protocol at a time (PIM-SM or DVMRP).

3. Configure a unicast protocol (RIP or OSPF) globally and on the interfaces where you want to configure PIM-SM.

   For information on RIP and OSPF, refer to *Configuring IP Routing Operations*.

   PIM-SM requires a unicast protocol to use in order to multicast traffic within the network when performing the Reverse Path Forwarding (RFP) check. PIM-SM uses the information from the unicast routing table to create and maintain the shared and shortest multicast tree that enables PIM-enabled routers to communicate. The unicast routing table must contain a route to every multicast source in the network as well as routes to PIM entities like the RPs and BSR.

4. To configure PIM-SM on an 8000 Series switch, the following configurations are required:

   — Enable PIM-SM globally.

   — Enable PIM-SM on individual interfaces.

— Configure one or several RPs for the groups that will be used by a multicast application in the network.

— Configure one or several BSRs to propagate RP information to all switches in the network.

— If connecting a PIM-SM domain to a DVMRP domain, configure the switch interconnecting the domains as an MBR switch with the corresponding PIM-SM interfaces enabled with PIM-SM, and DVMRP interfaces enabled with DVMRP.

Note: Routes to sources in a PIM domain should not have a lower cost through the DVMRP domain in order for multicast routing from these sources to work properly. MBR switches should be configured with this design guideline in mind.

Enabling PIM-SM globally

IGMP is required for PIM-SM. When you enable PIM-SM globally and on a particular interface, the IGMP parameters take effect.

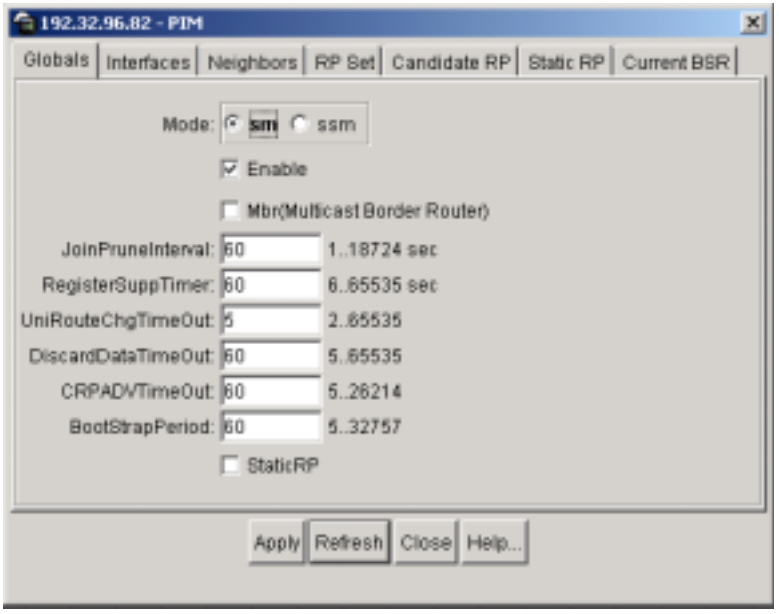
Note: To enable PIM-SSM globally, see "Enabling Source Specific Multicast (SSM) globally." Also note that when you change from one mode to another, an information message pops up to remind you that traffic will not stop immediately.

To enable PIM-SM globally:

1 From the Device Manager menu bar, choose IP Routing > PIM.

The PIM dialog box opens with the Globals tab displayed (Figure 64).

Figure 64 PIM dialog box—Globals tab



2 Click Mode: sm (sparse mode).

Note: You can use static RP when SSM is enabled for groups outside the SSM range.

3 Click Enable.

4 Click Apply.

Table 31 describes the PIM Globals tab fields.

Table 31 PIM Globals tab fields

Field	Description
Mode	Configures the mode on the routing switch: sm (sparse mode) or ssm (source-specific multicast).
Enable	Enables or disables PIM.

Table 31 PIM Globals tab fields (continued)

Field	Description
Mbr (Multicast Border Router)	Configures the router as a PIM multicast border router (PMBR). PMBRs connect PIM domains to other multicast routing domains and the rest of the Internet. In particular, the MBR on 8000 Series switches allow the connection of a PIM-SM domain to a DVMRP domain.
JoinPruneInterval	Specifies how long to wait (in seconds) before the PIM router sends out the next join/prune message to its upstream neighbors. The range is from 1 to 18724, and the default is 60 seconds.
RegisterSuppTimer	Specifies how long (in seconds) the DR suppresses sending registers to the RP. The timer starts when the DR receives a Register Stop message from the RP. The range is from 6 to 65535, and the default is 60 seconds.
UniRouteChgTimeOut	Specifies how often (in seconds) the switch polls the routing table manager (RTM) for unicast routing information updates to be used by PIM. The range is from 2 to 65535, and the default is 5 seconds. **Note:** Lowering this value increases how often the switch polls the RTM. This may affect the switch's performance, especially when there's a lot of traffic flowing through the switch.
DiscardDataTimeOut	Specifies how long (in seconds) to discard data until the Join is received from the RP. An ipmc discard record is created after a register packet is sent until the timer expires and/or when a Join is received. The range is from 5 to 65535, and the default is 60 seconds.
CRPADVTimeOut	Specifies how often (in seconds) that routers configured as candidate RPs send C-RP advertisement messages. When this timer expires, the C-RP sends an advertisement message to the elected BSR. The range is from 5 to 26214, and the default is 60 seconds.
BootStrapPeriod	Specifies the interval (in seconds) that the elected BSR waits between originating bootstrap messages. The range is from 5 to 32757, and the default is 60 seconds.
StaticRP	Enables or disables the Static RP feature. Static RP enables you to configure a static entry for a rendezvous point (RP). This feature enables you to communicate with switches from other vendors that do not use the BSR mechanism.

Enabling static RP

Static RP enables you to configure a static entry for a rendezvous point (RP). When configured, static RP ignores the BSR mechanism and uses the statically configured RPs only. This feature allows static RP-enabled 8000 Series switches to communicate with switches from other vendors that do not use the BSR mechanism.

For more information about static RP and other PIM-SM concepts, refer to Chapter 1, “IP Multicast concepts.”

Configuration considerations

Before you can configure a static RP, you must enable the following:

1. PIM-SM
2. Static RP

After meeting these prerequisites, keep in mind the following configuration considerations:

- A static RP-enabled switch cannot be configured as a BSR or as a C-RP.
- All dynamically learned BSR information is lost. However, if you disable static RP, the switch loses the static RP information and regains the BSR functionality.
- Static RPs do not age, that is they cannot time out.
- Switches do not advertise static RPs so, if a new PIM neighbor joins the network, it will not know about the static RP unless it is configured with that static RP.
- Configure all the switches in the network (including switches from other vendors) to map to the same RP.
- In a PIM domain with both static and dynamic RP switches, the static RP switches cannot have one of their (local) interfaces configured as RP.

- To avoid a single point of failure, you can configure redundant static RPs for the same group prefix. If there is a mix of Nortel and other vendor's switches across the network, you have to ensure that all switches/routers use the same active RP because other vendors may be using different algorithms to elect the active RP. 8000 Series switches use the hash function defined in the PIM-SM standard to elect the active RP; other vendors may use the lowest IP address to break the tie.
- Static RP configured on the switch is assumed to be alive as long as the switch has a unicast route to the static RP's network. If the switch loses this route, the static RP is invalidated and the hash algorithm is invoked to remap all affected groups. If the switch regains this route, the static RP is validated and the hash algorithm is invoked to remap the affected groups.

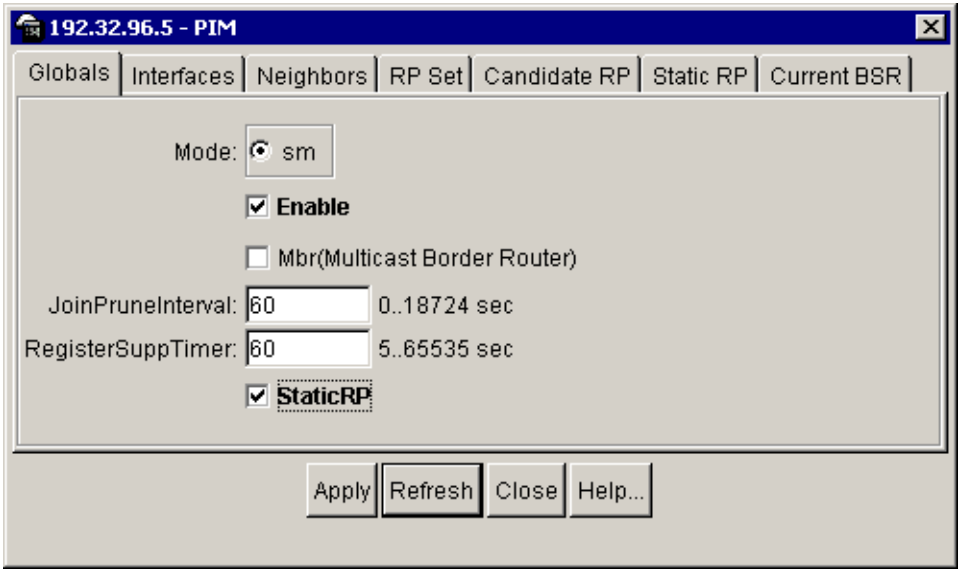
Enabling static RP procedure

To enable static RP:

1 From the Device Manager menu bar, choose IP Routing > PIM.

The PIM dialog box opens with the Globals tab displayed (Figure 65).

Figure 65 PIM dialog box—Globals tab



2 Click Mode: sm (sparse mode).

3 Click Enable.

4 Click Static RP.

5 Click Apply.

An information message pops up to remind you that traffic will not stop immediately, and that RP information learned through the BSR will be lost.

Note: Since a Static RP-enabled switch cannot be configured as a BSR, the Current BSR tab disappears from this dialog box once you click Apply.

6 Click Yes to continue.

Configuring static RP

To configure a static RP:

1 From the Device Manager menu bar, choose IP Routing > PIM.

The PIM dialog box opens with the Globals tab displayed.

2 Click the Static RP tab.

The Static RP tab opens (Figure 66).

Figure 66 PIM dialog box—Static RP tab

3 Click Insert.

The PIM, Insert Static RP dialog box opens (Figure 67).

Figure 67 PIM dialog box—Insert Static RP dialog box

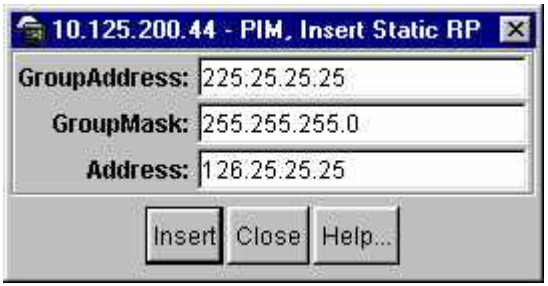


Table 32 describes the PIM Static RP fields.

Table 32 PIM Static RP tab fields

Field	Description
GroupAddress	The IP address of the multicast group. When combined with the group mask, it identifies the range of the multicast addresses that the RP handles.
GroupMask	The address mask of the multicast group. When combined with the group address, it identifies the range of the multicast addresses that the RP handles.
Address	The IP address of the static RP.
Status	Shows the current status of the static RP entry. The status is **valid** when the switch has a unicast route to the static RP's network and **invalid** otherwise.

Enabling PIM on a brouter port

When you enable PIM on a particular interface, you must also enable it globally. Otherwise, PIM will not work. See “Enabling PIM-SM globally” on page 184.

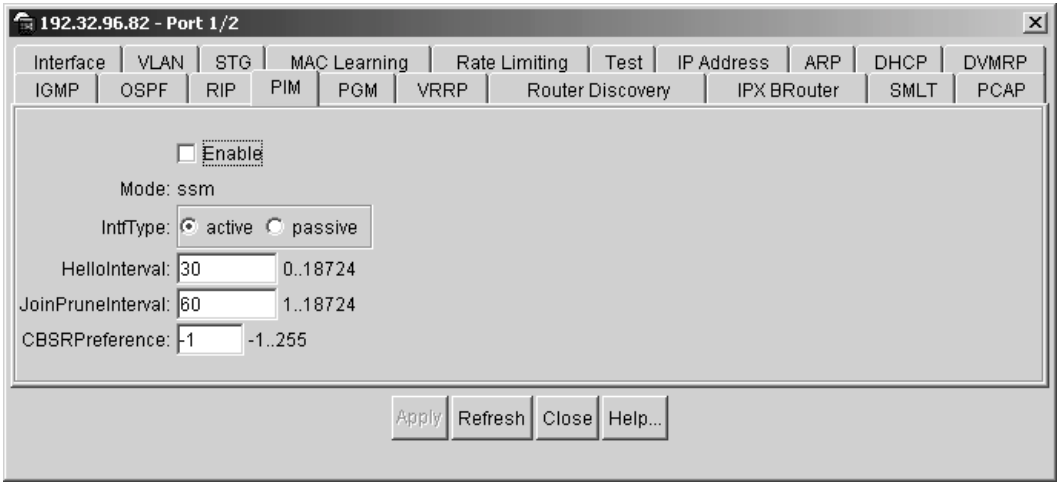
To enable PIM on a brouter port:

1. On the Device Manager, select a port.
2. From the Device Manager menu bar, choose Edit > Port.

   The Port dialog box opens with the Interface tab displayed.
3. Click the PIM tab.

   The PIM tab opens (Figure 68).

Figure 68 Port dialog box—PIM tab



4. Click Enable.
5. Click Apply.
6. Click Close.

Table 33 describes the PIM tab fields.

Table 33 PIM tab fields

Field	Description
Enable	Enables (true) or disables (false) PIM for the specified brouter port.
Mode	Displays the mode currently running on the routing switch.
IntfType	Specifies whether the selected interface is active or passive. An active interface allows PIM control traffic to be transmitted and received. A passive interface prevents PIM control traffic from being transmitted or received, thereby reducing the load on a system when there is a high number of PIM interfaces that need to be configured and these interfaces are connected to end users and not to other switches.
HelloInterval	Specifies how long to wait (in seconds) before the PIM router sends out the next hello message to neighboring routers. The default is 30 seconds.
JoinPruneInterval	Specifies how long to wait (in seconds) before the PIM router sends out the next join/prune message to its upstream neighbors. The default is 60 seconds.
CBSRPreference	Sets your preference for this local interface to become a Candidate BSR. The Candidate BSR with the highest BSR-priority and address is referred to as the preferred BSR. The default is -1, which indicates that the current interface is not a Candidate BSR.

Changing the interface type

Before you change the state (active or passive) of PIM on a brouter port, you must first disable PIM to prevent any instability in the PIM operations, especially when neighbors are present or when streams are received.

To change the state of PIM on a brouter port, use the following procedure:

1. On the Device Manager, select a port.
2. From the Device Manager menu bar, choose Edit > Port.

   The Port dialog box opens with the Interface tab displayed.

3 Click the PIM tab.

The PIM tab opens (Figure 68).

4 Make sure that Enable is not selected. If a check mark appears next to Enable, disable PIM by clicking the Enable check box.

5 Change the IntfType, if desired.

6 Click Apply.

7 Click Close.

To re-enable PIM on the brouter port:

1 Follow steps 1 through 3 above.

2 Select Enable.

3 Click Apply.

4 Click Close.

Configuring a candidate bootstrap router (C-BSR)

PIM-SM cannot run without a bootstrap router (BSR). Although a PIM-SM domain can have only one active BSR, you can configure additional routers as candidate BSRs (C-BSRs). C-BSRs provide backup protection in case the primary BSR fails.

The C-BSR with the highest configured priority becomes the BSR for the domain. If two C-BSRs have equal priority, the candidate with the higher IP address becomes the BSR. If you add a new C-BSR with a higher priority to the domain, it automatically becomes the new BSR.

To configure a C-BSR:

1 On the device view, select a port.

2 From the Device Manager menu bar, choose Edit > Port.

The Port dialog box opens with the Interface tab displayed.

3 Click the PIM tab.

The PIM tab opens (Figure 68).

4 Click Enable.

5 Set the CBSRPreference. The C-BSR with the highest BSR-preference and address becomes the active BSR. The default is -1, which indicates that the current interface is not a C-BSR.

6 Click Apply.

Enabling PIM on a VLAN interface

When you enable PIM on a particular VLAN, you must also enable it globally. Otherwise, PIM will not work. See “Enabling PIM-SM globally” on page 184.

To enable PIM on a VLAN:

1 From the Device Manager menu bar, choose VLAN > VLANs.

The VLAN dialog box opens with the Basic tab displayed.

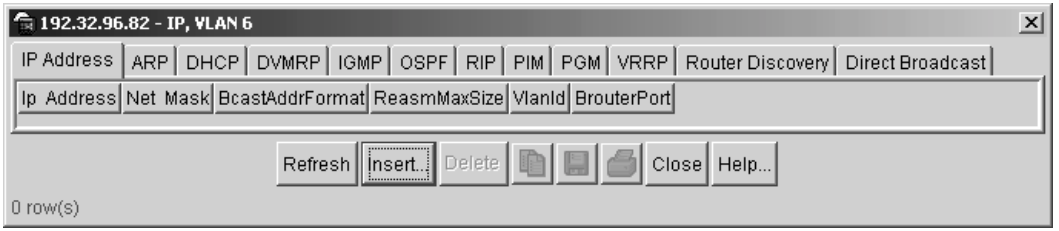
2 Select the VLAN ID that you want to configure with PIM.

Several buttons on the bottom of the dialog box become available.

3 Click IP.

The IP, VLAN dialog box opens with the IP Address tab displayed (Figure 69).

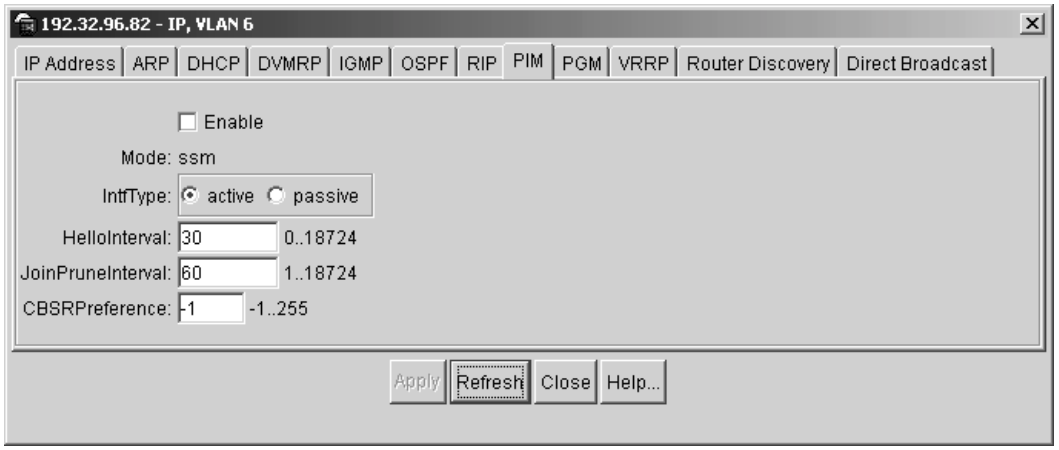
Figure 69 IP VLAN dialog box I



4 Click the PIM tab.

The PIM tab opens (Figure 70).

Figure 70 IP VLAN dialog box—PIM tab



5 Click Enable.

6 Click Apply.

7 Click Close.

Table 34 describes the VLAN PIM tab fields.

Table 34 VLAN PIM tab fields

Field	Description
Enable	Enables (true) or disables (false) PIM.
Mode	Displays the mode currently running on the routing switch. The valid modes are SSM and Sparse. This is a read-only field.
IntfType	Specifies whether the selected interface is active or passive. An active interface allows PIM control traffic to be transmitted and received. A passive interface prevents PIM control traffic from being transmitted or received, thereby reducing the load on a system when there is a high number of PIM interfaces that need to be configured and these interfaces are connected to end users and not to other switches.
HelloInterval	Specifies how long to wait (in seconds) before the PIM router sends out the next hello message to neighboring routers. The default is 30 seconds.

Table 34 VLAN PIM tab fields (continued)

Field	Description
JoinPruneInterval	Specifies how long to wait (in seconds) before the PIM router sends out the next join/prune message to its upstream neighbors. The default is 60 seconds.
CBSRPreference	Sets your preference for this local interface to become a Candidate BSR. The Candidate BSR with the highest BSR-priority and address is referred to as the preferred BSR. The default is -1, which indicates that the current interface is not a Candidate BSR.

Changing the VLAN interface type

Before you change the state (active or passive) of PIM on a VLAN interface, you must first disable PIM to prevent any instability in the PIM operations, especially when neighbors are present or when streams are received.

To change the state of PIM on a VLAN interface, use the following procedure:

1. From the Device Manager menu bar, choose VLAN > VLANs.

   The VLAN dialog box opens with the Basic tab displayed.
2. Select the VLAN ID that you want to configure with PIM.
3. Click IP.

   The IP, VLAN dialog box opens with the IP Address tab displayed (Figure 69).
4. Click the PIM tab.

   The PIM tab opens (Figure 70).
5. Make sure that Enable is not selected. If a check mark appears next to Enable, disable PIM by clicking the Enable check box.
6. Change the IntfType, if desired.
7. Click Apply.
8. Click Close.

To re-enable PIM on the VLAN interface:

1 Follow steps 1 through 4.

2 Select Enable.

3 Click Apply

4 Click Close.

Viewing and editing PIM interface parameters

To view or edit PIM parameters for a brouter port:

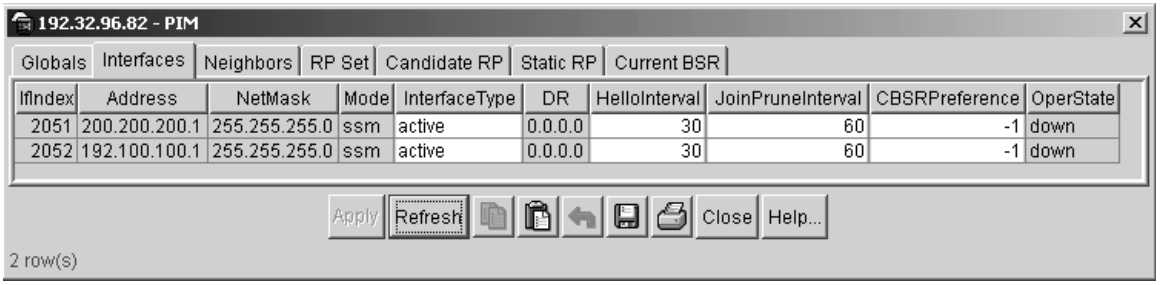
1 From the Device Manager menu bar, choose IP Routing > PIM.

The PIM dialog box opens with the Globals tab displayed.

2 Click the Interfaces tab.

The PIM dialog box, Interfaces tab opens (Figure 71).

Figure 71 PIM dialog box—Interfaces tab



Note: Before you change the state (active or passive) of a PIM interface using the Interface Type field, you must first disable PIM to prevent any instability in the PIM operations, especially when neighbors are present or when streams are received.

For instructions on disabling PIM on a brouter port and changing the state of a PIM interface, see "Changing the interface type" on page 192.

For instructions on disabling PIM on a VLAN interface and changing the state of PIM interface, see "Changing the VLAN interface type" on page 196.

Table 35 describes the PIM Interfaces tab fields.

Table 35 PIM Interfaces tab fields

Field	Description
IfIndex	Interface Index.
Address	The IP address of the PIM interface.
NetMask	The network mask for the IP address of the PIM interface.
Mode	The configured mode of this interface. The valid modes are SSM and Sparse. This is a read-only field.
Interface Type	Specifies whether the selected interface is active or passive. An active interface allows PIM control traffic to be transmitted and received. A passive interface prevents PIM control traffic from being transmitted or received, thereby reducing the load on a system when there is a high number of PIM interfaces that need to be configured and these interfaces are connected to end users and not to other switches. **Note:** You can change the interface type (passive or active) using this field only if the selected interface is disabled.
DR	The router with the highest IP address on a LAN designated to perform these tasks.
HelloInterval	Specifies how long to wait (in seconds) before the PIM switch sends out the next hello message to neighboring switches. The default is 30 seconds.
JoinPruneInterval	Specifies how long to wait (in seconds) before the PIM switch sends out the next join/prune message to its upstream neighbors. The default is 60 seconds.
CBSRPreference	Sets your preference for this local interface to become a Candidate BSR. The Candidate BSR with the highest BSR-priority and address is referred to as the preferred BSR. The default is -1, which indicates that the current interface is not a Candidate BSR.
OperState	Indicates the status of PIM on this interface: enabled or disabled.

Viewing PIM-SM neighbor parameters

To view PIM-SM neighbor parameters:

1 From the Device Manager menu bar, choose IP Routing > PIM.

The PIM dialog box opens with the Globals tab displayed (Figure 64).

2 Click the Neighbors tab.

The Neighbors tab opens (Figure 72).

Figure 72 PIM dialog box—Neighbors tab

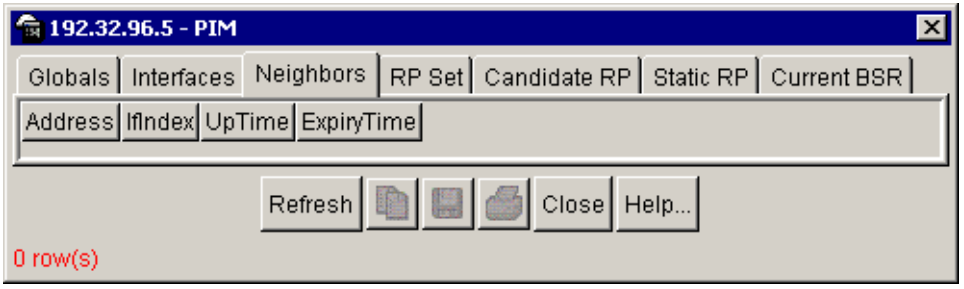


Table 36 describes the PIM Neighbors tab fields.

Table 36 PIM Neighbors tab fields

Field	Description
Address	The IP address of the PIM neighbor for which this entry contains information.
IfIndex	The slot/port number or VLAN ID of the interface used to reach this PIM neighbor.
UpTime	The elapsed time since this PIM neighbor last became a neighbor of the local router.
ExpiryTime	The time remaining before this PIM neighbor times out.

Viewing the RP Set parameters

RP Set is a list of rendezvous point addresses. The bootstrap router (BSR) constructs this list from C-RP advertisements and then distributes it to all PIM routers in the BSR's PIM domain.

To view the RP Set parameters:

1 From the Device Manager menu bar, choose IP Routing > PIM.

The PIM dialog box opens with the Globals tab displayed (Figure 64).

2 Click the RP Set tab.

The RP Set tab opens (Figure 73).

Figure 73 PIM dialog box—RP Set tab

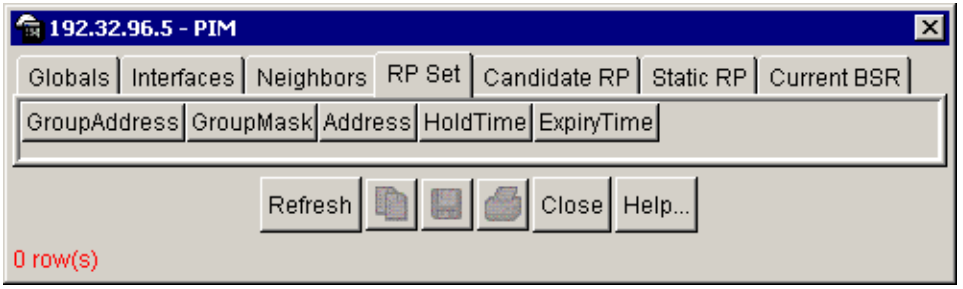


Table 37 describes the PIM RP Set tab fields.

Table 37 PIM RP Set tab fields

Field	Description
GroupAddress	The IP address of the multicast group. When combined with the group mask, it identifies the prefix that the local router uses to advertise itself as a C-RP.
GroupMask	The address mask of the multicast group. When combined with the group address, it identifies the prefix that the local router uses to advertise itself as a C-RP.
Address	The IP address of the C-RP.

Table 37 PIM RP Set tab fields (continued)

Field	Description
HoldTime	The time specified in a C-RP advertisement that the BSR uses to time out the RP. When the BSR receives an advertisement for the RP, it restarts the timer. If no advertisement arrives before the timer expires, the BSR removes that RP from the RP set.
ExpiryTime	The time remaining before this C-RP times out.
Component	A unique number identifying the protocol instance connected to each PIM domain.

Configuring a candidate RP

The following steps describe how to add a candidate rendezvous point (C-RP) to the RP Set.

To configure a C-RP:

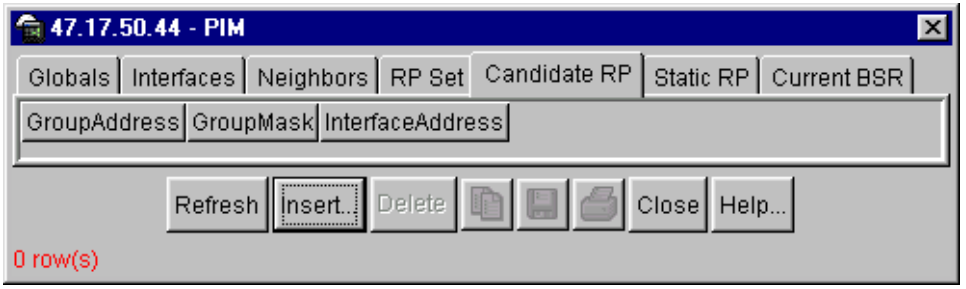
1. From the Device Manager menu bar, choose IP Routing > PIM.

   The PIM dialog box opens with the Globals tab displayed (Figure 64).

2. Click the Candidate RP tab.

   The Candidate RP tab opens (Figure 74).

Figure 74 PIM dialog box—Candidate RP tab



3. Click Insert.

   The PIM, Insert Candidate dialog box opens (Figure 75).

Figure 75 PIM dialog box—Insert Candidate RP dialog box

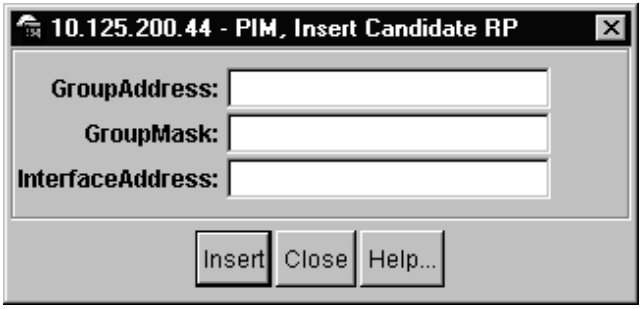


Table 38 describes the PIM Candidate RP fields.

Table 38 PIM Candidate RP tab fields

Field	Description
GroupAddress	The IP address of the multicast group. When combined with the group mask, it identifies the prefix that the local router uses to advertise itself as a C-RP.
GroupMask	The address mask of the multicast group. When combined with the group address, it identifies the prefix that the local router uses to advertise itself as a C-RP.
Address	The IP address of the C-RP. This address has to be one of the local PIM-SM enabled interfaces.

You can only configure one interface on an 8000 Series switch for multiple groups, that is, you cannot configure multiple interfaces for multiple groups.

The GroupMask value allows you to configure a Candidate RP for several groups in one configuration. For example, a Candidate RP configuration with a GroupAddress value of 224.0.0.0 and a GroupMask of 240.0.0.0 allows you to configure the Candidate RP for a multicast range from 224.0.0.0 to 239.255.255.255.

Viewing the current bootstrap router (BSR)

PIM-SM cannot run without a bootstrap router (BSR). Although a PIM-SM domain can have only one active BSR, you can configure additional routers as candidate BSRs (C-BSRs). A C-BSR provides backup protection in case the primary BSR fails.

To display information about the current bootstrap router (BSR) for a PIM-SM domain with Device Manager:

1. From the Device Manager menu bar, choose IP Routing > PIM.

   The PIM dialog box opens with the Globals tab displayed (Figure 64).

2. Click the Current BSR tab.

   The Current BSR tab opens (Figure 76).

Figure 76 PIM dialog box—Current BSR tab

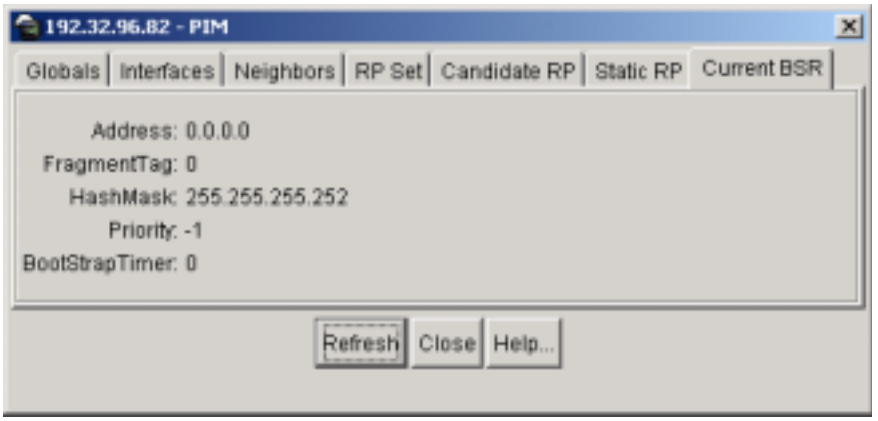


Table 39 describes the Current BSR tab fields.

Table 39 Current BSR tab fields

Field	Description
Address	The IP address of the current BSR for the local PIM domain.
FragmentTag	A randomly generated number that distinguishes fragments belonging to different Bootstrap messages. Fragments belonging to the same Bootstrap message carry the same 'Fragment Tag'.
HashMask	The mask used in the hash function to map a group to one of the C-RPs from the RP-Set. The hash-mask allows a small number of consecutive groups (e.g., 4) to always hash to the same RP.
Priority	The priority of the current BSR. The Candidate BSR (C-BSR) with the highest BSR-priority and address (referred to as the preferred BSR) is elected as the BSR for the domain.
Bootstrap Timer	When the Bootstrap Timer expires, the BSR sends out Bootstrap messages.

Configuring Source Specific Multicast (SSM)

Source Specific Multicast (SSM) optimizes PIM-SM by simplifying the many-to-many model (servers-to-receivers). Since most multicast applications distribute content to a group in one direction, SSM uses a one-to-many model that only uses a subset of the PIM-SM features. This model is more efficient and puts less of a load on multicast routing devices.

For more information about SSM concepts and terminology, refer to Chapter 1, "Multicast concepts."

Configuration prerequisites

SSM is a global configuration. When you enable SSM on a switch, it is enabled on all interfaces running PIM. On an SSM-enabled switch, SSM behavior is limited to the SSM group range. For non-SSM groups, the protocol behavior is PIM-SM.

Before you can configure SSM, you must prepare the router as follows:

1. Configure an IP interface. For information, refer to *Configuring IP Routing Operations*.
2. Configure a unicast protocol (RIP or OSPF) globally and on the interfaces where you want to configure PIM.

   For information on RIP and OSPF, refer to *Configuring IP Routing Operations*.

   PIM requires a unicast protocol in order to forward multicast traffic within the network when performing the Reverse Path Forwarding (RFP) check. PIM-SM uses the information from the unicast routing table to create and maintain the shared and shortest multicast tree that enables PIM-enabled routers to communicate. The unicast routing table must contain a route to every multicast source in the network as well as routes to PIM entities like the RPs and BSR.
3. Enable PIM globally.

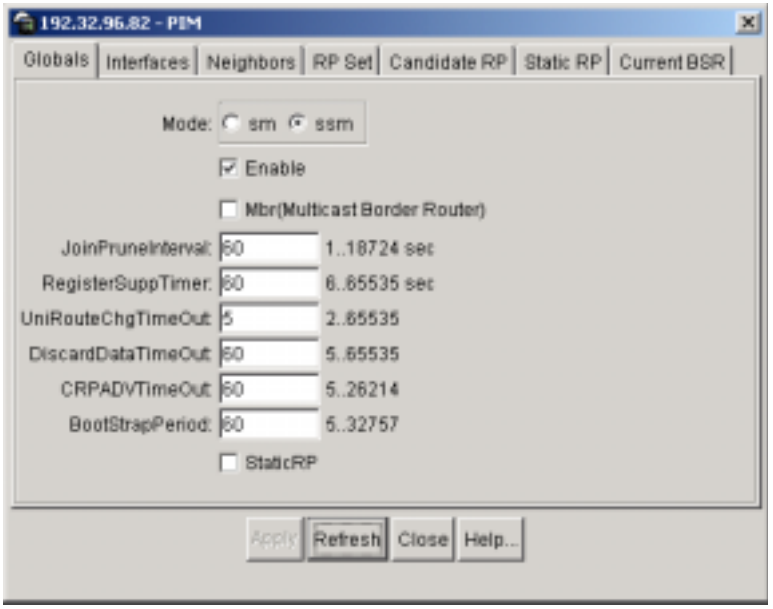
Enabling Source Specific Multicast (SSM) globally

To enable SSM globally:

1. From the Device Manager menu bar, choose IP Routing > PIM.

   The PIM dialog box opens with the Globals tab displayed (Figure 77).

Figure 77 PIM dialog box—Globals tab



2 Click Mode: ssm (source specific multicast).

3 Click Enable.

4 Click Apply.

An information message pops up to remind you that traffic will not stop immediately.

5 Click Yes to continue.

Note: After you enable PIM in SSM mode, the IGMP parameters take effect. To take full advantage of SSM, enable IGMPv3 if hosts attached to the switch are running IGMPv3 or configuring the SSM table.

For information on configuring IGMPv3, refer to "Configuring IGMP parameters on a brouter port" on page 94 or "Configuring IGMP parameters on a VLAN" on page 99."

For information on configuring the SSM group range and channel table, refer to "Configuring the SSM range and global parameters" on page 120" or "Configuring the SSM channel table" on page 123."

Table 40 describes the PIM Globals tab fields.

Table 40 PIM Globals tab fields

Field	Description
Mode	Configures the mode on the routing switch: sm (sparse mode) or ssm (source-specific multicast).
Enable	Enables or disables PIM.
Mbr (Multicast Border Router)	Configures the router as a PIM multicast border router (PMBR). PMBRs connect PIM domains to other multicast routing domains and the rest of the Internet. In particular, the MBR on 8000 Series switches allow the connection of a PIM-SM domain to a DVMRP domain.
JoinPruneInterval	Specifies how long to wait (in seconds) before the PIM router sends out the next join/prune message to its upstream neighbors. The range is from 1 to 18724, and the default is 60 seconds.
RegisterSuppTimer	Specifies how long (in seconds) the DR suppresses sending registers to the RP. The timer starts when the DR receives a Register Stop message from the RP. The range is from 6 to 65535, and the default is 60 seconds.
UniRouteChgTimeOut	Specifies how often (in seconds) the switch polls the routing table manager (RTM) for unicast routing information updates to be used by PIM. The range is from 2 to 65535, and the default is 5 seconds. **Note:** Lowering this value increases how often the switch polls the RTM. This may affect the switch's performance, especially when there's a lot of traffic flowing through the switch.
DiscardDataTimeOut	Specifies how long (in seconds) to discard data until the Join is received from the RP. An ipmc discard record is created after a register packet is sent until the timer expires and/or when a Join is received. The range is from 5 to 65535, and the default is 60 seconds.
CRPADVTimeOut	Specifies how often (in seconds) that routers configured as candidate RPs send C-RP advertisement messages. When this timer expires, the C-RP sends an advertisement message to the elected BSR. The range is from 5 to 26214, and the default is 60 seconds.

Table 40 PIM Globals tab fields (continued)

Field	Description
BootStrapPeriod	Specifies the interval (in seconds) that the elected BSR waits between originating bootstrap messages. The range is from 5 to 32757, and the default is 60 seconds.
StaticRP	Enables or disables the Static RP feature. Static RP enables you to configure a static entry for a rendezvous point (RP). This feature enables you to communicate with switches from other vendors that do not use the BSR mechanism.

Chapter 5
Configuring PGM using Device Manager

Pragmatic General Multicast (PGM) provides reliable, duplicate-free delivery of data packets while reducing network congestion. PGM guarantees that receivers either receive all data packets from transmissions and retransmissions, or can detect unrecoverable data packet loss. PGM is particularly well suited to ‘push’ applications with relatively small information transfers such as stock and news updates. DVMRP is used between routers to exchange multicast routing information. For more information about DVMRP concepts and terminology, refer to Chapter 1, “IP Multicast concepts.”

The 8000 Series switches implement the network element portion of PGM. They support the following PGM options:

- NAK list
- FEC (forwarding error correction)

The 8000 Series switch cannot serve as a DLR (designated local repairer) because DLRs require a large amount of buffering. Therefore, the null negative acknowledgement (NNAK) parameters in Device Manager are not supported.

This chapter describes the following topics:

Configuration prerequisites

To configure and use PGM on an 8000 Series switch, the switch must be running IP multicast with IGMP snooping and/or an IP multicast protocol such as DVMRP or PIM-SM. If PGM is configured without IP multicast enabled on a switch, PGM will not run and cannot be used.

To configure PGM on a switch, you need to perform the following steps:

1. Configure and enable IP multicast on the switch, particularly on the interfaces where PGM is required.
2. Enable PGM globally.
3. Enable PGM on the required interfaces.

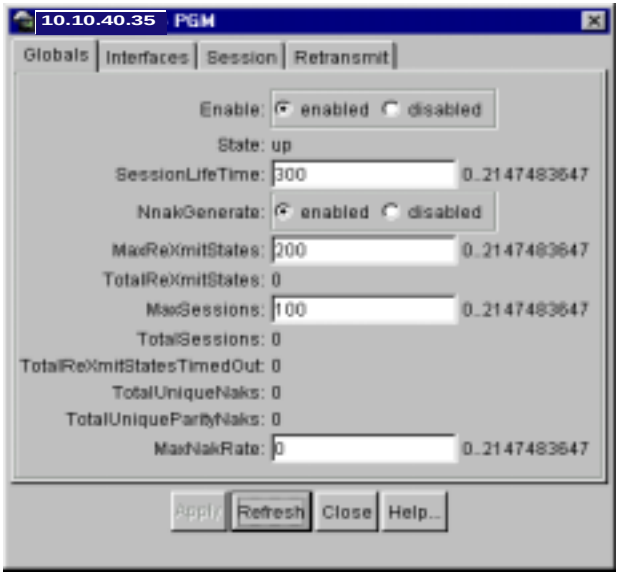
Enabling PGM globally

To enable PGM globally:

1 From the Device Manager menu bar, choose IP Routing > PGM.

The PGM dialog box opens with the Globals tab displayed (Figure 78).

Figure 78 PGM dialog box—Globals tab



2 Click enabled.

3 Click Apply.

Table 41 describes the PGM Globals tab fields.

Table 41 PGM Globals tab fields

Field	Description
Enable	Enables or disables PGM globally.
State	Displays the current state (up or down) of PGM.
SessionLifeTime	Specifies the length of idle time (in seconds) after which a session times out. Idle time is when no SPMs are received from the upstream. The default is 300 seconds.
NnakGenerate	This option is not supported in this release.
MaxReXmitStates	Configures the maximum number of retransmit state entries that the switch can create. Each entry has a unique NAK sequence number. The default is 200 entries.
TotalReXmitStates	Displays the total number of retransmit state entries in the retransmit table.
MaxSessions	Configures the maximum number of source path state sessions allowed on the switch. The default is 100 sessions.
TotalSessions	Displays the total number of source path state sessions in the PGM session entries table.
TotalReXmitStatesTimedOut	Displays the total number of retransmit state entries that were removed because they timed out.
TotalUniqueNaks	Displays the total number of unique NAKs received.
TotalUniqueParityNaks	Displays the total number of unique parity NAKs received.
MaxNakRate	Configures the maximum number of NAK transmission packets allowed per second. (This parameter is not currently implemented.)

Enabling PGM on an interface

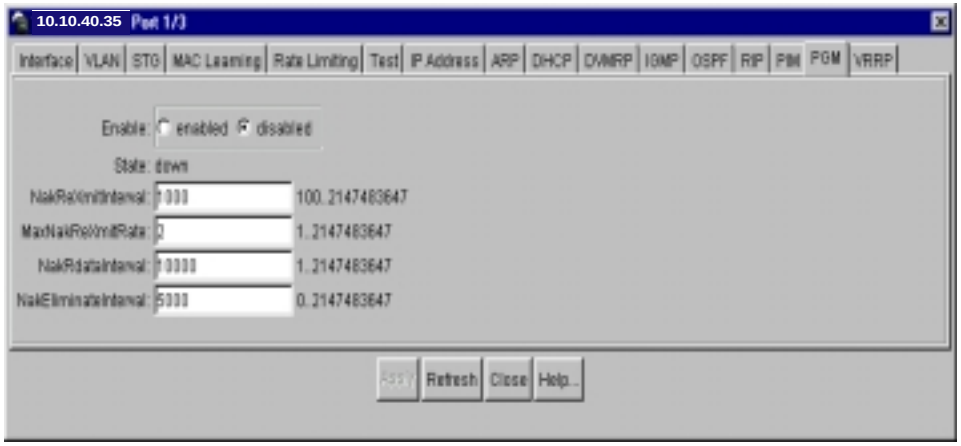
To enable PGM on an interface:

1. On the device view, select a port.
2. From the Device Manager menu bar, choose Edit > Port.

   The Port dialog box opens with the Interface tab displayed.
3. Click the PGM tab.

   The PGM tab opens (Figure 79).

Figure 79 Port dialog box—PGM tab



4. Click enabled.
5. Click Apply.

Table 42 describes the PGM tab fields.

Table 42 PGM port tab fields

Field	Description
Enable	Enables or disables PGM on this interface.
State	Indicates the current state (up or down) of PGM.
NakReXmitInterval	Specifies how long to wait for an NCF (in milliseconds) before retransmitting the NAK. The default is 1000 milliseconds.
MaxNakReXmitRate	Configures the maximum number of NAK retransmission packets allowed per second. The default is 2.
NakRdataInterval	Specifies how long to wait for RDATA (in milliseconds) after receiving an NCF. The default is 10000 milliseconds.
NakEliminateInterval	Specifies the length of time (in milliseconds) during which a network element (NE) eliminates duplicate NAKs. When this interval expires, the NE suspends NAK elimination until the first duplicate arrives. Once this NAK is forwarded, the NE once again eliminates duplicate NAKs for the specified interval. This parameter must be less than NakRdataInterval. The default is 5000 milliseconds.

Configuring VLANs with PGM

To enable PGM on a VLAN:

1. From the Device Manager menu bar, choose VLAN > VLANs.

   The VLAN dialog box opens with the Basic tab displayed.

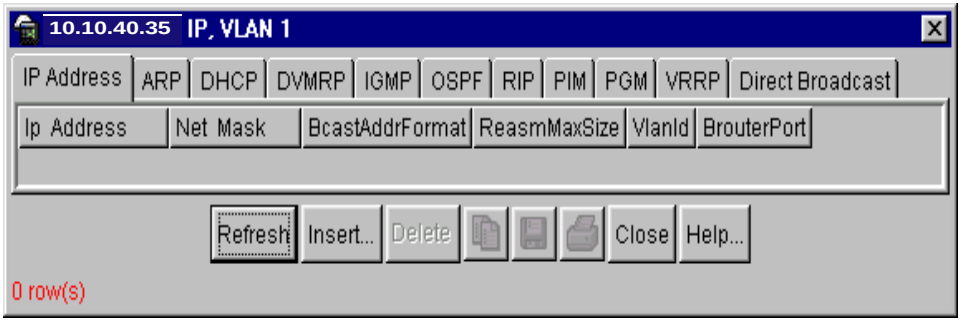
2. Select the VLAN Id that you want to configure with PGM.

   Several buttons on the bottom of the dialog box become available.

3. Click IP.

   The IP, VLAN dialog box opens with the IP Address tab displayed (Figure 80).

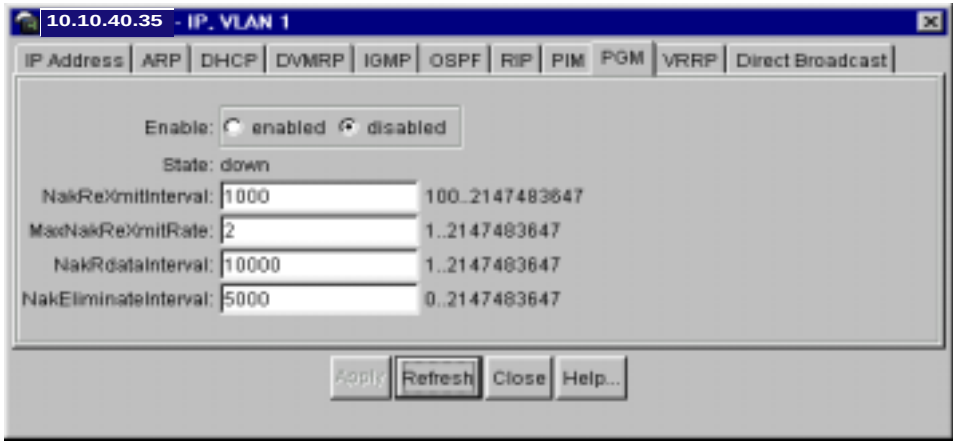
Figure 80 IP VLAN dialog box



4. Click the PGM tab.

   The PGM tab opens (Figure 81).

Figure 81 IP VLAN dialog box—PGM tab



5 Click enabled.

6 Click Apply.

Table 43 describes the PGM VLAN tab fields.

Table 43 IP, VLAN dialog box—PGM tab fields

Field	Description
Enable	Enables or disables PGM on this interface.
State	Indicates the current state (up or down) of PGM.
NakReXmitInterval	Specifies how long to wait for an NCF (in milliseconds) before retransmitting the NAK. The default is 1000 milliseconds.
MaxNakReXmitRate	Configures the maximum number of NAK retransmission packets allowed per second. The default is 2.
NakRdataInterval	Specifies how long to wait for RDATA (in milliseconds) after receiving an NCF. The default is 10000 milliseconds.
NakEliminateInterval	Specifies the length of time (in milliseconds) during which a network element (NE) eliminates duplicate NAKs. When this interval expires, the NE suspends NAK elimination until the first duplicate arrives. Once this NAK is forwarded, the NE once again eliminates duplicate NAKs for the specified interval. This parameter must be less than NakRdataInterval. The default is 5000 milliseconds.

Viewing and editing PGM interface parameters

To view or edit PGM interface parameters:

1 From the Device Manager menu bar, choose IP Routing > PGM.

The PGM dialog box opens with the Globals tab displayed (Figure 78 on page 213).

2 Click the Interfaces tab.

The Interfaces tab opens (Figure 82).

Figure 82 PGM dialog box—Interfaces tab

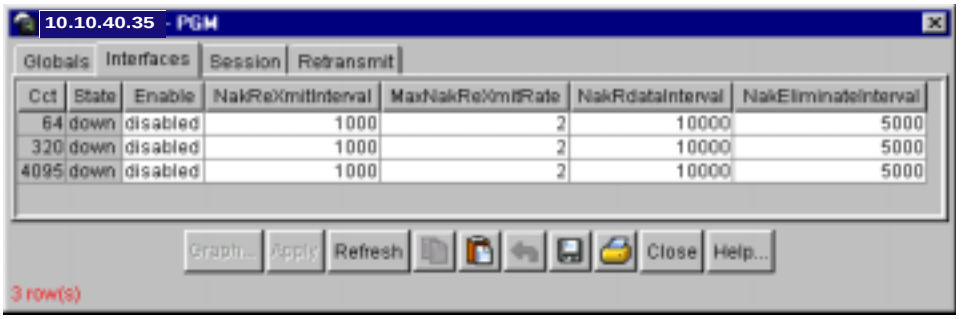


Table 44 describes the PGM Interfaces tab fields.

Table 44 PGM Interfaces tab fields

Field	Description
Cct	Displays the circuit number of the selected interface.
State	Displays the current state (up or down) of PGM.
Enable	Enables or disables PGM.
NakReXmitInterval	Specifies how long to wait for an NCF (in milliseconds) before retransmitting the NAK. The default is 1000 milliseconds.
MaxNakReXmitRate	Configures the maximum number of NAK retransmission packets allowed per second. The default is 2.

Table 44 PGM Interfaces tab fields (continued)

Field	Description
NakRdataInterval	Specifies how long to wait for RDATA (in milliseconds) after receiving an NCF. The default is 10000 milliseconds.
NakEliminateInterval	Specifies the length of time (in milliseconds) during which a network element (NE) eliminates duplicate NAKs. When this interval expires, the NE suspends NAK elimination until the first duplicate arrives. Once this NAK is forwarded, the NE once again eliminates duplicate NAKs for the specified interval. This parameter must be less than NakRdataInterval. The default is 5000 milliseconds.

Graphing PGM interface statistics

The following sections discuss the interface statistics that you can graph.

- "Graphing SPM and RDATA statistics for an interface," next
- "Graphing NAK, NNAK, and NCF statistics for an interface" on page 223

Note: All graphing tables have the following buttons: Line Chart, Area Chart, Bar Chart, Pie Chart, Export Data, Print table, Clear Counter, Close, and Help.

Graphing SPM and RDATA statistics for an interface

You can graph statistics on all SPM and RDATA packets that go through a selected interface.

To graph SPM and RDATA statistics:

1. From the Device Manager menu bar, choose IP Routing > PGM.

   The PGM dialog box opens with the Globals tab displayed.

2. Click the Interfaces tab.

   The Interfaces tab opens.

3. Select an interface.

   The Graph button at the bottom of the dialog box becomes available.

4. Click Graph.

   The PGM Interface dialog box opens with the Spms/Rdata tab displayed (Figure 83).

Figure 83 PGM Interface Graph dialog box—Spms/Rdata tab

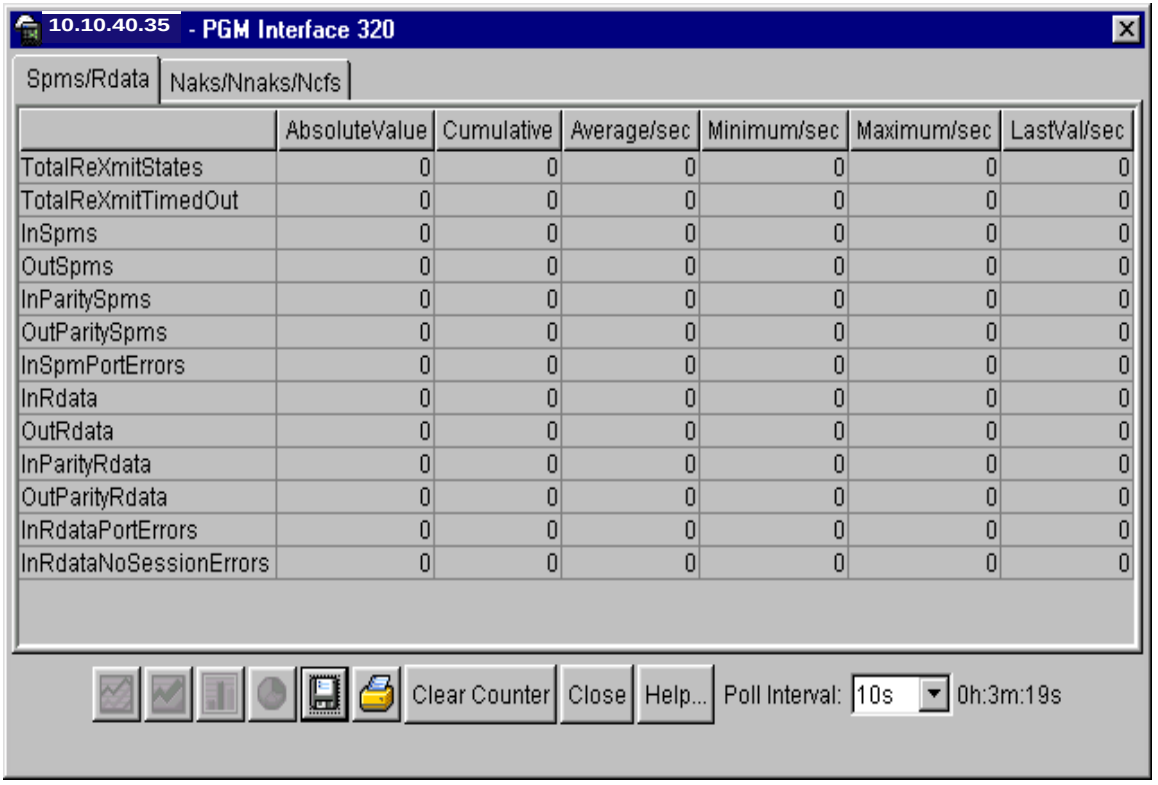


Table 45 describes the interface Spms/Rdata tab fields.

Table 45 Interface Spms/Rdata tab fields

Field	Description
TotalReXmitStates	Displays the total number of retransmit state entries for this interface.
TotalReXmitTimedOut	Displays the total number of timed out retransmit state entries for this interface.
InSpms	Displays the number of SPMs received on this interface.
OutSpms	Displays the number of SPMs sent out from this interface.
InParitySpms	Displays the number of parity SPMs received on this interface.

Table 45 Interface Spms/Rdata tab fields

Field	Description
OutParitySpms	Displays the number of parity SPMs sent out from this interface.
InSpmPortErrors	Displays the number of SPMs discarded because they were received on the wrong interface.
InRdata	Displays the number of RDATA packets received on this interface.
OutRdata	Displays the number of RDATA packets sent out from this interface.
InParityRdata	Displays the number of parity RDATA packets received on this interface.
OutParityRdata	Displays the number of parity RDATA packets sent out from this interface.
InRdataPortErrors	Displays the number of RDATA packets discarded because they were received on the wrong interface.
InRdataNoSessionErrors	Displays the number of RDATA packets discarded because there was no active session.

Graphing NAK, NNAK, and NCF statistics for an interface

To graph NAK, NNAK, and NCF statistics:

1. From the Device Manager menu bar, choose IP Routing > PGM.

   The PGM dialog box opens with the Globals tab displayed.

2. Click the Interfaces tab.

   The Interfaces tab opens.

3. Select an interface.

   The Graph button at the bottom of the dialog box becomes available.

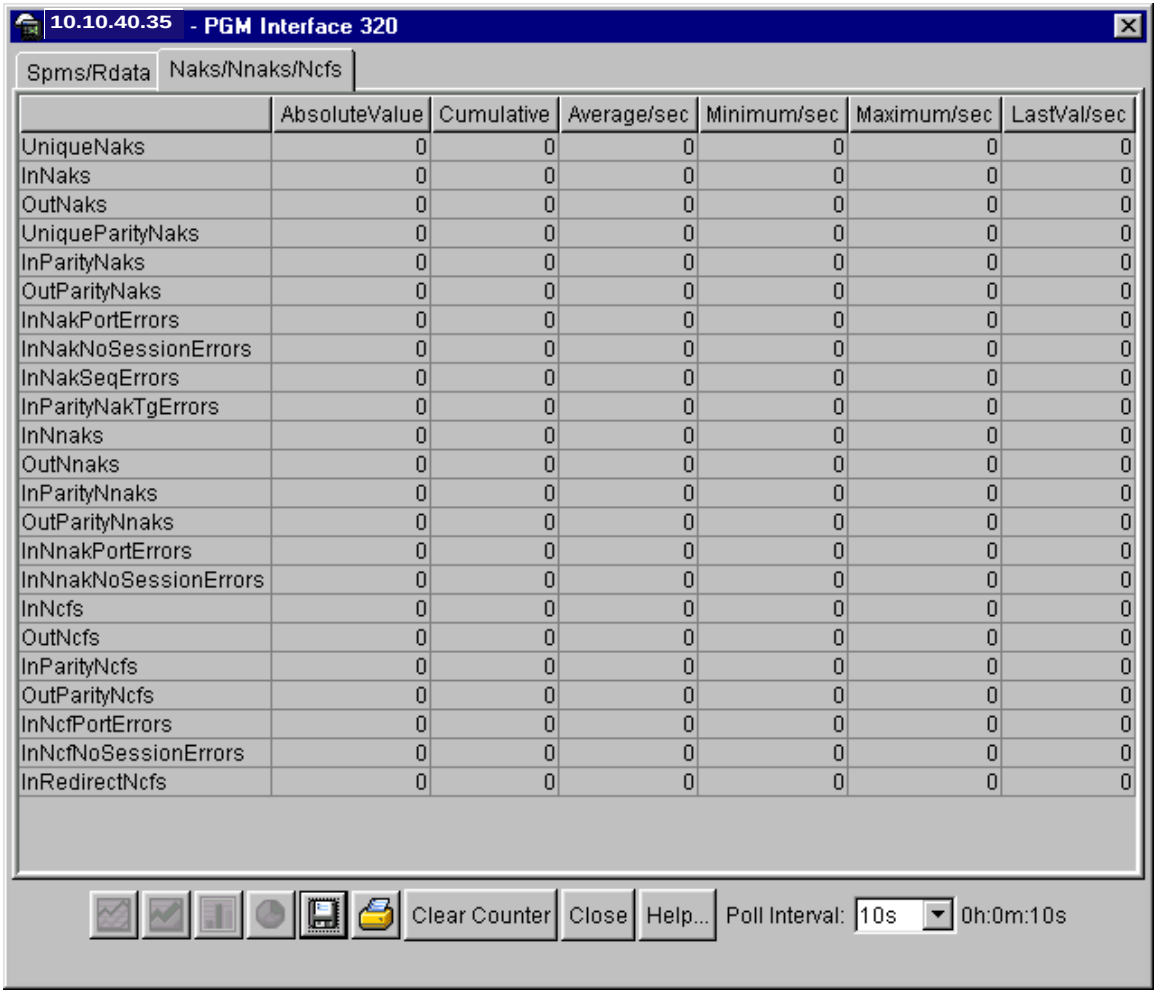
4. Click Graph.

   The PGM Interface dialog box opens with the Spms/Rdata tab displayed.

5. Click the Naks/Nnaks/Ncfs tab.

   The Naks/Nnaks/Ncfs tab opens (Figure 84).

Figure 84 PGM Interface Graph dialog box—Naks/Nnaks/Ncfs tab



	AbsoluteValue	Cumulative	Average/sec	Minimum/sec	Maximum/sec	LastVal/sec
UniqueNaks	0	0	0	0	0	0
InNaks	0	0	0	0	0	0
OutNaks	0	0	0	0	0	0
UniqueParityNaks	0	0	0	0	0	0
InParityNaks	0	0	0	0	0	0
OutParityNaks	0	0	0	0	0	0
InNakPortErrors	0	0	0	0	0	0
InNakNoSessionErrors	0	0	0	0	0	0
InNakSeqErrors	0	0	0	0	0	0
InParityNakTgErrors	0	0	0	0	0	0
InNnaks	0	0	0	0	0	0
OutNnaks	0	0	0	0	0	0
InParityNnaks	0	0	0	0	0	0
OutParityNnaks	0	0	0	0	0	0
InNnakPortErrors	0	0	0	0	0	0
InNnakNoSessionErrors	0	0	0	0	0	0
InNcfs	0	0	0	0	0	0
OutNcfs	0	0	0	0	0	0
InParityNcfs	0	0	0	0	0	0
OutParityNcfs	0	0	0	0	0	0
InNcfPortErrors	0	0	0	0	0	0
InNcfNoSessionErrors	0	0	0	0	0	0
InRedirectNcfs	0	0	0	0	0	0

Table 46 describes the interface Naks/Nnaks/Ncfs tab fields.

Table 46 Interface Naks/Nnaks/Ncfs tab fields

Field	Description
UniqueNaks	Displays the number of unique NAKs received on this interface.
InNaks	Displays the number of NAKs received on this interface.
OutNaks	Displays the number of unique NAKs sent out from this interface.
UniqueParityNaks	Displays the number of unique parity NAKs received on this interface.
InParityNaks	Displays the number of parity NAKs received on this interface.
OutParityNaks	Displays the number of parity NAKs sent out from this interface.
InNakPortErrors	Displays the number of NAKs discarded because they were received on the wrong interface.
InNakNoSessionErrors	Displays the number of NAKs discarded because there was no active session.
InNakSeqErrors	Displays the number of NAKs discarded because they were out of sequence.
InParityNakTgErrors	Displays the number of parity NAKs discarded because they were out of the parity TG window.
InNnaks	Displays the number of NNAKs received on this interface.
OutNnaks	Displays the number of NNAKs sent out from this interface.
InParityNnaks	Displays the number of parity NNAKs received on this interface.
OutParityNnaks	Displays the number of parity NNAKs sent out from this interface.
InNnakPortErrors	Displays the number of NNAKs discarded because they were received on the wrong interface.
InNnakNoSessionErrors	Displays the number of NNAKs discarded because there was no active session.
InNcfs	Displays the number of NCFs received on this interface.
OutNcfs	Displays the number of NCFs sent out from this interface.
InParityNcfs	Displays the number of parity NCFs received on this interface.

Table 46 Interface Naks/Nnaks/Ncfs tab fields (continued)

Field	Description
OutParityNcfs	Displays the number of parity NCFs sent out from this interface.
InNcfPortErrors	Displays the number of NCFs discarded because they were received on the wrong interface.
InNcfNoSessionErrors	Displays the number of NCFs discarded because there was no active session.
InRedirectNcfs	Displays the number of redirected NCFs received on this interface.

Viewing PGM session parameters

To view PGM session parameters:

1. From the Device Manager menu bar, choose IP Routing > PGM.

   The PGM dialog box opens with the Globals tab displayed.

2. Click the Session tab.

   The Session tab opens (Figure 85).

Figure 85 PGM dialog box—Session tab

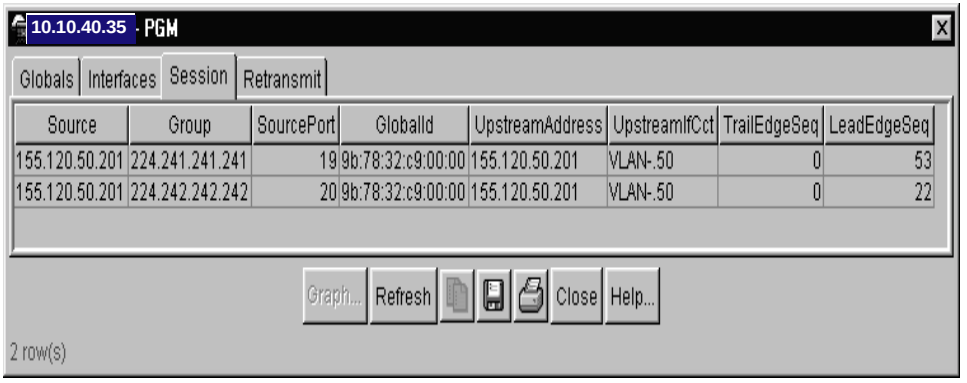


Table 47 describes the PGM Session tab fields.

Table 47 PGM Session tab fields

Field	Description
Source	Displays the source IP address for this session.
Group	Displays the destination group address for this session.
SourcePort	Displays the source port for this session.
GlobalId	Displays the global ID for this session.
UpstreamAddress	Displays the IP address of the upstream interface for this session.
UpstreamIfCct	Displays the circuit number of the upstream interface for this session.
TrailEdgeSeq	Displays the trailing edge sequence of the transfer window.
LeadEdgeSeq	Displays the leading edge sequence of the transfer window.

Graphing PGM session statistics

The following sections discuss the session statistics that you can graph.

- "Graphing SPM statistics for a session," next
- "Graphing NAK statistics for a session" on page 230

Note: All graphing tables have the following buttons: Line Chart, Area Chart, Bar Chart, Pie Chart, Export Data, Print table, Clear Counter, Close, and Help.

Graphing SPM statistics for a session

You can graph statistics on all SPM packets for a selected session.

To graph SPM statistics:

1. From the Device Manager menu bar, choose IP Routing > PGM.

   The PGM dialog box opens with the Globals tab displayed.

2. Click the Session tab.

   The Session tab opens.

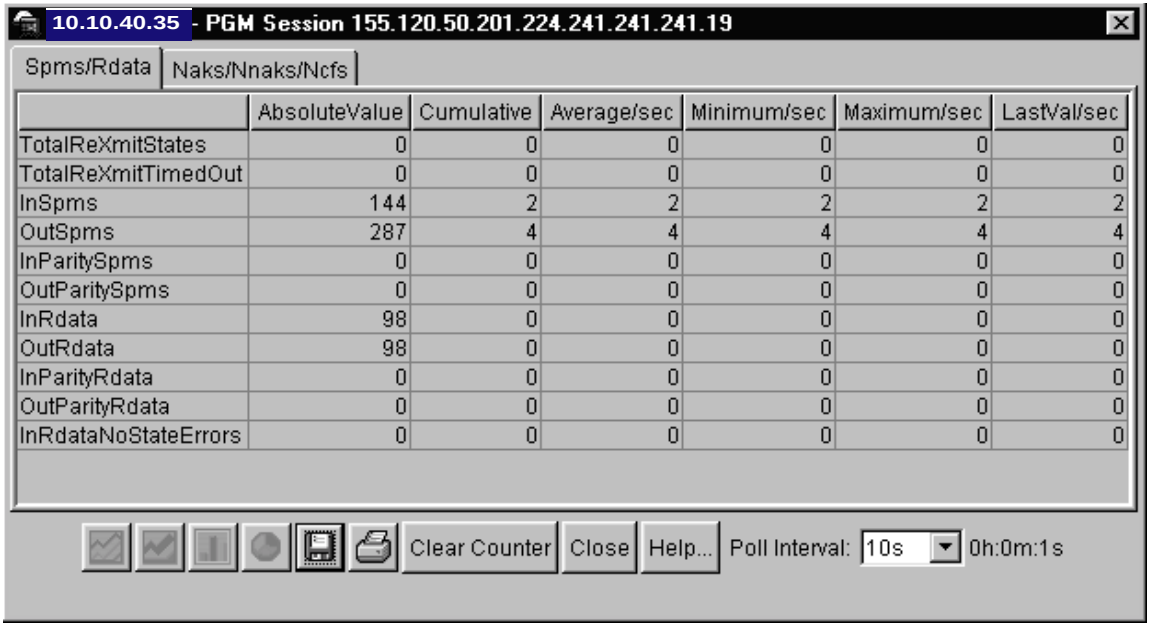
3. Select a session.

   The Graph button at the bottom of the dialog box becomes available.

4. Click Graph.

   The PGM Session dialog box opens with the Spms/Rdata tab displayed (Figure 86).

Figure 86 PGM Session Graph dialog box—Spms/Rdata tab



	AbsoluteValue	Cumulative	Average/sec	Minimum/sec	Maximum/sec	LastVal/sec
TotalReXmitStates	0	0	0	0	0	0
TotalReXmitTimedOut	0	0	0	0	0	0
InSpms	144	2	2	2	2	2
OutSpms	287	4	4	4	4	4
InParitySpms	0	0	0	0	0	0
OutParitySpms	0	0	0	0	0	0
InRdata	98	0	0	0	0	0
OutRdata	98	0	0	0	0	0
InParityRdata	0	0	0	0	0	0
OutParityRdata	0	0	0	0	0	0
InRdataNoStateErrors	0	0	0	0	0	0

Table 48 describes the session Spms/Rdata tab fields.

Table 48 Session Spms/Rdata tab fields

Field	Description
TotalReXmitStates	Displays the total number of retransmit state entries during this session.
TotalReXmitTimedOut	Displays the total number of timed out retransmit state entries during this session.
InSpms	Displays the number of SPMs received during this session.
OutSpms	Displays the number of SPMs sent out during this session.
InParitySpms	Displays the number of parity SPMs received during this session.
OutParitySpms	Displays the number of parity SPMs sent out during this session.
InRdata	Displays the number of RDATA packets received during this session.
OutRdata	Displays the number of RDATA packets sent out during this session.
InParityRdata	Displays the number of parity RDATA packets received during this session.
OutParityRdata	Displays the number of parity RDATA packets sent out during this session.
InRdataNoStateErrors	Displays the number of RDATA packets discarded because there was no active session.

Graphing NAK statistics for a session

To graph NAK statistics:

1. From the Device Manager menu bar, choose IP Routing > PGM.

   The PGM dialog box opens with the Globals tab displayed.

2. Click the Session tab.

   The Session tab opens.

3. Select a session.

   The Graph button at the bottom of the dialog box becomes available.

4. Click Graph.

   The PGM Session dialog box opens with the Spms/Rdata tab displayed.

5. Click the Naks/Nnaks/Ncfs tab.

   The Naks/Nnaks/Ncfs tab opens (Figure 87).

Figure 87 PGM Session Graph dialog box—Naks/Nnaks/Ncfs tab

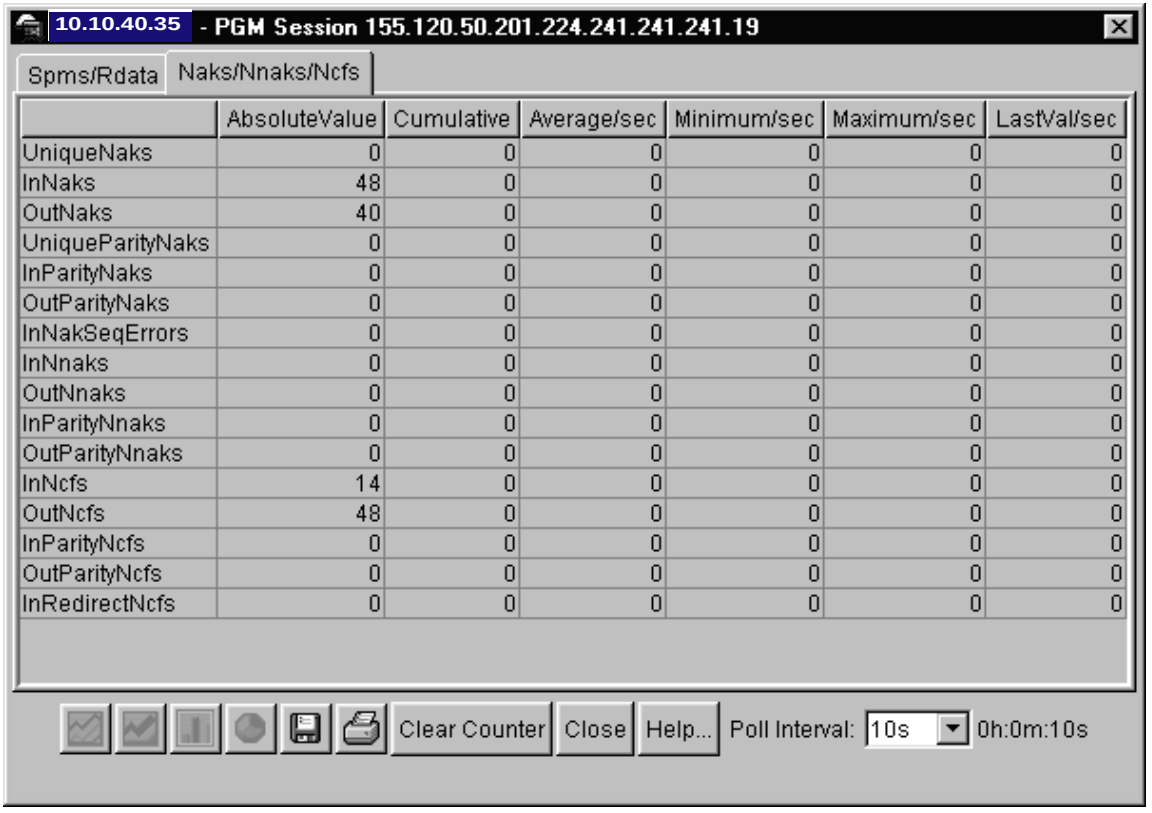


Table 49 describes the session Naks/Nnaks/Ncfs tab fields.

Table 49 Session Naks/Nnaks/Ncfs tab fields

Field	Description
UniqueNaks	Displays the number of unique NAKs received during this session.
InNaks	Displays the number of NAKs received during this session.
OutNaks	Displays the number of unique NAKs sent out during this session.
UniqueParityNaks	Displays the number of unique parity NAKs received during this session.

Table 49 Session Naks/Nnaks/Ncfs tab fields (continued)

Field	Description
InParityNaks	Displays the number of parity NAKs received during this session.
OutParityNaks	Displays the number of parity NAKs sent out during this session.
InNakSeqErrors	Displays the number of NAKs discarded because they were out of sequence.
InNnaks	Displays the number of NNAKs received during this session.
OutNnaks	Displays the number of NNAKs sent out during this session.
InParityNnaks	Displays the number of parity NNAKs received during this session.
OutParityNnaks	Displays the number of parity NNAKs sent out during this session.
InNcfs	Displays the number of NCFs received during this session.
OutNcfs	Displays the number of NCFs sent out during this session.
InParityNcfs	Displays the number of parity NCFs received during this session.
OutParityNcfs	Displays the number of parity NCFs sent out during this session.
InRedirectNcfs	Displays the number of redirected NCFs received during this session.

Viewing the Retransmit parameters

To view the retransmit parameters:

1 From the Device Manager menu bar, choose IP Routing > PGM.

The PGM dialog box opens with the Globals tab displayed.

2 Click the Retransmit tab.

The Retransmit tab opens (Figure 88).

Figure 88 PGM dialog box—Retransmit tab

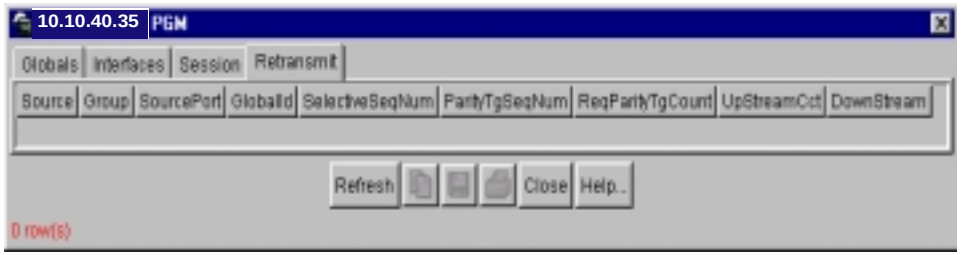


Table 50 describes the PGM Retransmit tab fields.

Table 50 PGM Retransmit tab fields

Field	Description
Source	Displays the source IP address for this entry.
Group	Displays the destination group address for this entry.
SourcePort	Displays the source port of this retransmit state.
GlobalId	Displays the global ID for this entry.
SelectiveSeqNum	Displays the selected sequence number for this entry.
ParityTgSeqNum	Displays the requested parity TG sequence number for this entry.
ReqParityTgCount	Displays the requested number of missing parity packets of the specified TG.
UpStreamCct	Displays the upstream circuit number from this entry.
DownStream	Displays the list of downstream interfaces from this entry.

Chapter 6
Viewing and editing multicast routes using Device Manager

The Multicast tabs allow you to view information about any layer 3 IP Multicast protocol interface set up on the switch.

This chapter describes the following topics:

Viewing multicast route information

To view multicast route information:

➔ From the Device Manager menu bar, choose IP Routing > Multicast.

The Multicast dialog box opens with the Routes tab displayed (Figure 89).

Figure 89 Multicast dialog box—Routes tab

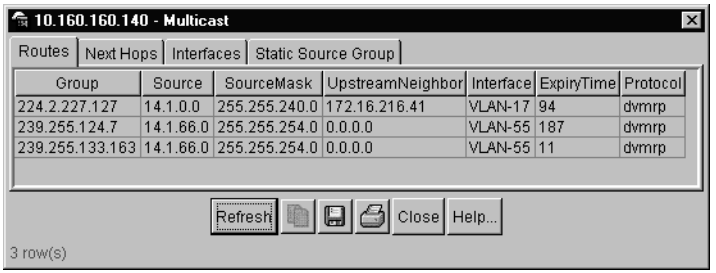


Table 51 describes the Routes tab fields.

Table 51 Routes tab fields

Field	Description
Group	The IP multicast group address for which this entry contains multicast routing information.
Source	The network address which, when combined with the corresponding route SourceMask value, identifies the sources for which this entry contains multicast routing information.
SourceMask	The network mask which, when combined with the corresponding route Source value, identifies the sources for which this entry contains multicast routing information.
UpstreamNeighbor	The address of the upstream neighbor (e.g., RPF neighbor) from which IP datagrams from these sources to this multicast address are received or 0.0.0.0 if the network is local.
Interface	The DVMRP interface, slot/port number, or VLAN ID on which IP datagrams sent by these sources to this multicast address are received.

Table 51 Routes tab fields (continued)

Field	Description
ExpiryTime	The amount of time remaining before this entry will be aged out. The value 0 indicates that the entry is not subject to aging.
Protocol	The routing protocol through which this route was learned. Currently only DVMRP is supported.

Viewing multicast next hop information

The Multicast Next Hops tab displays all multicast next hop information.

To open the Next Hops tab:

1. From the Device Manager menu bar, choose IP Routing > Multicast.

   The Multicast dialog box opens with the Routes tab displayed.

2. Click the Next Hops tab.

   The Next Hops tab opens (Figure 90).

Figure 90 Multicast dialog box—Next Hops tab

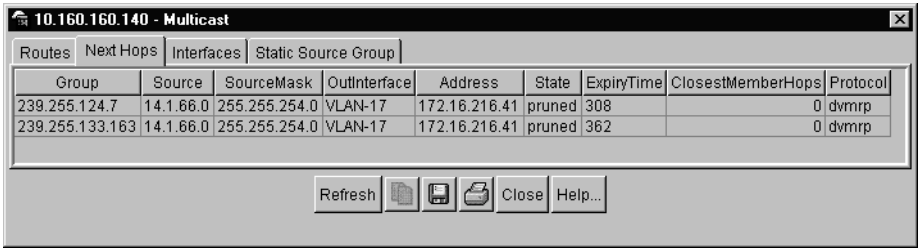


Table 52 describes the Next Hops tab fields.

Table 52 Next Hops tab fields

Field	Description
Group	The IP multicast group for which this entry specifies a next hop on an outgoing interface.
Source	The network address which, when combined with the corresponding next hop SourceMask value, identifies the source for which this entry specifies a next hop on an outgoing interface.
SourceMask	The network mask which, when combined with the corresponding next hop Source value, identifies the source for which this entry specifies a next hop on an outgoing interface.
OutInterface	The DVMRP interface slot/port number or VLAN ID for the outgoing interface for this next hop.
Address	The address of the next hop specific to this entry. For most interfaces, it is identical to the next hop group. NBMA interfaces, however, may have multiple next hop addresses out a single outgoing interface.
State	An indication of whether or not the outgoing interface and next hop represented by this entry is currently being used to forward IP datagrams. A Value of “forwarding” indicates it is currently being used; “pruned” indicates it is not being used.
ExpiryTime	The minimum amount of time remaining before this entry will be aged out. The value 0 indicates that the entry is not subject to aging.
ClosestMemberHops	The minimum number of hops between this router and any member of this IP Multicast group reached via this next hop on this outgoing interface. Any IP Multicast datagrams for the group that have a TTL less than this number of hops will not be forwarded to this next hop.
Protocol	The routing protocol through which this next hop was learned.Currently only DVMRP is supported.

Viewing and editing multicast interface information

To view and edit multicast interface information.

1 From the Device Manager menu bar, choose IP Routing > Multicast.

The Multicast dialog box opens with the Routes tab displayed.

2 Click the Interfaces tab.

The Interfaces tab opens (Figure 91).

Figure 91 Multicast dialog box—Interfaces tab

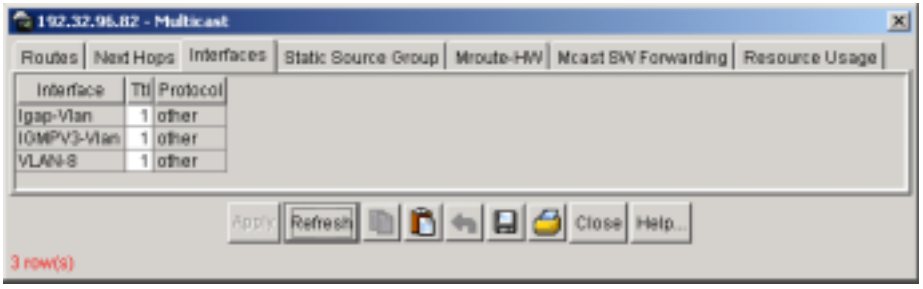


Table 53 describes the Interfaces tab fields.

Table 53 Multicast dialog box—Interfaces tab fields

Field	Description
Interface	The slot/port number or VLAN ID for which this entry contains information.
Ttl	The datagram time to live (TTL) threshold for the interface. Any IP multicast datagrams with a TTL less than this threshold is not forwarded out the interface. The default value of 1 means that all multicast packets are forwarded out the interface.
Protocol	The routing protocol running on this interface. Currently only DVMRP is supported.

Configuring multicast static source groups

Static source groups enable you to configure **static** source-group entries in the DVMRP or PIM multicast routing table. Neither DVMRP nor PIM can prune these entries from the distribution tree. In other words, even if there are no receivers in the group, the multicast stream for a static source-group entry stays active.

Configuration considerations

The Passport 8600 supports static source groups using one of several multicast protocols: DVMRP, PIM-SM (sparse mode), and PIM-SSM (source specific multicast). For conceptual information about DVMRP, PIM and static source groups, refer to Chapter 1, "IP Multicast concepts."

Before you can configure a static source group, you must globally enable one of the following protocols:

- DVMRP - To globally enable DVMRP, refer to "Enabling DVMRP globally" on page 135.
- PIM sparse mode (SM) - To globally enable PIM-SM, refer to "Enabling PIM-SM globally" on page 184.
- PIM source specific multicast mode (SSM) - To globally enable PIM-SSM, refer to "Enabling Source Specific Multicast (SSM) globally" on page 205.

After configuring static source groups, keep the following points in mind:

- The maximum number of static source groups should not exceed 1024.
- Disabling DVMRP or PIM causes the switch to deactivate all of the static source groups. When you re-enable DVMRP or PIM, the switch re-activates the static source groups.
- **Using DVMRP or PIM-SM**

  In DVMRP and PIM-SM configurations, the static source-group feature works for both specific source addresses and subnet addresses. This is achieved by using the SrcSubnetMask field (see "Adding a new static source group").

When the Network Mask is configured as 255.255.255.255, the full source address is used to match the (S,G) which is the specific source case. When the network mask field is configured as a subnet mask for the source, only the source subnet is used to match (S,G)s. The first entry in Figure 92 shows a subnet configuration and the second entry shows a source specific configuration.

- **Using PIM-SSM**

  In PIM-SSM configurations, static source groups have the following limitations:

  — **Subnets** - SSM static source groups work *only* with specific IP addresses. This means that static source groups cannot work with source subnets so the mask must be a full 32-bit mask, 255.255.255.255, and the source has to be a host address.

  — **SSM Channels** - Static source groups cannot conflict with SSM channels and vice versa. When you configure a static source group or an SSM channel, the switch performs a consistency check to make sure there are no conflicts. You cannot map one group (G) to different sources for both a static source group and an SSM channel. For SSM channel information, refer to "Configuring the SSM channel table" on page 123.

  If a group is already mapped to a source and you try to map it to a different source, the switch detects the conflict and displays an error message. For example, if G1 is already defined in the SSM channel table as (S1,G1), you cannot configure G1 as static source group (S2,G1). However, you can configure the same entry (S1,G1) in both the SSM channel table and as a static source group. As long as there is no conflict between the two tables, the configuration is allowed.

Viewing and editing static source groups

To view and edit static source groups:

1 From the Device Manager menu bar, choose IP Routing > Multicast.

The Multicast dialog box opens with the Routes tab displayed.

2 Click the Static Source Group tab.

The Static Source Group tab opens (Figure 92).

Figure 92 Multicast dialog box—Static Source Group tab

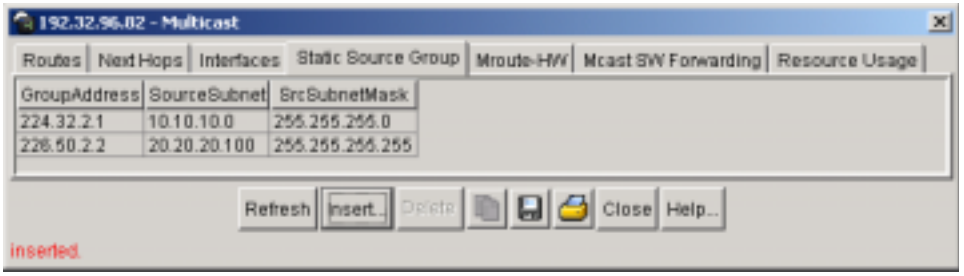


Table 54 describes the Static Source Group tab fields.

Table 54 Static Source Group tab fields

Field	Description
GroupAddress	The multicast group IP address for this static source-group entry.
SourceSubnet	The multicast source address for this static source-group entry. How you configure the source address depends on the protocol you are using and in what mode. For more information, refer to "Configuration considerations."
SrcSubnetMask	The source's subnet mask for this static source-group entry.

Adding a new static source group

The following steps describe how to add a *new* static source group. An attempt to add a duplicate of an existing source-group entry results in an error message.

1 From the Device Manager menu bar, choose IP Routing > Multicast.

The Multicast dialog box opens with the Routes tab displayed.

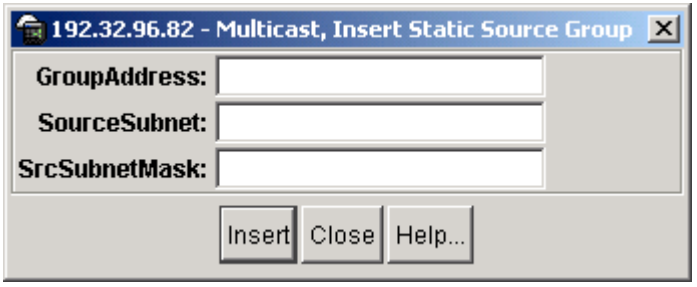
2 Click the Static Source Group tab.

The Static Source Group dialog box opens.

3 Click Insert.

The Multicast, Insert Static Source Group dialog box opens (Figure 93).

Figure 93 Multicast, Insert Static Source Group dialog box



4 Complete the information in the dialog box and Click Insert.

Note: To avoid conflicts between the static source group table and the SSM channel table, refer to "Configuration considerations" before filling out the fields in this dialog box.

Deleting a static source group

1. From the Device Manager menu bar, choose IP Routing > Multicast.

   The Multicast dialog box opens with the Routes tab displayed.

2. Click the Static Source Group tab.

   The Static Source Group tab opens.

3. Select the static source group that you want to delete.

   The Delete button is highlighted (Figure 94).

Figure 94 Static Source Group tab

4. Click Delete.

Troubleshooting DVMRP

The Mroute-HW tab provides an exact hardware view of existing IP multicast records and information on sender and receiver ports for every stream. When you select this tab, you are presented with a table and three additional tabs (Prunes, Sources, and EgressVLANs) that allow you to gather additional information on multicast hardware records. This section describes these new tabs and explains how to access them.

To perform DVMRP troubleshooting:

1. From the Device Manager menu bar, choose IP Routing > Multicast.

   The Multicast dialog box opens with the Routes tab displayed.

2. Click the Mroute-HW tab.

   The Mroute-HW tab opens (Figure 95).

   By default, all three buttons (Prunes, Sources, and EgressVLANs) in the dialog are disabled.

3. Click on any row in the table (representing the output of Mroute-HW).

   The Prunes, Sources, and EgressVLANs buttons are enabled (highlighted).

4. Click either the Prunes, Sources, or Egress Vlans buttons.

   Depending on your selection, the Prunes (Figure 96), Sources (Figure 97), or Egress VLANs (Figure 98) dialog box will open displaying further information about the stream selected in the table.

5. Click the Close button to return to the Multicast- Mroute-HW tab.

Figure 95 Multicast dialog box—Mroute-HW tab

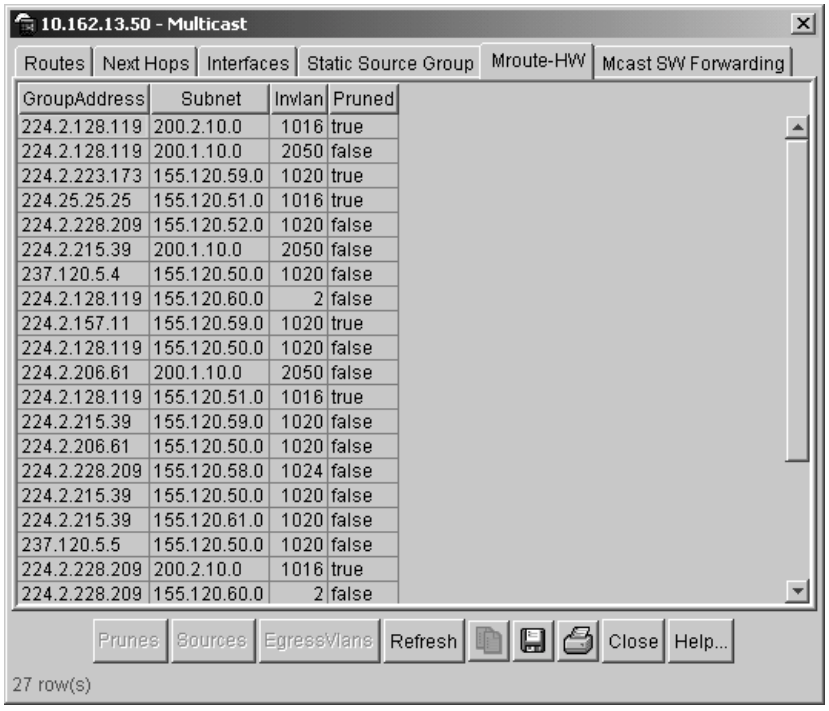


Table 55 describes the fields that appear on the Multicast dialog Mroute-HW tab.

Table 55 Mroute-HW tab fields

Field	Description
GroupAddress	The IP multicast group address for the multicast stream.
Subnet	The network address of the source subnet that has sources sending IP multicast traffic to the GroupAddress. **Note:** There can be several sources sending to that Group. You can use the Source tab to view these sources.
Invlan	The ingress VLAN ID where the traffic emanates for the multicast stream.
Pruned	True indicates that the multicast stream has been pruned back. False indicates it has not.

Mroute-HW—Prunes tab fields

The Prunes tab shows all of the prunes received for the Group address in the multicast stream selected from the Mroute-HW table.

Figure 96 displays the Prunes tab. The output of this tab shows all of the prunes received for the Group address in the multicast stream selected from the Mroute-HW table.

Figure 96 Multicast dialog box—Mroute-HW tab—Prunes tab

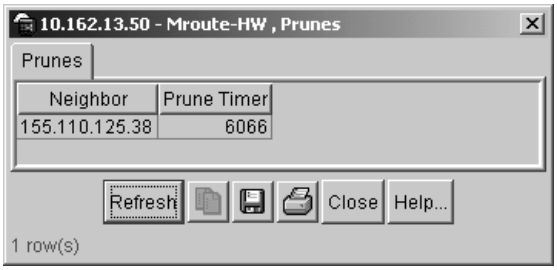


Table 56 describes the fields in the Prunes tab.

Table 56 Prunes tab fields

Field	Description
Neighbor	The IP address of the downstream neighbor from whom the prune has been received.
Prune Timer	The time left for the neighboring downstream router to send the graft message.

Mroute-HW—Sources tab fields

The Sources tab allows you to view all the sources on the subnet that are sending to the particular group selected in the Mroute-HW table.

Figure 97 displays the Sources tab. The Sources tab allows you to view all the sources on the subnet that are sending to the particular group selected in the Mroute-Hw table.

Figure 97 Multicast dialog box—Mroute-HW tab—Sources tab

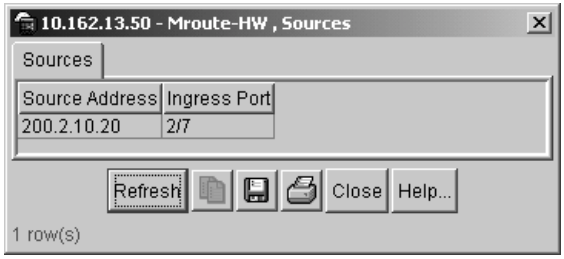


Table 57 describes the fields in the Sources tab.

Table 57 Sources tab fields

Field	Description
Source Address	The IP addresses of the sources on this particular subnet sending traffic to the multicast group for the selected entry in the Mroute-HW table.
Ingress Port	The corresponding ingress port in the multicast stream selected from the Mroute-HW table.

Mroute-HW—Egress VLANs tab fields

The Egress VLANs tab allows you to view the egress VLANs for the streams corresponding to the selected entry in the Mroute-Hw (subnet, Group) entry.

Figure 98 displays the Egress VLANs tab. The Egress VLANs tab allows you to view the egress VLANs for the streams corresponding to the selected entry in the Mroute-HW (subnet, Group) entry.

Figure 98 Multicast dialog box—Mroute-HW tab—Egress VLANs tab

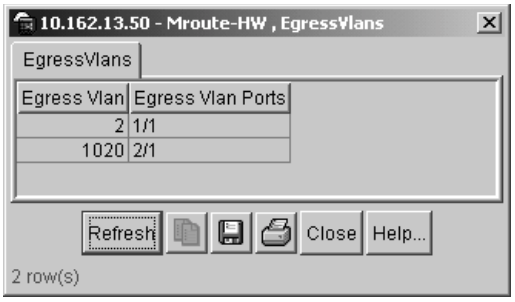


Table 58 describes the Egress VLANs tab fields.

Table 58 Egress VLANs tab fields

Field	Description
Egress Vlan	All the egress VLANs for the particular multicast stream selected from the Mroute-HW table.
Egress Vlan Ports	The corresponding ports for the particular multicast stream selected from the Mroute-HW table.

Configuring IP multicast software forwarding

The IP multicast software forwarding feature enables the CPU to initially forward IP multicast data until a hardware record is created. The CPU forwards the initial packets of a stream it receives and at the same time, creates a corresponding hardware record for any subsequent packets. The advantage to this feature is that it avoids any initial data loss experienced by multicast applications, and is most suited for low bandwidth.

The IP multicast software forwarding is a global system configuration feature that applies to all IP multicast enabled interfaces and protocols. When you enable IP multicast software forwarding, be aware that the hardware is still responsible for forwarding IP multicast traffic. Only initial data traffic is forwarded by the software. Thus, the intention here is not to replace hardware forwarding with software forwarding. By default, the feature is disabled.

Note: To avoid overloading the CPU, Nortel Networks recommends that you do not use the IP multicast software forwarding feature for video multicast applications.

To configure IP multicast software forwarding:

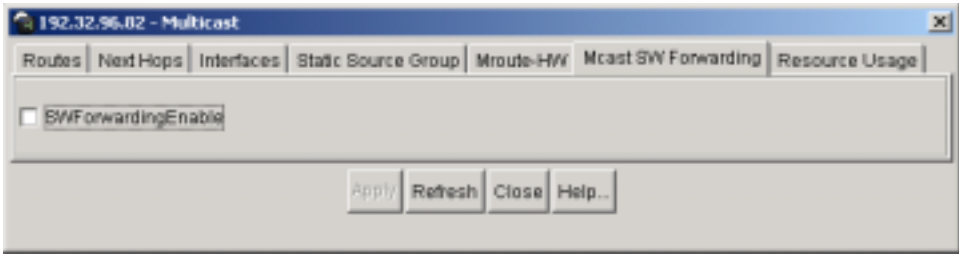
1. From the Device Manager menu bar, choose IP Routing > Multicast.

   The Multicast dialog box opens with the Routes tab displayed.

2. Click the Mcast SW Forwarding tab.

   The Mcast SW Forwarding tab opens (Figure 99).

Figure 99 Multicast dialog box—Mcast SW Forwarding tab



3 Click the SWForwardingEnable check box.

4 Click Apply to enable this feature.

The IP multicast software forwarding feature is now enabled.

Configuring the resource usage counter for multicast streams

The Passport 8600 enables you to query the number of ingress and egress IP multicast streams traversing your switch. Once you have set the thresholds for ingress and egress records, if the record-usage goes beyond the threshold, you will be notified by way of a trap on the console, logged message, or both.

Note: If you do not set the thresholds, Device Manager displays only the ingress and egress records that are currently in use.

To configure or query the number of ingress and egress IP multicast streams traversing your switch:

1 From the Device Manager menu bar select IP Routing > Multicast.

The Multicast dialog box opens with the Routes tab displayed.

2 Select the Resource Usage tab.

The Resource Usage tab opens (Figure 100).

Figure 100 Multicast Dialog box—Records Usage tab

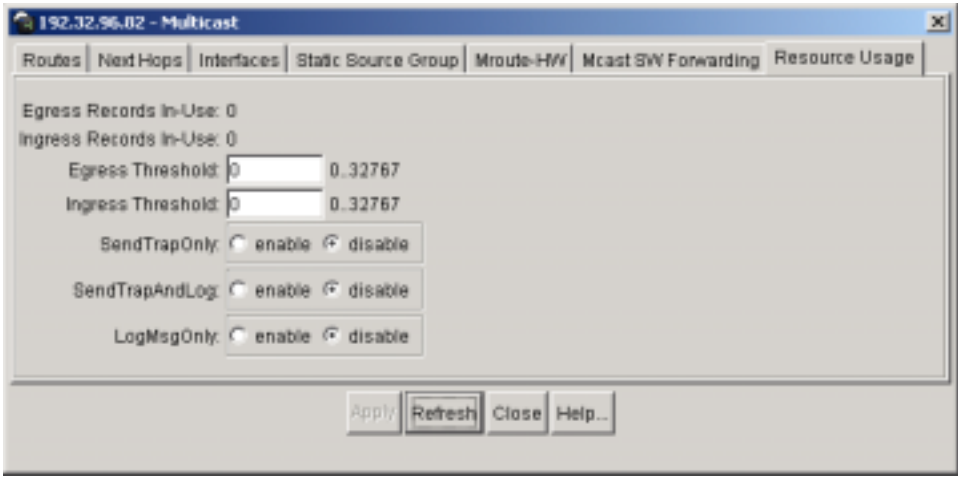


Table 59 describes the fields in the Resource Usage tab.

Table 59 Records Usage tab fields

Field	Description
Egress Records In-Use	Displays the number of egress records (peps) traversing the switch.
Ingress Records In-Use	Displays the number of ingress records (S, G) traversing the switch
Egress Threshold	Enter the egress threshold level (0..32767). A notification message is sent if this value is exceeded.
Ingress Threshold	Enter the ingress threshold level (0..32767). A notification message is sent if this value is exceeded.
Send Trap Only	Select enable to have trap only notification messages sent when the threshold level is exceeded. Select disable if selecting a different notification type.[1]
SendTrapAndLog	Select enable to have trap and log notification messages sent when the threshold level is exceeded. Select disable if selecting a different notification type.
LogMsgOnly	Select enable to have log only notification messages sent when the threshold level is exceeded. Select disable if selecting a different notification type.

1 You can set only one notification type.

Chapter 7
Configuring multicast flow distribution over MLT using Device Manager

Multicast flow distribution over MultiLink Trunking (MLT) provides a mechanism for distributing multicast streams over an MLT. This enables you to distribute the load on different ports of the MLT and aim (whenever possible) to achieve an even distribution of the streams.

To configure multicast flow distribution over MLT, you must enable it globally and per MLT. For more information about MLT concepts and terminology, refer to Chapter 1, “IP Multicast concepts.”

This chapter describes the following topics:

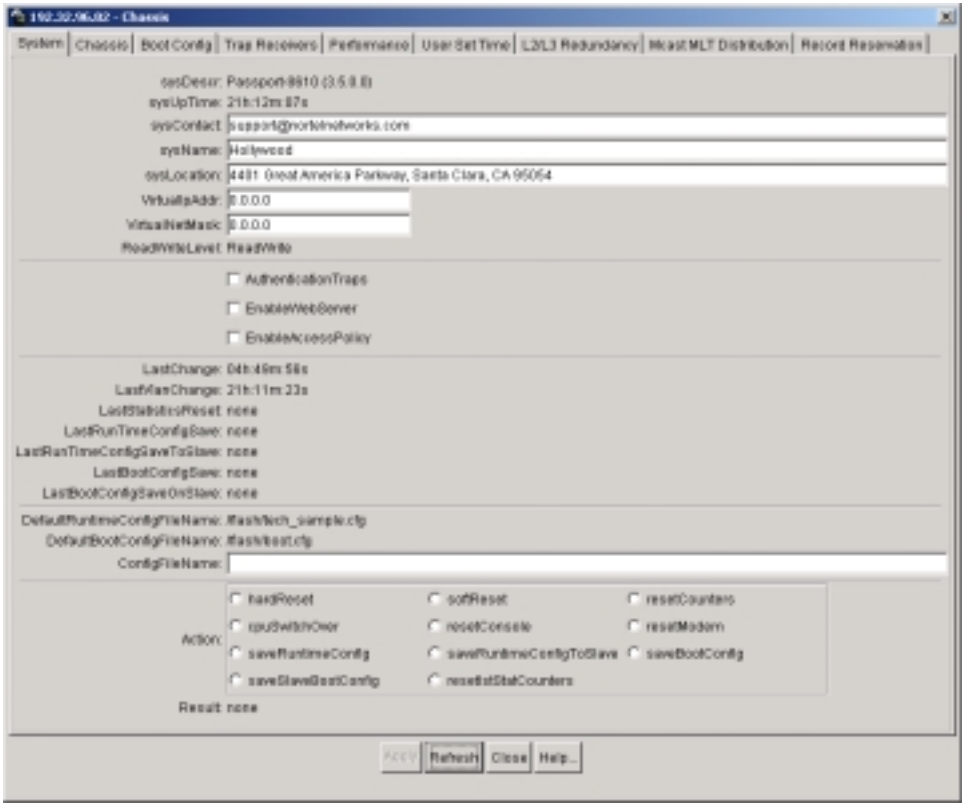
Enabling multicast flow distribution globally

To enable multicast flow distribution over MLT globally:

1 From the Device Manager menu bar, choose Edit > Chassis.

The Chassis dialog box opens with the System tab displayed (Figure 101).

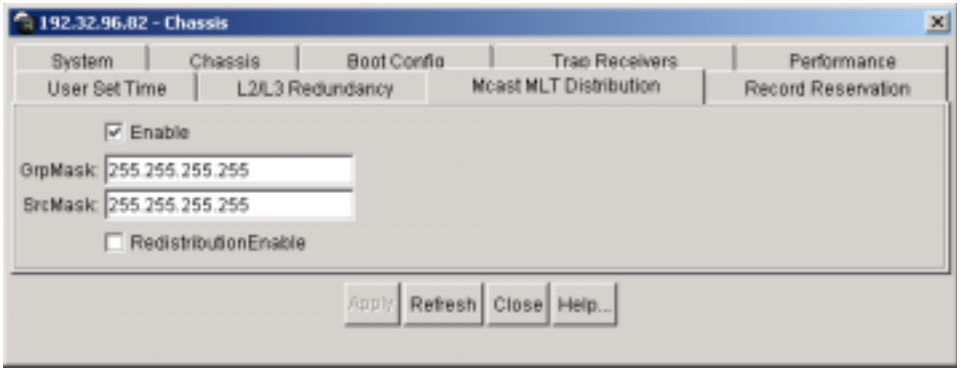
Figure 101 Chassis dialog box



2 Click the Mcast MLT Distribution tab.

The Mcast MLT Distribution tab opens (Figure 102).

Figure 102 Mcast MLT Distribution dialog box



3 Click Enable.

4 Optionally, enter a group IP address in the GrpMask field.

5 Optionally, enter a source IP address in the SrcMask field.

6 Optionally, click RedistributionEnable.

7 Click Apply.

When you select enable/disable or redistribution enable/disable, the following information message appears:

```
Enabling multicast redistribution over MLT may disrupt traffic
for existing streams on the MLT during redistribution. Do you
want to continue?
```

8 Click Yes to continue or No to abort the operation.

If you click Yes, multicast flow distribution over MLT is globally configured.

Table 60 describes the Mcast MLT Distribution tab fields.

Table 60 Mcast MLT Distribution tab fields

Field	Description
Enable	A check box that allows you to globally enable multicast flow distribution. The default is disabled.
GrpMask	A group mask to use when distributing multicast traffic over an MLT. The default is 255.255.255.255.

Table 60 Mcast MLT Distribution tab fields (continued)

Field	Description
SrcMask	A source mask to use when distributing multicast traffic over an MLT. The default is 255.255.255.255.
RedistributionEnable	A check box that allows you to enable or disable the multicast MLT redistribution feature. The default is disabled.

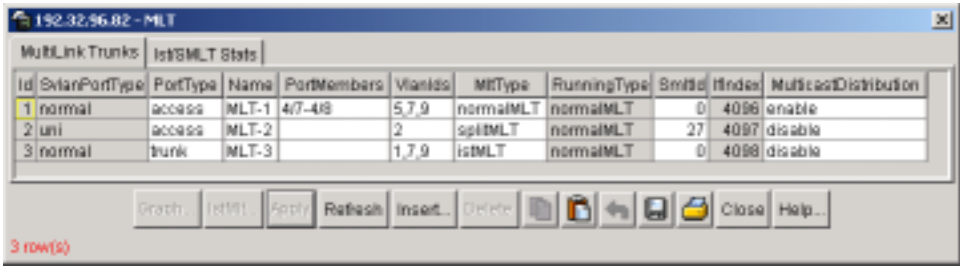
Enabling multicast flow distribution per MLT

To enable multicast flow distribution per MLT:

1 From the Device Manager menu bar, choose VLAN > MLT.

The MLT dialog box opens with the MultiLink Trunks tab displayed (Figure 103).

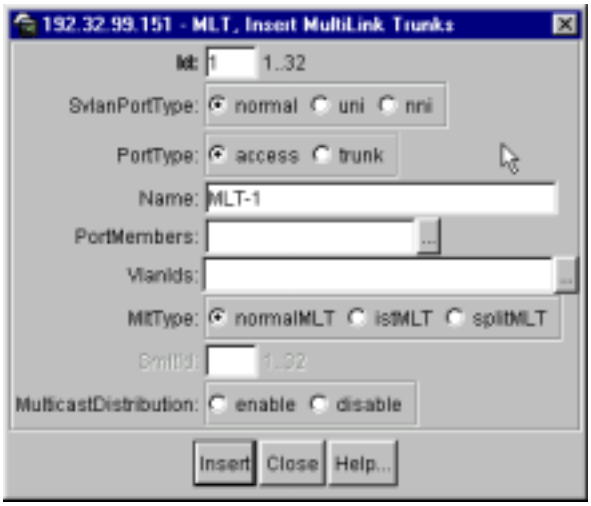
Figure 103 MLT dialog box



2 Click Insert.

The MLT, Insert MultiLink Trunks dialog box opens (Figure 104).

Figure 104 MLT, Insert MultiLink Trunks dialog box



3 Type the ID number for the MultiLink Trunk.

4 Select a stacked VLAN port type.

5 Select Port Type.

6 Type a name for the MultiLink Trunk port.

7 Select the ports to belong to the SMLT port.

8 Select the VLAN IDs to belong to the MultiLink Trunk port.

9 Select the MltType.

10 Enter the SMLT ID, from 1 - 32. Note that the SMLT ID has to be paired on each aggregation switch. The SMLT ID is the identification number that the IST uses to determine which SMLT to send information to. This number is identified between the two aggregation switches.

11 Select enable to activate multicast flow distribution.

12 Click Insert.

The MLT dialog box is updated as shown in (Figure 105).

Figure 105 Updated MLT dialog box

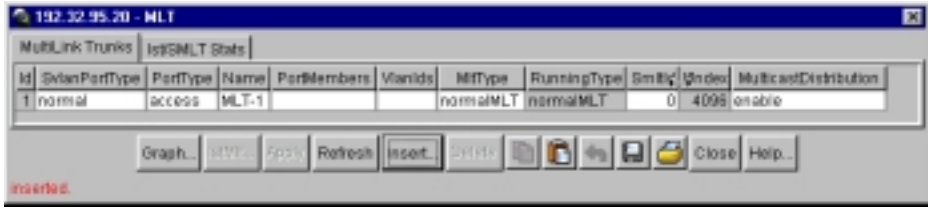


Table 61 describes the MultiLink Trunks tab fields.

Table 61 MultiLink Trunks tab fields

Field	Description
Id	A value that uniquely identifies the MultiLink Trunk associated with this entry.
SvlanPortType	Normal, uni, or nni stacked VLAN port.
PortType	Access or trunk port.
Name	The name given to the MLT.
PortMembers	The ports assigned to the MLT.
VlanIds	The VLANs to which the ports belong.
MltType	The type of MLT. Options here include: • normalMLT • istMLT • splitMLT
SmltId	The split MLT ID.
MulticastDistribution	Enable or disable multicast flow distribution.

Chapter 8
Configuring multicast MAC filtering using Device Manager

Multicast Media Access Control (MAC) filtering allows you to create a smaller flooding domain inside a VLAN. For a particular VLAN, you specify a multicast MAC address and a subset of ports. When clients send data to that designated MAC address, only that subset of ports will then receive the traffic. For more information about Multicast MAC filtering, refer to Chapter 1, "IP Multicast concepts."

This chapter describes the following topics:

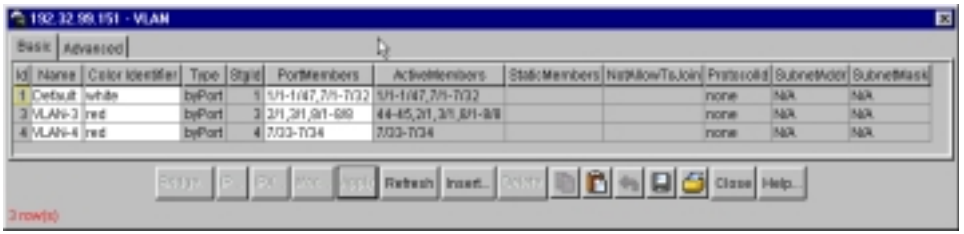
Configuring Layer 2 multicast MAC filtering

To configure the MAC address for Layer 2 multicast flooding:

1 From the Device Manager menu bar, choose VLAN > VLANs.

The VLAN dialog box opens with the Basic tab displayed (Figure 106). The Basic tab displays all defined VLANs, their configurations, and their current status.

Figure 106 VLAN dialog box—Basic tab

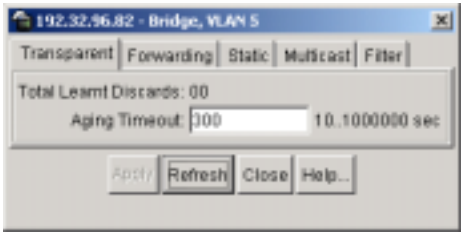


2 From the table, select a VLAN.

3 Click the Bridge button.

The Bridge dialog box opens with the Transparent tab displayed (Figure 107).

Figure 107 Bridge, VLAN dialog box—Transparent tab



4 Click the Multicast tab.

The Multicast tab opens (Figure 108).

Figure 108 Bridge, VLAN dialog box—Multicast tab

5 In the Multicast tab, click Insert.

The Bridge, VLAN, Insert Multicast MAC dialog box opens (Figure 109).

Figure 109 Bridge, VLAN, Insert Multicast MAC dialog box

6 In the Address field, type the MAC address for the multicast flooding domain.

7 Click the ellipsis (...) next to the ForwardingPorts text box and choose from the list of ports that appear.

8 Click Ok.

9 Click the ellipsis (...) next to the MltIds text box and choose from the list of MLT IDs that appear.

10 Click Ok.

11 When you finish entering the required information in the dialog box, click Insert.

Table 62 describes the Bridge, VLAN, Insert Multicast fields.

Table 62 Bridge, VLAN, Insert Multicast fields

Item	Description
Address	The MAC address for the multicast flooding domain.[1]
ForwardingPorts	The ports to be included in the multicast flooding domain.
MltIds	The MLTs that should be included in the multicast flooding domain.

1 This field does not accept MAC addresses beginning with 01:00:5e (01:00:5e:00:00:00 to 01:00:5e:ff:ff:ff inclusive). If you attempt to use this type of address, the following error message is displayed: `Error: Invalid MAV address`

Configuring Layer 3 multicast MAC filtering

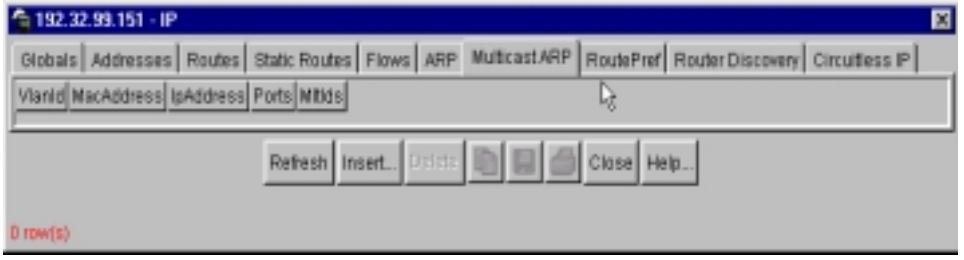
In Layer 3, the 8000 Series switch must be able to route an IP frame to a unicast IP address and flood it with a destination multicast MAC address. You must then manually define a static ARP entry that associates an IP address with a multicast MAC and flooding ports and MLT.

To configure the MAC address for Layer 3 multicast flooding:

1 From the Device Manager menu bar, choose IP Routing > IP > Multicast ARP.

The Multicast ARP tab opens (Figure 110).

Figure 110 Multicast ARP tab



2 To add a MAC address, click the Insert button.

The Insert Multicast dialog box opens (Figure 111).

Figure 111 Insert Multicast dialog box

a Click the arrow next to the VlanId text box to choose the VLAN.

b Enter the MAC address in the MacAddress text box.

c Enter the IP address in the IpAddress text box.

d Click the ellipsis (...) next to the Ports text box and choose from the list of ports that appear.

e Click Ok.

f Choose from the list of Mltids.

g When you finish entering the required information in the dialog box, click Insert.

You will then return to the Multicast ARP tab (Figure 110).

Table 63 describes the Multicast ARP fields.

Table 63 Multicast ARP fields

Item	Description
VlanID	The ID number of the VLAN for the multicast ARP.
MacAddress	The MAC address assigned to the IP address in the multicast ARP.[1]
IPAddress	The IP address of the multicast ARP.

Table 63 Multicast ARP fields

Item	Description
Ports	The ports that will receive the multicast flooding.
MltIDs	The ID of the MLT that receives the multicast flooding.

1 This field does not accept MAC addresses beginning with 01:00:5e (01:00:5e:00:00:00 to 01:00:5e:ff:ff:ff inclusive). If you attempt to use this type of address, the following error message is displayed: `Error: Invalid MAV address`

Chapter 9
Configuring IGMP using the CLI

The Internet Group Management Protocol (IGMP) is used by hosts to report their IP multicast group memberships to neighboring multicast routers. Configure IGMP on a per interface basis. For more information about IGMP concepts and terminology, see Chapter 1, "IP Multicast concepts."

This chapter describes the interface layer 3 IGMP commands for the switch. The **`config ip igmp info`** command displays information about the current global layer 3 IGMP configuration.

This chapter includes the following topics:

Roadmap of IGMP commands

The following roadmap lists all the IGMP commands and their parameters. After using the commands below to configure the Passport 8600, you can use the show commands to display information for a particular feature.

To facilitate troubleshooting, the Passport 8600 also provides *one* command (`show ip igmp show-all`) that lists all the show commands for IP IGMP and displays their configuration output. See "Displaying all IP IGMP show commands" on page 329.

Note: DVMRP or PIM multicasting must be enabled globally on the switch for these commands to take effect.

Use this list as a quick reference or click on any entry for more information:

Command	Parameter
`config ip igmp interface <ipaddr>`	`info`
	`flush <mrouter|sender| grp-member> [<SenderAddress>] [<GroupAddress>]`
	`last-memb-query-int <1/10 seconds>`
	`query-interval <seconds>`
	`query-max-resp <1/10 seconds>`
	`robustval <integer>`
	`router-alert <enable|disable>`
	`proxy-snoop <enable|disable>`
	`snoop <enable|disable>`
	`fast-leave <enable|disable>`
	`ssm-snoop <enable|disable>`
	`version <integer>`
`show ip igmp interface`	
`show ip igmp cache`	
`show ip igmp group`	

Command	Parameter
show ip igmp router-alert	
show ip igmp sender	
show ip igmp snoop	
config ip igmp fast-leave-mode	multiple-user
	one-user
show ip igmp info	
config ip igmp interface <ipaddr> access-control <name>	info
	delete <HostAddress> <HostMask>
	create <HostAddress> <HostMask> {deny-tx|deny-rx|deny-both|allow-only-tx|allow-only-rx|allow-only-both}
	mode <HostAddress> <HostMask> {deny-tx|deny-rx|deny-both|allow-only-tx|allow-only-rx|allow-only-both}
show ip igmp access	
config ip igmp interface <ipaddr> mrdisc	info
	mrdisc-enable <enable|disable>
	max-advertisement-interval [seconds]
	max-initial-advertisements [integer]
	max-initial advertisement-interval [seconds]
	min-advertisement-interval [seconds]
	neighbor-dead-interval [seconds]

Command	Parameter
show ip igmp mrdisc	
show ip igmp mrdisc-neighbors	
config ip igmp interface <ipaddr> static-members <GroupAddress>	info
	add <ports> <static|blocked>
	create <ports> <static|blocked>
	delete
	remove <ports> <static|blocked>
show ip igmp static	
config ip igmp ssm	info
	dynamic-learning <enable|disable>
	ssm-grp-range group <GroupAddress> mask <mask>
show ip igmp ssm-global	
config ip igmp ssm ssm-channel	info
	create group <GroupAddress> source <SourceAddress>
	delete group <GroupAddress>
	disable <all|group> [<GroupAddress>]
	enable <all|group> [<GroupAddress>]
show ip igmp ssm-channel	
config ethernet <ports> ip igmp	info
	flush <mrouter|sender| grp-member> [<SenderAddress>] [<GroupAddress>]
	last-memb-query-int <1/10 seconds>
	query-interval <seconds>
	fast-leave <enable|disable>
	query-max-resp <1/10 seconds>
	robustval <integer>
	router-alert <enable|disable>
	version <integer>

Command	Parameter
show ports info igmp [<ports>]	
config ethernet <ports> ip igmp access-control <name>	info
	create <HostAddress> <HostMask> {deny-tx|deny-rx|deny-both|allow-only-tx|allow-only-rx|allow-only-both}
	delete <HostAddress> <HostMask>
	mode <HostAddress> <HostMask> {deny-tx|deny-rx|deny-both|allow-only-tx|allow-only-rx|allow-only-both}
config vlan <vid> ip igmp	info
	del-mrouter <ports>
	flush <mrouter|sender| grp-member> [<SenderAddress>] [<GroupAddress>]
	last-memb-query-int <1/10 seconds>
	mrouter <ports>
	query-interval <seconds>
	query-max-resp <1/10 seconds>
	robustval <integer>
	router-alert <enable|disable>
	proxy-snoop <enable|disable>
	snoop <enable|disable>
	fast-leave <enable|disable>
	ssm-snoop <enable|disable>
	version <integer>
show vlan info igmp [<vid>]	
config vlan <vid> ip igmp access-control <name>	info

Command	Parameter
	create <HostAddress> <HostMask> {deny-tx|deny-rx|deny-both|allow-only-tx|allow-only-rx|allow-only-both}
	delete <HostAddress> <HostMask>
	mode <HostAddress> <HostMask> {deny-tx|deny-rx|deny-both|allow-only-tx|allow-only-rx|allow-only-both}
config vlan <vid> ip igmp mrdisc	info
	mrdisc-enable <enable|disable>
	max-advertisement- interval <seconds>
	max-initial- advertisements <integer>
	max-initial- advertisement-interval <seconds>
	min-advertisement- interval <seconds>
	neighbor-dead-interval <seconds>
config vlan <vid> ip igmp static-members <GroupAddress>	info
	add <ports> <static|blocked>
	create <ports> <static|blocked>
	delete
	remove <ports> <static|blocked>
config vlan <vid> ip igmp fast-leave-members	info
	enable <ports>
	disable <ports>

Command	Parameter
config ip igmp interface <ipaddr> stream-limit	info enable disable max-streams <integer>
config ip igmp interface <ipaddr> stream-limit-members	info enable <ports> max-streams <value> disable <ports> set <ports> max-streams <value>
show ip igmp stream-limit-interface show ip igmp stream-limit-port	
config ethernet <ports> ip igmp stream-limit	info enable disable max-streams <integer>
config vlan <vid> ip igmp stream-limit	info enable disable max-streams <integer>
config vlan <vid> ip igmp stream-limit-members	info enable <ports> max-streams <value> disable <ports>

Command	Parameter
	`set <ports> max-streams <value>`
`show ip igmp show-all [file <value>]`	

Configuration prerequisites and notes

Before you can configure IGMP, you must prepare the router as follows:

1. Configure an IP interface. For information, refer to *Configuring IP Routing Operations*.
2. Configure IGMP on a L2 interface by enabling IGMP snooping
   or
   Configure IGMP on a L3 interface by enabling multicast routing, i.e., DVMRP, PIM-SM or PIM-SSM.
   - To enable IGMP snooping on an interface, refer to "Configuring IGMP on an interface." To enable IGMP snooping on a VLAN, refer to "Configuring IGMP on a VLAN."
   - To enable DVMRP or PIM-SM on an IP interface, first enable them globally. (PIM-SSM is a global configuration; you cannot enable it per interface.)
     — To enable DVMRP globally, see "Configuring DVMRP globally."
     — To enable PIM-SM globally, see "Configuring PIM-SM globally."
     — To enable PIM-SSM globally, see "Configuring PIM-SSM globally."

Note: To drop IGMPv2 control packets that do not have the router alert option set, use the `config ip igmp interface` command and disable the `router-alert <enable|disable>` parameter.

Configuring IGMP on an interface

To configure IGMP on a specific interface, use the following command:

config ip igmp interface <*ipaddr*>

where:
ipaddr indicates the IP address of the selected interface.

This command includes the following parameters:

config ip igmp interface <*ipaddr*> followed by:	
info	Displays the access list of the IGMP interface.
flush <*mrouter*|*sender*|grp-member> [<*SenderAddress*>] [<*GroupAddress*>]	Flushes the specified table.
last-memb-query-int <*1/10 seconds*>	The maximum response time (in 1/10 seconds) that is inserted into group-specific queries sent in response to leave group messages. It is also the time between group-specific query messages. This value is not configurable for IGMPv1. Decreasing the value reduces the time to detect the loss of the last member of a group. • *seconds* is the range from 0 to 255, and the default is 10 tenth seconds. Nortel Networks recommends configuring this value between 3 and 10 (equal to 0.3 – 1.0 seconds).
query-interval <*seconds*>	Sets the frequency (in seconds) at which host query packets are transmitted on the interface. • *seconds* is the range from 1 to 65535 with a default of 125.

config ip igmp interface <*ipaddr*> followed by:	
query-max-resp <*1/10 seconds*>	The maximum response time (in 1/10 seconds) advertised in IGMPv2 general queries on this interface. This value is not configurable for IGMPv1. Smaller values allow a router to prune groups faster. • *integer* is an integer value with a range of 0 to 255, and the default is 100 tenth seconds (equal to 10 seconds). **Note:** This value must be less than the query-interval.
robustval <*integer*>	Allows tuning for the expected packet loss of a network. *integer* an integer value with a range of 2 to 255 seconds.The default value is 2 seconds. Increase the value if you expect the network to experience some packet loss.
router-alert <*enable*|*disable*>	Enables or disables the router alert option. When enabled, this parameter instructs the router to process packets not directly addressed to it. **Note:** To maximize your network performance, Nortel Networks recommends that you set this parameter according to the version of IGMP currently in use. • IGMPv1 - Disable • IGMPv2 - Enable • IGMPv3 - Enable
proxy-snoop <*enable*|*disable*>	Enables or disables the layer-3 proxy-snoop option.
snoop <*enable*|*disable*>	Enables or disables the layer-3 snoop option.
fast-leave <*enable*|*disable*>	Enables or disables the fast-leave option on the interface.
ssm-snoop <*enable*|*disable*>	Enables or disables support for PIM source-specific multicast (SSM) on the snooping interface.
version <*integer*>	Sets the version of IGMP that you want to configure on this interface. For IGMP to function correctly, all routers on a LAN must use the same version. • *integer* is an integer value with a value of 1, 2 or 3. The default value is 2 (IGMPv2).

Configuration example

This configuration example uses the commands described above to perform the following tasks:

- Set the last member query interval to 15 tenth seconds (equal to 1.5 seconds).
- Set the query interval to 100 seconds.
- Set the query maximum response time to 15 tenth seconds (equal to 1.5 seconds).
- Set the robustness value to 4 seconds.
- Enable IGMP version 3.
- Enable the fast leave option.
- Enable support for SSM on the snooping interface.

After configuring the parameters, use the **`info`** command to show a summary of the results.

```
PP:5/config/ip/igmp/interface/10.10.99.151# last-memb-query-int 15
PP:5/config/ip/igmp/interface/10.10.99.151# query-interval 100
PP:5/config/ip/igmp/interface/10.10.99.151# query-max-resp 50
PP:5/config/ip/igmp/interface/10.10.99.151# robustval 4
PP:5/config/ip/igmp/interface/10.10.99.151# ssm-snoop enable
PP:5/config/ip/igmp/interface/10.10.99.151# version 3
PP:5/config/ip/igmp/interface/10.10.99.151# fast-leave enable
PP:5/config/ip/igmp/interface/10.10.99.151# info

Sub-Context: access-list mrdisc static-members
Current Context:

         last-memb-query-int : 15
              query-interval : 100 sec(s)
              query-max-resp : 50
                   robustval : 4
                     version : 3
                  fast-leave : enable
                     mrouter :
                  ssm-snoop  : enable

8610co:5/config/ethernet/1/5/ip/igmp#
```

Showing IGMP interfaces

To display the information about the interfaces on which IGMP is enabled, use the following command:

```
show ip igmp interface
```

Figure 112 shows sample output for this command.

Figure 112 show ip igmp interface command output

```
8610/show/ip/igmp# interface

================================================================================
                                Igmp Interface
================================================================================
       QUERY                OPER             QUERY  WRONG             LASTMEM
IF     INTVL  STATUS VERS.  VERS   QUERIER    MAXRSPTQUERYJOINSROBUST QUERY
--------------------------------------------------------------------------------
P7/1   125    inact  2      2      0.0.0.0    10     0      0    2     1
V2     125    inact  2      2      0.0.0.0    10     0      0    2     1
V3     125    inact  2      2      0.0.0.0    10     0      0    2     1
V4     125    inact  2      2      0.0.0.0    10     0      0    2     1
V5     125    inact  2      2      0.0.0.0    10     0      0    2     1
V6     125    inact  2      2      0.0.0.0    10     0      0    2     1
V10    125    inact  2      2      0.0.0.0    10     0      0    2     1
V15    125    inact  2      2      0.0.0.0    10     0      0    2     1
V18    125    inact  2      2      0.0.0.0    10     0      0    2     1
V23    125   inact   2      2      0.0.0.0    10     0      0    2     1
V27    125   inact   2      2      0.0.0.0    10     0      0    2     1
V51    125   inact   2      2      0.0.0.0    10     0      0    2     1
V52    125   active  2      2      192.28.1.2010     0      1    2     1
```

Showing IGMP cache information

To display information about the IGMP cache, use the following command:

```
show ip igmp cache
```

Figure 113 shows sample output for this command.

Figure 113 show ip igmp cache command output

```
8610/show/ip/igmp# cache

================================================================================
                                  Igmp Cache
================================================================================
GRPADDR         INTERFACE  LASTREPORTER    EXPIRATION V1HOSTTIMER
--------------------------------------------------------------------------------
225.1.2.5       Vlan52     192.28.1.8      131        0
```

Showing IGMP group information

To display information about the IGMP group, use the following command:

```
show ip igmp group
```

Figure 114 shows sample output for this command.

Figure 114 show ip igmp group command output

```
8610/show/ip/igmp# group

================================================================================
                               Igmp Group
================================================================================
GRPADDR         INPORT     MEMBER          EXPIRATIONTYPE
--------------------------------------------------------------------------------
225.1.2.5       cpp        192.28.1.8      169
```

Showing IGMP router-alert status

To display the status of IGMP router alert, use the following command:

```
show ip igmp router-alert
```

Figure 115 shows sample output for this command.

Figure 115 Show ip igmp router-alert command

```
8610/show/ip/igmp# router-alert

================================================================================
                                Igmp RouterAlert
================================================================================
IFINDEX   ROUTER ALERT
          ENABLE
--------------------------------------------------------------------------------
V1        disable
```

Showing IGMP sender information

To display information about the IGMP senders, use the following command:

```
show ip igmp sender
```

Figure 116 shows sample output for this command.

Figure 116 show ip igmp sender command output

```
================================================================================
                                    Igmp Sender
================================================================================
GRPADDR         IFINDEX    MEMBER          PORT
--------------------------------------------------------------------------------
230.22.0.2      Vlan 20    126.1.1.3       1/1
230.22.0.2      Vlan 20    126.1.1.5       1/1
230.22.0.2      Vlan 20    126.1.1.6       1/1
230.22.0.2      Vlan 20    126.1.1.7       1/1
230.22.0.2      Vlan 20    126.1.1.8       1/1
230.22.0.254    Vlan 20    126.1.1.2       1/1
230.22.0.254    Vlan 20    126.1.1.5       1/1
230.22.0.254    Vlan 20    126.1.1.6       1/1
230.22.0.254    Vlan 20    126.1.1.7       1/1
230.22.0.254    Vlan 20    126.1.1.8       1/1
```

Showing IGMP snoop status

To display the status of IGMP snoop, use the following command:

```
show ip igmp snoop
```

Figure 117 shows sample output for this command.

Figure 117 show ip igmp snoop command

```
8610/show/ip/igmp# snoop
================================================================================
                                    Igmp Snooping
================================================================================
IFINDEX SNOOP   PROXY   SSM     STATIC          ACTIVE          MROUTER
        ENABLE  SNOOP   SNOOP   MROUTER         MROUTER         EXPIRATION
                ENABLE  ENABLE  PORTS           PORTS           TIME
--------------------------------------------------------------------------------
V3      false   false   false                                   0
V4      false   false   false                                   0
V8      false   false   false                                   0
```

Configuring fast leave mode

Fast leave mode provides one command that controls all IGMP fast-leave enabled interfaces. Using this global parameter, you can alter the leave processing on fast-leave enabled IGMPv2, IGMPv3, and IGMP snoop interfaces.

Note: Fast leave mode applies only to fast-leave enabled IGMP interfaces. It does not apply to IGAP interfaces, which ignore this mode.

To configure the fast leave mode, use the following command:

```
config ip igmp fast-leave-mode
```

This command includes the following parameters:

config ip igmp fast-leave-mode followed by:	
`multiple-user`	Removes from the group *only* the IGMP member who sent the Leave message. Traffic is not stopped if there are other receivers on the interface port. This is the default.
`one-user`	Removes all group members on a fast-leave enabled interface port upon receiving the first Leave message from a member. This behavior is the same as the conventional fast leave process.

Configuration example

When a single user is connected to an interface, there is no need to track if there are other users on the interface to perform the fast leave. In cases like this, you should change the mode to one-user.

- Use the **`config ip igmp fast-leave-mode one-user`** command to change the mode from the default (multiple user) to one user.
- Use the **`config ip igmp info`** command to show the result, which is the current mode setting.

```
Hollywood:5/config/ip/igmp# fast-leave-mode one-user
Hollywood:5/config/ip/igmp# info

Sub-Context: igap interface ssm
Current Context:

                  fast-leave-mode : one-user

Hollywood:5/config/ip/igmp#
```

Showing the current fast leave mode

To display the current fast leave mode, use the following command:

```
show ip igmp info
```

Figure 118 show ip igmp info command output

```
8610:5/config/ip/igmp# show ip igmp info

================================================================
                    Igmp System Parameters
================================================================
                  fast-leave-mode : one-user

8610:5/config/ip/igmp#
```

Configuring multicast access control for an IGMP interface

To configure multicast access control for a selected IGMP interface, use the following command:

`config ip igmp interface <ipaddr> access-control <name>`

where:
ipaddr is the IP address of the selected interface and
name is the name of the access policy. It can be 1 to 64 characters.

This command includes the following parameters:

config ip igmp interface <*ipaddr*> access-control <name> followed by:	
`info`	Displays the settings for the access-control parameter.
`create <HostAddress> <HostMask> {deny-tx|deny-rx|deny-both|allow-only-tx|allow-only-rx|allow-only-both}`	Creates an access control group entry for a specific IGMP interface. • *HostAddress* is the IP address of the host. See "Specifying host addresses and masks" for more information. • *HostMask* is the subnet mask used to determine the host or hosts covered by this configuration. You can use the host subnet mask to restrict access to a portion of the host's network. See "Specifying host addresses and masks" for more information. • `deny-tx|deny-rx|deny-both|allow-only-tx|allow-only-rx|allow-only-both` indicates the action you want for the specified IGMP interface. For example, if you specify deny-both, the interface will deny both transmitted and received traffic.

config ip igmp interface <*ipaddr*> access-control <name> followed by:	
delete <*HostAddress*> <*HostMask*>	Deletes the access control group entry for the specified IGMP interface. • *HostAddress* is the IP address of the host. • *HostMask* is the subnet mask used to determine the host or hosts covered by this configuration.
mode <*HostAddress*> <*HostMask*> {deny-tx|deny-rx|deny-both|allow-only-tx|allow-only-rx|allow-only-both}	Changes the access control group configuration. • *HostAddress* is the IP address of the host. • *HostMask* is the subnet mask used to determine the host or hosts covered by this configuration. • deny-tx|deny-rx|deny-both|allow-only-tx|allow-only-rx|allow-only-both indicates the action you want for the specified IGMP interface. For example, if you specify deny-both, the interface will deny both transmitted and received traffic.

Configuration example

User 1 has subscribed to the extended-basic channels, which includes basic channels plus the Asianet channels. The basic channels and the Asianet channels have a group range of 224.1.1.0 to 224.1.2.255 and 255.1.1.0, sent by sources belonging to the 192.32.16.0 and 192.32.32.0 networks, respectively.

The following example shows how to configure prefix lists (groups of addresses) for basic and Asianet channels, and to create access policies for this user. The access policies ensure that the user receives traffic only for those groups from sources belonging to the 192.32.16.0 and 192.32.32.0 networks. After configuring the parameters, use the **`info`** command to show a summary of the results.

```
8010:5# config ip prefix basic-channels
8010:5/config/ip/prefix/basic-channels# add-prefix 224.1.1.0/24
8010:5/config/ip/prefix/basic-channels# add-prefix 224.1.2.0/24
8010:5/config/ip/prefix/basic-channels# config ip prefix asia-net
8010:5/config/ip/prefix/asia-net# add-prefix 255.1.1.0/24
8010:5/config/ip/prefix/asia-net# config ip igmp interface 192.1.10.132
access-control basic-channels
8010:5/config/ip/igmp/interface/192.1.10.132/access-control/basic-channels#
create 192.32.16.0 255.255.255.0 allow-only-tx
8010:5/config/ip/igmp/interface/192.1.10.132/access-control/basic-channels#
config ip igmp interface 192.1.10.132 access-control asia-net
8010:5/config/ip/igmp/interface/192.1.10.132/access-control/asia-net#
create 192.32.32.0 255.255.255.0 allow-only-tx
8010:5/config/ip/igmp/interface/192.1.10.132/access-control/asia-net# info

Sub-Context:
Current Context:

                     create :

                          HostAddress - 192.32.16.0
                             HostMask - 255.255.255.0
                                 mode - allow-only-tx
                      mode :
                     delete : N/A

8010:5/config/ip/igmp/interface/192.1.10.132/access-control/asia-net#
```

Showing IGMP access control groups

To display information about the IGMP multicast access control groups, use the following command:

```
show ip igmp access
```

Figure 119 shows sample output for this command.

Figure 119 show ip igmp access command output

```
8610/show/ip/igmp# access

================================================================================
                                        Igmp Access
================================================================================
INTERFACE  GRP PREFIX       HOSTADDR         HOSTMASK         ACCESSMODE
--------------------------------------------------------------------------------
Vlan1001   TEST             142.1.1.10       255.255.255.255  deny-rx
```

Table 64 shows the field descriptions for the **`show ip igmp access`** command.

Table 64 show ip igmp access field descriptions

Field	Description
INTERFACE	Identifies the interface on which multicast access control is configured.
GRP PREFIX	An alphanumeric string that identifies the name of the access policy.
HOSTADDR	The IP address of the host. See "Specifying host addresses and masks" for more information.

Table 64 show ip igmp access field descriptions

Field	Description
HOSTMASK	The subnet mask used to determine the host or hosts covered by this configuration. You can use the host subnet mask to restrict access to a portion of the host's network. See "Specifying host addresses and masks" for more information.
ACCESSMODE	Specifies the action of the access policy. The options are: • deny-tx – deny IP multicast transmitted traffic. • deny-rx – deny IP multicast received traffic. • deny-both – deny both IP multicast transmitted and received traffic. • allow-only-rx – allow IP multicast transmitted traffic. • allow-only-rx – allow IP multicast received traffic. • allow-only-both – allow both IP multicast transmitted and received traffic.

Configuring IGMP multicast router discovery options

To configure the multicast route discovery options, use the following command:

`config ip igmp interface <ipaddr> mrdisc`

where:
ipaddr indicates the IP address of the selected interface.

Note: The Multicast Router Discovery protocol is not supported on brouter ports.

This command includes the following parameters:

config ip igmp interface <*ipaddr*> mrdisc followed by:	
`info`	Displays information about the multicast route discovery on the interface.
`mrdisc-enable <enable|disable>`	Enables or disables the multicast route discovery option.

config ip igmp interface <*ipaddr*> mrdisc followed by:	
`max-advertisement-interval [seconds]`	Sets the maximum number (in seconds) of multicast advertisements that can be configured on the switch. **Note**: To take effect, save the configuration and reset the switch.
`max-initial-advertisements [integer]`	Used to set the maximum number of initial multicast advertisements that can be configured on the switch. **Note**: To take effect, save the configuration and reset the switch.
`max-initial advertisement-interval [seconds]`	Used to set the maximum number (in seconds) of multicast advertisement intervals that can be configured on the switch. **Note**: To take effect, save the configuration and reset the switch.
`min-advertisement-interval [seconds]`	Used to set the minimum number (in seconds) of multicast advertisements that can be configured on the switch. **Note**: To take effect, save the configuration and reset the switch.
`neighbor-dead-interval [seconds]`	Sets the multicast route discovery dead interval—the number of seconds the switch's multicast route neighbors should wait before assuming that the multicast router is down. • *seconds* is a value from 1 to 59**.** The default is 30.

Showing IGMP multicast router discovery information

To display information about the IGMP multicast discovery routes, use the following command:

```
show ip igmp mrdisc
```

Figure 120 shows sample output for this command.

Figure 120 Show ip igmp mrdisc command

```
8610/show/ip/igmp# mrdisc

================================================================================
                              Igmp Mrdisc
================================================================================
VLAN ID      MRDISC    DISCOVERED RTR PORTS
--------------------------------------------------------------------------------
```

Showing IGMP multicast router discovery neighbors

To display information about the IGMP multicast router discovery neighbors, use the following command:

```
show ip igmp mrdisc-neighbors
```

Figure 121 shows sample output for this command.

Figure 121 Show ip igmp mrdisc-neighbors command

```
8610/show/ip/igmp# mrdisc-neighbors

================================================================================
                                    Igmp Mrdisc Neighbors
================================================================================
VLAN ID     SRC_PORT   IP Addr         Advert-int   QUERY-int    Robust-val
--------------------------------------------------------------------------------
```

Configuring IGMP interface static members

To configure the static members of a specific IGMP interface, use the following command:

```
config ip igmp interface <ipaddr> static-members
<GroupAddress>
```

where:
ipaddr indicates the IP address of the selected interface and
GroupAddress indicates the IP address of the selected multicast group.

This command includes the following parameters:

config ip igmp interface <*ipaddr*> static-members <GroupAddress> followed by:	
`info`	Displays information about the static members of the VLAN.
`add <ports> <static|blocked>`	Adds a static-member entry to the IGMP interface. • *ports* is the port or list of ports to which you want to redirect the multicast stream for this multicast group. • *static|blocked* sets the route to static or blocked.
`create <ports> <static|blocked>`	Creates static-members on the interface. • *ports* is the port or list of ports to which you want to redirect the multicast stream for this multicast group. • *static |blocked* sets the route to static or blocked.
`delete`	Deletes the static-members on the interface.
`remove <ports> <static|blocked>`	Removes slots/ports from the static-members of a protocol-based VLAN. • *ports* the port or list of ports you want to remove from the multicast stream. • *static |blocked* sets the multicast entry to static or blocked.

Showing IGMP static and blocked ports

To display information about the static and blocked ports for the IGMP-enabled interfaces, use the following command:

```
show ip igmp static
```

Figure 122 shows sample output for this command.

Figure 122 show ip igmp static command output

```
================================================================================
                                    Igmp Static
================================================================================
GRPADDR         INTERFACE  STATICPORTS     BLOCKEDPORTS
--------------------------------------------------------------------------------
230.20.20.2     Vlan2615   1/9-1/10        1/11-1/12
```

Configuring SSM dynamic learning and range group

To enable the IGMPv3 dynamic learning feature and to extend the default SSM range of 232/8 to include any IP multicast address, use the following command:

```
config ip igmp ssm
```

This command includes the following parameters:

`config ip igmp ssm` followed by:	
`info`	Displays the SSM range and the status of the SSM channel table entries.
`dynamic-learning <enable|disable>`	Enables the dynamic learning of SSM channel (S,G) pairs from IGMPv3 reports. As new SSM channels are learned, they appear in the SSM channel table, see "Configuring the SSM channel table."
`ssm-grp-range group <GroupAddress> mask <mask>`	Defines the SSM range. The SSM range parameter allows you to extend the default SSM range of 232/8 to include any IP multicast address. This feature enables you to configure existing applications without having to change their group configurations. **Note:** Before changing this setting, see "Changing the SSM range group." • *`GroupAddress`* is any IP multicast address within the range of 224.0.1.0 and 239.255.255.255. The default is 232.0.0.0. • *mask* is the IP address mask of the multicast group. The default is 255.0.0.0.

Changing the SSM range group

Note: This procedure re-initializes PIM and temporarily stops all PIM traffic. For those multicast groups out of SSM range (i.e. under PIM-SM behavior), it also causes an RP relearn delay of up to 60 seconds. This delay can be longer if the BSR is local.

To change the SSM range group address, you have to perform the following steps:

1. Disable PIM.

   ```
   config ip pim disable
   ```

   If you forget to disable PIM, the following error message appears.

   ```
   Error: PIM is enabled in SSM mode, disable PIM
   ```

2. Delete each entry in the SSM channel table.

   ```
   config ip igmp ssm-channel delete group <GroupAddress>
   ```

   If you forget to delete the SSM channels, the following error message appears.

   ```
   Error: SSM source group table not empty
   ```

3. Enter the new IP multicast group address.

   ```
   config ip igmp ssm ssm-grp-range group <value> mask <value>
   ```

   The following message appears to warn you that every static mroute entry that falls into the new SSM range will be deleted.

   ```
   WARNING: All Static Source Group entries in the SSM range will
   be deleted

   Do you wish to change SSM range (y/n) ?
   ```

4. Enter Y.

5. Enable PIM.

   ```
   config ip pim enable
   ```

Configuration example

This configuration example uses the commands described above to perform the following tasks:

- Define the SSM range group address (234.0.0.0) and mask (255.0.0.0).
- Enable dynamic learning from IGMPv3 reports.

After configuring the parameters, use the **info** command to show a summary of the results.

```
PP8610:5# config ip pim disable
PP8610:5# config ip igmp ssm ssm-grp group 234.0.0.0 mask 255.0.0.0

WARNING: All Static Source Group entries in the SSM range will be
deleted

Do you wish to change SSM range (y/n) ? y
PP8610:5# config ip igmp ssm dynamic-learning enable
PP8610:5# config ip igmp ssm info


Sub-Context: clear config dump monitor show test trace wsm sam
Current Context:

            dynamic-learning : enable
               ssm-grp-range : 234.0.0.0/255.0.0.0

PP8610:5#
```

Showing SSM group range and dynamic learning status

To display the SSM group range and the status of dynamic learning, use the following command:

```
show ip igmp ssm-global
```

Figure 126 shows sample output for this command.

Figure 123 show ip igmp ssm-global command output

```
8610# show/ip/igmp# ssm-global

================================================================================
                                      Igmp Ssm Global
================================================================================
DYNAMIC LEARNING     SSM GROUP RANGE
--------------------------------------------------------------------------------
enable               234.0.0.0/255.0.0.0

8610:5/show/ip/igmp#
```

Configuring the SSM channel table

The SSM channel table consists of entries that map groups to their sending source. SSM channels cannot conflict with static source groups and vice versa. When you configure an SSM channel or a static source group, the switch performs a consistency check to make sure there are no conflicts. You cannot map one group (G) to different sources for both a static source group and an SSM channel. For more information, refer to "Configuring multicast static source groups" on page 467.

The consistency check mentioned above applies to all SSM channel entries, even if they are disabled. Disabling an entry means that it becomes inactive. It does not delete the entry, and you can re-enable it at any time.

When you disable an SSM channel, the Passport 8600 stops any multicast traffic from the specified source to the specified group. If desired, you can use this static setting as a security feature to block traffic from a certain source to a specific group.

To configure the SSM channel table, use the following command:

```
config ip igmp ssm ssm-channel
```

This command includes the following parameters:

config ip igmp ssm ssm-channel followed by:	
`info`	Displays the SSM range and the status of the SSM channel table entries.
`create group <GroupAddress> source <SourceAddress>`	Creates a static SSM channel table entry by specifying the group and source IP addresses. • *`GroupAddress`* is any IP multicast address within the SSM range defined by `ssm-grp-range group`. • *`SourceAddress`* is any IP host address that will be sending traffic to the group.
`delete group <GroupAddress>`	Deletes the SSM channel table entry that you specify. • *`GroupAddress`* is the IP multicast address of the table entry you want to delete.

config ip igmp ssm ssm-channel followed by:	
disable <*all*|*group*> [<*GroupAddress*>]	Disables the admin state for all static entries in the SSM channel table (*all*) or for a specific entry (*group*). This setting does not affect the dynamically learned entries. This state determines whether or not the switch uses the static entry or saves it for future use. The default is enable for each entry. • *all* refers to all the static entries in the SSM channel table. • *group* requires the *GroupAddress* of the entry you want to disable.
enable <*all*|*group*> [<*GroupAddress*>]	Enables the admin state for all static entries in the SSM channel table (*all*) or for a specific entry (*group*). This setting does not affect the dynamically learned entries. This state determines whether or not the switch uses the static entry or saves it for future use. The default is enable for each entry. • *all* refers to all the static entries in the SSM channel table. • *group* requires the *GroupAddress* of the entry you want to disable.

Configuration example

This configuration example uses the commands described above to perform the following tasks:

- Create an SSM channel table entry for the multicast group 234.0.1.0 and the source at 192.32.99.151.
- Set the admin state to enable all the static SSM channel table entries.

After configuring the parameters, use the **info** command to show a summary of the results.

```
PP8610:5# config ip igmp ssm ssm-channel create group 234.0.1.0
source 192.32.99.151
PP8610:5# config ip igmp ssm ssm-channel enable all
PP8610:5# config ip igmp ssm ssm-channel info

Sub-Context: clear config dump monitor show test trace wsm sam
Current Context:

                      create :
                               group : 234.0.1.0
                              source : 192.32.99.151
                        admin status : enabled
                       learning-mode : static

                               group : 234.10.10.0
                              source : 255.0.0.0
                        admin status : enabled
                       learning-mode : static

                      delete : N/A
                     disable : N/A
                      enable : N/A

PP8610:5#
```

Showing SSM channel information

To display the list of SSM channels, use the following command:

```
show ip igmp ssm-channel
```

Figure 126 shows sample output for this command.

Figure 124 show ip igmp ssm-channel command output

```
8610# show/ip/igmp# ssm-channel

================================================================================
                                      Igmp Ssm Channel
================================================================================
GROUP           SOURCE          MODE       ACTIVE     STATUS
--------------------------------------------------------------------------------
234.17.0.1      255.255.255.255 static     false      enabled
234.17.0.2      255.255.255.255 static     false      enabled

8610:5/show/ip/igmp#
```

Configuring IGMP Ethernet ports

To configure IGMP on specific ethernet ports, use the following command:

`config ethernet <ports> ip igmp`

where:
ports use the convention {slot/port[-slot/port][, ...]}.

This command includes the following parameters

config ethernet <*ports*> ip igmp followed by:	
`info`	Displays IGMP settings on the port.
`flush <mrouter|sender|grp-member> [<SenderAddress>] [<GroupAddress>]`	Flushes the specified table.
`last-memb-query-int <1/10 seconds>`	The maximum response time (in 1/10 seconds) that is inserted into group-specific queries sent in response to leave group messages. It is also the time between group-specific query messages. This value is not configurable for IGMPv1. Decreasing the value reduces the time to detect the loss of the last member of a group. • *seconds* is the range from 0 to 255, and the default is 10 tenth seconds. Nortel Networks recommends configuring this value between 3 and 10 (equal to 0.3 – 1.0 seconds).
`query-interval <seconds>`	Sets the frequency (in seconds) at which host query packets are transmitted on the port. • *seconds* is the range of 1 to 65535 seconds. The default value is 125 seconds.
`fast-leave <enable|disable>`	Enables or disables the fast-leave mode, which allows a switch to immediately stop forwarding a multicast group's traffic as soon as an IGMPv2 leave group message is received on an interface.

config ethernet <*ports*> ip igmp followed by:	
query-max-resp <*1/10 seconds*>	The maximum response time (in 1/10 seconds) advertised in IGMPv2 general queries on this interface. This value is not configurable for IGMPv1. Smaller values allow a router to prune groups faster. • *integer* is an integer value with a range of 0 to 255, and the default is 100 tenth seconds (equal to 10 seconds). **Note:** This value must be less than the query-interval.
robustval <*integer*>	Allows tuning for the expected packet loss of a network. • *integer* is the range of 2 to 255 with a default of 2. Increase the value if you expect the network to experience packet loss.
router-alert <*enable*|*disable*>	Enables or disables the router alert option. When enabled, this parameter instructs the router to process packets not directly addressed to it. **Note:** To maximize your network performance, Nortel Networks recommends that you set this parameter according to the version of IGMP currently in use. • IGMPv1 - Disable • IGMPv2 - Enable • IGMPv3 - Enable
version <*integer*>	Sets the version of IGMP that you want to configure on this port. For IGMP to function correctly, all routers on a LAN must use the same version. • *integer* is an integer value with a value of 1, 2 or 3. The default value is 2 (IGMPv2).

Figure 125 shows sample output for the **config ethernet <*ports*> ip igmp info** command.

Figure 125 config ethernet ip igmp info command output

```
8610# config ethernet 9/2 ip igmp info

Sub-Context: access-list
Current Context:

         last-memb-query-int : 1
              query-interval : 125
              query-max-resp : 10
                   robustval : 2
                     version : 2
                  fast-leave : disable
```

Showing IGMP port information

To display information about the specified port or for all ports, use the following command:

`show ports info igmp [<ports>]`

where:
ports use the convention {slot/port[-slot/port][, ...]}.

Figure 126 shows sample output for this command.

Figure 126 show ports info igmp command (partial output)

```
8610# show ports info igmp

================================================================================
                                      Port Ip Igmp
================================================================================
PORT QUERY QUERY ROBUST VERSION LAST  PROXY  SNOOP  SSM    FAST
NUM  INTVL MAX                  MEMB  SNOOP  ENABLE SNOOP  LEAVE
           RESP                 QUERY ENABLE        ENABLE ENABLE
--------------------------------------------------------------------------------
1/1  125   100   2      2       10    false  false  false  false
1/2  125   100   2      2       10    false  false  false  false
1/3  125   100   2      2       10    false  false  false  false
1/4  125   100   2      2       10    false  false  false  false
1/5  125   100   2      2       10    false  false  false  false
1/6  125   100   2      2       10    false  false  false  false
```

Configuring multicast access control for an IGMP Ethernet port

To configure multicast access control for a selected IGMP Ethernet port, use the following command:

`config ethernet <ports> ip igmp access-control <name>`

where:
ports uses the convention {slot/port[-slot/port][,...]}.
name is the name of the access policy. It can be 1 to 64 characters.

This command includes the following parameters:

config ethernet <ports> ip igmp access-control <name> followed by:	
`info`	Displays the settings for the access-control parameter.
`create <HostAddress> <HostMask> {deny-tx|deny-rx|deny-both|allow-only-tx|allow-only-rx|allow-only-both}`	Creates an access control group entry for a specific IGMP Ethernet port. • *HostAddress* is the IP address of the host. See "Specifying host addresses and masks" for more information. • *HostMask* is the subnet mask used to determine the host or hosts covered by this configuration. You can use the host subnet mask to restrict access to a portion of the host's network. See "Specifying host addresses and masks" for more information. • `deny-tx|deny-rx|deny-both|allow-only-tx|allow-only-rx|allow-only-both` indicates the action you want for the specified IGMP Ethernet port. For example, if you specify deny-both, the interface will deny both transmitted and received traffic.

config ethernet <ports> ip igmp access-control <name> followed by:	
`delete <HostAddress> <HostMask>`	Deletes the access control group entry for the specified IGMP interface. • *HostAddress* is the IP address of the host. • *HostMask* is the subnet mask used to determine the host or hosts covered by this configuration.
`mode <HostAddress> <HostMask> {deny-tx|deny-rx|deny-both|allow-only-tx|allow-only-rx|allow-only-both}`	Changes the access control group configuration. • *HostAddress* is the IP address of the host. • *HostMask* is the subnet mask used to determine the host or hosts covered by this configuration. • `deny-tx|deny-rx|deny-both|allow-only-tx|allow-only-rx|allow-only-both` indicates the action you want for the specified IGMP interface. For example, if you specify deny-both, the interface will deny both transmitted and received traffic.

Configuration example

User 1 has subscribed to the extended-basic channels, which includes basic channels plus the Asianet channels. The basic channels and the Asianet channels have a group range of 224.1.1.0 to 224.1.2.255 and 255.1.1.0, sent by sources belonging to the 192.32.16.0 and 192.32.32.0 networks, respectively.

The following example shows how to configure prefix lists (groups of addresses) for basic and Asianet channels, and to create access policies for this user. The access policies ensure that the user receives traffic only for those groups from sources belonging to the 192.32.16.0 and 192.32.32.0 networks. After configuring the parameters, use the **`info`** command to show a summary of the results.

```
8010:5# config ip prefix basic-channels
8010:5/config/ip/prefix/basic-channels# add-prefix 224.1.1.0/24
8010:5/config/ip/prefix/basic-channels# add-prefix 224.1.2.0/24
8010:5/config/ip/prefix/basic-channels# config ip prefix asia-net
8010:5/config/ip/prefix/asia-net# add-prefix 255.1.1.0/24
8010:5/config/ip/prefix/asia-net# config ethernet 4/1 ip igmp
access-control basic-channels
8010:5/config/ethernet/4/1/ip/igmp/access-control/basic-channels# create
192.32.16.0 255.255.255.0 allow-only-tx
8010:5/config/ethernet/4/1/ip/igmp/access-control/basic-channels# config
ethernet 4/1 ip igmp access-control asia-net
8010:5/config/ethernet/4/1/ip/igmp/access-control/asia-net# create
192.32.32.0 255.255.255.0 allow-only-tx
8010:5/config/ethernet/4/1/ip/igmp/access-control/asia-net# info

Sub-Context:
Current Context:

                     create :

                          HostAddress - 192.32.16.0
                             HostMask - 255.255.255.0
                                 mode - allow-only-tx
                      mode :
                     delete : N/A

8010:5/config/ethernet/4/1/ip/igmp/access-control/asia-net#
```

Configuring IGMP on a VLAN

To configure IGMP on a VLAN, use the following command:

```
config vlan <vid> ip igmp
```

where:
vid is a VLAN ID from 1 to 4094.

This command includes the following parameters:

config vlan <*vid*> ip igmp followed by:	
`info`	Displays IGMP settings on the VLAN.
`del-mrouter <ports>`	Deletes multicast router ports.
`flush <mrouter|sender|grp-member> [<SenderAddress>] [<GroupAddress>]`	Flushes the specified table.
`last-memb-query-int <1/10 seconds>`	The maximum response time (in 1/10 seconds) that is inserted into group-specific queries sent in response to leave group messages. It is also the time between group-specific query messages. This value is not configurable for IGMPv1. Decreasing the value reduces the time to detect the loss of the last member of a group. • *seconds* is the range from 0 to 255, and the default is 10 tenth seconds. Nortel Networks recommends configuring this value between 3 and 10 (equal to 0.3 – 1.0 seconds).
`mrouter <ports>`	Adds multicast router ports.
`query-interval <seconds>`	Sets the frequency (in seconds) at which host query packets are transmitted on the VLAN. • *seconds* is the range from 1 to 65535. The default value is 125 seconds.

config vlan <*vid*> ip igmp followed by:	
query-max-resp <*1/10 seconds*>	The maximum response time (in 1/10 seconds) advertised in IGMPv2 general queries on this interface. This value is not configurable for IGMPv1. Smaller values allow a router to prune groups faster. • *seconds* is an integer value with a range of 0 to 255, and the default is 100 tenth seconds (equal to 10 seconds). **Note:** This value must be less than the query-interval.
robustval <*integer*>	Allows tuning for the expected packet loss of a network. • *integer* is an integer value with a range of 2 to 255 seconds. The default value is 2 seconds. Increase the value if you expect the network to experience loss.
router-alert <*enable*|*disable*>	Enables or disables the router alert option. When enabled, this parameter instructs the router to process packets not directly addressed to it. **Note:** To maximize your network performance, Nortel Networks recommends that you set this parameter according to the version of IGMP currently in use. • IGMPv1 - Disable • IGMPv2 - Enable • IGMPv3 - Enable
proxy-snoop <*enable*|*disable*>	Enables or disables the proxy-snoop option globally for the VLAN.
snoop <*enable*|*disable*>	Enables or disables the snoop option for the VLAN.
fast-leave <*enable*|*disable*>	Removes a given port from receiving a leave message from any member of any given group, and the normal IGMP behavior is skipped.
ssm-snoop <*enable*|*disable*>	Enables or disables support for PIM source-specific multicast (SSM) on the snooping interface.
version <*integer*>	Sets the version of IGMP that you want to configure on this interface. For IGMP to function correctly, all routers on a LAN must use the same version. • *integer* is an integer value with a value of 1, 2 or 3. The default value is 2 (IGMPv2).

Configuration example

This configuration example uses the commands described above to perform the following tasks:

- Set the last member query interval to 15 tenth seconds (equal to 1.5 seconds).
- Set the query interval to 100 seconds.
- Set the query maximum response time to 15 tenth seconds (equal to 1.5 seconds).
- Set the robustness value to 4 seconds.
- Enable IGMP version 3.
- Enable proxy snoop for the VLAN.
- Enable snoop for the VLAN.
- Enable support for SSM on the snooping interface.
- Enable the fast leave option.

After configuring the parameters, use the **`info`** command to show a summary of the results.

```
8610co:5/config/vlan/2/ip/igmp# last-memb-query-int 15
8610co:5/config/vlan/2/ip/igmp# query-interval 100
8610co:5/config/vlan/2/ip/igmp# query-max-resp 50
8610co:5/config/vlan/2/ip/igmp# robustval 4
8610co:5/config/vlan/2/ip/igmp# ssm-snoop enable
8610co:5/config/vlan/2/ip/igmp# version 3
8610co:5/config/vlan/2/ip/igmp# proxy-snoop enable
8610co:5/config/vlan/2/ip/igmp# snoop enable
8610co:5/config/vlan/2/ip/igmp# fast-leave enable
8610co:5/config/vlan/2/ip/igmp# info

Sub-Context: access-list mrdisc static-members fast-leave-members
Current Context:

         last-memb-query-int : 15
              query-interval : 100 sec(s)
              query-max-resp : 50
                   robustval : 4
                     version : 3
               proxy-snoop  : enable
                     snoop  : enable
                    mrouter :
                  ssm-snoop  : enable
                  fast-leave : enable


8610:5/config/vlan/2/ip/igmp#
```

Showing IGMP VLAN information

To display the IGMP configuration information for all VLANs on the switch or for a specified VLAN, use the following command:

```
show vlan info igmp [<vid>]
```

where:
vid is a VLAN ID from 1 to 4092.

Figure 127 shows sample output for this command.

Figure 127 show vlan info igmp command output

```
8610# show vlan info igmp

================================================================================
                                        Vlan Ip Igmp
================================================================================
VLAN QUERY QUERY ROBUST VERSION LAST  PROXY  SNOOP  SSM    FAST   FAST
ID   INTVL MAX                  MEMB  SNOOP  ENABLE SNOOP  LEAVE  LEAVE
           RESP                 QUERY ENABLE        ENABLE ENABLE PORTS
--------------------------------------------------------------------------------
1    125   100   2      2       10    false  false  false  false
2    125   100   2      2       10    false  false  false  false
3    125   100   2      2       10    false  false  false  true
4    125   100   2      3       10    false  false  false  false
5    125   100   2      2       10    false  false  false  false
6    125   100   2      2       10    false  false  false  false
```

Configuring multicast access control for a VLAN

To configure multicast access control for a VLAN, use the following command:

`config vlan <vid> ip igmp access-control <name>`

where:
vid is a VLAN ID from 1 to 4092.
name is the name of the access policy. It can be 1 to 64 characters.

This command includes the following parameters:

config vlan <vid> ip igmp access-control <name> followed by:	
`info`	Displays the settings for the access-control parameter.
`create <HostAddress> <HostMask> {deny-tx|deny-rx|deny-both|allow-only-tx|allow-only-rx|allow-only-both}`	Creates an access control group entry for a specified VLAN. • *HostAddress* is the IP address of the host. See "Specifying host addresses and masks" for more information. • *HostMask* is the subnet mask used to determine the host or hosts covered by this configuration. You can use the host subnet mask to restrict access to a portion of the host's network. See "Specifying host addresses and masks" for more information. • `deny-tx|deny-rx|deny-both|allow-only-tx|allow-only-rx|allow-only-both` indicates the action you want for the specified VLAN. For example, if you specify deny-both, the VLAN will deny both transmitted and received traffic.

config vlan <vid> ip igmp access-control <name> followed by:	
`delete <HostAddress> <HostMask>`	Deletes the access control group entry for the specified VLAN. • *HostAddress* is the IP address of the host. • *HostMask* is the subnet mask used to determine the host or hosts covered by this configuration.
`mode <HostAddress> <HostMask> {deny-tx|deny-rx|deny-both|allow-only-tx|allow-only-rx|allow-only-both}`	Changes the access control group configuration. • *HostAddress* is the IP address of the host. • *HostMask* is the subnet mask used to determine the host or hosts covered by this configuration. • `deny-tx|deny-rx|deny-both|allow-only-tx|allow-only-rx|allow-only-both` indicates the action you want for the specified VLAN. For example, if you specify deny-both, the VLAN will deny both transmitted and received traffic.

Configuration example

User 2 belongs to VLAN 2 and has subscribed to the extended-basic channels, which includes basic channels plus the Asianet channels. The basic channels and the Asianet channels have a group range of 224.1.1.0 to 224.1.2.255 and 255.1.1.0, sent by sources belonging to the 192.32.16.0 and 192.32.32.0 networks, respectively.

The following example shows how to configure prefix lists (groups of addresses) for basic and Asianet channels, and to create access policies for this user. The access policies ensure that the user receives traffic only for those groups from sources belonging to the 192.32.16.0 and 192.32.32.0 networks. After configuring the parameters, use the **`info`** command to show a summary of the results.

```
8010:5# config ip prefix basic-channels
8010:5/config/ip/prefix/basic-channels# add-prefix 224.1.1.0/24
8010:5/config/ip/prefix/basic-channels# add-prefix 224.1.2.0/24
8010:5/config/ip/prefix/basic-channels# config ip prefix asia-net
8010:5/config/ip/prefix/asia-net# add-prefix 255.1.1.0/24
8010:5/config/ip/prefix/asia-net# config vlan 2 ip igmp access-control
basic-channels
8010:5/config/vlan/2/ip/igmp/access-control/basic-channels# create
192.32.16.0 255.255.255.0 allow-only-tx
8010:5/config/vlan/2/ip/igmp/access-control/basic-channels# config vlan 2
ip igmp access-control asia-net
8010:5/config/vlan/2/ip/igmp/access-control/asia-net# create 192.32.32.0
255.255.255.0 allow-only-tx
8010:5/config/vlan/2/ip/igmp/access-control/asia-net# info

Sub-Context:
Current Context:

                     create :

                          HostAddress - 192.32.16.0
                             HostMask - 255.255.255.0
                                 mode - allow-only-tx
                      mode :
                     delete : N/A

8010:5/config/vlan/2/ip/igmp/access-control/asia-net#
```

Configuring IGMP multicast router discovery on a VLAN

To configure IGMP multicast discovery routes on a VLAN, use the following command:

```
config vlan <vid> ip igmp mrdisc
```

where:
vid is a VLAN ID from 1 to 4092.

This command includes the following parameters:

config vlan <*vid*> ip igmp mrdisc followed by:	
`info`	Displays multicast route discovery parameters on the VLAN.
`mrdisc-enable <enable|disable>`	Enables multicast route discovery on the VLAN.
`max-advertisement-interval <seconds>`	Used to set the maximum number (in seconds) of multicast advertisements that can be configured on the VLAN.
`max-initial-advertisements <integer>`	Used to set the maximum number of initial multicast advertisements that can be configured on the VLAN.
`max-initial-advertisement-interval <seconds>`	Used to set the maximum number of initial multicast advertisements that can be configured on the VLAN.
`min-advertisement-interval <seconds>`	Used to set the minimum number (in seconds) of multicast advertisements that can be configured on the VLAN.
`neighbor-dead-interval <seconds>`	Sets the multicast route discovery dead interval—the number of seconds the switch's multicast route neighbors should wait before assuming that the multicast router is down.

Configuring IGMP static members on a VLAN

To configure IGMP static members on a VLAN, use the following command:

`config vlan <vid> ip igmp static-members <GroupAddress>`

where:
vid is a VLAN ID from 1 to 4092 and
GroupAddress indicates the IP address of the selected multicast group.

This command includes the following parameters:

config vlan <*vid*> ip igmp static-members <GroupAddress> followed by:	
`info`	Displays information about the static members of the VLAN. *GroupAddress* is the multicast group address of the multicast stream.
`add <ports> <static|blocked>`	Adds a static-member entry to the VLAN. • *GroupAddress* is the multicast group address of the multicast stream. • *ports* is the port or list of ports to which you want to redirect the multicast stream for this multicast group. • *static|blocked* sets the route to static or blocked.
`create <ports> <static|blocked>`	Creates a static-member entry to the VLAN. • *GroupAddress* is the multicast group address of the multicast stream. • *ports* is the port or list of ports to which you want to redirect the multicast stream for this multicast group. • *static|blocked* sets the route to static or blocked.

config vlan <*vid*> ip igmp static-members <GroupAddress> followed by:	
`delete`	Deletes a static-member entry to the VLAN. • *GroupAddress* is the multicast group address of the multicast stream.
`remove <ports> <static|blocked>`	Removes a port from the static-member entry to the VLAN. • *GroupAddress* is the multicast group address of the multicast stream. • *ports>* is the port or list of ports to which you want to redirect the multicast stream for this multicast group. • *static* | *blocked* sets the route to static or blocked.

Configuring IGMP fast-leave members on a VLAN

To configure IGMP fast-leave members on a VLAN, use the following command:

```
config vlan <vid> ip igmp fast-leave-members
```

where:
vid is a VLAN ID from 1 to 4092.

This command includes the following parameters:

config vlan <*vid*> ip igmp fast-leave-members followed by:	
`info`	Displays information about the fast-leave members of the VLAN.
`enable <ports>`	Enables members to join a fast-leave group on a given port on the VLAN. • *ports* is the port or list of ports to which you want to join the fast-leave group.
`disable <ports>`	Removes a given port from receiving a leave message from any member of any given group, and the normal IGMP behavior is skipped.

Configuring multicast stream limitation

Multicast stream limitation enables providers to limit the number of multicast groups that can join a VLAN. By limiting the number of concurrent multicast streams, providers can protect the bandwidth on a specific interface and control access to multicast streams.

The maximum number of streams can be set independently. Once a stream limit is met, joins to new streams are dropped. This allows service provider to control the overall bandwidth usage in addition to restricting users from attaching more than the allowed TV sets to a given link.

This section includes the following topics:

Configuring multicast stream limitation on an interface

To configure multicast stream limitation on a specific interface, use the following command:

```
config ip igmp interface <ipaddr> stream-limit
```

where:
ipaddr indicates the IP address of the selected interface.

This command includes the following parameters:

config ip igmp interface <*ipaddr*> stream-limit followed by:	
`info`	Displays information about the stream limits set on this interface.
`enable`	Enables stream limitation on this interface.
`disable`	Disables stream limitation on this interface.
`max-streams <integer>`	Sets the maximum number of allowed streams on this interface. The range is from 0 to 65535, and the default is 4.

Configuration example

This configuration example uses the commands described above to perform the following tasks:

- Enable multicast stream limitation on the interface at IP address 10.0.6.2.
- Set the maximum number of allowed streams to 8.

After configuring the parameters, use the **`info`** command to show a summary of the results.

```
8610:5/config/ip/igmp/interface/10.0.6.2/stream-limit# enable
8610:5/config/ip/igmp/interface/10.0.6.2/stream-limit#
max-streams 8
8610:5/config/ip/igmp/interface/10.0.6.2/stream-limit# info

Sub-Context:
Current Context:

                     enable : TRUE
                max-streams : 8
                num-streams : 0

8610:5/config/ip/igmp/interface/10.0.6.2/stream-limit#
```

Configuring multicast stream limitation members on an interface

To configure multicast stream limitation on ports of the specified interface, use the following command:

```
config ip igmp interface <ipaddr> stream-limit-members
```

where:
ipaddr indicates the IP address of the selected interface.

This command includes the following parameters:

config ip igmp interface <*ipaddr*> stream-limit-members followed by:	
`info`	Displays information about the stream limit members set on individual ports for this interface.
`enable <ports> max-streams <value>`	Enables stream limitation and sets the maximum number of allowed streams for the specified ports on this interface. The number of allowed streams cannot exceed the maximum number for the interface. The range is from 0 to 65535, and the default is 4.
`disable <ports>`	Disables stream limitation for the specified ports on this interface.
`set <ports> max-streams <value>`	Sets the maximum number of allowed streams for the specified ports on this interface. The range is from 0 to 65535, and the default is 4.

Configuration example

This configuration example uses the commands described above to perform the following tasks:

- Enable multicast stream limitation on ports 1/3 to 1/8 and set the maximum allowed number of streams to 6 for these ports.
- Set the maximum number of allowed streams for ports 1/3 to 1/8 to 8.

After configuring the parameters, use the **info** command to show a summary of the results.

```
8610:5/config/ip/igmp/interface/192.32.96.82/stream-limit-members#
enable 1/3-1/8 max-streams 6
8610:5/config/ip/igmp/interface/192.32.96.82/stream-limit-members#
set 1/3-1/8 max-streams 8
8610:5/config/ip/igmp/interface/192.32.96.82/stream-limit-members#
info

Sub-Context:
Current Context:
        enable:


            port - 1/3
            max-streams - 8
            num-streams - 0


            port - 1/8
            max-streams - 8
            num-streams - 0
        disable : N/A
        set : N/A

8610:5/config/ip/igmp/interface/192.32.96.82/stream-limit-members#
```

Showing multicast stream limitations per interface

To display information about the interfaces on which multicast stream limitation is enabled, use the following command:

```
show ip igmp stream-limit-interface
```

Figure 112 shows sample output for this command.

Figure 128 show ip igmp interface command output

```
8610:5# show ip igmp stream-limit-interface

================================================================================
                    Igmp Stream Limitation Per Interface
================================================================================
INTERFACE  MAX STREAMS     NUM STREAMS
--------------------------------------------------------------------------------
1/3        4               0
5/1        4               0
Vlan 3     4               0

8610:5#
```

Showing multicast stream limitations per port

To display multicast stream limitation information for the ports on a specific interface, use the following command:

```
show ip igmp stream-limit-port
```

Figure 129 shows sample output for this command.

Figure 129 show ip igmp interface command output

```
8610:5# show ip igmp stream-limit-port

================================================================================
                       Igmp Stream Limitation Per Port
================================================================================
INTERFACE  PORT       MAX STREAMS     NUM STREAMS
--------------------------------------------------------------------------------
---
Vlan 3     2/1        4               0
Vlan 3     2/2        4               0
Vlan 4     10/14      4               0
Vlan 4     10/15      4               0

8610:5#
```

Configuring multicast stream limitation on an Ethernet port

To configure multicast stream limitation on an Ethernet port, use the following command:

```
config ethernet <ports> ip igmp stream-limit
```

where:
ports use the convention {slot/port[-slot/port][, ...]}.

This command includes the following parameters:

config ethernet <*ports*> ip igmp stream-limit followed by:	
`info`	Displays information about the stream limits set on this port.
`enable`	Enables stream limitation on this port.
`disable`	Disables stream limitation on this port.
`max-streams <integer>`	Sets the maximum number of allowed streams on this port. The range is from 0 to 65535, and the default is 4.

Configuration example

This configuration example uses the commands described above to perform the following tasks:

- Enable multicast stream limitation on the Ethernet port 1/3.
- Set the maximum number of allowed streams to 8.

After configuring the parameters, use the **info** command to show a summary of the results.

```
8610:5/config/ethernet/1/3/ip/igmp/stream-limit# enable
8610:5/config/ethernet/1/3/ip/igmp/stream-limit# max-streams 8
8610:5/config/ethernet/1/3/ip/igmp/stream-limit# info

Sub-Context:
Current Context:

                     enable : TRUE
                max-streams : 8
                num-streams : 0

8610:5/config/ethernet/1/3/ip/igmp/stream-limit#
```

Configuring multicast stream limitation on a VLAN

To configure multicast stream limitation on a specific VLAN, use the following command:

`config vlan <vid> ip igmp stream-limit`

where:
vid is a VLAN ID from 1 to 4093.

This command includes the following parameters:

config vlan <*vid*> ip igmp stream-limit followed by:	
`info`	Displays information about the stream limits set on this VLAN.
`enable`	Enables stream limitation on this VLAN.
`disable`	Disables stream limitation on this VLAN.
`max-streams <integer>`	Sets the maximum number of allowed streams on this interface. The range is from 0 to 65535, and the default is 4.

Configuration example

This configuration example uses the commands described above to perform the following tasks:

- Enable multicast stream limitation on VLAN 3.
- Set the maximum number of allowed streams to 8.

After configuring the parameters, use the **`info`** command to show a summary of the results.

```
8610:5/config/vlan/3/ip/igmp/stream-limit# enable
8610:5/config/vlan/3/ip/igmp/stream-limit# max-streams 8
8610:5/config/vlan/3/ip/igmp/stream-limit# info

Sub-Context:
Current Context:

                     enable : TRUE
                max-streams : 8
                num-streams : 0

8610:5/config/vlan/3/ip/igmp/stream-limit#
```

Configuring multicast stream limitation members on a VLAN

To configure multicast stream limitation on ports of a specific VLAN, use the following command:

```
config vlan <vid> ip igmp stream-limit-members
```

where:
`vid` is a VLAN ID from 1 to 4093.

This command includes the following parameters:

config vlan <*vid*> ip igmp stream-limit-members followed by:	
`info`	Displays information about the stream limit members set on individual ports for this VLAN.
`enable <ports> max-streams <value>`	Enables stream limitation and sets the maximum number of allowed streams for the specified ports on this VLAN. The number of allowed streams cannot exceed the maximum number for the VLAN. The range is from 0 to 65535, and the default is 4.
`disable <ports>`	Disables stream limitation for the specified ports on this VLAN.
`set <ports> max-streams <value>`	Sets the maximum number of allowed streams for the specified ports on this VLAN. The range is from 0 to 65535, and the default is 4.

Configuration example

This configuration example uses the commands described above to perform the following tasks:

- Enable multicast stream limitation on ports 1/3 to 1/8 and set the maximum allowed number of streams to 6 for this interface.
- Set the maximum number of allowed streams for ports 1/3 to 1/8 to 8.

After configuring the parameters, use the **`info`** command to show a summary of the results.

```
8610:5/config/vlan/3/ip/igmp/stream-limit-members# enable 1/3-1/8
max-streams 6
8610:5/config/vlan/3/ip/igmp/stream-limit-members# set 1/3-1/8
max-streams 8
8610:5/config/vlan/3/ip/igmp/stream-limit-members# info


Sub-Context:
Current Context:
        enable:
```

```
        port - 1/3
        max-streams - 8
        num-streams - 0

        port - 1/8
        max-streams - 8
        num-streams - 0
    disable : N/A
    set : N/A

8610:5/config/vlan/3/ip/igmp/stream-limit-members#
```

Displaying all IP IGMP show commands

The **show ip igmp show-all** command displays all relevant IP IGMP information.

The command uses the syntax:

`show ip igmp show-all [file <value>]`

where *<value>* is the filename to which the output will be redirected.

Figure 130 shows sample output for the **show ip igmp show-all** command.

Figure 130 show ip igmp show-all command output

```
Passport-8600:5# show ip igmp show-all


# show ip igmp access


================================================================================
                                    Igmp Access
================================================================================
GRPADDR          INTERFACE  HOSTADDR         HOSTMASK         ACCESSMODE
--------------------------------------------------------------------------------
225.1.1.1        Vlan1      10.10.10.0       255.255.255.0    denyRX



# show ip igmp cache


================================================================================
                                    Igmp Cache
================================================================================
GRPADDR         INTERFACE  LASTREPORTER    EXPIRATION V1HOSTTIMER
--------------------------------------------------------------------------------
224.2.199.42    Vlan1010   20.3.10.130     203        0
225.1.1.1       Vlan1000   20.3.0.130      194        0
225.1.1.1       Vlan1010   20.3.10.59      161        0
225.1.1.1       Vlan1020   20.3.20.133     193        0
225.1.1.1       Vlan1030   20.3.30.59      165        0
```

Chapter 10
Configuring DVMRP using the CLI

Distance Vector Multicast Routing Protocol (DVMRP) is used between routers to exchange their multicast routing information. The protocol can be configured on a VLAN, but it must be enabled globally in order to take effect. For more information about DVMRP concepts and terminology, see Chapter 1, “IP Multicast concepts.”

For instructions on how to configure DVMRP static source groups, refer to Chapter 13, “Viewing and editing multicast routes using the CLI.”

This chapter includes the following topics:

Roadmap of DVMRP commands

The following roadmap lists all the DVMRP commands and their parameters. After using the commands below to configure the Passport 8600, you can use the show commands to display information for a particular feature.

To facilitate troubleshooting, the Passport 8600 also provides *one* command (`show ip dvmrp show-all`) that lists all the show commands for IP DVMRP and displays their configuration output. See "Displaying all IP DVMRP show commands" on page 383.

Use this list as a quick reference or click on any entry for more information:

Command	Parameter
`config ip dvmrp`	`info`
	`disable`
	`enable`
	`leaf-timeout <integer>`
	`nbr-timeout <integer>`
	`nbr-probe-interval <integer>`
	`triggered-update- interval <integer>`
	`update-interval <integer>`
	`fwd-cache-timeout <integer>`
	`route-expiration-timeout <integer>`
	`route-discard-timeout <integer>`
	`route-switch-timeout <integer>`
	`show-next-hop-table <enable|disable>`
`config ip dvmrp interface <ipaddr>`	`info`
	`advertise-self <enable|disable>`
	`create <active|passive>`
	`default-listen <enable|disable>`

Command	Parameter
	default-supply <enable|disable>
	default-supply-metric <cost>
	disable
	enable
	in-policy <policy name>
	interface-type <active|passive>
	metric <cost>
	out-policy <policy name>
show ip dvmrp info	
show ip dvmrp interface	
show ip dvmrp neighbor	
show ip dvmrp next-hop	
show ip dvmrp route	
config ethernet <ports> ip dvmrp	info
	advertise-self <enable|disable>
	create <active|passive>
	default-listen <enable|disable>
	default-supply <enable|disable>
	default-supply-metric <cost>
	disable
	enable
	in-policy <policy name>
	interface-type <active|passive>
	metric <cost>
	out-policy <policy name>
config vlan <vid> ip dvmrp	info
	advertise-self <enable|disable>
	create <active|passive>

Command	Parameter
	default-listen <enable|disable>
	default-supply <enable|disable>
	default-supply-metric <cost>
	disable
	enable
	in-policy <policy name>
	interface-type <active|passive>
	metric <cost>
	out-policy <policy name>
config ip prefix-list <prefix-list-name>	
	info
	add-prefix <ipaddr/mask> [maskLenFrom <value>] [maskLenTo <value>]
	delete
	name <name>
	remove-prefix <ipaddr/mask>
config ip route-policy <policy name> seq <seq number>	action <permit|deny>
	create
	disable
	enable
	match-protocol> <protocol name>
	match-metric <metric>
	match-network <prefix-list>
	match-next-hop <prefix-list>
	match-route-src <prefix-list>
	name <policy name>
	set-metric <metric-value>

Command	Parameter
show vlan info dvmrp [<vid>]	
show ports info dvmrp [<ports>]	
show ip dvmrp show-all [file <value>]	

Configuration prerequisites

Before you can configure DVMRP, you must prepare the router as follows:

1. Configure an IP interface. For information, refer to *Configuring IP Routing Operations*.
2. Disable PIM-SM from the interface on which you want to configure DVMRP because you cannot configure PIM-SM and DVMRP on the same interface. For information, refer to Chapter 11, "Configuring PIM using the CLI."

Note: Changing the configuration from PIM to DVMRP, or from DVMRP to PIM, is not recommended while multicast traffic is flowing on the network.

   a. A *switch* can have a mix of DVMRP and PIM-SM interfaces if it is configured as an multicast border router (MBR).

   b. An *interface* can only be configured with one multicast routing protocol at a time (PIM-SM or DVMRP).

3. Enable DVMRP globally.

   To enable DVMRP globally, see "Configuring DVMRP globally."

Configuring DVMRP globally

To configure DVMRP globally, use the following command:

```
config ip dvmrp
```

This command includes the following parameters:

config ip dvmrp followed by:	
`info`	Displays DVMRP settings on the switch.
`disable`	Globally disables DVMRP on the switch.
`enable`	Globally enables DVMRP on the switch.
`leaf-timeout <integer>`	Sets the length of time (in seconds) the router waits for a response from a neighbor before considering the attached network to be a leaf network. • *integer* is the range of 25 to 4000 seconds. The default value is 125 seconds.
`nbr-timeout <integer>`	Sets the length of time (in seconds) the router waits to receive a report from a neighbor before considering the connection inactive. • *integer* is the range of 35 to 8000 seconds. The default value is 35 seconds.
`nbr-probe-interval <integer>`	Sets the time interval (in seconds) for the DVMRP router to send a neighbor probe message on its interface. • *integer* is the range of 5 to 30 seconds. The default value is 10 seconds.
`triggered-update-interval <integer>`	Sets the time interval (in seconds) between triggered update messages sent when routing information changes. • *integer* is the range of 5 to 1000 seconds. The default value is 5 seconds.
`update-interval <integer>`	Sets the time interval (in seconds) between DVMRP router update messages. • *<integer>* is the range of 10 to 2000 seconds. The default value is 60 seconds.
`fwd-cache-timeout <integer>`	Sets the forward cache timeout (in seconds). • *<integer>* is the range of 300 to 86400 seconds. The default value is 300 seconds.

config ip dvmrp followed by:	
route-expiration-timeout <*integer*>	Sets the route expiration timeout (in seconds). • <*integer*> is the range of 20 to 4000 seconds. The default value is 140 seconds.
route-discard-timeout <*integer*>	Sets the route discard timeout (in seconds). • <*integer*> is the range of 40 to 8000. The default value is 260 seconds.
route-switch-timeout <*integer*>	Sets the route switch timeout (in seconds). • <*integer*> is the range of 20 to 2000. The default value is 140 seconds.
show-next-hop-table <enable|disable>	Enables or disables showing information about the DVMRP next hops. See "Showing DVMRP next hops" on page 342.

Figure 131 shows sample output for the **config ip dvmrp info** command.

Figure 131 config ip dvmrp info command output

```
8610# config ip dvmrp info

Sub-Context:
Current Context:

                        enable  :  true
                update-interval  :   60
     triggered-update-interval  :  5
                   leaf-timeout  :  200
                    nbr-timeout  :  35
              nbr-probe-interval  :  10
               fwd-cache-timeout  :  300
            route-expire-timeout  :  140
              route-disc-timeout  :  260
            route-switch-timeout  :  140
```

Configuring DVMRP on an interface

To configure DVMRP on a specific interface, use the following command:

`config ip dvmrp interface <ipaddr>`

where:
ipaddr indicates the IP address of the selected interface.

This command includes the following parameters:

config ip dvmrp interface <ipaddr> followed by:	
info	Displays information about the specified DVMRP local router interface.
advertise-self <enable|disable>	Enables or disables the advertisement of local routes for the selected interface to other switches in the network. See "Applying the advertisement of local networks policy to an interface" on page 371
create <active|passive>	Sets the interface type: active or passive. See "Creating a passive interface" on page 375.
default-listen <enable|disable>	Learns the default route over the specified interface if this feature is enabled on the interface. The default setting is enable. See "Applying the default route policy to an interface" on page 349.
default-supply <enable|disable>	Generates and advertises the default route when enabled on the interface. The default setting is disable. See "Applying the default route policy to an interface" on page 349.
default-supply-metric <cost>	Advertises the specified metric over the interface if you have configured the interface to supply the default route. The range is 1 to 31 hops. The default setting is 1 hop. See "Applying the default route policy to an interface" on page 349.
disable	Disables DVMRP on the local router interface.
enable	Enables DVMRP on the local router interface.
in-policy <policy name>	Applies a DVMRP accept policy. See "Applying a DVMRP accept policy to an interface" on page 368.
interface-type <active|passive>	Configure an interface as active or passive. See "Configuring an active or passive interface type" on page 376.

config ip dvmrp interface <*ipaddr*> followed by:	
metric <*cost*>	Sets the cost metric (maximum number of hops) for the router interface. *cost* is the range of 1 to 31.
out-policy <*policy name*>	Applies a DVMRP accept policy. See "Applying a DVMRP announce policy to an interface" on page 360.

Showing DVMRP group information

To display information about the general DVMRP group, use the following command:

```
show ip dvmrp info
```

Figure 132 shows sample output for this command.

Figure 132 show ip dvmrp info command output

```
8610# show ip dvmrp info

================================================================
                        Dvmrp General Group
================================================================
                      AdminStat  :  enabled
                          Genid  :  152
                        Version  :  3
                      NumRoutes  :  0
             NumReachableRoutes  :  0

                 UpdateInterval  :  60
        TriggeredUpdateInterval  :  5
                    LeafTimeOut  :  200
                     NbrTimeOut  :  35
                NbrProbeInterval  :  10
                  FwdCacheTimeout  :  300
              RouteExpireTimeout  :  140
             RouteDiscardTimeout  :  260
              RouteSwitchTimeout  :  140
```

Showing DVMRP neighbors

To display information about the configured DVMRP neighbors, use the following command:

```
show ip dvmrp neighbor
```

Figure 133 shows sample output for this command.

Figure 133 show ip dvmrp neighbor command output

```
8610# show ip dvmrp neighbor

================================================================================
                                    Dvmrp Neighbor
================================================================================
INTERFACE  ADDRESS        EXPIRE GENID      MAJVER MINVER CAPABILITY    STATE
--------------------------------------------------------------------------------
```

Showing DVMRP next hops

Note: Before you can show DVMRP next hops, you have to enable showing the table by entering the following command:
`config ip dvmrp show-next-hop-table enable`

Showing the next-hop table is disabled by default, however, you can save the setting of this command in the configuration for the switch. Disabling this setting avoids using the large amount of memory required for these tables in a scaled multicast environment with a large number of VLANs. For more information, see "Configuring DVMRP globally" on page 337.

To display information about the DVMRP next hops, use the following command:

```
show ip dvmrp next-hop
```

Figure 134 shows sample output for this command.

Figure 134 show ip dvmrp next-hop command output

```
8610/show/ip/dvmrp# next-hop

================================================================================
                              Dvmrp Next Hop
================================================================================
SOURCE          MASK            INTERFACE  TYPE
--------------------------------------------------------------------------------
10.160.140.0   255.255.255.0   Vlan52     leaf
10.28.1.0      255.255.255.0   Vlan52
```

Showing DVMRP routes

To display information about the DVMRP routes, use the following command:

```
show ip dvmrp route
```

Figure 135 shows sample output for this command.

Figure 135 show ip dvmrp route command output

```
8610/show/ip/dvmrp# route

================================================================================
                                  Dvmrp Route
================================================================================
SOURCE          MASK            UPSTREAM_NBR    INTERFACE  METRIC EXPIRE
--------------------------------------------------------------------------------
---
10.160.140.0   255.255.255.0   0.0.0.0         Vlan53     32     115
10.28.1.0      255.255.255.0   0.0.0.0         Vlan52     1      215
```

Configuring DVMRP on Ethernet ports

To configure DVMRP at the port level, use the following command:

```
config ethernet <ports> ip dvmrp
```

where:
ports use the convention {slot/port[-slot/port][, ...]}.

DVMRP must be enabled globally for these settings to take effect.

This command includes the following parameters:

config ethernet <*ports*> ip dvmrp followed by:	
`info`	Displays DVMRP settings on the port.
`advertise-self <enable|disable>`	Enables or disables the advertisement of local routes for the selected port to other switches in the network. See “Applying the advertisement of local networks policy over a port” on page 373.
`create <active|passive>`	Sets the interface type: active or passive. See “Configuring an active or passive port type” on page 379.
`default-listen <enable|disable>`	Learns the default route over the specified port if this feature is enabled on the interface. The default setting is enable. See “Applying the default route policy to a port” on page 353.
`default-supply <enable|disable>`	Generates and advertises the default route when enabled on the port. The default setting is disable. See “Applying the default route policy to a port” on page 353.
`default-supply-metric <cost>`	Advertises the specified metric over the port if you have configured the port to supply the default route. The range is 1 to 31 hops. The default setting is 1 hop. See “Applying the default route policy to a port” on page 353.
`disable`	Disables DVMRP on the port.
`enable`	Enables DVMRP on the port.
`in-policy <policy name>`	Applies a DVMRP accept policy. See “Applying a DVMRP accept policy to a port” on page 370.

config ethernet <*ports*> ip dvmrp followed by:	
`interface-type <active|passive>`	Configure an interface as active or passive. See "Configuring an active or passive port type" on page 379.
`metric <cost>`	Sets the DVMRP route metric. *cost* is the maximum number of hops with a value of 1 to 31.
`out-policy <policy name>`	Applies a DVMRP accept policy. See "Applying a DVMRP announce policy to a port" on page 362.

Figure 136 shows sample output for this command.

Figure 136 config ethernet ip dvmrp info command output

```
8610# config ethernet 9/3 ip dvmrp info

Sub-Context:
Current Context:

                      dvmrp : disable
                     metric : 1
```

Configuring DVMRP on a VLAN

To configure DVMRP on a VLAN, use the following command:

```
config vlan <vid> ip dvmrp
```

where:
vid is a VLAN ID from 1 to 4092.

This command includes the following parameters:

config vlan <*vid*> ip dvmrp followed by:	
`info`	Displays DVMRP settings on the VLAN.
`advertise-self <enable|disable>`	Enables or disables the advertisement of local routes for the selected VLAN to other switches in the network. See "Applying the advertisement of local networks policy over a VLAN" on page 372.
`create <active|passive>`	Sets the interface type: active or passive. See "Configuring an active or passive VLAN type" on page 378.
`default-listen <enable|disable>`	Learns the default route over the specified VLAN if this feature is enabled on the interface. The default setting is enable. See "Applying the default route policy to a VLAN" on page 351.
`default-supply <enable|disable>`	Generates and advertises the default route when enabled on the VLAN. The default setting is disable. See "Applying the default route policy to a VLAN" on page 351.
`default-supply-metric <cost>`	Advertises the specified metric over the VLAN if you have configured the VLAN to supply the default route. The range is 1 to 31 hops. The default setting is 1 hop. See "Applying the default route policy to a VLAN" on page 351.
`disable`	Disables DVMRP on the VLAN.
`enable`	Enables DVMRP on the VLAN.
`in-policy <policy name>`	Applies a DVMRP accept policy. See "Applying a DVMRP accept policy to a VLAN" on page 369.
`interface-type <active|passive>`	Configure an interface as active or passive. See "Configuring an active or passive VLAN type" on page 378.

config vlan <*vid*> ip dvmrp followed by:	
metric <*cost*>	Sets the DVMRP route metric. *cost* is the maximum number of hops with a value of 1 to 31.
out-policy <*policy name*>	Applies a DVMRP accept policy. See “Applying a DVMRP announce policy to a VLAN” on page 361.

Figure 137 shows sample output for this command.

Figure 137 config vlan ip dvmrp info command output

```
8610# config vlan 1 ip dvmrp info

Sub-Context:
Current Context:

                      dvmrp : enable
                     metric : 1
```

Configuring DVMRP routing policies

DVMRP routing policies allow you to improve the management of the DVMRP routing tables by providing control of how the routing table is populated and how the routes are exchanged between 8000 series switches. These routing policies, when enabled, can be applied to an interface that can be either a VLAN or a brouter port.

This section includes the following topics:

Configuring default route policies

This section includes the following tasks that describe how to set up your default route configuration using the command line interface:

Before you apply the default route policy to the switch, you must perform the procedures provided in “Configuration prerequisites” on page 336.

To display DVMRP default route configuration information for an interface, VLAN, or port, refer to “Displaying DVMRP routing policy information” on page 380.

Applying the default route policy to an interface

To apply the default route policy to an interface, use the following command:

`config ip dvmrp interface <ipaddr>`

where:
ipaddr indicates the IP address of the selected interface.

This command includes the following parameters:

config ip dvmrp interface <ipaddr> followed by:	
`default-listen <enable|disable>`	Learns the default route over the specified interface if this feature is enabled on the interface. The options are enable and disable. The default setting is enable.
`default-supply <enable|disable>`	Generates and advertises the default route when enabled on the interface. The options are enable and disable. The default setting is disable.
`default-supply-metric <cost>`	Advertises the specified metric over the interface if you have configured the interface to supply the default route. The range is 1 to 31 hops. The default setting is 1 hop.

Configuration examples

The following configuration example uses the commands described above to enable the switch to learn the default route over interface 100.100.100.2. After configuring these parameters, use the **`info`** command to show a summary of the results.

```
8610:5/config/ip/dvmrp/interface/100.100.100.2# default-listen
enable
8610:5/config/ip/dvmrp/interface/100.100.100.2# info

Sub-Context:
Current Context:

               enable : true
               metric : 1
       interface-type : passive
            in-policy : N/A
           out-policy : N/A
       advertise-self : disable
       default-listen : enable
       default-supply : disable
default-supply-metric : 1
```

The following configuration example uses the commands described above to enable the switch to generate and advertise the default route over interface 100.100.100.6. After configuring these parameters, use the **info** command to show a summary of the results.

```
8610:5/config/ip/dvmrp/interface/100.100.100.6# default-supply
enable
8610:5/config/ip/dvmrp/interface/100.100.100.6#
default-supply-metric 3
8610:5/config/ip/dvmrp/interface/100.100.100.6# info

Sub-Context:
Current Context:

               enable : true
               metric : 1
       interface-type : passive
            in-policy : N/A
           out-policy : N/A
       advertise-self : enable
       default-listen : disable
       default-supply : enable
default-supply-metric : 3
```

Applying the default route policy to a VLAN

To apply the default route policy to a VLAN, use the following command:

```
config vlan <vid> ip dvmrp
```

where:
vid is a VLAN ID from 1 to 4092.

This command includes the following parameters:

config vlan <*vlanid*> ip dvmrp followed by:	
`default-listen`	Learns the default route over the specified VLAN if this feature is enabled on the VLAN. The options are enable and disable. The default setting is enable.
`default-supply`	Generates and advertises only the default route when enabled on the VLAN. No other route is advertised to the neighbors on this VLAN. The options are enable and disable. The default setting is disable.
`default-supply-metric`	Advertises the specified metric over the VLAN if you have configured the VLAN to supply the default route. The range is 1 to 31 hops. The default setting is 1 hop.

Configuration example

The following configuration example uses the commands described above to enable the switch to learn the default route over VLAN 100 and disables the VLAN from advertising the default route. After configuring these parameters, use the **`info`** command to show a summary of the results.

```
8610:5/config/vlan/100/ip/dvmrp# default-listen enable
8610:5/config/vlan/100/ip/dvmrp# default-supply disable
8610:5/config/vlan/100/ip/dvmrp# info

Sub-Context:
Current Context:

                      dvmrp : enable
                     metric : 1
              interface-type : passive
                   in-policy : N/A
                  out-policy : N/A
              advertise-self : disable
              default-listen : enable
              default-supply : disable
        default-supply-metric : 3
```

Applying the default route policy to a port

To apply the default route policy to a port, use the following command:

```
config ethernet <ports> ip dvmrp
```

where:
ports use the convention {slot/port[-slot/port][, ...]}.

This command includes the following parameters:

config ethernet <*ports*> ip dvmrp followed by:	
`default-listen`	Learns the default route over the specified port if this feature is enabled on the port. The options are enable and disable. The default setting is enable.
`default-supply`	Generates and advertises only the default route when enabled on the port. No other route is advertised to the neighbors on this port. The options are enable and disable. The default setting is disable.
`default-supply-metric`	Advertises the specified metric over the port if you have configured the port to supply the default route. The range is 1 to 31 hops. The default setting is 1 hop.

Configuration example

The following configuration example uses the commands described above to configure port 9 of the card in slot 1 to listen for the default route and disables the port from advertising the default route. After configuring these parameters, use the **`info`** command to show a summary of the results.

```
8610:5/config/ethernet/1/9/ip/dvmrp# default-listen enable
8610:5/config/ethernet/1/9/ip/dvmrp# default-supply disable
8610:5/config/ethernet/1/9/ip/dvmrp# info

Sub-Context:
Current Context:

                       dvmrp : enable
                      metric : 1
              interface-type : active
                   in-policy : N/A
                  out-policy : N/A
              advertise-self : disable
              default-listen : enable
              default-supply : disable
        default-supply-metric : 3
```

Configuring DVMRP announce policies

This section includes the following tasks that describe how to set up your announce policy configuration using the command line interface:

Before you create and apply a DVMRP announce policy to the switch, you must perform the procedures provided in "Configuration prerequisites" on page 336.

Note: Deleting an announce policy from an interface, VLAN or port means that you change the configuration. It does not mean that you delete the policy itself.

To display DVMRP announce policy configuration information for an interface, VLAN, or port, refer to "Displaying DVMRP routing policy information" on page 380.

Creating a DVMRP announce policy

Before you can apply an announce policy to an interface, VLAN, or port, you must first create and configure the policy. An announce policy must be configured on an interface.

You can create one or more IP prefix lists and apply that list to any IP route policy. A prefix list with a 32 bit mask is equivalent to an address. A prefix list with a mask less than 32 bits can be used as a network. If you configure the MaskLenFrom field to be less than MaskLenUpto field, it can also be used as a range.

To create prefix list(s) of networks to be used by the DVMRP policy, use the following command:

`config ip prefix-list <prefix-list-name>`

where:
prefix-list-name indicates the name of the specified prefix list, which is a string length from 1 to 64.

This command includes the following parameters:

config ip prefix-list <prefix-list-name> followed by:	
`info`	Displays all of the prefixes in a given list.
`add-prefix <ipaddr/mask> [maskLenFrom <value>] [maskLenTo <value>]`	Adds a prefix entry to the prefix list. `<ipaddr/mask>` is the IP address and mask. `maskLenFrom <value>` is the lower bound of mask length. The default is the mask length. `maskLenTo <value>` is the higher bound mask length. The default is the mask length. **Note:** Lower bound and higher bound mask lengths together can define a range of networks.
`delete`	Deletes the prefix list.
`name <name>`	The name command is used to rename the specified prefix list. The name length can be from 1 to 64 characters.
`remove-prefix <ipaddr/mask>`	Removes a prefix entry from the prefix list. `ipaddr/mask>` is the IP address and mask.

To configure a DVMRP policy, use the following command:

`config ip route-policy <policy name> seq <seq number>`

where:
policy-name indicates the name of the specified policy, which is a string length from 1 to 64.
seq number indicates the number of the specified policy, which is a number from 1 to 65535.

Note: Not all of the `route-policy seq` parameters apply to the process of creating a DVMRP policy. The table below describes the parameters that you must use to create the DVMRP policy. For information on the other parameters for this command, refer to *Configuring IP Routing Operations*.

This command includes the following parameters:

config ip route-policy <policy name> seq <seq number> followed by:	
action <*permit*|*deny*>	Specifies the action to be taken when a policy is selected for a specific route. This can be permit or deny. Permit allows the route, deny ignores the route.
create	Creates a route policy with a policy name and a sequence number. Note: When creating a route policy in the CLI, the ID is internally generated using an automated algorithm. When you create a route policy in Device Manager, you can manually assign the ID number.
disable	Disables a route policy with a policy name and a sequence number.
enable	Enables a route policy with a policy name and a sequence number.
match-protocol> <*protocol name*>	Matches the protocol through which the route is learned, if configured.

config ip route-policy <policy name> seq <seq number> followed by:	
match-metric <*metric*>	Matches the metric of the incoming advertisement or existing route against the specified value, if configured. If 0, then this field is ignored. • <*metric*> is 1 to 65535. The default is 0.
match-network <*prefix-list*>	Matches the destination network against the contents of the specified prefix list(s), if configured. • <*prefix-list*> specify the name of up to four defined prefix list by name separated by a comma.
match-next-hop <*prefix-list*>	Matches the previous hop IP address of the route against the contents of the specified prefix list, if configured. This field applies only to non-local routes. • <*prefix-list*> specify the name of up to four defined prefix list by name separated by a comma.
match-route-src <*prefix-list*>	Matches the previous hop IP address for DVMRP routes against the contents of the specified prefix list, if configured. • <*prefix-list*> specify the name of up to four defined prefix list by name separated by a comma.
name <*policy name*>	Renames a policy once it has been created. This command changes the name field for all sequence numbers under the given policy.
set-metric <*metric-value*>	Sets the metric value for the route while announcing a redistributing, if configured. The default is 0. If the default is configured, the original cost of the route is advertised into DVMRP.

Configuration example

The following configuration example uses the above commands to create a DVMRP announce policy. In this example, a single prefix list is created (prefix1) (refer to command line 1 below) and IP address 4.4.4.4/24 is added to the prefix list (refer command line 2 below).

After the prefix list is created, the policy is configured (refer to command lines 3 through 7 below), the prefix list is applied to the match-network parameter of the DVMRP policy (refer to command line 8 below), and the new policy is applied to VLAN 3 (refer to command line 9 below).

```
1. 8610:5/config/vlan/3/ip# config ip prefix-list prefix1
2. 8610:5/config/ip/prefix-list/prefix1# add 4.4.4.4/24
3. 8610:5# config ip route-policy policy1
4. 8610:5/config/ip/route-policy/policy1# seq 1
5. 8610:5/config/ip/route-policy/policy1/seq/1# create
6. 8610:5/config/ip/route-policy/policy1/seq/1# action deny
7. 8610:5/config/ip/route-policy/policy1/seq/1# enable
8. 8610:5/config/ip/route-policy/policy1/seq/1# match-network
   prefix1
9. 8610:5/config/vlan/3/ip dvmrp out-policy policy1
```

Note: When this configuration is applied to VLAN 3, the switch does not announce DVMRP routes to network 4.4.4.0 to the neighbor switches on VLAN 3.

Applying a DVMRP announce policy to an interface

To apply a DVMRP announce policy to an interface, use the following command:

```
config ip dvmrp interface <ipaddr> out-policy <policy name>
```

where:
ipaddr is the address of the interface and *policy name* is the name of the applicable announce policy you created.

Configuration example

The following configuration example uses the above command to apply a DVMRP announce policy to an interface. In this example, the announce policy named “policy1” is applied to interface 2.2.2.2.

```
8610:5/config/ip/dvmrp/interface/2.2.2.2# out-policy policy1
```

Deleting a DVMRP announce policy from an interface

To delete a DVMRP announce policy from an interface, use the following command:

```
config ip dvmrp interface <ipaddr> out-policy ""
```

where:
"" are double quotes that indicate the policy used in the current session.

Configuration example

The following configuration example uses the above command to delete the DVMRP announce policy from an interface. In this example, the announce policy currently set on interface 2.2.2.2 is deleted.

```
8610:5/config/ip/dvmrp/interface/2.2.2.2# out-policy ""
```

Applying a DVMRP announce policy to a VLAN

To apply a DVMRP announce policy to a VLAN, use the following command:

```
config vlan <vid> ip dvmrp out-policy <policy name>
```

where:
vid is the number of the VLAN and *policy name* is the name of the applicable announce policy you created.

Configuration example

The following configuration example uses the above command to apply a DVMRP announce policy to a VLAN. In this example, the announce policy named “policy1” is applied to VLAN 5.

```
8610:5/config/vlan/vlan5/ip/dvmrp# out-policy policy1
```

Deleting a DVMRP announce policy from a VLAN

To delete a DVMRP announce policy from a VLAN, use the following command:

```
config vlan <vid> ip dvmrp out-policy ""
```

where:
vid is the number of the VLAN and *""* are double quotes that indicate the policy used in the current session.

Configuration example

The following configuration example uses the above command to delete the DVMRP announce policy from a VLAN. In this example, the announce policy currently set on VLAN 5 is deleted.

```
8610:5/config/vlan/vlan5/ip/dvmrp# out-policy ""
```

Applying a DVMRP announce policy to a port

To apply a DVMRP announce policy to a port, use the following command:

```
config ether <port> ip dvmrp out-policy <policy name>
```

where:
port is the number of the port and *policy name* is the name of the applicable announce policy you created.

Configuration example

The following configuration example uses the above command to apply a DVMRP announce policy to a port. In this example, the announce policy named "policy1" is applied to port 1/5.

```
8610:5/config/ether/1/5/ip/dvmrp# out-policy policy1
```

Deleting a DVMRP announce policy from a port

To delete a DVMRP announce policy from a port, use the following command:

```
config ether <port> ip dvmrp out-policy ""
```

where:
port is the number of the port and *""* are double quotes that indicate the policy used in the current session.

Configuration example

The following configuration example uses the above command to delete the DVMRP announce policy from a port. In this example, the announce policy currently set on port 1/5 is deleted.

```
8610:5/config/ether/1/5/ip/dvmrp# out-policy ""
```

Configuring DVMRP accept policies

This section includes the following tasks that describe how to set up your accept policy configuration using the command line interface:

Before you create and apply a DVMRP accept policy to the switch, you must perform the procedures provided in "Configuration prerequisites" on page 336.

Note: Deleting an accept policy from an interface, VLAN or port means that you change the configuration. It does not mean that you delete the policy itself.

To display DVMRP accept policy configuration information for an interface, VLAN, or port, refer to "Displaying DVMRP routing policy information" on page 380.

Creating a DVMRP accept policy

Before you can apply an accept policy to an interface, VLAN, or port, you must first create and configure the policy. An accept policy must be configured on an interface.

You can create one or more IP prefix lists and apply that list to any IP route policy. A prefix list with a 32 bit mask is equivalent to an address. A prefix list with a mask less than 32 bits can be used as a network. If you configure the MaskLenFrom field to be less than MaskLenUpto field, it can also be used as a range.

To create prefix list(s) of networks to be used by the DVMRP policy, use the following command:

```
config ip prefix-list <prefix-list-name>
```

where:
prefix-list-name indicates the name of the specified prefix list, which is a string length from 1 to 64.

This command includes the following parameters:

config ip prefix-list <*prefix-list-name*> followed by:	
`info`	Displays all of the prefixes in a given list.
`add-prefix <ipaddr/mask> [maskLenFrom <value>] [maskLenTo <value>]`	Adds a prefix entry to the prefix list. `<ipaddr/mask>` is the IP address and mask. `maskLenFrom <value>` is the lower bound of mask length. The default is the mask length. `maskLenTo <value>` is the higher bound mask length. The default is the mask length. **Note:** Lower bound and higher bound mask lengths together can define a range of networks.
`delete`	Deletes the prefix list.
`name <name>`	The name command is used to rename the specified prefix list. The name length can be from 1 to 64 characters.
`remove-prefix <ipaddr/mask>`	Removes a prefix entry from the prefix list. `ipaddr/mask>` is the IP address and mask.

To configure a DVMRP policy, use the following command:

`config ip route-policy <policy name> seq <seq number>`

where:
policy-name indicates the name of the specified policy, which is a string length from 1 to 64.
seq number indicates the number of the specified policy, which is a number from 1 to 65535.

Note: Not all of the `route-policy seq` parameters apply to the process of creating a DVMRP policy. The table below describes the parameters that you must use to create the DVMRP policy. For information on the other parameters for this command, refer to *Configuring IP Routing Operations*.

This command includes the following parameters:

config ip route-policy <policy name> seq <seq number> followed by:	
`action <permit|deny>`	Specifies the action to be taken when a policy is selected for a specific route. This can be permit or deny. Permit allows the route, deny ignores the route.
`create`	Creates a route policy with a policy name and a sequence number. Note: When creating a route policy in the CLI, the ID is internally generated using an automated algorithm. When you create a route policy in Device Manager, you can manually assign the ID number.
`disable`	Disables a route policy with a policy name and a sequence number.
`enable`	Enables a route policy with a policy name and a sequence number.
`match-protocol <protocol name>`	Matches the protocol through which the route is learned, if configured.

config ip route-policy <policy name> seq <seq number> followed by:	
match-metric <*metric*>	Matches the metric of the incoming advertisement or existing route against the specified value, if configured. If 0, then this field is ignored. • <*metric*> is 1 to 65535. The default is 0.
match-network <*prefix-list*>	Matches the destination network against the contents of the specified prefix list(s), if configured. • <*prefix-list*> specify the name of up to four defined prefix list by name separated by a comma.
match-next-hop <*prefix-list*>	Matches the previous hop IP address of the route against the contents of the specified prefix list, if configured. This field applies only to non-local routes. • <*prefix-list*> specify the name of up to four defined prefix list by name separated by a comma.
match-route-src <*prefix-list*>	Matches the previous hop IP address for DVMRP routes against the contents of the specified prefix list, if configured. • <*prefix-list*> specify the name of up to four defined prefix list by name separated by a comma.
name <*policy name*>	Renames a policy once it has been created. This command changes the name field for all sequence numbers under the given policy.
set-metric <*metric-value*>	Sets the metric value for the route while announcing a redistributing, if configured. The default is 0. If the default is configured, the original cost of the route is advertised into DVMRP.

Configuration example

The following configuration example uses the above commands to create a DVMRP accept policy. In this example, a single prefix list is created (prefix2) (refer to command line 1 below) and IP address 4.4.4.4/24 is added to the prefix list (refer command line 2 below). After the prefix list is created, the policy is configured (refer to command lines 3 through 7 below), the prefix list is applied to the match-network parameter of the DVMRP policy (refer to command line 8 below), and the new policy is applied to VLAN 5 (refer to command line 9).

```
1. 8610:5/config/vlan/5/ip# config ip prefix-list prefix2
2. 8610:5/config/ip/prefix-list/prefix2# add 4.4.4.4/24
3. 8610:5# config ip route-policy policy2
4. 8610:5/config/ip/route-policy/policy2# seq 1
5. 8610:5/config/ip/route-policy/policy2/seq/1# create
6. 8610:5/config/ip/route-policy/policy2/seq/1# action deny
7. 8610:5/config/ip/route-policy/policy2/seq/1# enable
8. 8610:5/config/ip/route-policy/policy2/seq/1# match-network
   prefix2
9. 8610:5/config/vlan/5/ip dvmrp in-policy policy2
```

Applying a DVMRP accept policy to an interface

To apply a DVMRP accept policy to an interface, use the following command:

```
config ip dvmrp interface <ipaddr> in-policy <policy name>
```

where:
ipaddr is the address of the interface and *policy name* is the name of the applicable accept policy you created.

Configuration example

The following configuration example uses the above command to apply a DVMRP accept policy to an interface. In this example, the announce policy named “policy2” is applied to interface 3.3.3.3.

```
8610:5/config/ip/dvmrp/interface/3.3.3.3# in-policy policy2
```

Deleting a DVMRP accept policy from an interface

To delete a DVMRP accept policy from an interface, use the following command:

```
config ip dvmrp interface <ipaddr> in-policy ""
```

where:
"" are double quotes that indicate the policy used in the current session.

Configuration example

The following configuration example uses the above command to delete the DVMRP accept policy from an interface. In this example, the accept policy currently set on interface 3.3.3.3 is deleted.

```
8610:5/config/ip/dvmrp/interface/3.3.3.3# in-policy ""
```

Applying a DVMRP accept policy to a VLAN

To apply a DVMRP accept policy to a VLAN, use the following command:

```
config vlan <vid> ip dvmrp in-policy <policy name>
```

where:
vid is the number of the VLAN and *policy name* is the name of the applicable accept policy you created.

Configuration example

The following configuration example uses the above command to apply a DVMRP accept policy to a VLAN. In this example, the announce policy named "policy2" is applied to VLAN 3.

```
8610:5/config/vlan/vlan3/ip/dvmrp# in-policy policy2
```

Deleting a DVMRP accept policy from a VLAN

To delete a DVMRP accept policy from a VLAN, use the following command:

```
config vlan <vid> ip dvmrp in-policy ""
```

where:
vid is the number of the VLAN and *""* are double quotes that indicate the policy used in the current session.

Configuration example

The following configuration example uses the above command to delete the DVMRP accept policy from a VLAN. In this example, the accept policy currently set on VLAN 3 is deleted.

```
8610:5/config/vlan/vlan3/ip/dvmrp# in-policy ""
```

Applying a DVMRP accept policy to a port

To apply a DVMRP accept policy to a port, use the following command:

```
config ether <port> ip dvmrp in-policy <policy name>
```

where:
port is the number of the port and *policy name* is the name of the applicable announce policy you created.

Configuration example

The following configuration example uses the above command to apply a DVMRP accept policy to a port. In this example, the announce policy named "policy2" is applied to port 1/5.

```
8610:5/config/ether/1/5/ip/dvmrp# in-policy policy2
```

Deleting a DVMRP accept policy from a port

To delete a DVMRP accept policy from a port, use the following command:

```
config ether <port> ip dvmrp in-policy ""
```

where:
port is the number of the port and *""* are double quotes that indicate the policy used in the current session.

Configuration example

The following configuration example uses the above command to delete the DVMRP accept policy from a port. In this example, the accept policy currently set on port 1/5 is deleted.

```
8610:5/config/ether/1/5/ip/dvmrp# in-policy ""
```

Configuring the advertisement of local network policies

This section includes the following tasks that describe how to configure the advertisement of local networks policy using the command line interface:

Before you apply the advertisement of local networks policy to the switch, you must perform the procedures provided in "Configuration prerequisites" on page 336.

To display DVMRP advertisement of local networks policy configuration information for an interface, VLAN, or port, refer to "Displaying DVMRP routing policy information" on page 380.

Applying the advertisement of local networks policy to an interface

To apply the advertisement of local networks to an interface, use the following command:

```
config ip dvmrp interface <ipaddr> advertise-self
```

where:
ipaddr is the address of the interface.

This command includes the following parameters:

config ip dvmrp interface <*ipaddr*> advertise-self followed by:	
`enable`	Enables the advertisement of local routes for the selected interface to other switches in the network.
`disable`	Disables the advertisement of local routes for the selected interface to other switches in the network.

Configuration example

The following configuration example uses the above command to disable the advertisement of local routes on interface 100.100.100.2. After configuring these parameters, use the **`info`** command to show a summary of the results:

```
8610:5/config/ip/dvmrp/interface/100.100.100.2# advertise-self
disable
8610:5/config/ip/dvmrp/interface/100.100.100.2# info

Sub-Context:
Current Context:

                      enable : true
                      metric : 1
               interface-type : passive
                    in-policy : N/A
                   out-policy : N/A
               advertise-self : disable
               default-listen : enable
               default-supply : disable
       default-supply-metric : 3
```

Applying the advertisement of local networks policy over a VLAN

To apply the advertisement of local networks to a VLAN, use the following command:

`config vlan <vid> ip dvmrp advertise-self`

where:
vid is the number of the VLAN.

This command includes the following parameters:

`config vlan <vid> ip dvmrp advertise-self` followed by:	
`enable`	Enables the advertisement of local routes over the selected VLAN to other switches in the network.
`disable`	Disables the advertisement of local routes over the selected VLAN to other switches in the network.

Configuration example

The following configuration example uses the above command to enable the advertisement of local routes on VLAN 100. After configuring these parameters, use the **`info`** command to show a summary of the results:

```
8610:5/config/vlan/100/ip/dvmrp# advertise-self enable
8610:5/config/vlan/100/ip/dvmrp# info

Sub-Context:
Current Context:

                       dvmrp : enable
                      metric : 1
               interface-type : active
                    in-policy : N/A
                   out-policy : N/A
               advertise-self : enable
               default-listen : enable
               default-supply : disable
        default-supply-metric : 3
```

Applying the advertisement of local networks policy over a port

To apply the advertisement of local networks to a port, use the following command:

`config ether <port> ip dvmrp advertise-self`

where:
`port` is the number of the port.

This command includes the following parameters:

`config ether <port> ip dvmrp advertise-self` followed by:	
`enable`	Enables the advertisement of local routes over the selected port to other switches in the network.
`disable`	Disables the advertisement of local routes over the selected port to other switches in the network.

Configuration example

The following configuration example uses the above command to disable the advertisement of local routes on port 9 of the card in slot 1. After configuring these parameters, use the **`info`** command to show a summary of the results:

```
8610:5/config/ethernet/1/9/ip/dvmrp# advertise-self disable
8610:5/config/ethernet/1/9/ip/dvmrp# info

Sub-Context:
Current Context:

                       dvmrp : enable
                      metric : 1
               interface-type : active
                    in-policy : N/A
                   out-policy : N/A
               advertise-self : disable
               default-listen : enable
               default-supply : disable
        default-supply-metric : 3
```

Configuring a DVMRP interface type

This section includes the following tasks that describe how to configure an interface type using the command line interface:

Before you apply the DVMRP passive interface policy to the switch, you must perform the procedures provided in "Configuration prerequisites" on page 336.

To display DVMRP interface type configuration information for an interface, VLAN, or port, refer to "Displaying DVMRP routing policy information" on page 380.

Creating a passive interface

To create a passive interface, use the following command:

```
config ip dvmrp interface <ipaddr> create
```

where:
ipaddr is the address of the interface.

This command includes the following parameters:

config ip dvmrp interface <*ipaddr*> create followed by:	
passive	Interface drops all types of incoming DVMRP packets from neighbors and will not send out any probes or route reports to its neighbor switches.
active	Interface receives all types of incoming DVMRP packets from neighbors and sends out any probes or route reports to its neighbor switches.

Configuration example

The following configuration example uses the above command to create a passive interface named 100.100.100.2. After configuring these parameters, use the **`info`** command to show a summary of the results.

```
8610:5/config/ip/dvmrp/interface/100.100.100.2# create passive
8610:5/config/ip/dvmrp/interface/100.100.100.2# info

Sub-Context:
Current Context:

                      enable : true
                      metric : 1
              interface-type : passive
                   in-policy : N/A
                  out-policy : N/A
              advertise-self : disable
              default-listen : enable
              default-supply : disable
      default-supply-metric : 3
```

Configuring an active or passive interface type

To configure an interface as active or passive, use the following command:

`config ip dvmrp interface <`*`ipaddr`*`> interface-type`

where:
`ipaddr` is the address of the selected interface.

This command includes the following parameters:

`config ip dvmrp interface <`*`ipaddr`*`> interface-type` followed by:	
`passive`	Interface drops all types of incoming DVMRP packets from neighbors and will not send out any probes or route reports to its neighbor switches.
`active`	Interface receives all types of incoming DVMRP packets from neighbors and sends out any probes or route reports to its neighbor switches.

Configuration example

The following configuration example uses the above command to set interface 100.100.100.2 active. After configuring these parameters, use the **info** command to show a summary of the results.

```
8610:5/config/ip/dvmrp/interface/100.100.100.2# interface-type
active
8610:5/config/ip/dvmrp/interface/100.100.100.2# info

Sub-Context:
Current Context:

                      enable : true
                      metric : 1
               interface-type : active
                    in-policy : N/A
                   out-policy : N/A
               advertise-self : disable
               default-listen : enable
               default-supply : disable
       default-supply-metric : 3
```

Configuring an active or passive VLAN type

To configure a VLAN interface as active or passive, use the following command:

```
config vlan <vid> ip dvmrp interface-type
```

where:
vid is a VLAN ID from 1 to 4092.

This command includes the following parameters:

config vlan <*vid*> ip dvmrp interface-type followed by:	
passive	Interface drops all types of incoming DVMRP packets from neighbors and will not send out any probes or route reports to its neighbor switches.
active	Interface receives all types of incoming DVMRP packets from neighbors and sends out any probes or route reports to its neighbor switches.

Configuration example

The following configuration example uses the above command to set VLAN 100 passive. After configuring these parameters, use the **info** command to show a summary of the results.

```
8610:5/config/vlan/100/ip/dvmrp# interface-type active
8610:5/config/vlan/100/ip/dvmrp# info

Sub-Context:
Current Context:

                      dvmrp : enable
                     metric : 1
              interface-type : passive
                   in-policy : N/A
                  out-policy : N/A
              advertise-self : disable
              default-listen : enable
              default-supply : disable
       default-supply-metric : 3
```

Configuring an active or passive port type

To configure a port interface as active or passive, use the following command:

```
config ethernet <port> ip dvmrp interface-type
```

where:
port is the number of the port.

This command includes the following parameters:

config ethernet <*port*> ip dvmrp interface-type followed by:	
passive	Interface drops all types of incoming DVMRP packets from neighbors and will not send out any probes or route reports to its neighbor switches.
active	Interface receives all types of incoming DVMRP packets from neighbors and sends out any probes or route reports to its neighbor switches.

Configuration example

The following configuration example uses the above command to set port 9 in slot 1 is set as active. After configuring these parameters, use the **info** command to show a summary of the results.

```
8610:5/config/ethernet/1/9/ip/dvmrp# interface-type active
8610:5/config/ethernet/1/9/ip/dvmrp# info

Sub-Context:
Current Context:

                      dvmrp : enable
                     metric : 1
              interface-type : active
                   in-policy : N/A
                  out-policy : N/A
              advertise-self : disable
              default-listen : enable
              default-supply : disable
       default-supply-metric : 3
```

Displaying DVMRP routing policy information

This section describes the procedures for displaying DVMRP configuration information for an interface, VLAN, and port.

Displaying DVMRP routing policy information for an interface

To display DVMRP route policy information for the DVMRP interface configuration(s) on the switch, use the following command:

```
show ip dvmrp interface
```

Figure 138 shows sample output for the **`show ip dvmrp interface`** command.

Figure 138 DVMRP interface configuration information

```
8610:5/config/vlan/3/ip# show ip dvmrp interface

================================================================================
                          Dvmrp Interface
================================================================================
                                        DEFAULT DEFAULT DEFAULT ADVERTISE
IF        ADDR            METRIC OPERSTAT LISTEN  SUPPLY  METRIC  SELF
--------------------------------------------------------------------------------
Port1/1   192.32.96.18    1      down     enable  disable 1       enable
Vlan2     10.10.10.10     1      down     enable  disable 1       enable
Vlan3     3.3.3.3         1      down     enable  disable 1       enable
--------------------------------------------------------------------------------
IF        ADDR            IN-POLICY       OUT-POLICY      INTF TYPE
--------------------------------------------------------------------------------
Port1/1  192.32.96.18                                     Active
Vlan2    10.10.10.10                                      Active
Vlan3    3.3.3.3                                          Active
```

Displaying DVMRP routing policy information for a VLAN

To display DVMRP route policy information for the DVMRP VLAN configuration(s) on the switch, use the following command:

```
show vlan info dvmrp [<vid>]
```

where:
vid is a VLAN ID from 1 to 4092.

Figure 139 shows sample output for the **show vlan info dvmrp** command.

Figure 139 DVMRP VLAN configuration information

```
8610:5> show vlan info dvmrp

================================================================================
                              Vlan Ip Dvmrp
================================================================================
VLAN  DVMRP            DEFAULT DEFAULT DEFAULT ADVERTISE
ID    ENABLE  METRIC   LISTEN  SUPPLY  METRIC  SELF
--------------------------------------------------------------------------------
1     disable 1        enable  disable 1       enable
3     enable  1        enable  disable 1       enable
10    disable 1        enable  disable 1       enable
100   enable  1        enable  disable 3       disable
200   disable 1        enable  disable 1       enable
```

Displaying DVMRP routing policy information for a port

To display DVMRP route policy information for the DVMRP port configuration(s) on the switch, use the following command:

```
show ports info dvmrp [<ports>]
```

Figure 140 shows sample output for the **show ports info dvmrp** command.

Figure 140 DVMRP port configuration information

```
8610:5> show ports info dvmrp

================================================================================
                              Port Ip Dvmrp
================================================================================
PORT  DVMRP            DEFAULT DEFAULT DEFAULT ADVERTISE
NUM   ENABLE  METRIC   LISTEN  SUPPLY  METRIC  SELF
--------------------------------------------------------------------------------
1/1   disable 1        enable  disable 1       enable
1/2   disable 1        enable  disable 1       enable
1/3   disable 1        enable  disable 1       enable
1/4   disable 1        enable  disable 1       enable
1/5   disable 1        enable  disable 1       enable
1/6   disable 1        enable  disable 1       enable
1/7   disable 1        enable  disable 1       enable
1/8   disable 1        enable  disable 1       enable
1/9   disable 1        enable  disable 1       enable
1/10  disable 1        enable  disable 1       enable
1/11  disable 1        enable  disable 1       enable
1/12  disable 1        enable  disable 1       enable
1/13  disable 1        enable  disable 1       enable
1/14  disable 1        enable  disable 1       enable
1/15  disable 1        enable  disable 1       enable
1/16  disable 1        enable  disable 1       enable
1/17  disable 1        enable  disable 1       enable
1/18  disable 1        enable  disable 1       enable
1/19  disable 1        enable  disable 1       enable
1/20  disable 1        enable  disable 1       enable
1/21  disable 1        enable  disable 1       enable
3/1   disable 1        enable  disable 1       enable
3/2   disable 1        enable  disable 1       enable
3/3   disable 1        enable  disable 1       enable
3/4   disable 1        enable  disable 1       enable
3/5   disable 1        enable  disable 1       enable
3/6   disable 1        enable  disable 1       enable
```

Displaying all IP DVMRP show commands

The **show ip dvmrp show-all** command displays all relevant IP DVMRP information.

The command uses the syntax:

```
show ip dvmrp show-all [file <value>]
```

where <*value*> is the filename to which the output will be redirected.

Figure 141 shows sample output for the **show ip dvmrp show-all** command.

Figure 141 show ip dvmrp show-all command output

```
Passport-8610:5# show ip dvmrp show-all

# show ip dvmrp info

================================================================
                                      Dvmrp General Group
================================================================
AdminStat               : disabled
Genid                   : 0
Version                 : (null)
NumRoutes               : 0
NumReachableRoutes      : 0

UpdateInterval          : 60
TriggeredUpdateInterval : 5
LeafTimeOut             : 125
NbrTimeOut              : 35
NbrProbeInterval        : 10
FwdCacheTimeout         : 300
RouteExpireTimeout      : 140
RouteDiscardTimeout     : 260
RouteSwitchTimeout      : 140
ShowNextHopTable        : disable

# show ip dvmrp interface

================================================================
                                      Dvmrp Interface
================================================================
IF        ADDR            METRIC     OPERSTAT   ADVSELF
----------------------------------------------------------------
Vlan1     128.1.1.2       1          down       enable
```

Chapter 11
Configuring PIM using the CLI

This chapter describes the commands used to configure PIM on your Passport 8000 Series switch. There are two PIM modes, sparse mode (SM) and source specific multicast (SSM). The following section describes PIM-SM. For information on PIM-SSM, refer to "Configuring Source Specific Multicast (SSM)" on page 429.

Protocol Independent Multicast-Sparse Mode (PIM-SM) supports multicast groups that are spread out across large areas of a company or on the Internet.

- What makes PIM-SM protocol-independent? — PIM-SM does not maintain its own or depend on a specific multicast protocol to maintain unicast routing tables. PIM-SM uses the routing table information from any underlying unicast routing protocol, such as RIP or OSPF.
- How does it multicast? — PIM-SM sends one stream of data to the network where it is replicated to all interested receivers.
- What is sparse mode? — Instead of using a "push" model. PIM-SM uses a "pull" model in which receivers pull down multicast traffic. For sparsely populated networks, PIM-SM is more efficient than dense-mode protocols because it sends multicast traffic only to those routers that belong to a specific multicast group and that choose to receive the traffic.

The 8000 Series switches support the following for PIM-SM:

- RP functionality
- Redundant RP configuration where several RPs can be configured for the same group(s)
- RP load sharing where several RPs can be configured in the same PIM domain
- BSR functionality
- Redundant BSR functionality

- MBR functionality to connect a PIM-SM domain to a DVMRP domain. When you configure an 8000 Series switch with MBR functionality, you can have some interfaces running PIM-SM and other interfaces running DVMRP to interconnect a PIM-SM domain to a DVMRP domain.

For more information about PIM concepts and terminology, see Chapter 1, "IP Multicast concepts."

For instructions on how to configure PIM static source groups, refer to Chapter 13, "Viewing and editing multicast routes using the CLI."

This chapter includes the following topics:

Roadmap of PIM commands

The following roadmap lists all the PIM commands and their parameters. After using the commands below to configure the Passport 8600, you can use the show commands to display information for a particular feature.

To facilitate troubleshooting, the Passport 8600 also provides *one* command (`show ip pim show-all`) that lists all the show commands for IP PIM and displays their configuration output. See "Displaying all IP PIM show commands" on page 433.

Use this list as a quick reference or click on any entry for more information:

Command	Parameter
`config ip pim`	`info`
	`disable`
	`enable`
	`mode <sparse|ssm>`
	`bootstrap-period <integer>`
	`c-rp-adv-timeout <integer>`
	`disc-data-timeout <integer>`
	`activity-chk-interval <integer>`
	`joinprune-interval <integer>`
	`register-suppression-timeout <integer>`
	`unicast-route-change-timeout <integer>`
`show ip pim info`	
`config ip pim mbr`	`info`
	`disable`
	`enable`

Command	Parameter
config ip pim interface <ipaddr>	info
	create <active|passive>
	disable
	enable
	hellointerval <seconds>
	interface-type <active|passive>
	joinprune-interval <seconds>
show ip pim interface	
show ip pim neighbor	
config ip pim candbsr interface <ipaddr>	info
	enable preference <value>
	disable
config ip pim candrp	info
	add grp <ipaddr> mask <ipmask> rp <ipaddr>
	delete grp <ipaddr> mask <ipmask>
show ip pim rp-set	
show ip pim candidate-rp	
show ip pim active-rp <group>	
show ip pim active-rp	
show ip pim bsr	
show ip pim mroute	
config ip pim static-rp	info
	add grp <ipaddr> mask <ipmask> rp <ipaddr>
	delete grp <ipaddr> mask <ipmask> rp <ipaddr>

Command	Parameter
	disable
	enable
show ip pim static-rp	
config ethernet <ports> ip pim	info
	disable
	create <active|passive>
	enable
	hellointerval <seconds>
	interface-type <active|passive>
	joinprune-interval <seconds>
config ethernet <ports> ip pim candbsr	info
	enable preference <value>
	disable
config vlan <vid> ip pim	info
	disable
	create <active|passive>
	enable
	hellointerval <seconds>
	interface-type <active|passive>
	joinprune-interval <seconds>
config vlan <vid> ip pim candbsr	info
	enable preference <value>
	disable

Command	Parameter
config ip pim debug-pimmsg	info
	assert <true=1|false=2>
	bstrap <true=1|false=2>
	group <ipaddress>
	hello <true=1|false=2>
	joinprune <true=1|false=2>
	pimdbgtrace <true=1|false=2>
	pimdbglog <true=1|false=2>
	register <true=1|false=2>
	regstop <true=1|false=2>
	rp-adv <true=1|false=2>
	send <true=1|false=2>
	rcv <true=1|false=2>
	source <ipaddress>
show ip pim show-all [file <value>]	

PIM-SM configuration prerequisites

Before you can configure PIM-SM, you must prepare the switch as follows:

1. Configure an IP interface. For information, refer to *Configuring IP Routing Operations*.
2. Disable DVMRP from the interface on which you want to configure PIM-SM because you cannot configure PIM-SM and DVMRP on the same interface. For information, refer to Chapter 10, "Configuring DVMRP using the CLI."

Note: Changing the configuration from PIM to DVMRP, or from DVMRP to PIM, is not recommended while multicast traffic is flowing on the network.

   a. A *switch* can have a mix of DVMRP and PIM-SM interfaces if it is configured as an multicast border router (MBR).

   b. An *interface* can only be configured with one multicast routing protocol at a time (PIM-SM or DVMRP).

3. Configure a unicast protocol (RIP or OSPF) globally and on the interfaces where you want to configure PIM-SM. For information on RIP and OSPF, refer to *Configuring IP Routing Operations*.

   PIM-SM requires a unicast protocol to use in order to multicast traffic within the network when performing the Reverse Path Forwarding (RFP) check. PIM-SM uses the information from the unicast routing table to create and maintain the shared and shortest multicast tree that enables PIM-enabled routers to communicate. The unicast routing table must contain a route to every multicast source in the network as well as routes to PIM entities like the RPs and BSR.

4. To configure PIM-SM on an 8000 Series switch, the following configurations are required:

   - Enable PIM-SM globally.

   - Enable PIM-SM on individual interfaces.

   - Configure one or several RPs for the groups that will be used by a multicast application in the network.

- Configure one or several BSRs to propagate RP information to all switches in the network.

-If connecting a PIM-SM domain to a DVMRP domain, configure the switch interconnecting the domains as an MBR switch with the corresponding PIM-SM interfaces enabled with PIM-SM, and DVMRP interfaces enabled with DVMRP.

Note: Routes to sources in a PIM domain should not have a lower cost through the DVMRP domain in order for multicast routing from these sources to work properly. MBR switches should be configured with this design guideline in mind.

Configuring PIM-SM globally

To enable or disable PIM-SM globally on the switch, use the following command:

```
config ip pim
```

This command includes the following parameters:

config ip pim followed by:	
`info`	Displays current PIM settings on the switch.
`disable`	Globally disables PIM on the switch.
`enable`	Globally enables PIM on the switch.
`mode <sparse|ssm>`	The configured mode of this interface: sparse or ssm (source-specific multicast).[1]
`bootstrap-period <integer>`	Specifies the interval (in seconds) that the elected BSR waits between originating bootstrap messages. • *integer* is a number in the range from 5 to 32757. The default is 60.
`c-rp-adv-timeout <integer>`	Specifies how often (in seconds) that routers configured as candidate RPs send C-RP advertisement messages. When this timer expires, the C-RP sends an advertisement message to the elected BSR. • *integer* is a number in the range from 5 to 26214. The default is 60.

config ip pim followed by:	
`disc-data-timeout <integer>`	Specifies how long (in seconds) to discard data until the Join is received from the RP. An ipmc discard record is created after a register packet is sent until the the timer expires and/or when a Join is received. • *integer* is a number in the range from 5 to 65535. The default is 60.
`activity-chk-interval <integer>`	Specifies how often (in seconds) to check traffic activity for a multicast group. The lower the value means the more often the switch checks the activity. • *integer* is 15, 30 or 210. The default is 30. **Notes:** • Before you can change the activity-chk-interval, you have to disable PIM globally. • Nortel Networks recommends an activity check interval of 30 seconds. • On IGAP-enabled interfaces, set the activity check interval to 30 seconds or less. • On non-IGAP enabled interfaces, you may want to set the activity check interval to 210 seconds for systems that have a large number (200+) of S,G streams.
`joinprune-interval <integer>`	Specifies how long to wait (in seconds) before the PIM router sends out the next join/prune message to its upstream neighbors. • *integer* is a number in the range from 1 to 18724. The default is 60.
`register-suppression-timeout <integer>`	Specifies how long (in seconds) the DR suppresses sending registers to the RP. The timer starts when the DR receives a Register Stop message from the RP. • *integer* is a number in the range from 6 to 65535. The default is 60.
`unicast-route-change-timeout <integer>`	Specifies how often (in seconds) the switch polls the routing table manager (RTM) for unicast routing information updates to be used by PIM. **Note:** Lowering this value increases how often the switch polls the RTM. This may affect the switch's performance, especially when there's a lot of traffic flowing through the switch. • *integer* is a number in the range from 2 to 65535. The default is 5.

1 To enable PIM-SSM globally, see "Configuring PIM-SSM globally" on page 431." Also note that when you change from one mode to another, an information message pops up to remind you that traffic will not stop immediately.

Figure 142 shows sample output for the **`config ip pim info`** command.

Figure 142 config ip pim info command output

```
8610:5/config/ip/pim# info

Sub-Context: mbr candbsr interface candrp debug-pimmsg static-rp
Current Context:

                            enable : true
                  global mode : ssm
                               mbr : Disabled
             activity-chk-interval : 30
                  bootstrap-period : 60
                  c-rp-adv-timeout : 60
               discard-data-timeout : 60
                  reg-suppr-timeout : 60
          uni-route-change-timeout : 5
                joinprune-interval : 60

8610:5/config/ip/pim# ac
```

Showing PIM group information

To display the global status of PIM on the switch, use the following command:

```
show ip pim info
```

Figure 143 shows sample output for this command.

Figure 143 show ip pim info command output

```
Hollywood:5# show ip pim info

================================================================
                        Pim General Group
================================================================
PimStat                : enabled
Mode                   : ssm
Mbr                    : disabled
StaticRP               : disabled
ActivityChkInterval    : 30
BootstrapPeriod        : 60
CRPAdvTimeout          : 60
DiscDataTimeout        : 60
RegSupprTimeout        : 60
UniRouteChangeTimeout  : 5
JoinPruneInt           : 60
```

Configuring a PIM multicast border router (PMBR)

PIM multicast border routers (PMBRs) connect PIM domains to other multicast routing domains and the rest of the Internet. The MBR functionality on an 8000 Series switch allows the interconnection of a PIM-SM domain to a DVMRP domain.

To configure the switch as a PMBR, use the following command:

```
config ip pim mbr
```

This command includes the following parameters:

config ip pim mbr followed by:	
info	Displays the current PMBR configuration setting.
disable	Disables PMBR on the switch.
enable	Enables PMBR on the switch.

Configuring PIM on an interface

When you enable PIM on a particular interface, you must also enable it globally. Otherwise, PIM will not work. See "Configuring PIM-SM globally" on page 392.

To configure PIM on a specific interface, use the following command:

```
config ip pim interface <ipaddr>
```

where:
ipaddr indicates the IP address of the selected interface.

This command includes the following parameters:

config ip pim interface <*ipaddr*> followed by:	
`info`	Displays current PIM configuration settings on the local switch interface.
`create <active|passive>`	Enables PIM on a specific interface with a specific type. An active interface allows PIM control traffic to be transmitted and received. A passive interface prevents PIM control traffic from being transmitted or received, thereby reducing the load on a system. This feature is useful when there is a high number of PIM interfaces and these interfaces are connected to end users; not to other switches.
`disable`	Disables PIM on the local switch interface.
`enable`	Enables PIM on the local switch interface.
`hellointerval <seconds>`	Specifies how long to wait (in seconds) before the PIM switch sends out the next hello message to neighboring switches. The default is 30 seconds.
`interface-type <active|passive>`	Specifies whether the selected interface is active or passive. See `create <active|passive>` for a description of active and passive interfaces. `interface-type` allows you to change the state of a PIM interface after it's been created. It can be changed only when PIM is disabled on the specified interface.
`joinprune-interval <seconds>`	Specifies how long to wait (in seconds) before the PIM switch sends out the next join/prune message to its upstream neighbors. The default is 60 seconds.

Configuration example

The following example shows how to create a PIM passive interface and display information about that interface.

```
8610:5/config/ip/pim# interface 128.3.1.1 create passive
8610:5/config/ip/pim/interface/128.3.1.1# info

Sub-Context:
Current Context:

                      enable : true
                        mode : sparse
              interface-type : passive
                joinpruneint : 60
                    cbsrpref : -1 (disabled)

8610:5/config/ip/pim#
```

Changing the interface type

Before changing the interface type, you must first disable PIM on the interface. Use the following commands to change the interface type from active to passive:

```
config ip pim interface <ipaddr> disable
config ip pim interface <ipaddr> interface-type passive
config ip pim interface <ipaddr> enable
```

Showing PIM interface information

To display information about the PIM-SM interface setup on the switch, use the following command:

```
show ip pim interface
```

Figure 144 shows sample output for this command.

Figure 144 show ip pim interface command output

```
8010:5# show ip pim inter

================================================================================================================================
                                        Pim Interface
================================================================================================================================
IF        ADDR            MASK            MODE       DR              HLINT  JPINT  CBSPR          OPSTAT INTF TYPE
--------------------------------------------------------------------------------------------------------------------------------
Vlan41    152.31.16.66    255.255.255.240 ssm        152.31.16.66    30     60     -1  (disabled)  up     active
Vlan42    152.31.24.66    255.255.255.240 ssm        152.31.24.66    30     60     -1  (disabled)  up     active
Vlan51    152.31.28.1     255.255.255.224 ssm        152.31.28.1     30     60     -1  (disabled)  up     active
Vlan52    152.31.28.33    255.255.255.224 ssm        152.31.28.33    30     60     -1  (disabled)  up     active
Vlan53    152.31.28.65    255.255.255.224 ssm        152.31.28.65    30     60     -1  (disabled)  up     active
Vlan61    152.31.28.97    255.255.255.224 ssm        0.0.0.0         30     60     -1  (disabled)  down   active
Vlan62    152.31.28.129   255.255.255.224 ssm        0.0.0.0         30     60     -1  (disabled)  down   active
Vlan1001  146.1.1.254     255.255.255.0   ssm        146.1.1.254     768    60     -1  (disabled)  up     active
Vlan1002  146.1.2.254     255.255.255.0   ssm        146.1.2.254     512    60     -1  (disabled)  up     active

8010:5#
```

Table 65 describes the **`show ip pim interface`** parameters.

Table 65 show ip pim interface parameters

Field	Description
IF	The slot/port number or VLAN ID of the interface on which PIM is enabled.
ADDR	The IP address of the PIM interface.
MASK	The network mask for the IP address of the PIM interface.
MODE	The configured mode of this interface. The valid modes are SSM and Sparse.
DR	Shows the designated router (DR) for this interface.
HLINT	Specifies how long to wait (in seconds) before the PIM switch sends out the next hello message to neighboring switches. The default hello interval is 30 seconds.
JPINT	Specifies how long to wait (in seconds) before the PIM switch sends out the next join/prune message to its upstream neighbors. The default join/prune interval is 60 seconds.
CBSPR	The preference for this local interface to become a Candidate BSR. The Candidate BSR with the highest BSR-priority and address is referred to as the preferred BSR. The default is -1, which indicates that the current interface is not a Candidate BSR.
OPSTAT	Indicates the status of PIM on this interface: up or down.
INTF TYPE	Indicates whether the PIM interface is active or passive.

Showing PIM neighbor information

To display information about the neighboring routers configured with PIM-SM, use the following command:

```
show ip pim neighbor
```

Figure 145 shows sample output for this command.

Figure 145 show ip pim neighbor command output

```
================================================================
=
                        Pim Neighbor
================================================================
INTERFACE       ADDRESS                 UPTIME           EXPIRE
----------------------------------------------------------------
160             155.110.125.22          15h:19m:56s      102
```

Table 66 describes the Pim Neighbor parameters.

Table 66 show ip pim neighbor parameters

Field	Description
INTERFACE	The slot/port number or VLAN ID of the interface used to reach this PIM neighbor.
ADDRESS	The IP address of the PIM neighbor for which this entry contains information.
UPTIME	The elapsed time since this PIM neighbor last became a neighbor of the local router.
EXPIRE	The time remaining before this PIM neighbor times out.

Configuring a candidate BSR on an interface

PIM-SM cannot run without a bootstrap router (BSR). Although a PIM-SM domain can have only one active BSR, you can configure additional routers as candidate BSRs (C-BSRs). C-BSRs provide backup protection in case the primary BSR fails.

The C-BSR with the highest configured preference becomes the BSR for the domain. If two C-BSRs have equal preference, the candidate with the higher IP address becomes the BSR. If you add a new C-BSR with a higher preference to the domain, it automatically becomes the new BSR.

To configure a candidate BSR on a specific interface, use the following command:

```
config ip pim candbsr interface <ipaddr>
```

where:
ipaddr indicates the IP address of the selected interface.

This command includes the following parameters:

config ip pim candbsr interface <*ipaddr*> followed by:	
`info`	Displays the candidate BSR preference setting for this interface (Figure 146).
`enable preference <value>`	Enables the Candidate BSR on this interface and sets its preference value to become a BSR. The Candidate BSR with the highest BSR preference and address is referred to as the preferred BSR. The default is -1, which indicates that the current interface is not a Candidate BSR.
`disable`	Disables the Candidate BSR on this interface.

Figure 146 config ip pim candbsr interface command output

```
8610:5/config/ip/pim/candbsr/interface 2.2.2.2# info

Sub-Context:
Current Context:

            cbsr preference : -1  (disabled)
```

Configuring a candidate rendezvous point (C-RP)

To configure a rendezvous point (RP) in the RP set, use the following command:

```
config ip pim candrp
```

This command includes the following parameters:

config ip pim candrp followed by:	
`info`	Displays current RP configuration settings on the local router interface.
`add grp <ipaddr> mask <ipmask> rp <ipaddr>`	Adds a candidate RP to the RP set. • `add grp <ipaddr>` - The IP address of the multicast group. When combined with the group mask, it identifies the prefix that the local router uses to advertise itself as a C-RP. • `mask <ipmask>` - The address mask of the multicast group. When combined with the group address, it identifies the prefix that the local router uses to advertise itself as a C-RP. • `rp <ipaddr>` - The IP address of the C-RP. This address has to be one of the local PIM-SM enabled interfaces.
`delete grp <ipaddr> mask <ipmask>`	Deletes a candidate RP from the RP set. • `delete` • `grp <ipaddr>` - The IP address of the multicast group. When combined with the group mask, it identifies the prefix that the local router uses to advertise itself as a C-RP. • `mask <ipmask>` - The address mask of the multicast group. When combined with the group address, it identifies the prefix that the local router uses to advertise itself as a C-RP.

You can only configure one interface on an 8000 Series switch for multiple groups, that is, you cannot configure multiple interfaces for multiple groups.

The `mask` value allows you to configure a candidate RP for several groups in one configuration. For example, a candidate RP configuration with a group address of 224.0.0.0 and a group mask of 240.0.0.0 allows you to configure the candidate RP for a multicast range from 224.0.0.0 to 239.255.255.255.

Showing rendezvous point (RP) set information

To display information about the rendezvous points (RPs) for this PIM-SM domain, use the following command:

```
show ip pim rp-set
```

Figure 147 shows sample output for this command.

Figure 147 show ip pim rp-set command output

```
================================================================================
                                Pim RPSet
================================================================================
GRPADDRESS    GRPMASK       ADDRESS       COMPONENT     HOLDTIME      EXPTIME
--------------------------------------------------------------------------------
224.0.0.0     240.0.0.0     192.60.60.1      0            150           107
```

Table 67 describes the Pim RPSet parameters.

Table 67 show ip pim rp-set parameters

Field	Description
GRPADDRESS	The IP address of the multicast group. When combined with the group mask, it identifies the prefix that the local router uses to advertise itself as a C-RP.
GRPMASK	The address mask of the multicast group. When combined with the group address, it identifies the prefix that the local router uses to advertise itself as a C-RP.
ADDRESS	The IP address of the C-RP.
COMPONENT	A unique number identifying the protocol instance connected to each PIM domain.
HOLDTIME	The time specified in a C-RP advertisement that the BSR uses to time out the RP. When the BSR receives an advertisement for the RP, it restarts the timer. If no advertisement arrives before the timer expires, the BSR removes that RP from the RP set.
EXPTIME	The time remaining before this C-RP times out.

Showing candidate RP information

To display information about the candidate rendezvous points (C-RPs) for this PIM-SM domain, use the following command:

```
show ip pim candidate-rp
```

Figure 148 shows sample output for this command.

Figure 148 show ip pim candidate-rp command output

```
================================================================
                Pim Candidate RP Table
================================================================
GRPADDR             GRPMASK             RPADDR
----------------------------------------------------------------
228.1.1.1           255.255.255.0       128.125.202.1
```

Table 68 describes the Pim Candidate RP Table parameters.

Table 68 show ip pim candidate-rp parameters

Field	Description
GRPADDR	The IP address of the multicast group. When combined with the group mask, it identifies the prefix that the local router uses to advertise itself as a C-RP.
GRPMASK	The address mask of the multicast group. When combined with the group address, it identifies the prefix that the local router uses to advertise itself as a C-RP.
RPADDR	The IP address of the C-RP. This address has to be one of the local PIM-SM enabled interfaces.

Showing the active RP for a specific group

To display information about the active rendezvous point (RP) for a specific group, use the following command:

```
show ip pim active-rp <group>
```

Figure 149 shows sample output for this command.

Figure 149 show ip pim active-rp 228.1.2.3 command output

```
8610# show ip pim active-rp 228.1.2.3
================================================================
                Pim Grp->RP Active RP Table
================================================================
GRPADDR             RP-ADDR             RP-PRIORITY
----------------------------------------------------------------
228.1.2.3           192.60.60.1          0
```

Table 69 describes the Pim Grp->RP Active RP Table parameters.

Table 69 show ip pim active-rp <group> parameter

Field	Description
GRPADDR	The IP address of the multicast group. When combined with the group mask, it identifies the prefix that the local router uses to advertise itself as a C-RP.
RP-ADDR	The IP address of the C-RP. This address has to be one of the local PIM-SM enabled interfaces.
RP-PRIORITY	The priority of the RP. C-RPs should send C-RP advertising messages with this field set to ‘0’, which is the highest priority.

Showing the active RP for all groups

To display information about the active rendezvous point (RP) for all the running multicast groups on the switch, use the following command:

```
show ip pim active-rp
```

Figure 150 shows sample output for this command.

Figure 150 show ip pim candidate-rp command output

```
================================================================
                Pim Grp->RP Active RP Table
================================================================
GRPADDR             RP-ADDR             RP-PRIORITY
----------------------------------------------------------------
225.2.1.67          192.60.60.1          0
```

Table 70 describes the Pim Grp->RP Active RP Table parameters.

Table 70 show ip pim active-rp parameters

Field	Description
GRPADDR	The IP address of the multicast group. When combined with the group mask, it identifies the prefix that the local router uses to advertise itself as a C-RP.
RP-ADDR	The IP address of the C-RP. This address has to be one of the local PIM-SM enabled interfaces.
RP-PRIORITY	The priority of the RP. C-RPs should send C-RP advertising messages with this field set to ‘0’, which is the highest priority.

Showing bootstrap router (BSR) information

To display information about the bootstrap router (BSR) for this PIM-SM domain, use the following command:

```
show ip pim bsr
```

Figure 151 shows sample output for this command.

Figure 151 show ip pim bsr command output

```
================================================================
             Current BootStrap Router Info
================================================================
Current BSR address: 192.60.60.1
Current BSR priority: 100
Current BSR HashMask: 255.255.255.252
Current BSR Fragment Tag: 984
Pim Bootstrap Timer: 44
```

Table 71 describes the Current BootStrap Router Info parameters.

Table 71 show ip pim bsr parameters

Field	Description
Current BSR address	The IP address of the current BSR for the local PIM domain.
Current BSR priority	The priority of the current BSR. The Candidate BSR (C-BSR) with the highest BSR-priority and address (referred to as the preferred BSR) is elected as the BSR for the domain.
Current BSR HashMask	The mask used in the hash function to map a group to one of the C-RPs from the RP-Set. The hash-mask allows a small number of consecutive groups (e.g., 4) to always hash to the same RP.
Current BSR Fragment Tag	A randomly generated number that distinguishes fragments belonging to different Bootstrap messages. Fragments belonging to the same Bootstrap message carry the same ‘Fragment Tag’.
Pim Bootstrap Timer	When the Bootstrap Timer expires, the BSR sends out Bootstrap messages.

Showing PIM route information

To display information from the route table, use the following command:

```
show ip pim mroute
```

Figure 152 shows sample output for this command.

Figure 152 show ip pim mroute command output

```
================================================================================
                              Pim Multicast Route
================================================================================
Src: 0.0.0.0       Grp: 225.2.1.67   RP: 192.60.60.1 Upstream: NULL
Flags: WC RP CACHE
Incoming  Port: Vlan0-cpp,
Outgoing Ports: Vlan2-1/15, Vlan3-1/17,
Joined   Ports: Vlan2-1/15, Vlan3-1/17,
Pruned   Ports:
Leaf     Ports:
Asserted Ports:
Prune Pending Ports:
Assert Winner Ifs:
Assert Loser Ifs:
TIMERS:  Entry   JP   RS  Assert VIFS:  0  1  2  3
           181     0    0    0          0  181  165  0
                       AssertVifTimer:  0  0  0  0
--------------------------------------------------------------------------------
Src: 172.20.20.3   Grp: 225.2.1.67   RP: 192.60.60.1 Upstream: NULL
 Flags: SPT CACHE SG
 Incoming  Port: Port1/47  ,
 Outgoing Ports: Vlan2-1/15, Vlan3-1/17,
 Joined   Ports: Vlan2-1/15, Vlan3-1/17,
 Pruned   Ports:
 Leaf     Ports:
 Asserted Ports:
 Prune Pending Ports:
 Assert Winner Ifs:
 Assert Loser Ifs:
 TIMERS:  Entry   JP   RS  Assert VIFS:  0  1  2  3
            201     51    0    0          0  201  200  0
                       AssertVifTimer:  0  0  0  0
--------------------------------------------------------------------------------
Total Num of Entries Displayed 2
Flags Legend:
SPT = Shortest path tree, WC=(*,Grp) entry, RP=Rendezvous Point tree, CACHE=Kernel Cache,
ASSERTED=Asserted, SG=(Src,Grp) entry, PMBR=(*,*,RP) entry, FWD_TO_RP=Forwarding to RP,
FWD_TO_DR=Forwarding to DR
--------------------------------------------------------------------------------
```

Configuring a static rendezvous point (RP)

Static RP enables you to configure a static entry for a rendezvous point (RP). When configured, static RP ignores the BSR mechanism and uses the statically configured RPs only. This feature allows static RP-enabled 8000 Series switches to communicate with switches from other vendors that do not use the BSR mechanism. For more information about static RP and other PIM-SM concepts, see Chapter 1, “IP Multicast concepts.”

Static RP configuration considerations

Before you can configure a static RP, you must enable PIM in sparse mode (sm) and enable Static RP as shown in the next section.

After meeting these prerequisites, keep in mind the following configuration considerations:

- A static RP-enabled switch cannot be configured as a BSR or as a C-RP.
- All dynamically learned BSR information is lost. However, if you disable static RP, the switch loses the static RP information and regains the BSR functionality.
- Static RPs do not age, that is they cannot time out.
- Switches do not advertise static RPs so, if a new PIM neighbor joins the network, it will not know about the static RP unless it is configured with that static RP.
- Configure all the switches in the network (including switches from other vendors) to map to the same RP.
- In a PIM domain with both static and dynamic RP switches, the static RP switches cannot have one of their (local) interfaces configured as RP.
- To avoid a single point of failure, you can configure redundant static RPs for the same group prefix. If there is a mix of Nortel and other vendor’s switches across the network, you have to ensure that all switches/routers use the same active RP because other vendors may be using different algorithms to elect the active RP. 8000 Series switches use the hash function defined in the PIM-SM standard to elect the active RP; other vendors may use the lowest IP address to break the tie.

- Static RP configured on the switch is assumed to be alive as long as the switch has a unicast route to the static RP's network. If the switch loses this route, the static RP is invalidated and the hash algorithm is invoked to remap all affected groups. If the switch regains this route, the static RP is validated and the hash algorithm is invoked to remap the affected groups.

Configuring static RP

To configure a static RP, use the following command:

```
config ip pim static-rp
```

This command includes the following parameters:

config ip pim static-rp followed by:	
`info`	Displays current PIM settings on the switch.
`add grp <ipaddr> mask <ipmask> rp <ipaddr>`	Adds a static RP entry to the RP set. • `grp <ipaddr>` - The IP address of the multicast group. When combined with the group mask, it identifies the range of the multicast addresses that the RP handles. • `mask <ipmask>` - The address mask of the multicast group. When combined with the group address, it identifies the range of the multicast addresses that the RP handles. • `rp <ipaddr>` - The IP address of the static RP.
`delete grp <ipaddr> mask <ipmask> rp <ipaddr>`	Deletes a static RP entry from the RP set. • `grp <ipaddr>` - The IP address of the multicast group. When combined with the group mask, it identifies the range of the multicast addresses that the RP handles. • `mask <ipmask>` - The address mask of the multicast group. When combined with the group address, it identifies the range of the multicast addresses that the RP handles. • `rp <ipaddr>` - The IP address of the static RP.
`disable`	Disables static RP on the switch.
`enable`	Enables static RP on the switch.

Configuration example

This configuration example uses the commands described above to enable static RP and to add a static RP entry. After configuring the parameters, use the **`info`** command to show a summary of the results.

```
SwitchA:5/config/ip/pim/static-rp#
SwitchA:5/config/ip/pim/static-rp# enable

WARNING: RP information learnt dynamically through BSR
functionality will be lost.

Do you wish to enable Static RP? (y/n) ? y
SwitchA:5/config/ip/pim/static-rp# add grp 239.255.0.0 mask
255.255.0.0 rp 100.1.1.1
SwitchA:5/config/ip/pim/static-rp# info

Sub-Context:
Current Context:

static-rp: enabled

Group Address: 239.255.0.0
Group Mask: 255.255.0.0
RP Address: 100.1.1.1
Status: valid


SwitchA:5/config/ip/pim/static-rp#
```

Showing the static RP table

To display the static RP table, use the following command:

```
show ip pim static-rp
```

Figure 153 shows sample output for this command.

Figure 153 show ip pim static-rp command output

```
================================================================
                        Pim Static RP Table
================================================================
GRPADDR          GRPMASK          RPADDR           STATUS
----------------------------------------------------------------
239.255.0.0      255.255.0.0      100.1.1.1        valid
```

Configuring PIM on an Ethernet (brouter) port

When you enable PIM on an Ethernet port, you must also enable it globally. Otherwise, PIM will not work. See "Configuring PIM-SM globally" on page 392.

To configure PIM on a brouter port, use the following command:

```
config ethernet <ports> ip pim
```

where:
ports uses the convention {slot/port[-slot/port][,...]}.

This command includes the following parameters:

config ethernet <*ports*> ip pim followed by:	
`info`	Displays current PIM configuration settings on the selected brouter port.
`disable`	Disables PIM on the selected brouter port.
`create <active|passive>`	Enables PIM on a specific brouter port with a specific type. An active port allows PIM control traffic to be transmitted and received. A passive port prevents PIM control traffic from being transmitted or received, thereby reducing the load on a system. This feature is useful when there is a high number of PIM interfaces and these interfaces are connected to end users; not to other switches.
`enable`	Enables PIM on the selected port.
`hellointerval <seconds>`	Specifies how long to wait (in seconds) before the PIM switch sends out the next hello message to neighboring switches. The default is 30 seconds.
`interface-type <active|passive>`	Specifies whether the selected port is active or passive. See `create <active|passive>` for a description of active and passive ports. `interface-type` allows you to change the state of a PIM interface after it's been created. It can be changed only when PIM is disabled on the specified port.
`joinprune-interval <seconds>`	Specifies how long to wait (in seconds) before the PIM switch sends out the next join/prune message to its upstream neighbors. The default is 60 seconds.

Figure 154 shows sample output for the **config ethernet ip pim info** command.

Figure 154 config ethernet ip pim info command output

```
8010:5/config/ethernet/2/1/ip/pim# info

Sub-Context: candbsr
Current Context:

                          pim : disable
                         mode : ssm
                interface-type : active
                      helloint : 30
                         jpint : 60
                      cbsrpref : -1  (disabled)

8010:5/config/ethernet/2/1/ip/pim#
```

Changing the port interface type

Before changing the port interface type, you must first disable PIM. Use the following commands to change the interface type from active to passive:

```
config ethernet <ports> ip pim disable
config ethernet <ports> ip pim interface-type passive
config ethernet <ports> ip pim enable
```

Configuring a candidate BSR on an Ethernet port

PIM-SM cannot run without a bootstrap router (BSR). Although a PIM-SM domain can have only one active BSR, you can configure additional routers as candidate BSRs (C-BSRs). C-BSRs provide backup protection in case the primary BSR fails.

The C-BSR with the highest configured preference becomes the BSR for the domain. If two C-BSRs have equal preference, the candidate with the higher IP address becomes the BSR. If you add a new C-BSR with a higher preference to the domain, it automatically becomes the new BSR.

To configure a candidate BSR on an Ethernet port, use the following command:

```
config ethernet <ports> ip pim candbsr
```

where:
ports uses the convention {slot/port[-slot/port][,...]}.

This command includes the following parameters:

config ethernet <*ports*> ip pim candbsr followed by:	
info	Displays the candidate BSR preference setting for this interface (Figure 155).
enable preference <*value*>	Enables the Candidate BSR on this interface and sets its preference value to become a BSR. The Candidate BSR with the highest BSR preference and address is referred to as the preferred BSR. The default is -1, which indicates that the current interface is not a Candidate BSR.
disable	Disables the Candidate BSR on this interface.

Figure 155 config ethernet ip pim candbsr command output

```
8610:5/config/ethernet/4/1/ip/pim/candbsr# info

Sub-Context:
Current Context:

             cbsr preference : -1  (disabled)
```

Configuring PIM on a VLAN

When you enable PIM on a particular VLAN, you must also enable it globally. Otherwise, PIM will not work. See “Configuring PIM-SM globally” on page 392.

To configure PIM on a VLAN, use the following command:

```
config vlan <vid> ip pim
```

where:
vid is a VLAN ID from 1 to 4092.

This command includes the following parameters:

config vlan <*vid*> ip pim followed by:	
info	Displays current PIM configuration settings on the selected VLAN.
disable	Disables PIM on the selected VLAN.
create <active|passive>	Enables PIM on a specific VLAN with a specific type. • active allows PIM control traffic to be transmitted and received. • passive prevents PIM control traffic from being transmitted or received, thereby reducing the load on a system. This feature is useful when there is a high number of PIM interfaces and these interfaces are connected to end users; not to other switches.
enable	Enables PIM on the selected VLAN.
hellointerval <*seconds*>	Specifies how long to wait (in seconds) before the PIM switch sends out the next hello message to neighboring switches. The default is 30 seconds.
interface-type <active|passive>	Specifies whether the selected interface is active or passive. See create <active|passive> for a description of active and passive interfaces. interface-type allows you to change the state of a PIM interface after it's been created. It can be changed only when PIM is disabled on the specified interface
joinprune-interval <*seconds*>	Specifies how long to wait (in seconds) before the PIM switch sends out the next join/prune message to its upstream neighbors. The default is 60 seconds.

Figure 156 shows sample output for this command.

Figure 156 config vlan ip pim info command output

```
8010:5/config/vlan/2/ip/pim# info

Sub-Context: candbsr
Current Context:

                          pim : disable
                         mode : ssm
                interface-type : active
                      helloint : 30
                         jpint : 60
                      cbsrpref : -1  (disabled)
```

Changing the VLAN interface type

Before changing the interface type, you must first disable PIM on the VLAN. Use the following commands to change the interface type from active to passive:

```
config vlan <vid> ip pim disable
config vlan <vid> ip pim interface-type passive
config vlan <vid> ip pim enable
```

Showing PIM information for VLANs

To display information about the PIM-SM interface setup for VLANs, use the following command:

```
show vlan info pim
```

Figure 157 shows sample output for this command.

Figure 157 show vlan info pim command output

```
8010:5# show vlan info pim

================================================================================
                                    Vlan Ip Pim
================================================================================

VLAN-ID   PIM-ENABLE MODE    HELLOINT  JPINT   CBSRPREF      INTF TYPE
--------------------------------------------------------------------------------
1         disable    ssm     30        60      -1  (disabled) active
2         disable    ssm     30        60      -1  (disabled) active
3         enable     ssm     30        60      -1  (disabled) active
4         enable     ssm     30        60      -1  (disabled) active

8010:5#
```

Table 72 describes the **`show vlan ip pim`** parameters.

Table 72 show vlan ip pim parameters

Field	Description
VLAN-ID	Identifies the VLAN.
PIM-ENABLE	The state of PIM on the VLAN.
MODE	The configured mode of this VLAN. The valid modes are SSM and Sparse.
HELLOINT	Indicates how long to wait (in seconds) before the PIM switch sends out the next hello message to neighboring switches. The default hello interval is 30 seconds.
JPINT	Indicates how long to wait (in seconds) before the PIM switch sends out the next join/prune message to its upstream neighbors. The default join/prune interval is 60 seconds.
CBSR PREF	The preference for this local interface to become a Candidate BSR. The Candidate BSR with the highest BSR-priority and address is referred to as the preferred BSR. The default is -1, which indicates that the current interface is not a Candidate BSR.
INTF TYPE	Indicates whether the PIM interface is active or passive.

Configuring a candidate BSR on a VLAN

PIM-SM cannot run without a bootstrap router (BSR). Although a PIM-SM domain can have only one active BSR, you can configure additional routers as candidate BSRs (C-BSRs). C-BSRs provide backup protection in case the primary BSR fails.

The C-BSR with the highest configured preference becomes the BSR for the domain. If two C-BSRs have equal preference, the candidate with the higher IP address becomes the BSR. If you add a new C-BSR with a higher preference to the domain, it automatically becomes the new BSR.

To configure a candidate BSR on a VLAN, use the following command:

```
config vlan <vid> ip pim candbsr
```

where:
vid is a VLAN ID from 1 to 4092.

This command includes the following parameters:

config vlan <*vid*> ip pim candbsr followed by:	
`info`	Displays the candidate BSR preference setting for this interface (Figure 158).
`enable preference <value>`	Enables the Candidate BSR on this interface and sets its preference value to become a BSR. The Candidate BSR with the highest BSR preference and address is referred to as the preferred BSR. The default is -1, which indicates that the current interface is not a Candidate BSR.
`disable`	Disables the Candidate BSR on this interface.

Figure 158 config vlan ip pim candbsr command output

```
8610:5/config/vlan/3/ip/pim/candbsr# info

Sub-Context:
Current Context:

            cbsr preference : -1  (disabled)
```

Configuring PIM debug trace commands

To configure PIM protocol traces for troubleshooting, use the following command:

```
config ip pim debug-pimmsg
```

This command includes the following parameters:

Note: For the following parameter values, 1=true and 2=false. The default value for each parameter is 2 (false).

config ip pim debug-pimmsg followed by:	
`info`	Displays current PIM debug trace flag settings on the switch.
`assert <true=1|false=2>`	Allows you to set the switch to display the assert debug traces.
`bstrap <true=1|false=2>`	Allows you to set the switch to display bootstrap debug traces.
`group <ipaddress>`	Allows you to set the switch to display debug traces from a specific group ip-address.
`hello <true=1|false=2>`	Allows you to set the switch to display hello debug traces.
`joinprune <true=1|false=2>`	Allows you to set the switch to display join/prune debug traces.
`pimdbgtrace <true=1|false=2>`	Allows you to set the switch to display pim debug traces.
`pimdbglog <true=1|false=2>`	Allows you to control whether the switch logs debug traces.
`register <true=1|false=2>`	Allows you to set the switch to display register debug traces.
`regstop <true=1|false=2>`	Allows you to set the switch to display register stop debug traces.
`rp-adv <true=1|false=2>`	Allows you to set the switch to display rp advertisement debug traces.

config ip pim debug-pimmsg followed by:	
send <true=1|false=2>	Allows you to set the switch to display send debug traces.
rcv <true=1|false=2>	Allows you to set the switch to display received debug traces.
source <*ipaddress*>	Allows you to set the switch to display debug traces from a specific source ip-address.

Figure 159 shows sample output for the **config ip pim debug-pimmsg info** command.

Figure 159 config ip pim debug-pimmsg info command output

```
8610:3/config/ip/pim/debug-pimmsg# info
                      assert : false
                      bstrap : false
                       hello : false
                   joinprune : false
                 pimdbgtrace : false
                   pimdbglog : false
                    register : false
                     regstop : false
                      rp-adv : false
                        send : false
                         rcv : false
```

Tips for using the debug trace commands

Debug trace command values allow you to control debug traces for specific PIM protocol message types. For examples of debug trace output, see "Debug trace command sample output" on page 422.

The following tips can help you use the debug trace commands:

- All *configured* debug trace messages can be set to true <1> or false <2> by entering the following command at the console or Telnet session:

  ```
  config ip pim debug-pimmsg pimdbgtrace <1|2>
  ```

  To stop the debug trace messages output at any time, enter the following command:

  ```
  config ip pim debug-pimmsg pimdbgtrace 2
  ```

- To display trace messages *forwarded* by the switch, set the **send** value to 1. To display trace messages *received* by the switch, set the **rcv** value to 1.

  You can also simultaneously display *forwarded* and *received* debug trace messages by setting both **send** and **rcv** values to 1. For example, to simultaneously display Hello messages forwarded and received by the switch, type the following commands:

  ```
  config ip pim debug-pimmsg hello 1
  config ip pim debug-pimmsg send 1
  config ip pim debug-pimmsg rcv 1
  ```

- You can save debug trace messages in a log file, or you can display the messages on your console. For example, to display (and log) a debug trace, use the following command:

  ```
  config ip pim debug-pimmsg pimdbglog 1
  ```

  where:
  1 = true (debug trace messages are logged)
  2 = false (debug trace messages are displayed only, not logged).

- To disable previously enabled register messages, type the following command:

  ```
  config ip pim debug-pimmsg register 2
  ```

- To display debug trace messages from a specific interface, type the following command:

```
config ip pim debug-pimmsg source <ipaddress>
```

The above command ensures that messages from any other interface will not be shown.

Debug trace command sample output

This section shows sample debug trace command output. This section includes the following commands:

Assert debug trace send/receive output

To display assert *send/receive* debug traces from a switch, use the following commands:

```
config ip pim debug-pimmsg pimdbgtrace 1
config ip pim debug-pimmsg assert 1
config ip pim debug-pimmsg send 1
config ip pim debug-pimmsg rcv 1
```

Figure 160 shows the assert *send/receive* debug trace output sent by the assert winner switch and received by the assert loser switch.

Figure 160 Assert debug trace send/receive output example

```
8610:5/config/ip/pim/debug-pimmsg# pimdbgtrace 1
8610:5/config/ip/pim/debug-pimmsg# assert 1
8610:5/config/ip/pim/debug-pimmsg# send 1
8610:5/config/ip/pim/debug-pimmsg# rcv 1

[000 12:12:42:851] PIM Assert SENT Src= 11.11.11.121: Dst= 224.0.0.13
Group Address= 234.0.0.1/32 Source Address= 1.1.121.100
Assert Preference= 0, Assert Metric= 1, RPT Bit = 0

[000 12:12:45:235] PIM Assert RECEIVED Src= 11.11.11.121: Dst= 224.0.0.13
Group Address= 234.0.0.1/32 Source Address= 1.1.121.100
```

Bootstrap debug trace send/receive output

To display bootstrap *send/receive* debug traces from a switch, use the following commands:

```
config ip pim debug-pimmsg pimdbgtrace 1
config ip pim debug-pimmsg bstrap 1
config ip pim debug-pimmsg send 1
config ip pim debug-pimmsg rcv 1
```

Figure 161 shows the bootstrap *send/receive* debug trace output sent by a switch and received by a neighboring switch.

Figure 161 Bootstrap debug trace send/receive output example

```
8610:5/config/ip/pim/debug-pimmsg# pimdbgtrace 1
8610:5/config/ip/pim/debug-pimmsg# bstrap 1
8610:5/config/ip/pim/debug-pimmsg# send 1
8610:5/config/ip/pim/debug-pimmsg# rcv 1

Group Address= 224.0.0.0/4
RP = 155.110.125.34, RP-Holdtime = 150, RP-Priority= 0
RP = 155.110.125.22, RP-Holdtime = 150, RP-Priority= 0
[000 05:29:12:795] PIM Bootstrap SENT  Src= 155.109.182.25 : Dst = 224.0.0.13
BSR = 155.110.125.22 ,Fragment Tag = 1746, Hash Mask Len = 30, BSR-priority = 3

Group Address= 224.0.0.0/4
RP = 155.110.125.34, RP-Holdtime = 150, RP-Priority= 0
RP = 155.110.125.22, RP-Holdtime = 150, RP-Priority= 0
[000 05:29:13:095]PIM Bootstrap RECEIVED Src= 155.109.182.18: Dst = 224.0.0.13
BSR = 155.110.125.22,Fragment Tag = 1746, Hash Mask Len = 30, BSR-priority = 3
```

Hello debug trace send/receive output

To display hello *send/receive* debug traces from a switch, use the following commands:

```
config ip pim debug-pimmsg pimdbgtrace 1
config ip pim debug-pimmsg hello 1
config ip pim debug-pimmsg send 1
config ip pim debug-pimmsg rcv 1
```

Figure 162 shows the hello *send/receive* debug trace output sent by a switch and received by a neighboring switch.

Figure 162 Hello debug trace send/receive output example

```
8610:5/config/ip/pim/debug-pimmsg# pimdbgtrace 1
8610:5/config/ip/pim/debug-pimmsg# hello 1
8610:5/config/ip/pim/debug-pimmsg# send 1
8610:5/config/ip/pim/debug-pimmsg# rcv 1

[0000 6:27:02:061]PIM Hello RECEIVED Src=155.0.0.38:Dst=224.0.0.13 HoldTime=105

[000 06:27:23:511]PIM Hello SENT Src=100.100.100.1:Dst=224.0.0.13 HoldTime=105

[000 06:27:26:511]PIM Hello SENT Src=155.110.125.37:Dst=224.0.0.13 HoldTime=105
```

Joinprune debug trace send/receive output

To display joinprune *send/receive* debug traces from a switch, use the following commands:

```
config ip pim debug-pimmsg pimdbgtrace 1
config ip pim debug-pimmsg joinprune 1
config ip pim debug-pimmsg send 1
config ip pim debug-pimmsg rcv 1
```

Figure 163 shows the joinprune *send/receive* debug trace output sent by a downstream neighbor switch and received by an upstream neighbor switch.

Figure 163 Joinprune debug trace send/receive output example

```
8610:5/config/ip/pim/debug-pimmsg# pimdbgtrace 1
8610:5/config/ip/pim/debug-pimmsg# joinprune 1
8610:5/config/ip/pim/debug-pimmsg# send 1
8610:5/config/ip/pim/debug-pimmsg# rcv 1

[000 06:38:39:745] PIM Join/Prune  SENT  Src 155.110.125.37 : dst 224.0.0.13
UpstreamNbr = 155.110.125.38, Num Groups = 4 , HoldTime = 210
Group-Address  224.0.0.0/4, Joined Sources = 0 , Pruned Sources = 0
Group-Address  224.17.17.17/32, Joined Sources = 0 , Pruned Sources = 1
Pruned Sources = 155.120.50.201/32 WC =0  RP = 1 ,

Group-Address  224.2.206.61/32, Joined Sources = 0 , Pruned Sources = 4
Pruned Sources =
100.100.100.25/32 WC =0  RP = 1 ,155.120.50.165/32 WC =0  RP = 1,
155.120.50.201/32 WC =0  RP = 1 ,155.120.50.202/32 WC =0  RP = 1,

Group-Address  224.0.0.0/4, Joined Sources = 1 , Pruned Sources = 0
Joined Sources = 155.110.125.34/32 WC =1  RP = 1,

[000 06:38:59:078] PIM Join/Prune RECEIVED  Src 155.110.125.38 : dst 224.0.0.13
UpstreamNbr = 155.110.125.37, Num Groups = 12 , HoldTime = 210
Group-Address  234.26.89.193/32, Joined Sources = 5 , Pruned Sources = 0
Joined Sources =
141.1.1.10/32 WC= 0 RP= 0 ,141.1.1.11/32 WC= 0 RP= 0,141.1.1.11/32 WC= 0 RP= 0,
147.1.1.13/32 WC= 0 RP= 0 ,147.1.1.14/32 WC= 0 RP= 0,
```

Register debug trace send/receive output

To display register *send/receive* debug traces from a switch, use the following commands:

```
config ip pim debug-pimmsg pimdbgtrace 1
config ip pim debug-pimmsg register 1
config ip pim debug-pimmsg send 1
config ip pim debug-pimmsg rcv 1
```

Figure 164 shows the register *send/receive* debug trace output sent by the source DR and received by the RP.

Figure 164 Register debug trace send/receive output example

```
8610:5/config/ip/pim/debug-pimmsg# pimdbgtrace 1
8610:5/config/ip/pim/debug-pimmsg# register 1
8610:5/config/ip/pim/debug-pimmsg# send 1
8610:5/config/ip/pim/debug-pimmsg# rcv 1

[000 16:08:25:187] PIM Register SENT Src = 100.1.2.120 : Dst = 192.60.60.1
BorderBit= 0, NullRegisterBit= 0
Src = 100.1.2.3 , Group = 225.2.1.67

[000 16:04:42:237] PIM Register RECEIVED Src = 100.1.2.120 : Dst = 192.60.60.1
BorderBit= 0, NullRegisterBit= 0
```

Regstop debug trace send/receive output

To display regstop *send/receive* debug traces from a switch, use the following commands:

```
config ip pim debug-pimmsg pimdbgtrace 1
config ip pim debug-pimmsg regstop 1
config ip pim debug-pimmsg send 1
config ip pim debug-pimmsg rcv 1
```

Figure 165 shows the regstop *send/receive* debug trace output sent by the RP and received by the source DR.

Figure 165 Regstop debug trace send/receive output example

```
8610:5/config/ip/pim/debug-pimmsg# pimdbgtrace 1
8610:5/config/ip/pim/debug-pimmsg# regstop 1
8610:5/config/ip/pim/debug-pimmsg# send 1
8610:5/config/ip/pim/debug-pimmsg# rcv 1

[000 16:04:42:237] PIM Register Stop SENT RP= 192.60.60.1: Dst= 100.1.2.120
Group Address= 225.2.1.67/32, Source Address = 100.1.2.3

[000 16:08:25:221] PIM Register Stop RECEIVED RP= 192.60.60.1: Dst= 100.1.2.120
Group Address= 225.2.1.67/32, Source Address = 100.1.2.3
```

Rp-adv debug trace send/receive output

To display rp-adv *send/receive* debug traces from the bootstrap switch, use the following commands:

```
config ip pim debug-pimmsg pimdbgtrace 1
config ip pim debug-pimmsg rp-adv 1
config ip pim debug-pimmsg send 1
config ip pim debug-pimmsg rcv 1
```

Figure 166 shows the rp-adv *send/receive* debug trace output sent by the candidate RP and received by the bootstrap switch.

Figure 166 Rp-adv debug trace send/receive output example

```
8610:5/config/ip/pim/debug-pimmsg# pimdbgtrace 1
8610:5/config/ip/pim/debug-pimmsg# rp-adv 1
8610:5/config/ip/pim/debug-pimmsg# send 1
8610:5/config/ip/pim/debug-pimmsg# rcv 1

[000 16:16:05:887] PIM Cand RP Adv. SENT Src= 192.30.30.1: Dst= 192.60.60.1
RP 192.30.30.1, Prefix cnt = 1, Priority= 0, Holdtime= 150

Group Addresses= 224.0.0.0/4

[000 16:13:25:104] PIM Cand RP Adv. RECEIVED Src= 192.30.30.1: Dst=192.60.60.1
RP 192.30.30.1, Prefix cnt = 1, Priority= 0, Holdtime= 150

Group Addresses= 224.0.0.0/4
```

Configuring Source Specific Multicast (SSM)

Source Specific Multicast (SSM) optimizes PIM-SM by simplifying the many-to-many model (servers-to-receivers). Since most multicast applications distribute content to a group in one direction, SSM uses a one-to-many model that only uses a subset of the PIM-SM features. This model is more efficient and puts less of a load on multicast routing devices. For more information about SSM concepts and terminology, refer to Chapter 1, “IP Multicast concepts.”

PIM-SSM configuration prerequisites

SSM is a global configuration. When you enable SSM on a switch, it is enabled on all interfaces running PIM. On an SSM-enabled switch, SSM behavior is limited to the SSM group range. For non-SSM groups, the protocol behavior is PIM-SM.

Before you can configure SSM, you must prepare the router as follows:

1. Configure an IP interface. For information, refer to *Configuring IP Routing Operations*.
2. Configure a unicast protocol (RIP or OSPF) globally and on the interfaces where you want to configure PIM. For information on RIP and OSPF, refer to *Configuring IP Routing Operations*.

   PIM requires a unicast protocol in order to forward multicast traffic within the network when performing the Reverse Path Forwarding (RFP) check. PIM-SM uses the information from the unicast routing table to create and maintain the shared and shortest multicast tree that enables PIM-enabled routers to communicate. The unicast routing table must contain a route to every multicast source in the network as well as routes to PIM entities like the RPs and BSR.
3. Enable PIM globally.

Configuring PIM-SSM globally

To enable or disable PIM-SSM globally on the switch, use the following commands:

```
config ip pim enable
config ip pim mode ssm
```

When changing modes from SSM to sparse, the following warning message appears:

```
Dynamic mode change from SSM is not allowed, please disable PIM.
```

To change modes from SSM to sparse, use the following commands:

```
config ip pim disable
config ip pim mode sparse
config ip pim enable
```

Note: After you enable PIM in SSM mode, the IGMP parameters take effect. To take full advantage of SSM, enable IGMPv3 if hosts attached to the switch are running IGMPv3 or configuring the SSM table.

For information on configuring IGMPv3, refer to "Configuring IGMP on an interface" on page 275" or "Configuring IGMP on a VLAN" on page 307."

For information on configuring the SSM group range and channel table, refer to "Showing SSM group range and dynamic learning status" on page 295" or "Configuring the SSM channel table" on page 296."

The `config ip pim` command includes the following parameters:

`config ip pim` followed by:	
`info`	Displays current PIM settings on the switch.
`disable`	Globally disables PIM on the switch.

config ip pim followed by:	
`enable`	Globally enables PIM on the switch.
`mode <sparse|ssm>`	The configured mode of this interface: sparse or ssm (source-specific multicast).
`bootstrap-period <integer>`	Specifies the interval (in seconds) that the elected BSR waits between originating bootstrap messages. • *integer* is a number in the range from 5 to 32757. The default is 60.
`c-rp-adv-timeout <integer>`	Specifies how often (in seconds) that routers configured as candidate RPs send C-RP advertisement messages. When this timer expires, the C-RP sends an advertisement message to the elected BSR. • *integer* is a number in the range from 5 to 26214. The default is 60.
`disc-data-timeout <integer>`	Specifies how long (in seconds) to discard data until the Join is received from the RP. An ipmc discard record is created after a register packet is sent until the the timer expires and/or when a Join is received. • *integer* is a number in the range from 5 to 65535. The default is 60.
`activity-chk-interval`	15, 30 or 210
`joinprune-interval <integer>`	Specifies how long to wait (in seconds) before the PIM router sends out the next join/prune message to its upstream neighbors. • *integer* is a number in the range from 1 to 18724. The default is 60.
`register-suppression-timeout <integer>`	Specifies how long (in seconds) the DR suppresses sending registers to the RP. The timer starts when the DR receives a Register Stop message from the RP. • *integer* is a number in the range from 6 to 65535. The default is 60.
`unicast-route-change-timeout <integer>`	Specifies how often (in seconds) the switch polls the routing table manager (RTM) for unicast routing information updates to be used by PIM. **Note:** Lowering this value increases how often the switch polls the RTM. This may affect the switch's performance, especially when there's a lot of traffic flowing through the switch. • *integer* is a number in the range from 2 to 65535. The default is 5.

Configuration example

This configuration example uses the commands described above to globally enable PIM in SSM mode and to set the timers. After configuring the parameters, use the **info** command to show a summary of the results.

```
8610co:5/config/ip/pim# enable
8610co:5/config/ip/pim# mode ssm
8610co:5/config/ip/pim# register-suppression-timeout 60
8610co:5/config/ip/pim# joinprune-interval 60
8610co:5/config/ip/pim# info

Sub-Context: mbr interface candrp debug-pimmsg static-rp
Current Context:

                          enable : true
                     global mode : ssm
                             mbr : Disabled
                reg-suppr-timeout : 60
               joinprune-interval : 60

8610co:5/config/ip/pim#
```

Displaying all IP PIM show commands

The **show ip pim show-all** command displays all relevant IP PIM information.

The command uses the syntax:

`show ip pim show-all [file <value>]`

where *<value>* is the filename to which the output will be redirected.

Figure 167 shows sample output for the **show ip pim show-all** command.

Figure 167 show ip pim show-all command output

```
P8600-CORE1:5#
P8600-CORE1:5# show ip pim show-all

# show ip pim active-rp

================================================================================
                                      Pim Grp->RP Active RP Table
================================================================================
GRPADDR          RP-ADDR          RP-PRIORITY
--------------------------------------------------------------------------------
224.1.1.1         10.163.97.2       0
224.1.1.2         10.163.97.2       0
224.1.1.3         10.163.97.2       0
224.1.1.8         10.163.97.2       0
224.1.1.9         10.163.97.2       0
224.1.1.10        10.163.97.2       0
224.2.1.1         10.163.97.9       0
224.2.1.2         10.163.97.9       0
224.2.1.3         10.163.97.9       0
224.2.1.4         10.163.97.9       0
224.2.1.5         10.163.97.9       0
224.2.1.6         10.163.97.9       0
224.2.1.7         10.163.97.9       0
224.2.1.8         10.163.97.9       0
224.2.1.9         10.163.97.9       0

# show ip pim bsr

================================================================================
                                      Current BootStrap Router Info
================================================================================

Current BSR address: 10.163.99.1
Current BSR priority: 200
Current BSR HashMask: 255.255.255.252
Current BSR Fragment Tag: 4414
Pim Bootstrap Timer : 9

# show ip pim info
```

Chapter 12
Configuring PGM using the CLI

Pragmatic General Multicast (PGM) provides reliable, duplicate-free delivery of data packets while reducing network congestion. PGM guarantees that receivers either receive all data packets from transmissions and retransmissions, or can detect unrecoverable data packet loss. PGM is particularly well suited to ‘push’ applications with relatively small information transfers such as stock and news updates.

For more information about PGM concepts and terminology, see Chapter 1, “IP Multicast concepts.”

This chapter includes the following topics:

Roadmap of PGM commands

The following roadmap lists all the PGM commands and their parameters. After using the commands below to configure the Passport 8600, you can use the show commands to display information for a particular feature.

To facilitate troubleshooting, the Passport 8600 also provides *one* command (`show ip pgm show-all`) that lists all the show commands for IP PGM and displays their configuration output. See "Displaying all IP PGM show commands" on page 460.

Use this list as a quick reference or click on any entry for more information:

Command	Parameter
`config ip pgm`	`info`
	`state <enable|disable>`
	`session-life-time <integer>`
	`nnak-generate <enable|disable>`
	`max-rexmit-state <integer>`
	`max-sessions <integer>`
`show ip pgm global`	
`show ip pgm retransmit`	
`show ip pgm session`	
`config ip pgm interface <ipaddr>`	`info`
	`state <enable|disable>`
	`nak-re-xmit-int <integer>`
	`max-nak-re-xmit-cnt <integer>`
	`max-nak-rdata-int <integer>`
	`nak-eliminate-int <integer>`
`show ip pgm interface config`	
`show ip pgm interface error general`	
`show ip pgm interface error nak`	

Command	Parameter
show ip pgm interface stat general	
show ip pgm interface stat nak	
show ip pgm interface stat parity	
config ethernet <ports> ip pgm	info
	state <enable|disable>
	nak-re-xmit-int <integer>
	max-nak-re-xmit-cnt <integer>
	max-nak-rdata-int <integer>
	nak-eliminate-int <integer>
config vlan <vid> ip pgm	info
	state <enable|disable>
	nak-re-xmit-int <integer>
	max-nak-re-xmit-cnt <integer>
	max-nak-rdata-int <integer>
	nak-eliminate-int <integer>
show ip pgm show-all [file <value>]	

Configuration considerations and prerequisites

The 8000 Series switches implement the network element portion of PGM. They support the following PGM options:

- NAK list
- FEC (forwarding error correction)

The 8000 Series switches cannot serve as a DLR because DLRs require a large amount of buffering. Therefore, the null negative acknowledgement (NNAK) parameters in the CLI are not supported.

To configure and use PGM on an 8000 Series switch, the switch must be running IP multicast with IGMP snooping and/or an IP multicast protocol such as DVMRP or PIM-SM. If PGM is configured without IP multicast enabled on a switch, PGM will not run and cannot be used.

To configure PGM on a switch, you need to perform the following steps:

1. Configure and enable IP multicast on the switch, particularly on the interfaces where PGM is required.
2. Enable PGM globally.
3. Enable PGM on the required interfaces.

Configuring PGM globally

To configure PGM globally on the switch, use the following command:

```
config ip pgm
```

This command includes the following parameters:

config ip pgm followed by:	
`info`	Displays current PGM settings on the switch.
`state <enable|disable>`	Displays the current state (up or down) of PGM.
`session-life-time <integer>`	Specifies the length of idle time (in seconds) after which a session times out. Idle time is when no SPMs are received from the upstream. The default value is 300 seconds.
`nnak-generate <enable|disable>`	When enabled, the DLR that receives redirected NAKs for which it has the RDATA sends a null NAK (NNAK) to the original source.
`max-rexmit-state <integer>`	Configures the maximum number of retransmit state entries that the switch can create. Each entry has a unique NAK sequence number. The default value is 200 entries.
`max-sessions <integer>`	Configures the maximum number of source path state sessions allowed on the switch. The default value is 100 sessions.

Figure 168 shows sample output for the **`config ip pgm info`** command.

Figure 168 config ip pgm info command output

```
8610:5/config/ip/pgm# info

Sub-Context: interface
Current Context:

                        state : enabled
           session-life-time : 300
               nnak-generate : enabled
            max-rexmit-state : 200
                max-sessions : 100
```

Showing PGM global information

To display the PGM global status on the switch, use the following command:

```
show ip pgm global
```

Figure 169 shows sample output for this command.

Figure 169 show ip pgm global command output

```
8610:5/show/ip/pgm# global
                       enable : enabled
                        state : down
           session-life-time : 300
               nnak-generate : 2
          max-re-xmit-states : 200
        total-re-xmit-states : 0
                max-sessions : 100
              total-sessions : 0
total-re-xmit-states-timeout : 0
           total-unique-naks : 0
    total-unique-parity-naks : 0
```

Table 73 describes the **`show ip pgm global`** parameters.

Table 73 show ip pgm global parameters

Field	Description
enable	Displays whether PGM is globally enabled or disabled.
state	Displays the current state (up or down) of PGM.
session-life-time	Displays the length of idle time (in seconds) after which a session times out. Idle time is when no SPMs are received from the upstream. The default is 300 seconds.
nnak-generate	When enabled, the DLR that receives redirected NAKs for which it has the RDATA sends a NULL NAK to the original source.
max-re-xmit-states	Displays the maximum number of retransmit state entries that the switch can create. Each entry has a unique NAK sequence number. The default is 200 entries.
total-re-xmit-states	Displays the total number of retransmit state entries in the retransmit table.
max-sessions	Displays the maximum number of source path state sessions allowed on the switch. The default is 100 sessions.
total-sessions	Displays the total number of source path state sessions in the PGM session entries table.
total-re-xmit-states-timeout	Displays the total number of retransmit state entries that were removed because they timed out.
total-unique-naks	Displays the total number of unique NAKs received.
total-unique-parity-naks	Displays the total number of unique parity NAKs received.

Showing PGM retransmission statistics

To display the PGM retransmission statistics, use the following command:

```
show ip pgm retransmit
```

Figure 170 shows sample output for this command.

Figure 170 show ip pgm retransmit command output

```
8610:5/show/ip/pgm# retransmit

================================================================================
                            Pgm Retransmit statistics
================================================================================
SOURCE   GLOBAL           SOURCE     GROUP    SEQ_NUM    UPSTREAM    DOWNSTREAM
PORT     ID                                   TG/CNT     CCT
--------------------------------------------------------------------------------
19     9b:78:32:c9:0:0     23         23       7          2050        2030
```

Table 74 describes the **`show ip pgm`** `retransmit` parameters.

Table 74 show ip pgm retransmit parameters

Field	Description
SOURCE PORT	Displays the source port of this retransmit state.
GLOBAL ID	Displays the global ID for this entry.
SOURCE	Displays the source IP address for this entry.
GROUP	Displays the destination group address for this entry.
SEQ_NUM TG/CNT	Displays the selected sequence number for this entry.
UPSTREAM CCT	Displays the upstream circuit number from this entry.
DOWNSTREAM	Displays the list of downstream interfaces from this entry.

Showing PGM session statistics

To display the PGM session statistics, use the following command:

```
show ip pgm session
```

Figure 171 shows sample output for this command.

Figure 171 show ip pgm session command output

```
8610:5/show/ip/pgm# session
 Total # number of sessions are 1

================================================================================
                           Pgm Session statistics
================================================================================
SOURCE   GLOBAL           SOURCE        GROUP           UPSTREAM        UPSTRM
PORT     ID                                           ADDRESS         IF_CCT
--------------------------------------------------------------------------------
19    9b:78:32:c9:0:0       155.120.50.201 224.241.241.241  155.120.50.201   2050

--------------------------------------------------------------------------------
SOURCE   GLOBAL             TRAIL    LEAD     IN       OUT    TOTAL     TOTAL
PORT     ID                 EDGE     EDGE     SPMS     SPMS   RE_XMIT   RE_XMIT
                            SEQ      SEQ                      STATES    TIMEOUT
--------------------------------------------------------------------------------
19     9b:78:32:c9:0:0     0        237      407      813    0         0

--------------------------------------------------------------------------------
SOURCE   GLOBAL           IN     OUT    IN_RDATA  UNIQUE   IN    OUT   IN_NAK
PORT     ID               RDATA  RDATA  NO_STATE  NAKS     NAKS  NAKS  SEQ
                                       ERRORS                         ERRORS
--------------------------------------------------------------------------------
19    9b:78:32:c9:0:0     98     98     0         0        48    40    0

--------------------------------------------------------------------------------
SOURCE   GLOBAL               IN       OUT      IN       OUT      IN_REDIRECTED
PORT     ID                   NNAKS    NNAKS    NCFS     NCFS     NCFS
--------------------------------------------------------------------------------
19    9b:78:32:c9:0:0         0        0        2        0        0

--------------------------------------------------------------------------------
SOURCE   GLOBAL             IN       OUT      IN       OUT    IN         OUT
PORT     ID                 PARITY   PARITY   PARITY   PARITY PARITY     PARITY
                            NAK      NAK      RDATA    RDATA  NCF        NCF
--------------------------------------------------------------------------------
19     9b:78:32:c9:0:0     0        0        2        3      0         0

--------------------------------------------------------------------------------
SOURCE   GLOBAL             IN       OUT      UNIQUE
PORT     ID                 PARITY   PARITY   PARITY
                            SPM      SPM      NAKS
--------------------------------------------------------------------------------
19    9b:78:32:c9:0:0       3        0        8
```

Table 75 describes the **`show ip pgm session`** parameters.

Table 75 show ip pgm session parameters

Field	Description
SOURCE PORT	Displays the source port for this session.
GLOBAL ID	Displays the global ID for this session.
SOURCE	Displays the source IP address for this session.
GROUP	Displays the destination group address for this session.
UPSTREAM ADDRESS	Displays the IP address of the upstream interface for this session.
UPSTREAM IF_CCT	Displays the circuit number of the upstream interface for this session.
TRAIL EDGE SEQ	Displays the trailing edge sequence of the transfer window.
LEAD EDGE SEQ	Displays the leading edge sequence of the transfer window.
IN SPMS	Displays the number of SPMs received during this session.
OUT SPMS	Displays the number of SPMs sent out during this session.
TOTAL RE_XMIT STATES	Displays the total number of retransmit state entries during this session.
TOTAL RE_XMIT TIMEOUT	Displays the total number of timed out retransmit state entries during this session.
IN RDATA	Displays the number of RDATA packets received during this session.
OUT RDATA	Displays the number of RDATA packets sent out during this session.
IN_RDATA NO_STATE ERORS	Displays the number of RDATA packets discarded because there was no active session.
UNIQUE NAKS	Displays the number of unique NAKs received during this session.
IN NAKS	Displays the number of NAKs received during this session.
OUT NAKS	Displays the number of unique NAKs sent out during this session.
IN_NAK SEQ ERRORS	Displays the number of NAKs discarded because they were out of sequence.
IN NNAKS	Displays the number of NNAKs received during this session.
OUT NNAKS	Displays the number of NNAKs sent out during this session.
IN NCFS	Displays the number of NCFs received during this session.
OUT NCFS	Displays the number of NCFs sent out during this session.

Table 75 show ip pgm session parameters (continued)

Field	Description
IN_REDIRECTED NCFS	Displays the number of redirected NCFs received during this session.
IN_PARITY_NAK	Displays the number of parity NAKs received during this session.
OUT_PARITY_NAK	Displays the number of parity NAKs sent out during this session.
IN_PARITY_RDATA	Displays the number of parity RDATA packets received during this session.
OUT_PARITY_RDATA	Displays the number of parity RDATA packets sent out during this session.
IN_PARITY_NCF	Displays the number of parity NCFs received during this session.
OUT_PARITY_NCF	Displays the number of parity NCFs sent out during this session.
IN_PARITY_SPM	Displays the number of parity SPMs received during this session.
OUT_PARITY_SPM	Displays the number of parity SPMs sent out during this session.
UNIQUE_PARITY_NAKS	Displays the number of unique parity NAKs received during this session.

Configuring PGM on an interface

To configure PGM on a specific interface, use the following command:

`config ip pgm interface <ipaddr>`

where:
ipaddr indicates the IP address of the selected interface.

This command includes the following parameters:

config ip pgm interface <ipaddr> followed by:	
`info`	Displays current PGM settings on the selected interface.
`state <enable|disable>`	Indicates the current state (enable or disable) of PGM on the selected interface.
`nak-re-xmit-int <integer>`	Specifies how long to wait for an NCF (in milliseconds) before retransmitting the NAK. The default value is 1000 milliseconds.
`max-nak-re-xmit-cnt <integer>`	Configures the maximum number of NAK retransmission packets allowed per second. The default value is 2 pps.
`max-nak-rdata-int <integer>`	Specifies how long to wait for RDATA (in milliseconds) after receiving an NCF. The default value is 10000 milliseconds.
`nak-eliminate-int <integer>`	Specifies the length of time (in milliseconds) during which a network element (NE) eliminates duplicate NAKs. When this interval expires, the NE suspends NAK elimination until the first duplicate arrives. Once this NAK is forwarded, the NE once again eliminates duplicate NAKs for the specified interval. This parameter must be less than `max-nak-rdata-int`. The default value is 5000 milliseconds.

Figure 172 shows sample output for the **`Config ip pgm interface info`** command.

Figure 172 config ip pgm interface info command output

```
8610:5/config/ip/pgm/interface/10.10.3.1# info

Sub-Context:
Current Context:

                        state : disabled
              nak-re-xmit-int : 1000
          max-nak-re-xmit-cnt : 2
            max-nak-rdata-int : 10000
            nak-eliminate-int : 5000
```

Showing PGM interface commands

There are three types of show interface commands:

- Interface configurations

  "Showing PGM interface configurations," next
- Interface errors

  "Showing PGM interface errors" on page 450

  "Showing PGM interface nak errors" on page 451
- Interface statistics

  "Showing PGM interface statistics" on page 452

  "Showing PGM interface nak statistics" on page 454

  "Showing PGM interface parity statistics" on page 455

Showing PGM interface configurations

To display information about the current PGM configuration on the selected interface, use the following command:

```
show ip pgm interface config
```

Figure 173 shows sample output for this command.

Figure 173 show ip pgm interface config command output

```
8610:5/show/ip/pgm/interface# config

================================================================================================
                          Pgm Interface Configuration
================================================================================================
CCT       ENABLE   STATE  NAK_RE_XMIT   MAX_NAK_RE    NAK_RDATA   NAK_ELIMINATE
                          INTERVAL      XMIT_COUNT    INTERVAL    INTERVAL
------------------------------------------------------------------------------------------------
Port1/1   enabled  down   1000          2             10000       5000

Port5/1   enabled  down   1000          2             10000       5000
```

Table 76 describes the **`show ip pgm interface config`** parameters.

Table 76 show ip pgm interface config parameters

Field	Description
CCT	Displays the circuit number of the selected interface.
ENABLE	Displays whether PGM is enabled or disabled on this interface.
STATE	Indicates the current state (up or down) of PGM.
NAK_RE_XMIT INTERVAL	Specifies how long to wait for an NCF (in milliseconds) before retransmitting the NAK. The default is 1000 milliseconds.
MAX_NAK_RE XMIT_COUNT	Displays the maximum number of NAK retransmission packets allowed per second.
NAK_RDATA INTERVAL	Displays how long to wait for RDATA (in milliseconds) after receiving an NCF.
NAK_ELIMINATE INTERVAL	Displays the length of time (in milliseconds) during which a network element (NE) eliminates duplicate NAKs. When this interval expires, the NE suspends NAK elimination until the first duplicate arrives. Once this NAK is forwarded, the NE once again eliminates duplicate NAKs for the specified interval. This parameter must be less than the NAK_RDATA INTERVAL.

Showing PGM interface errors

To display general information about errors that occurred on the selected interface, use the following command:

```
show ip pgm interface error general
```

Figure 174 shows sample output for this command.

Figure 174 show ip pgm interface error general command output

```
8610:5/show/ip/pgm/interface/error# general

================================================================================================
                    Pgm Interface General Error Statistics
================================================================================================
CCT          IN_SPM      IN_RDATA      IN_RDATA        IN_NCF      IN_NCF
             PORT        PORT          NO_SESSSION     PORT        NO_SESSION
             ERRORS      ERRORS        ERRORS          ERRORS      ERRORS
------------------------------------------------------------------------------------------------
Port1/1      3           2             0               1           0

Port5/1      0           1             2               0           1
```

Table 77 describes the **`show ip pgm interface error general`** parameters.

Table 77 show ip pgm interface error general parameters

Field	Description
CCT	Displays the circuit number of the selected interface.
IN_SPM PORT ERRORS	Displays the number of SPMs discarded because they were received on the wrong interface.
IN_RDATA PORT ERRORS	Displays the number of RDATA packets discarded because they were received on the wrong interface.
IN_RDATA NO_SESSION ERRORS	Displays the number of RDATA packets discarded because there was no active session.

Table 77 show ip pgm interface error general parameters (continued)

Field	Description
IN_NCF PORT ERRORS	Displays the number of NCFs discarded because they were received on the wrong interface.
IN_NCF NO_SESSION ERRORS	Displays the number of NCFs discarded because there was no active session.

Showing PGM interface nak errors

To display information about NAK and NNAK errors that occurred on the selected interface, use the following command:

```
show ip pgm interface error nak
```

Figure 175 shows sample output for this command.

Figure 175 show ip pgm interface error nak command output

```
8610:5/show/ip/pgm/interface/error# nak

================================================================================================
                          Pgm Interface NAK Error statistics
================================================================================================
CCT          IN_NAK   IN_NAK      IN_NAK     IN_NNAK     IN_NNAK       PARITY
             PORT     NO_SESSION  SEQ        PORT        NO_SESSION    NAK_TG
             ERRORS   ERRORS      ERRORS     ERRORS      ERRORS        ERRORS
------------------------------------------------------------------------------------------------
Port1/1      0        0           0          0           0             0

Port5/1      0        0           0          0           0             0
```

Table 78 describes the **`show ip pgm interface error nak`** parameters.

Table 78 show ip pgm interface error nak parameters

Field	Description
CCT	Displays the circuit number of the selected interface.
IN_NAK PORT ERRORS	Displays the number of NAKs discarded because they were received on the wrong interface.
IN_NAK NO_SESSION ERRORS	Displays the number of NAKs discarded because there was no active session.
IN_NAK SEQ ERRORS	Displays the number of NAKs discarded because they were out of sequence.
IN_NNAK PORT ERRORS	Displays the number of NNAKs discarded because they were received on the wrong interface.
IN_NNAK NO_SESSION ERRORS	Displays the number of NNAKs discarded because there was no active session.
PARITY NAK_TG ERRORS	Displays the number of parity NAKs discarded because they were out of the parity TG window.

Showing PGM interface statistics

To display general statistics about the selected interface, use the following command:

```
show ip pgm interface stat general
```

Figure 176 shows sample output for this command.

Figure 176 show ip pgm interface stat general command output

```
8610:5/show/ip/pgm/interface/stat# general

================================================================================================
                        Pgm Interface General Statistics
================================================================================================
CCT       TOTAL    TOTAL     IN     OUT    IN       OUT    IN     OUT    IN
          REXMIT   REXMIT    SPMS   SPMS   RDATA    RDATA  NCFS   NCFS   REDIRECT
          STATES   TIMEOUT                                             NCFS
------------------------------------------------------------------------------------------------
Port1/1   0        0         274    273    9        0      2      0      0

Port5/1   0        0         109    110    14       0      2      0      0
```

Table 79 describes the **`show ip pgm interface stat general`** parameters.

Table 79 show ip pgm interface stat general parameters

Field	Description
CCT	Displays the circuit number of the selected interface.
TOTAL REXMIT STATES	Displays the total number of retransmit state entries for this interface.
TOTAL REXMIT TIMEOUT	Displays the total number of timed out retransmit state entries for this interface.
IN SPMS	Displays the number of SPMs received on this interface.
OUT SPMS	Displays the number of SPMs sent out from this interface.
IN RDATA	Displays the number of RDATA packets received on this interface.
OUT RDATA	Displays the number of RDATA packets sent out from this interface.
IN NCFS	Displays the number of NCFs received on this interface.
OUT NCFS	Displays the number of NCFs sent out from this interface.
IN REDIRECT NCFS	Displays the number of redirected NCFs received on this interface.

Showing PGM interface nak statistics

To display information about NAK and NNAK statistics on the selected interface, use the following command:

```
show ip pgm interface stat nak
```

Figure 177 shows sample output for this command.

Figure 177 show ip pgm interface stat nak command output

```
8610:5/show/ip/pgm/interface/stat# nak

================================================================================================
                          Pgm Interface NAK statistics
================================================================================================
CCT          UNIQUE_NAKS     IN_NAKS    OUT_NAKS        IN_NNAKS    OUT_NNAKS
------------------------------------------------------------------------------------------------
Port1/1           2              0          0               0           0

Port5/1           1              0          0               0           0

------------------------------------------------------------------------------------------------
```

Table 80 describes the **`show ip pgm interface stat nak`** parameters.

Table 80 show ip pgm interface stat nak parameters

Field	Description
CCT	Displays the circuit number of the selected interface.
UNIQUE_NAKS	Displays the number of unique NAKs received on this interface.
IN_NAKS	Displays the number of NAKs received on this interface.
OUT_NAKS	Displays the number of unique NAKs sent out from this interface.
IN_NNAKS	Displays the number of NNAKs received on this interface.
OUT_NNAKS	Displays the number of NNAKs sent out from this interface.

Showing PGM interface parity statistics

To display parity information about the selected interface, use the following command:

```
show ip pgm interface stat parity
```

Figure 178 shows sample output for this command.

Figure 178 show ip pgm interface stat parity command output

```
8610:5/show/ip/pgm/interface/stat# parity

================================================================================================
                          Pgm Interface Parity Statistics
================================================================================================
CCT          IN      OUT       IN      OUT      IN      OUT     IN      OUT     UNIQUE
             SPMS    SPMS      RDATA   RDATA    NCFS    NCFS    NAKS    NAKS    NAKS
------------------------------------------------------------------------------------------------
Port1/1      86      87        2       0        2       0       0       0       0

Port5/1      211     212       6       0        2       0       0       0       0
```

Table 81 describes the **`show ip pgm interface stat parity`** parameters.

Table 81 show ip pgm interface stat parity parameters

Field	Description
CCT	Displays the circuit number of the selected interface.
IN SPMS	Displays the number of SPMs received on this interface.
OUT SPMS	Displays the number of SPMs sent out from this interface.
IN RDATA	Displays the number of RDATA packets received on this interface.
OUT RDATA	Displays the number of RDATA packets sent out from this interface.
IN NCFS	Displays the number of NCFs received on this interface.
OUT NCFS	Displays the number of NCFs sent out from this interface.
IN NAKS	Displays the number of NAKs received on this interface.

Table 81 show ip pgm interface stat parity parameters (continued)

Field	Description
OUT NAKS	Displays the number of unique NAKs sent out from this interface.
UNIQUE NAKS	Displays the number of unique NAKs received on this interface.

Configuring PGM on Ethernet ports

To configure PGM at the port level, use the following command:

`config ethernet <ports> ip pgm`

where:
ports use the convention {slot/port[-slot/port][,...]}.

This command includes the following parameters:

config ethernet <*ports*> ip pgm followed by:	
`info`	Displays current pgm settings on the selected port.
`state <enable|disable>`	Indicates the current state (enable or disable) of PGM on the selected port.
`nak-re-xmit-int <integer>`	Specifies how long to wait for an NCF (in milliseconds) before retransmitting the NAK. The default value is 1000 milliseconds.
`max-nak-re-xmit-cnt <integer>`	Configures the maximum number of NAK retransmission packets allowed per second. The default value is 2.

config ethernet <*ports*> ip pgm followed by:	
max-nak-rdata-int <*integer*>	Specifies how long to wait for RDATA (in milliseconds) after receiving an NCF. The default value is 10000 milliseconds.
nak-eliminate-int <*integer*>	Specifies the length of time (in milliseconds) during which a network element (NE) eliminates duplicate NAKs. When this interval expires, the NE suspends NAK elimination until the first duplicate arrives. Once this NAK is forwarded, the NE once again eliminates duplicate NAKs for the specified interval. This parameter must be less than max-nak-rdata-int. The default value is 5000 milliseconds.

Table 179 shows sample output for the **config ethernet <*ports*> ip pgm info** command.

Figure 179 config ethernet ip pgm info command output

```
8610:5/config/ethernet/1/1/ip/pgm# info
                        state : enabled
              nak-re-xmit-int : 1000
          max-nak-re-xmit-cnt : 2
            max-nak-rdata-int : 10000
            nak-eliminate-int : 5000
```

Configuring PGM on a VLAN

To configure PGM on a VLAN, use the following command:

`config vlan <vid> ip pgm`

where:
vid is a VLAN ID from 1 to 4092.

This command includes the following parameters:

config vlan <*vid*> ip pgm followed by:	
`info`	Displays current pgm settings on the selected VLAN.
`state <enable|disable>`	Indicates the current state (enable or disable) of PGM on the selected VLAN.
`nak-re-xmit-int <integer>`	Specifies how long to wait for an NCF (in milliseconds) before retransmitting the NAK. The default value is 1000 milliseconds.
`max-nak-re-xmit-cnt <integer>`	Configures the maximum number of NAK retransmission packets allowed per second. The default value is 2.
`max-nak-rdata-int <integer>`	Specifies how long to wait for RDATA (in milliseconds) after receiving an NCF. The default value is 10000 milliseconds.
`nak-eliminate-int <integer>`	Specifies the length of time (in milliseconds) during which a network element (NE) eliminates duplicate NAKs. When this interval expires, the NE suspends NAK elimination until the first duplicate arrives. Once this NAK is forwarded, the NE once again eliminates duplicate NAKs for the specified interval. This parameter must be less than `max-nak-rdata-int`. The default value is 5000 milliseconds.

Figure 180 shows sample output for the **`config vlan <vid> ip pgm info`** command.

Figure 180 config vlan ip pgm info command output

```
8610:5/config/vlan/2/ip/pgm# info
                        state : enabled
              nak-re-xmit-int : 1000
          max-nak-re-xmit-cnt : 2
            max-nak-rdata-int : 10000
            nak-eliminate-int : 5000
```

Displaying all IP PGM show commands

The **show ip pgm show-all** command displays all relevant IP PGM information.

The command uses the syntax:

`show ip pgm show-all [file <value>]`

where <*value*> is the filename to which the output will be redirected.

Figure 181 shows sample output for the **show ip pgm show-all** command.

Figure 181 show ip pgm show-all command output

```
Passport-8610:5# show ip pgm show-all

# show ip pgm global

                      enable : disabled
                       state : down
          session-life-time : 300
              nnak-generate : 1
        max-re-xmit-states : 200
       total-re-xmit-states : 0
               max-sessions : 100
             total-sessions : 0
       total-re-xmit-states-timeout : 0
          total-unique-naks : 0
       total-unique-parity-naks : 0

# show ip pgm interface config

================================================================================
                                    Pgm Interface Configuration
================================================================================
CCT  ENABLE    STATE    NAK_RE_XMIT  MAX_NAK_RE   NAK_RDATA    NAK_ELIMINATE
                        INTERVAL     XMIT_COUNT   INTERVAL     INTERVAL
--------------------------------------------------------------------------------
Port5/1  disabled  down     1000         2            10000        5000
Vlan1    disabled  down     1000         2            10000        5000
Vlan0    disabled  down     1000         2            10000        5000
```

Chapter 13
Viewing and editing multicast routes using the CLI

The multicast route commands (mroute commands) allow you to configure and view IP multicast routing parameters on the switch.

For more information about multicast concepts and terminology, see Chapter 1, "IP Multicast concepts."

This chapter includes the following topics:

Roadmap of multicast route commands

The following roadmap lists all the multicast route (mroute) commands and their parameters. After using the commands below to configure the Passport 8600, you can use the show commands to display information for a particular feature.

To facilitate troubleshooting, the Passport 8600 also provides *one* command (`show ip mroute show-all`) that lists all the show commands for IP mroutes and displays their configuration output. See “Displaying all IP mroute show commands” on page 480.

Use this list as a quick reference or click on any entry for more information:

Command	Parameter
`config ip mroute`	`info`
`config ip mroute interface <ipaddr>`	`info` `ttl <ttl>`

`config ip mroute static-source-group <GroupSubnet>`	`info`
	`create <SourceSubnet> <SrcSubnetMask>`
	`delete <SourceSubnet> <SrcSubnetMask>`

`config sys mcast-software-forwarding`	`info`
	`disable`
	`enable`

`show ip mroute interface`	
`show ip mroute next-hop`	
`show ip mroute route`	
`show ip mroute static-source-group [<GroupAddress>]`	

Command	Parameter
show ip mroute-hw group-trace	
show ip mroute-hw group-prune-state	
show sys mcast-software-forwarding	
config ip mroute resource-usage	info
	egress-Threshold <integer>
	ingress-Threshold <integer>
	send-Trap-And-Log <enable|disable>
	trap-Msg-Only <enable|disable>
	log-Msg-Only <enable|disable>
show ip mroute-hw resource-usage	
show ip mroute show-all [file <value>]	

Displaying multicast routes

To display information about the multicast routes configured on the switch, use the following command:

```
config ip mroute
```

This command includes the following parameters:

config ip mroute followed by:	
info	Displays information about the multicast route.

Showing a multicast route's next hop

To display information about the next hop for the multicast route(s) set up on the switch, use the following command:

```
show ip mroute next-hop
```

Figure 182 shows sample output for this command.

Figure 182 show ip mroute next-hop command output

```
8610# show ip mroute next-hop

================================================================================
                              Mroute Next Hop
================================================================================
INTERFACE   GROUP   SOURCESRCMASK   ADDRESS    STATE  EXPTIME   CLOSEHOP PROTOCOL

--------------------------------------------------------------------------------
```

Showing multicast route information

To display information about the multicast route(s) set up on the switch, use the following command:

```
show ip mroute route
```

Figure 183 shows sample output for this command.

Figure 183 show ip mroute route command output

```
8610# show ip mroute route

================================================================================
                                  Mroute Route
================================================================================
GROUP           SOURCE          SRCMASK         UPSTREAM_NBR    IF    EXPIR PROT
--------------------------------------------------------------------------------
```

Configuring a multicast route on an interface

To configure multicast routing on a specific interface, use the following command:

```
config ip mroute interface <ipaddr>
```

where:
ipaddr indicates the IP address of the selected interface.

This command includes the following parameters:

config ip mroute interface <ipaddr> followed by:	
`info`	Displays information about the multicast route interface.
`ttl <ttl>`	Sets the default time-to-live threshold for the multicast route interface. The range (in seconds) is 1 to 255.

Showing multicast routes on an interface

To display information about the multicast route(s) set up on the switch for a specific interface, use the following command:

```
show ip mroute interface
```

Figure 184 shows sample output for this command.

Figure 184 show ip mroute interface command output

```
8610# show ip mroute interface

================================================================
                        Mroute Interface
================================================================
INTERFACE  TTL   PROTOCOL
----------------------------------------------------------------
Vlan20     1     dvmrp
Vlan21     1     dvmrp
```

Configuring multicast static source groups

Static source groups enable you to configure **static** source-group entries in the DVMRP or PIM multicast routing table. Neither DVMRP nor PIM can prune these entries from the distribution tree. In other words, even if there are no receivers in the group, the multicast stream for a static source-group entry stays active.

Configuration considerations

The Passport 8600 supports static source groups using one of several multicast protocols: DVMRP, PIM-SM (sparse mode), and PIM-SSM (source specific multicast). For conceptual information about DVMRP, PIM and static source groups, refer to Chapter 1, "IP Multicast concepts."

Before you can configure a static source group, you must globally enable one of the following protocols:

- DVMRP - To globally enable DVMRP, refer to "Configuring DVMRP globally" on page 337."
- PIM sparse mode (SM) - To globally enable PIM-SM, refer to "Configuring PIM-SM globally" on page 392."
- PIM source specific multicast mode (SSM) - To globally enable PIM-SSM, refer to "Configuring Source Specific Multicast (SSM)" on page 429."

After configuring static source groups, keep the following points in mind:

- The maximum number of static source groups should not exceed 1024.
- Disabling DVMRP or PIM causes the switch to deactivate all of the static source groups. When you re-enable DVMRP or PIM, the switch re-activates the static source groups.
- **Using DVMRP or PIM-SM**

  In DVMRP and PIM-SM configurations, the static source-group feature works for both specific source addresses and subnet addresses. This is achieved by using the `create <SourceSubnet> <SubnetMask>` parameter (see "Viewing and editing static source groups").

When the Network Mask is configured as 255.255.255.255, the full source address is used to match the (S,G) which is the specific source case. When the network mask field is configured as a subnet mask for the source, only the source subnet is used to match (S,G)s. The first entry in Figure 185 shows a subnet configuration and the second entry shows a source specific configuration.

- **Using PIM-SSM**

  In PIM-SSM configurations, static source groups have the following limitations:

  — **Subnets** - SSM static source groups work *only* with specific IP addresses. This means that static source groups cannot work with source subnets so the mask must be a full 32-bit mask, 255.255.255.255.

  — **SSM Channels** - Static source groups cannot conflict with SSM channels and vice versa. When you configure a static source group or an SSM channel, the switch performs a consistency check to make sure there are no conflicts. You cannot map one group (G) to different sources for both a static source group and an SSM channel. For SSM channel information, refer to "Configuring SSM dynamic learning and range group" on page 293.

  If a group is already mapped to a source and you try to map it to a different source, the switch detects the conflict and displays an error message. For example, if G1 is already defined in the SSM channel table as (S1,G1), you cannot configure G1 as static source group (S2,G1). However, you can configure the same entry (S1,G1) in both the SSM channel table and as a static source group. As long as there is no conflict between the two tables, the configuration is allowed.

Viewing and editing static source groups

To configure a static source-group entry in the DVMRP or PIM multicast routing table, use the following command:

```
config ip mroute static-source-group <GroupSubnet>
```

where:
GroupSubnet is the IP address of the multicast group.

This command includes the following parameters:

config ip mroute static-source-group <GroupSubnet> followed by:	
`info`	Displays information about the source-group entry.
`create <SourceSubnet> <SrcSubnetMask>`	Creates a new static multicast source-group entry. You cannot create duplicate groups.[1] • *SourceSubnet* is the multicast source address for this static source-group entry. How you configure the source address depends on the protocol you are using and in what mode. For more information, refer to "Configuration considerations." • *SrcSubnetMask* is the source's subnet mask for this static source-group entry.
`delete <SourceSubnet> <SrcSubnetMask>`	Deletes the source-group entry from the static source-group table.

1 To avoid conflicts between the static source group table and the SSM channel table, refer to "Configuration considerations" before creating a static source group.

Configuration example

This configuration example uses the commands described above to perform the following tasks:

- Create a static source group for two multicast groups: 224.32.2.1 and 226.50.2.2.

  The static mroute for group 224.32.2.1 is for a source subnet 10.10.10.0/24.

  The static mroute for group 226.50.2.2 is for host 20.20.20.100/32.

- Use the **`info`** command to show a summary of the results.

```
Passport-8610:5/config/ip/mroute# static-source-group 224.32.2.1
Passport-8610:5/config/ip/mroute/static-source-group/224.32.2.1#
create 10.10.10.0 255.255.255.0
Passport-8610:5/config/ip/mroute/static-source-group/224.32.2.1#
info

Sub-Context:
Current Context:

                     create :
                               Source Address - 10.10.10.0
                           Source Subnet Mask - 255.255.255.0
                     delete : N/A

Passport-8610:5/config/ip/mroute/static-source-group/224.32.2.1#



Passport-8610:5/config/ip/mroute# static-source-group 226.50.2.2
Passport-8610:5/config/ip/mroute/static-source-group/226.50.2.2#
create 20.20.20.100 255.255.255.255
Passport-8610:5/config/ip/mroute/static-source-group/226.50.2.2#
info

Sub-Context:
Current Context:

                     create :
                               Source Address - 20.20.20.100
                           Source Subnet Mask - 255.255.255.255
                     delete : N/A

Passport-8610:5/config/ip/mroute/static-source-group/226.50.2.2#
```

Showing multicast static source groups

To display information about the static source groups on the current interface, use the following command:

```
show ip mroute static-source-group [<GroupAddress>]
```

You can see all the valid entries that were created. If the entry was created with "x" bit mask, it shows as "x" bit in the output.

Figure 185 shows sample output for both configurations of the **`show ip mroute static-source-group`** command.

Figure 185 show ip mroute static-source-group command output

```
8610:5# show ip mroute static-source-group

================================================================
          IP Multicast Static Source Group Table
================================================================
Group              Source             Subnet
Address            Address            Mask
----------------------------------------------------------------
224.32.2.1         10.10.10.0         255.255.255.0
226.50.2.2         20.20.20.100       255.255.255.255
----------------------------------------------------------------

Total:- 2
```

Showing DVMRP troubleshooting information

The `mroute-hw` command provides an exact hardware view of existing IP multicast records and information on sender and receiver ports for every stream.

To display DVMRP troubleshooting information, use the following command:

```
show ip mroute-hw group-trace
```

and

```
show ip mroute-hw group-prune-state
```

Figure 186 shows sample output for the group-trace grp command.
Figure 187 shows sample output for the group-trace src command.
Figure 188 shows sample output for the group-prune-state grp command.

`show ip mroute-hw` followed by:	
`group-trace` [`src` <*`value`*>] [`grp` <*`value`*>]	You use the `show ip mroute-hw group-trace` command as follows: • When you use it by itself, the output includes all the group entries found in the hardware records. • When you follow the command with `grp` <*`value`*>, the output includes all the entries corresponding to the specified Group Address (Figure 186). • When you follow the command with `src` <*`value`*> and `grp` <*`value`*>, the output includes only the specified Source-Group pair (Figure 187).
`group-prune-state` [`grp` <*`value`*>]	You use the `show ip mroute-hw group-prune-state` command as follows: • When you use it by itself, the output includes all the group entries found in the hardware records. • When you follow the command with `grp` <*`value`*>, the output includes all the entries corresponding to the specified Group Address (Figure 188).

Figure 186 show ip mroute-hw group-trace grp command output

```
Passport-8610:5# show ip mroute-hw group-trace grp
239.255.48.189
================================================================
                        Group-Trace
================================================================
GROUP            SOURCE  SENDING  TOTAL     IN   IN    OUT    OUT
ADDRESS          ADDRESS SUBNET   SESSIONS VLAN PORT  VLAN PORTS
239.255.48.189 1.2.3.5 1.2.3.0   1         25  1/25    5     1/1
239.255.48.189 5.5.5.4  5.5.5.0   1          5  1/1    25    1/25
                                                      5     1/1

Total 2
```

Figure 187 show ip mroute-hw group-trace src grp command output

```
Passport-8610:5# show ip mroute-hw group-trace src 1.2.3.5
grp 239.255.48.189
================================================================
                        Group-Trace
================================================================
GROUP            SOURCE  SENDING  TOTAL     IN   IN    OUT    OUT
ADDRESS          ADDRESS SUBNET   SESSIONS VLAN PORT  VLAN PORTS
239.255.48.189 1.2.3.5 1.2.3.0   1         25  1/25    5     1/1
```

Figure 188 show ip mroute-hw group-prune-state grp command output

```
Passport-8610:5# show ip mroute-hw group-prune-state grp
239.255.12.189
================================================================
                      Group Prune State
================================================================
GROUP            SOURCE    PRUNED    TIME LEFT     PRUNE
ADDRESS          ADDRESS             FOR GRAFT     RECEIVED FROM
239.255.12.189   1.2.3.5   FALSE     0
239.255.12.189   5.5.5.4   TRUE      8821          28.2.2.7

Total 2
```

Table 82 describes the output fields that appear in Figure 186, Figure 187, and Figure 188.

Table 82 show ip mroute-hw group-trace and group-prune-state output fields

Field	Description
Group Address	The IP multicast group address for the multicast stream.
Source Address	The IP addresses of the sources on this particular subnet sending traffic to the multicast group for the selected entry in the Mroute-HW table.
Sending Subnet	The network address of the source subnet that has sources sending IP multicast traffic to the group address. **Note:** There can be several sources sending to that group. Use the Source tab to view these sources.
Total Sessions	One session includes a combination of group address, subnet and ingress VLAN information. The total number of sessions indicates how many sources in the same subnet are sending the traffic for the given group address and ingress VLAN.
In Vlan	The ingress VLAN ID where the traffic emanates for the multicast stream.
In Port	The corresponding ingress port in the multicast stream selected from the Mroute-HW table.
Out Vlan	All the egress VLANs for the particular multicast stream selected from the Mroute-HW table.
Out Port	The corresponding ports for the particular multicast stream selected from the Mroute-HW table.
Pruned	True indicates that the multicast stream has been pruned back. False indicates it has not.
Time left for Graft	The time left for the neighboring downstream router to send the graft message.
Prune received from	The IP address of the downstream neighbor from whom the prune has been received.

Configuring IP multicast software forwarding

The IP multicast software forwarding feature enables the CPU to initially forward IP multicast data until a hardware record is created. The CPU forwards the initial packets of a stream it receives and at the same time, creates a corresponding hardware record for any subsequent packets. The advantage to this feature is that it avoids any initial data loss experienced by multicast applications, and is most suited for low bandwidth.

The IP multicast software forwarding is a global system configuration feature that applies to all IP multicast enabled interfaces and protocols. When you enable IP multicast software forwarding, be aware that the hardware is still responsible for forwarding IP multicast traffic. Only initial data traffic is forwarded by the software. Thus, the intention here is not to replace hardware forwarding with software forwarding. By default, the feature is disabled.

Note: To avoid overloading the CPU, Nortel Networks recommends that you do not use the IP multicast software forwarding feature for video multicast applications.

To configure IP multicast software forwarding, use the following command:

```
config sys mcast-software-forwarding
```

This command includes the following parameters:

config sys mcast-software-forwarding followed by:	
`info`	Displays the current `config sys mcast-software-forwarding` information.
`disable`	Disables IP multicast software forwarding. This is the default.
`enable`	Enables IP multicast software forwarding. The default is disable.

Figure 189 config sys mcast-software-forwarding info command output

```
Passport-8610:5# config sys mcast-software-forwarding info

Sub-Context: clear config dump monitor show test trace wsm
Current Context:

                    enable    :disabled

Passport-8610:5#
```

Showing the software forwarding configuration

To display the current IP multicast software forwarding configuration, use the following command:

`show sys mcast-software-forwarding`

Figure 190 shows sample output for this command.

Figure 190 show sys mcast-software-forwarding command output

```
Passport-8610:5# show sys mcast-software-forwarding

================================================================
                        Mcast Software Forwarding
================================================================
McastSoftwareForwarding :disabled

Passport-8610:5#
```

Configuring the resource usage counter for multicast streams

The Passport 8600 enables you to query the number of ingress and egress IP multicast streams traversing your switch. Once you have set the thresholds for ingress and egress records, if the record-usage goes beyond the threshold, you will be notified by way of a trap on the console, logged message, or both.

Note: If you do not set the thresholds, the CLI displays only the ingress and egress records that are currently in use. To see these records, enter one of the following commands:

```
config ip mroute resource-usage info
```

```
show ip mroute-hw resource-usage
```

To configure the record usage counter and notification method, use the following command:

```
config ip mroute resource-usage
```

This command includes the following parameters:

config ip mroute resource-usage followed by:	
`info`	Displays the record usage counter's current configuration.
`egress-Threshold <integer>`	Sets the egress record threshold (S,G). A notification message is sent if this value is exceeded. *integer* is a value between 0 and 32767.
`ingress-Threshold <integer>`	Sets the ingress record threshold (peps). A notification message is sent if this value is exceeded. *integer* is a value between 0 and 32767.
`send-Trap-And-Log <enable|disable>`	Sets the notification method to sending both a trap message and a log message when the threshold level is exceeded.[1]

config ip mroute resource-usage followed by:	
`trap-Msg-Only <enable|disable>`	Sets the notification method to sending only a trap message when the threshold level is exceeded.
`log-Msg-Only <enable|disable>`	Sets the notification method to sending only a log message when the threshold level is exceeded.

1 You can set only one notification type.

Configuration example

This configuration example uses the commands described above to perform the following tasks:

- Set the egress threshold to 200.
- Set the ingress threshold to 100.
- Enable the log message notification method.
- Use the `info` command to show a summary of the results.

```
8610:5/config/ip/mroute/resource-usage# egress-Threshold 200
8610:5/config/ip/mroute/resource-usage# ingress-Threshold 100
8610:5/config/ip/mroute/resource-usage# log-Msg-Only enable
8610:5/config/ip/mroute/resource-usage# info

Sub-Context:
Current Context:

                      Egress Records InUse : 0
                     Ingress Records InUse : 0
                          Egress Threshold : 200
                         Ingress Threshold : 100
                              Log Msg Only : true
                            Send Trap Only : false
                     Send Trap And Log Msg : false
8610:5/config/ip/mroute/resource-usage#
```

Showing the hardware resource usage output

To display hardware resource usage output, enter the CLI command

```
show ip mroute-hw resource-usage
```

Figure 191 displays sample output for this command:

Figure 191 `show ip mroute-hw resource-usage` command output

```
PP8600:6# show ip mroute-hw resource-usage

================================================================================
                                  Multicast Hardware Record Usage
================================================================================
EGRESS      INGRESS     EGRESS      INGRESS     LOG MSG   SEND TRAP  SEND TRAP
REC IN-USE REC IN-USE THRESHOLD   THRESHOLD  ONLY      ONLY        AND LOG
--------------------------------------------------------------------------------
0           0           200         100         true      false      false

PP8600:6#
```

where:

EGRESS REC IN-USE displays the number of egress records (peps) that are in use traversing the switch.

INGRESS REC IN-USE is the number of S,G records that are in use traversing the switch.

Displaying all IP mroute show commands

The **show ip mroute show-all** command displays all relevant IP mroute information.

The command uses the syntax:

```
show ip mroute show-all [file <value>]
```

where <*value*> is the filename to which the output will be redirected.

Figure 192 shows sample output for the **show ip mroute show-all** command.

Figure 192 show ip mroute show-all command output

```
Passport-8600:5# show ip mroute show-all

# show ip mroute interface

================================================================================
                                      Mroute Interface
================================================================================
INTERFACE  TTL   PROTOCOL
--------------------------------------------------------------------------------
Port7/7    1     dvmrp
Port7/8    1     dvmrp
Vlan10     1     dvmrp
Vlan1000   1     dvmrp
Vlan1010   1     dvmrp
Vlan1020   1     dvmrp
Vlan1030   1     dvmrp
Vlan1040   1     dvmrp
Vlan1050   1     dvmrp
Vlan1060   1     dvmrp
Vlan1070   1     dvmrp
Vlan1080   1     dvmrp
Vlan1090   1     dvmrp
Vlan1400   1     none
Vlan1500   1     none

# show ip mroute next-hop
```

Chapter 14
Configuring multicast flow distribution over MLT using the CLI

Multicast flow distribution over MultiLink Trunking (MLT) provides a mechanism for distributing multicast streams over an MLT. This enables you to distribute the load on different ports of the MLT and aim (whenever possible) to achieve an even distribution of the streams.

To configure multicast flow distribution over MLT, you must enable it globally and per MLT. For more information about MLT, see *Configuring Layer 2 Operations: VLANs, Spanning Tree, and Mulitlink Trunking*.

This chapter includes the following topics:

Roadmap of multicast MLT commands

The following roadmap lists all the multicast MLT commands and their parameters. Use this list as a quick reference or click on any entry for more information:

Command	Parameter
config sys mcast-mlt-distribution	info
	enable
	disable
	grp-mask <grp-mask>
	src-mask <src-mask>
	redistribution <enable|disable>
config mlt <mltid> mcast-distribution	enable
	disable
show sys mcast-mlt-distribution	

Configuring multicast flow distribution globally

To configure multicast flow distribution over MLT globally, use the following command.

```
config sys mcast-mlt-distribution
```

This command includes the following parameters:

config sys mcast-mlt-distribution followed by:	
`info`	Displays the current `config sys mcast-mlt-distribution` information.
`enable`	Enables multicast MLT distribution globally.
`disable`	Disables multicast MLT distribution. This is the default.
`grp-mask <grp-mask>`	Specifies a group mask to use when distributing multicast traffic over an MLT. The default is 255.255.255.255.
`src-mask <src-mask>`	Specifies a source mask to use when distributing multicast traffic over an MLT. The default is 255.255.255.255. Ensure that the mask values for *`grp-mask`* and *`src-mask`* are contiguous.
`redistribution <enable|disable>`	Enables or disables the multicast MLT redistribution feature. The default is disabled.

Configuration example

This configuration example uses the commands described above to perform the following tasks:

- Enable multicast flow distribution over MLT globally.
- Set the mask for the group so that it takes into account the last byte of the group address.
- Set the mask for the source so that it takes into account the last two bytes of the source IP address.

- Enable redistribution to allow streams to be redistributed in case of changes in the MLT.

After configuring the parameters, use the **`info`** command to show a summary of the results.

```
8610:5# config sys mcast-mlt-distribution enable
8610:5# config sys mcast-mlt-distribution grp-mask 0.0.0.255
8610:5# config sys mcast-mlt-distribution src-mask 0.0.255.255
8610:5# config sys mcast-mlt-distribution redistribution enable
8610:5# config sys mcast-mlt-distribution info

Sub-Context: clear config dump monitor show test trace
Current Context:

                    enable    :enabled
                    grpmask   :0.0.0.255
                    srcmask   :0.0.255.255
              redistribution  :enabled

8610:5#
```

Configuring multicast flow distribution per MLT

To enable multicast flow distribution per MLT, use the following command:

```
config mlt <mltid> mcast-distribution
```

where:
mltid is the MultiLink Trunking ID, which is {1..6} for an 8100 switch, and {1..32} for an 8600 switch.

This command includes the following parameters:

config mlt <mltid> mcast-distribution followed by:	
enable	Enables multicast MLT distribution on the specified MLT.
disable	Disables multicast MLT distribution on the specified MLT. This is the default.

Showing the multicast MLT distribution show command

To display the current multicast over MLT configuration, use the following command:

```
show sys mcast-mlt-distribution
```

Figure 193 shows sample output for this command.

Figure 193 show sys mcast-mlt-distribution command output

```
8610:5# show sys mcast-mlt-distribution

================================================================
                        Mcast Over MLT Global Group
================================================================
McastOverMLtStat    :enabled
GrpMask             :0.0.0.255
SrcMask             :0.0.255.255
Redistribution      :enabled

8610:5#
```

Note you can also use the **`show mlt info`** command to display whether multicast flow distribution is enabled per MLT.

Chapter 15
Configuring multicast MAC filtering using the CLI

Multicast MAC filtering allows you to create a smaller flooding domain inside a VLAN. For a particular VLAN, you specify a multicast MAC address and a subset of ports. When clients send data to that designated MAC address, only that subset of ports will then receive the traffic.

For more information about multicast MAC filtering, see Chapter 1, “IP Multicast concepts.”

This chapter includes the following topics:

Roadmap of multicast MAC filtering commands

The following roadmap lists all the multicast MAC filtering commands and their parameters. Use this list as a quick reference or click on any entry for more information:

Command	Parameter
config vlan <vid> static-mcastmac	info
	add mac <value> [port <value>] [mlt <value>]
	add-mlt <mid> mac <value>
	add-ports <ports> mac <value>
	delete mac <value>
	delete-mlt <mid> mac <value>
	delete-ports <ports> mac <value>
config ip arp static-mcastmac	info
	add mac <value> ip <value> vlan <value> [port <value>] [mlt <value>]
	delete <ipaddr>
show vlan info static-mcastmac [<vid>]	
show ip arp static-mcastmac	
show vlan info ports [<vid>]	
show vlan info all [<vid>] [by <value>]	

Configuring Layer 2 multicast MAC filtering

To configure Layer 2 multicast MAC filtering, use the following command:

```
config vlan <vid> static-mcastmac
```

where:
vid is a VLAN from 1 to 4092.

This command has the following parameters:

config vlan <vid> static-mcastmac followed by:	
`info`	Displays current settings.
`add mac <value> [port <value>] [mlt <value>]`	Adds VLAN static multicast MAC entries, where: • mac <*value*> is the MAC address.[1] • port <*value*> is the port to receive the multicast flooding. • mlt <value is the MID.
`add-mlt <mid> mac <value>`	Adds MLT to VLAN static multicast MAC entries.
`add-ports <ports> mac <value>`	Adds ports to VLAN static multicast MAC entries.
`delete mac <value>`	Deletes VLAN static multicast MAC entries.
`delete-mlt <mid> mac <value>`	Deletes MLT-to-VLAN static multicast MAC entries.
`delete-ports <ports> mac <value>`	Deletes ports from VLAN static multicast MAC entries.

1 This parameter does not accept MAC addresses beginning with 01:00:5e (01:00:5e:00:00:00 to 01:00:5e:ff:ff:ff inclusive). If you attempt to use this type of address, the following error message is displayed: `Error: Invalid MAC address`

Configuration example

This configuration example uses the commands described above to perform the following tasks:

- Add multicast MAC address 01:02:03:04:05:06 as a static MAC in VLAN 2.
- Add ports and an MLT group so that traffic destined for the MAC address is forwarded to ports 4/1 through 4/4 and MLT 1, instead of being flooded to all VLAN 2 ports.

After configuring the parameters, use the **`info`** command to show a summary of the results.

```
8610:5# config vlan 3 static-mcastmac add mac 01:02:03:04:05:06
port 4/1-4/4 mlt 1
8610:5# config vlan 3 static-mcastmac info
Sub-Context:
Current Context:

                        add:
                       macaddress - :   01:02:03:04:05:06
                       portmember -     4/1-4/4
                       mltgroups -      1

                       remove: N/A
8610:5#
```

Configuring Layer 3 multicast MAC filtering

To configure Layer 3 multicast MAC filtering, use the following command:

```
config ip arp static-mcastmac
```

This command has the following parameters:

config ip arp static-mcastmac followed by	
`info`	Displays current settings.
`add mac <value> ip <value> vlan <value> [port <value>] [mlt <value>]`	Adds static multicast MAC entries, where: • mac <*value*> is the MAC address.[1] • ip <*value*> is the IP address. • vlan <*value*> is the VLAN ID number. • port <*value*> is the port to receive the multicast flooding. • mlt <*value*> is the MID.
`delete <ipaddr>`	Deletes static multicast MAC entries.

1 This parameter does not accept MAC addresses beginning with 01:00:5e (01:00:5e:00:00:00 to 01:00:5e:ff:ff:ff inclusive). If you attempt to use this type of address, the following error message is displayed: `Error: Invalid MAC address`

Configuration example

This configuration example uses the commands described above to perform the following tasks:

- Add multicast MAC address 01:01:01:01:01:02 as a static ARP entry in VLAN 2.
- Add ports and an MLT group so that traffic destined for the MAC address is forwarded to ports 4/14 and 4/43, and MLT 1, instead of being flooded to all VLAN 2 ports.

After configuring the parameters, use the **`info`** command to show a summary of the results.

```
8610:5# config ip arp static-mcastmac add mac 01:01:01:01:01:02 ip
2.2.2.100 vlan 2 port 4/14-4/43 mlt 1
8610:5# config ip arp static-mcastmac info
================================================================
                    Ip Static Multicast MAC Arp
================================================================
IP_ADDRESS    MAC_ADDRESS         VLAN   PORT      MLT ID
2.2.2.100     01:01:01:01:01:02   2      4/14-4/43 1


Total 1
8610:5#
```

Showing the Layer 2 multicast MAC filters

To display the Layer 2 multicast MAC filters, use the following command:

```
show vlan info static-mcastmac [<vid>]
```

where:
vid is the VLAN ID from 1 to 4092. Entering a *vid* is optional. When you enter a *vid,* the command displays information for the specified VLAN. Without the *vid*, the command displays information for all the configured VLANs.

Figure 194 shows sample output of this command.

Figure 194 show vlan info static-mcastmac command output

```
-8610:5# show vlan info static-mcastmac
================================================================
                        Vlan Mcastmac
================================================================
VLAN_ID   MAC_ADDRESS         PORT_LIST        MLT_GROUPS
2         01:02:03:04:05:06   4/1, 4/4         N/A
2         01:01:01:01:01:02   4/1              N/A
2         01:01:02:02:03:03   4/1              N/A
2         01:03:0e:02:04:02   4/1              N/A
2         01:01:05:06:05:06   4/1              N/A
3         01:01:01:02:02:02   4/43              1
```

Showing the Layer 3 multicast MAC ARP data

To display Layer 3 multicast MAC ARP data, use the following command:

```
show ip arp static-mcastmac
```

Figure 195 shows sample output of this command.

Figure 195 show ip arp static-mcastmac command output

```
8610:5# show ip arp static-mcastmac

================================================================
                Ip Static Multicast MAC Arp
================================================================
IP_ADDRESS    MAC_ADDRESS         VLAN   PORT      MLT ID
3.3.3.6       01:01:01:02:02:02   3      4/43      1
2.2.2.100     01:01:01:01:01:02   2      4/1-4/2   -
2.2.2.200     01:01:02:02:03:03   2      4/1       -
2.2.2.201     01:03:0e:02:04:02   2      4/1       -
2.2.2.222     01:01:05:06:05:06   2      4/1       -
```

Showing VLAN port data

To display VLAN port data, use the following command:

```
show vlan info ports [<vid>]
```

Figure 196 shows sample output of this command.

Figure 196 show vlan info ports command output

```
8610:5# show vlan info ports
================================================================
                        Vlan Port
================================================================
VLAN   PORT           ACTIVE          STATIC    NOT_ALLOW
ID     MEMBER         MEMBER          MEMBER    MEMBER
1      4/5 4/10-4/38  4/5, 4/10-4/38
       4/43-4/48      4/43-4/48

2      4/1-4/4        4/1-4/4

3      4/39-4/42      4/39-4/43
```

Showing the multicast VLAN information

To display information about all the VLANs, use the following command:

```
show vlan info all [<vid>] [by <value>]
```

Figure 197 shows sample output of this command.

Figure 197 show vlan info all command output

```
8610:5# show vlan info ports

================================================================
             Static Mcast Mac
================================================================
VLAN_ID   MAC_ADDRESS         PORT_LIST        MLT_GROUPS
3         01:02:03:04:03:04   10/3, 10/5       N/A

Total Entries: 1
```

Index

F

H

I

L

M

N

P

R

S

T

V