

Part No. 314719-C Rev 00  
May 2004

4655 Great America Parkway  
Santa Clara, CA 95054

# Configuring IP Multicast Routing Operations

Passport 8000 Series Software Release 3.7



**NORTEL**  
**NETWORKS™**

## Copyright © 2004 Nortel Networks

All rights reserved. May 2004.

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

---

<b>Preface</b> .....	<b>29</b>
Before you begin .....	29
Text conventions .....	30
Acronyms .....	31
Hard-copy technical manuals .....	32
How to get help .....	32
<b>Chapter 1</b>	
<b>IP Multicast concepts</b> .....	<b>33</b>
Overview of IP Multicast .....	34
Multicast host groups .....	36
Multicast addresses .....	37
Multicast protocols .....	37
Static source groups .....	38
Internet Group Management Protocol (IGMP) .....	39
IGMP queries .....	39
IGMP host reports .....	40
Host leave messages .....	41
Fast leave feature .....	41
Fast leave mode .....	41
8000 Series implementation of IGMP .....	42
IGMP snoop .....	43
IGMP proxy .....	43
IGMP versions .....	44
Multicast access control feature .....	44
Multicast access control policy types .....	46
deny-tx .....	46
deny-rx .....	47
deny-both .....	48
allow-only-tx .....	48
allow-only-rx .....	49
allow-only-both .....	49

---

Specifying host addresses and masks .....	49
Multicast stream limitation feature .....	50
Multicast Router Discovery Protocol (MRDISC) .....	51
Distance Vector Multicast Routing Protocol (DVMRP) .....	52
Reverse path forwarding .....	53
Pruning and grafting .....	53
DVMRP concepts and terminology .....	54
Neighbor connections .....	54
Source route advertisements .....	54
How DVMRP chooses a route .....	55
Routing table .....	55
Shortest-path trees .....	56
DVMRP static source groups .....	56
DVMRP routing policies .....	57
Default route policy .....	57
Announce policy .....	59
Accept policy .....	61
Advertisement of local networks policy .....	63
DVMRP passive interface policy .....	64
8000 Series implementation of DVMRP .....	64
Protocol Independent Multicast-Sparse Mode (PIM-SM) .....	65
PIM-SM concepts and terminology .....	66
Hosts .....	66
PIM-SM domain .....	66
Designated router (DR) .....	67
Rendezvous-Point (RP) router .....	67
Bootstrap router .....	69
Join/prune messages .....	69
Register and register-stop messages .....	70
Shared trees and shortest-path trees .....	70
Shared trees .....	70
Shortest-path trees .....	70
Receiver joining group .....	72
Receiver leaving group .....	72
Source sending packets to group .....	72

---

Required elements for PIM-SM operation .....	73
PIM-SM simplified example .....	74
PIM-SM static source groups .....	75
PIM-SSM (Source Specific Multicast) .....	75
SSM features .....	76
PIM-SSM architecture .....	76
8000 Series implementation of SSM and IGMP .....	78
SSM range .....	78
SSM channel table .....	79
SSM and IGMPv2 .....	79
SSM and IGMPv3 .....	80
PIM-SSM static source groups .....	82
Configuration limitations .....	82
PIM passive interfaces .....	82
Pragmatic General Multicast (PGM) .....	84
PGM concepts and terminology .....	85
Transport session identifiers (TSIs) .....	85
Source path messages (SPMs) .....	85
Negative acknowledgements (NAKs) .....	85
NAK confirmations (NCFs) .....	86
Designated local repairers (DLRs) .....	86
PGM network element .....	86
Multicast flow distribution over MLT .....	87
Distribution algorithm .....	87
Traffic redistribution .....	89
Configuring multicast MLT distribution .....	90
Multicast MAC filtering .....	91
Configuration example .....	92
<b>Chapter 2</b>	
<b>Configuring IGMP using Device Manager .....</b>	<b>93</b>
Configuration prerequisites and notes .....	94
Configuring IGMP parameters on a brouter port .....	94
Configuring fast leave mode and enabling trap/logs .....	97
Configuring IGMP parameters on a VLAN .....	100

---

---

Enabling IGMP snooping on a VLAN .....	103
Viewing IGMP cache information .....	104
Viewing and editing the IGMP interface table .....	106
Viewing multicast router discovery information .....	109
Viewing IGMP snooping information .....	111
Viewing IGMP group information .....	112
Creating and viewing IGMP static information .....	114
Configuring multicast access control .....	116
Configuring a prefix list .....	116
Configuring multicast access control for an interface .....	118
Configuring IGMP sender entries .....	121
Configuring the SSM range and global parameters .....	122
Configuring the SSM channel table .....	126
Configuring multicast stream limitation .....	129
Configuring multicast stream limitation on an interface .....	129
Configuring multicast stream limitation members .....	131
Adding a multicast stream limitation member .....	132
Deleting a multicast stream limitation member .....	133
Configuring multicast stream limitation on an Ethernet port .....	134
Configuring multicast stream limitation on a VLAN .....	136

### **Chapter 3**

## **Configuring DVMRP using Device Manager .....** 139

Configuration prerequisites .....	140
Enabling DVMRP globally .....	141
Enabling DVMRP on a brouter port .....	143
Enabling DVMRP on a VLAN .....	146
Viewing and editing DVMRP interface parameters .....	149
Viewing and editing DVMRP interface advance parameters .....	150
Viewing DVMRP neighbor parameters .....	152
Viewing DVMRP learned routes .....	153
Viewing DVMRP next hop information .....	154
Configuring DVMRP routing policies .....	156
Configuring default route policies .....	156
Applying the default route policy to an interface .....	157

---

Applying the default route policy to a VLAN .....	158
Applying the default route policy to a port .....	159
Configuring DVMRP announce policies .....	160
Creating a DVMRP announce policy .....	160
Applying a DVMRP announce policy to an interface .....	167
Applying a DVMRP announce policy to a VLAN .....	168
Applying a DVMRP announce policy to a port .....	169
Configuring DVMRP accept policies .....	170
Creating a DVMRP accept policy .....	171
Applying a DVMRP accept policy to an interface .....	173
Applying a DVMRP accept policy to a VLAN .....	174
Applying a DVMRP accept policy to a port .....	175
Configuring the advertisement of local network policies .....	176
Apply the advertisement of local networks policy over an interface .....	177
Apply the advertisement of local networks policy over a VLAN .....	178
Apply the advertisement of local networks policy over a port .....	179
Configuring a DVMRP interface type .....	180
Configuring an active or passive interface type .....	181
Configuring an active or passive VLAN type .....	182
Configuring an active or passive port type .....	183
Displaying DVMRP routing policy information .....	184
Displaying DVMRP routing policy information for an interface .....	184
Displaying DVMRP routing policy information for a VLAN .....	185
Displaying DVMRP routing policy information for a port .....	185
<b>Chapter 4</b>	
<b>Configuring PIM using Device Manager .....</b>	<b>187</b>
Configuration prerequisites .....	189
Enabling PIM-SM globally .....	190
Enabling static RP .....	193
Configuration considerations .....	193
Enabling static RP procedure .....	194
Configuring static RP .....	195
Enabling PIM on a brouter port .....	197
Changing the interface type .....	198

---

---

Configuring a candidate bootstrap router (C-BSR) .....	199
Enabling PIM on a VLAN interface .....	200
Changing the VLAN interface type .....	202
Viewing and editing PIM interface parameters .....	203
Viewing PIM-SM neighbor parameters .....	206
Viewing the RP Set parameters .....	207
Configuring a candidate RP .....	208
Viewing the current bootstrap router (BSR) .....	210
Configuring Source Specific Multicast (SSM) .....	211
Configuration prerequisites .....	211
Enabling Source Specific Multicast (SSM) globally .....	212

## **Chapter 5**

### **Configuring PGM using Device Manager..... 217**

Configuration prerequisites .....	218
Enabling PGM globally .....	219
Enabling PGM on an interface .....	221
Configuring VLANs with PGM .....	223
Viewing and editing PGM interface parameters .....	226
Graphing PGM interface statistics .....	227
Graphing SPM and RDATA statistics for an interface .....	228
Graphing NAK, NNAK, and NCF statistics for an interface .....	230
Viewing PGM session parameters .....	233
Graphing PGM session statistics .....	234
Graphing SPM statistics for a session .....	235
Graphing NAK statistics for a session .....	237
Viewing the Retransmit parameters .....	240

## **Chapter 6**

### **Viewing and editing multicast routes using Device Manager ..... 243**

Viewing multicast route information .....	244
Viewing multicast next hop information .....	245
Viewing and editing multicast interface information .....	247
Configuring multicast static source groups .....	248

---

Configuration considerations . . . . .	248
Viewing and editing static source groups . . . . .	250
Adding a new static source group . . . . .	251
Deleting a static source group . . . . .	252
Troubleshooting DVMRP . . . . .	253
Mroute-HW—Prunes tab fields . . . . .	255
Mroute-HW—Sources tab fields . . . . .	256
Mroute-HW—Egress VLANs tab fields . . . . .	257
Configuring IP multicast software forwarding . . . . .	258
Configuring the resource usage counter for multicast streams . . . . .	259
<b>Chapter 7</b>	
<b>Configuring multicast flow distribution over MLT using Device Manager . . . . .</b>	<b>261</b>
Enabling multicast flow distribution globally . . . . .	262
Enabling multicast flow distribution per MLT . . . . .	265
<b>Chapter 8</b>	
<b>Configuring multicast MAC filtering using Device Manager . . . . .</b>	<b>269</b>
Configuring Layer 2 multicast MAC filtering . . . . .	270
Configuring Layer 3 multicast MAC filtering . . . . .	272
<b>Chapter 9</b>	
<b>Configuring IGMP using the CLI. . . . .</b>	<b>275</b>
Roadmap of IGMP commands . . . . .	277
Configuration prerequisites and notes . . . . .	278
Configuring IGMP on an interface . . . . .	285
Showing IGMP interfaces . . . . .	288
Showing IGMP cache information . . . . .	290
Showing IGMP group information . . . . .	290
Showing IGMP router-alert status . . . . .	291
Showing IGMP sender information . . . . .	291
Showing IGMP snoop status . . . . .	292
Configuring fast leave mode and enabling trap/logs . . . . .	293
Showing the current fast leave mode . . . . .	295

---

---

Configuring multicast access control for an IGMP interface .....	296
Showing IGMP access control groups .....	299
Configuring IGMP multicast router discovery options .....	300
Showing IGMP multicast router discovery information .....	302
Showing IGMP multicast router discovery neighbors .....	302
Configuring IGMP interface static members .....	303
Showing IGMP static and blocked ports .....	304
Configuring SSM dynamic learning and range group .....	306
Showing SSM group range and dynamic learning status .....	308
Configuring the SSM channel table .....	309
Showing SSM channel information .....	311
Configuring IGMP Ethernet ports .....	313
Showing IGMP port information .....	315
Configuring multicast access control for an IGMP Ethernet port .....	317
Configuring IGMP on a VLAN .....	320
Showing IGMP VLAN information .....	324
Configuring multicast access control for a VLAN .....	325
Configuring IGMP multicast router discovery on a VLAN .....	328
Configuring IGMP static members on a VLAN .....	329
Configuring IGMP fast-leave members on a VLAN .....	331
Configuring multicast stream limitation .....	332
Configuring multicast stream limitation on an interface .....	332
Configuring multicast stream limitation members on an interface .....	334
Showing multicast stream limitations per interface .....	335
Showing multicast stream limitations per port .....	336
Configuring multicast stream limitation on an Ethernet port .....	337
Configuring multicast stream limitation on a VLAN .....	338
Configuring multicast stream limitation members on a VLAN .....	339
Displaying all IP IGMP show commands .....	342
<b>Chapter 10</b>	
<b>Configuring DVMRP using the CLI .....</b>	<b>343</b>
Roadmap of DVMRP commands .....	344
Configuration prerequisites .....	348

---

Configuring DVMRP globally	349
Configuring DVMRP on an interface	352
Showing DVMRP group information	353
Showing DVMRP neighbors	354
Showing DVMRP next hops	355
Showing DVMRP routes	356
Configuring DVMRP on Ethernet ports	357
Configuring DVMRP on a VLAN	359
Configuring DVMRP routing policies	361
Configuring default route policies	361
Applying the default route policy to an interface	362
Applying the default route policy to a VLAN	364
Applying the default route policy to a port	366
Configuring DVMRP announce policies	368
Creating a DVMRP announce policy	368
Applying a DVMRP announce policy to an interface	373
Deleting a DVMRP announce policy from an interface	373
Applying a DVMRP announce policy to a VLAN	374
Deleting a DVMRP announce policy from a VLAN	374
Applying a DVMRP announce policy to a port	375
Deleting a DVMRP announce policy from a port	375
Configuring DVMRP accept policies	376
Creating a DVMRP accept policy	376
Applying a DVMRP accept policy to an interface	381
Deleting a DVMRP accept policy from an interface	381
Applying a DVMRP accept policy to a VLAN	382
Deleting a DVMRP accept policy from a VLAN	382
Applying a DVMRP accept policy to a port	383
Deleting a DVMRP accept policy from a port	383
Configuring the advertisement of local network policies	384
Applying the advertisement of local networks policy to an interface	384
Applying the advertisement of local networks policy over a VLAN	385
Applying the advertisement of local networks policy over a port	386
Configuring a DVMRP interface type	388
Creating a passive interface	388

---

Configuring an active or passive interface type . . . . .	389
Configuring an active or passive VLAN type . . . . .	391
Configuring an active or passive port type . . . . .	392
Displaying DVMRP routing policy information . . . . .	393
Displaying DVMRP routing policy information for an interface . . . . .	393
Displaying DVMRP routing policy information for a VLAN . . . . .	394
Displaying DVMRP routing policy information for a port . . . . .	394
Displaying all IP DVMRP show commands . . . . .	396

## **Chapter 11**

### **Configuring PIM using the CLI . . . . . 399**

Roadmap of PIM commands . . . . .	401
PIM-SM configuration prerequisites . . . . .	405
Configuring PIM-SM globally . . . . .	406
Showing PIM group information . . . . .	408
Configuring a PIM multicast border router (PMBR) . . . . .	409
Configuring PIM on an interface . . . . .	410
Changing the interface type . . . . .	411
Showing PIM interface information . . . . .	411
Showing PIM neighbor information . . . . .	414
Configuring a candidate BSR on an interface . . . . .	415
Configuring a candidate rendezvous point (C-RP) . . . . .	416
Showing rendezvous point (RP) set information . . . . .	417
Showing candidate RP information . . . . .	418
Showing the active RP for a specific group . . . . .	419
Showing the active RP for all groups . . . . .	420
Showing bootstrap router (BSR) information . . . . .	421
Showing PIM route information . . . . .	422
Configuring a static rendezvous point (RP) . . . . .	423
Static RP configuration considerations . . . . .	423
Configuring static RP . . . . .	424
Showing the static RP table . . . . .	426
Configuring PIM on an Ethernet (brouter) port . . . . .	427
Changing the port interface type . . . . .	428
Configuring a candidate BSR on an Ethernet port . . . . .	428

---

Configuring PIM on a VLAN .....	429
Changing the VLAN interface type .....	431
Showing PIM information for VLANs .....	431
Configuring a candidate BSR on a VLAN .....	433
Configuring PIM debug trace commands .....	434
Tips for using the debug trace commands .....	436
Debug trace command sample output .....	437
Assert debug trace send/receive output .....	438
Bootstrap debug trace send/receive output .....	439
Hello debug trace send/receive output .....	440
Joinprune debug trace send/receive output .....	441
Register debug trace send/receive output .....	442
Regstop debug trace send/receive output .....	443
Rp-adv debug trace send/receive output .....	444
Configuring Source Specific Multicast (SSM) .....	444
PIM-SSM configuration prerequisites .....	445
Configuring PIM-SSM globally .....	446
Displaying all IP PIM show commands .....	448
<b>Chapter 12</b>	
<b>Configuring PGM using the CLI .....</b>	<b>451</b>
Roadmap of PGM commands .....	452
Configuration considerations and prerequisites .....	454
Configuring PGM globally .....	455
Showing PGM global information .....	456
Showing PGM retransmission statistics .....	458
Showing PGM session statistics .....	459
Configuring PGM on an interface .....	463
Showing PGM interface commands .....	464
Showing PGM interface configurations .....	464
Showing PGM interface errors .....	466
Showing PGM interface NAK errors .....	467
Showing PGM interface statistics .....	468
Showing PGM interface NAK statistics .....	470
Showing PGM interface parity statistics .....	471

---

Configuring PGM on Ethernet ports . . . . .	472
Configuring PGM on a VLAN . . . . .	474
Displaying all IP PGM show commands . . . . .	476

## **Chapter 13**

### **Viewing and editing multicast routes using the CLI. . . . . 477**

Roadmap of multicast route commands . . . . .	478
Displaying multicast routes . . . . .	480
Showing a multicast route's next hop . . . . .	480
Showing multicast route information . . . . .	481
Configuring a multicast route on an interface . . . . .	481
Showing multicast routes on an interface . . . . .	482
Configuring multicast static source groups . . . . .	483
Configuration considerations . . . . .	483
Viewing and editing static source groups . . . . .	485
Showing multicast static source groups . . . . .	487
Showing DVMRP troubleshooting information . . . . .	488
Configuring IP multicast software forwarding . . . . .	491
Showing the software forwarding configuration . . . . .	492
Configuring the resource usage counter for multicast streams . . . . .	493
Showing the hardware resource usage output . . . . .	495
Displaying all IP mroute show commands . . . . .	496

## **Chapter 14**

### **Configuring multicast flow distribution over MLT using the CLI. . . . . 497**

Roadmap of multicast MLT commands . . . . .	498
Configuring multicast flow distribution globally . . . . .	499
Configuring multicast flow distribution per MLT . . . . .	501
Showing the multicast MLT distribution show command . . . . .	502

## **Chapter 15**

### **Configuring multicast MAC filtering using the CLI. . . . . 503**

Roadmap of multicast MAC filtering commands . . . . .	504
Configuring Layer 2 multicast MAC filtering . . . . .	505
Configuring Layer 3 multicast MAC filtering . . . . .	507

---

Showing the Layer 2 multicast MAC filters .....	509
Showing the Layer 3 multicast MAC ARP data .....	510
Showing VLAN port data .....	511
Showing the multicast VLAN information .....	512
<b>Index .....</b>	<b>513</b>



---

# Figures

---

Figure 1	Multicast distribution tree and broadcasting	34
Figure 2	Pruning routers from a distribution tree	35
Figure 3	Data flow using deny-tx policy	47
Figure 4	Data flow using deny-rx policy	47
Figure 5	Data flow using deny-both policy	48
Figure 6	Default route configuration example	58
Figure 7	DVMRP announce policy logic	60
Figure 8	Announce policy configuration example	61
Figure 9	DVMRP accept Policy logic	62
Figure 10	Accept policy configuration example	63
Figure 11	Advertisement of local networks policy configuration example	64
Figure 12	Shared tree and shortest-path tree	71
Figure 13	PIM-SM simplified example	74
Figure 14	PIM-SSM Architecture	77
Figure 15	Port dialog box—Interface tab	95
Figure 16	Port dialog box—IGMP tab	96
Figure 17	IGMP dialog box— Global tab	98
Figure 18	IP, VLAN dialog box—IGMP tab	101
Figure 19	IGMP dialog box—Cache tab	105
Figure 20	IGMP dialog box—Interface tab	106
Figure 21	IGMP dialog box—Multicast Router Discovery tab	109
Figure 22	IGMP dialog box—Snoop tab	111
Figure 23	IGMP dialog box—Groups tab	113
Figure 24	IGMP and IGMP, Insert Static dialog boxes	115
Figure 25	Policy dialog box—Prefix List tab	116
Figure 26	Policy, Insert Prefix List dialog box	117
Figure 27	IGMP dialog box —Access Control tab	118
Figure 28	IGMP, Insert Access Control dialog box	118
Figure 29	IgmpNewAccessIflIndex dialog box	119
Figure 30	IGMP, Insert Access dialog box with VLAN ID	119
Figure 31	IGMP dialog box —Sender tab	121
Figure 32	IGMP dialog box—SsmGlobal tab	123

---

Figure 33	IGMP dialog box—SsmChannel tab	127
Figure 34	IGMP, Insert SsmChannel dialog box	127
Figure 35	IGMP dialog box—SsmChannel tab	128
Figure 36	IGMP dialog box—StreamLimit tab	130
Figure 37	IGMP dialog box—StreamLimit Members tab	131
Figure 38	IGMP, Insert StreamLimit Members dialog box	132
Figure 39	IGMP dialog box—StreamLimit Members tab	133
Figure 40	Port dialog box—Interface tab	134
Figure 41	Port dialog box—IGMP tab	135
Figure 42	IP, VLAN dialog box—IGMP tab	137
Figure 43	DVMRP dialog box—Globals tab	141
Figure 44	Port dialog box—DVMRP tab	144
Figure 45	VLAN dialog box—Basic tab	146
Figure 46	IP, VLAN dialog box—IP Address tab	146
Figure 47	IP, VLAN dialog box—DVMRP tab	147
Figure 48	DVMRP dialog box—Interfaces tab	149
Figure 49	DVMRP dialog box—Interface Advance tab	150
Figure 50	DVMRP dialog box—Neighbors tab	152
Figure 51	DVMRP dialog box—Routes tab	153
Figure 52	DVMRP dialog box—Next Hops tab	155
Figure 53	Policy dialog box—Prefix List tab	161
Figure 54	Prefix List tab—Policy, Insert Prefix List dialog box	161
Figure 55	Policy dialog box—Route Policy tab	162
Figure 56	Route Policy tab—Policy, Insert Route Policy dialog box	163
Figure 57	Policy dialog box—DVMRP In/Out Policy tab	166
Figure 58	DVMRP Interface tab—OutPolicy dialog box	167
Figure 59	DVMRP VLAN tab—OutPolicy dialog box	168
Figure 60	DVMRP Port tab—OutPolicy dialog box	169
Figure 61	DVMRP Interface tab—InPolicy dialog box	173
Figure 62	DVMRP VLAN tab—InPolicy dialog box	174
Figure 63	DVMRP Port tab—InPolicy dialog box	175
Figure 64	PIM dialog box—Globals tab	191
Figure 65	PIM dialog box—Globals tab	194
Figure 66	PIM dialog box—Static RP tab	195
Figure 67	PIM dialog box—Insert Static RP dialog box	196

---

Figure 68	Port dialog box—PIM tab	197
Figure 69	IP VLAN dialog box	200
Figure 70	IP VLAN dialog box—PIM tab	201
Figure 71	PIM dialog box—Interfaces tab	203
Figure 72	PIM dialog box—Neighbors tab	206
Figure 73	PIM dialog box—RP Set tab	207
Figure 74	PIM dialog box—Candidate RP tab	208
Figure 75	PIM dialog box—Insert Candidate RP dialog box	209
Figure 76	PIM dialog box—Current BSR tab	210
Figure 77	PIM dialog box—Globals tab	213
Figure 78	PGM dialog box—Globals tab	219
Figure 79	Port dialog box—PGM tab	221
Figure 80	IP VLAN dialog box	223
Figure 81	IP VLAN dialog box—PGM tab	224
Figure 82	PGM dialog box—Interfaces tab	226
Figure 83	PGM Interface Graph dialog box—Spms/Rdata tab	229
Figure 84	PGM Interface Graph dialog box—Naks/Nnaks/Ncfs tab	231
Figure 85	PGM dialog box—Session tab	233
Figure 86	PGM Session Graph dialog box—Spms/Rdata tab	235
Figure 87	PGM Session Graph dialog box—Naks/Nnaks/Ncfs tab	238
Figure 88	PGM dialog box—Retransmit tab	240
Figure 89	Multicast dialog box—Routes tab	244
Figure 90	Multicast dialog box—Next Hops tab	245
Figure 91	Multicast dialog box—Interfaces tab	247
Figure 92	Multicast dialog box—Static Source Group tab	250
Figure 93	Multicast, Insert Static Source Group dialog box	251
Figure 94	Static Source Group tab	252
Figure 95	Multicast dialog box—Mroute-HW tab	254
Figure 96	Multicast dialog box—Mroute-HW tab—Prunes tab	255
Figure 97	Multicast dialog box—Mroute-HW tab—Sources tab	256
Figure 98	Multicast dialog box—Mroute-HW tab—Egress VLANs tab	257
Figure 99	Multicast dialog box—Mcast SW Forwarding tab	258
Figure 100	Multicast Dialog box—Records Usage tab	260
Figure 101	Chassis tab	263
Figure 102	Mcast MLT Distribution dialog box	264

---

Figure 103	MLT dialog box	265
Figure 104	MLT_LACP Insert Multilink/LACP dialog box	266
Figure 105	Updated MLT dialog box	266
Figure 106	VLAN dialog box—Basic tab	270
Figure 107	Bridge, VLAN dialog box—Transparent tab	270
Figure 108	Bridge, VLAN dialog box—Multicast tab	271
Figure 109	Bridge, VLAN, Insert Multicast MAC dialog box	271
Figure 110	Multicast ARP tab	272
Figure 111	Insert Multicast dialog box	273
Figure 112	show ip igmp interface command output	289
Figure 113	show ip igmp cache command output	290
Figure 114	show ip igmp group command output	290
Figure 115	Show ip igmp router-alert command	291
Figure 116	show ip igmp sender command output	292
Figure 117	show ip igmp snoop command	292
Figure 118	show ip igmp info command output	295
Figure 119	show ip igmp access command output	299
Figure 120	Show ip igmp mrdisc command	302
Figure 121	Show ip igmp mrdisc-neighbors command	302
Figure 122	show ip igmp static command output	305
Figure 123	show ip igmp ssm-global command output	308
Figure 124	show ip igmp ssm-channel command output	312
Figure 125	config ethernet ip igmp info command output	315
Figure 126	show ports info igmp command (partial output)	316
Figure 127	show vlan info igmp command output	324
Figure 128	show ip igmp interface command output	336
Figure 129	show ip igmp interface command output	336
Figure 130	show ip igmp show-all command output	342
Figure 131	config ip dvmrp info command output	351
Figure 132	show ip dvmrp info command output	353
Figure 133	show ip dvmrp neighbor command output	354
Figure 134	show ip dvmrp next-hop command output	355
Figure 135	show ip dvmrp route command output	356
Figure 136	config ethernet ip dvmrp info command output	358
Figure 137	config vlan ip dvmrp info command output	360

---

Figure 138	DVMRP interface configuration information	393
Figure 139	DVMRP VLAN configuration information	394
Figure 140	DVMRP port configuration information	395
Figure 141	show ip dvmrp show-all command output	397
Figure 142	config ip pim info command output	408
Figure 143	show ip pim info command output	409
Figure 144	show ip pim interface command output	412
Figure 145	show ip pim neighbor command output	414
Figure 146	config ip pim candbsr interface command output	415
Figure 147	show ip pim rp-set command output	417
Figure 148	show ip pim candidate-rp command output	418
Figure 149	show ip pim active-rp 228.1.2.3 command output	419
Figure 150	show ip pim candidate-rp command output	420
Figure 151	show ip pim bsr command output	421
Figure 152	show ip pim mroute command output	422
Figure 153	show ip pim static-rp command output	426
Figure 154	config ethernet ip pim info command output	428
Figure 155	config ethernet ip pim candbsr command output	429
Figure 156	config vlan ip pim info command output	431
Figure 157	show vlan info pim command output	432
Figure 158	config vlan ip pim candbsr command output	433
Figure 159	config ip pim debug-pimmsg info command output	435
Figure 160	Assert debug trace send/receive output example	438
Figure 161	Bootstrap debug trace send/receive output example	439
Figure 162	Hello debug trace send/receive output example	440
Figure 163	Joinprune debug trace send/receive output example	441
Figure 164	Register debug trace send/receive output example	442
Figure 165	Regstop debug trace send/receive output example	443
Figure 166	Rp-adv debug trace send/receive output example	444
Figure 167	show ip pim show-all command output	449
Figure 168	config ip pgm info command output	456
Figure 169	show ip pgm global command output	456
Figure 170	show ip pgm retransmit command output	458
Figure 171	show ip pgm session command output	460
Figure 172	config ip pgm interface info command output	464

---

Figure 173	show ip pgm interface config command output	465
Figure 174	show ip pgm interface error general command output	466
Figure 175	show ip pgm interface error nak command output	467
Figure 176	show ip pgm interface stat general command output	469
Figure 177	show ip pgm interface stat nak command output	470
Figure 178	show ip pgm interface stat parity command output	471
Figure 179	config ethernet ip pgm info command output	473
Figure 180	config vlan ip pgm info command output	475
Figure 181	show ip pgm show-all command output	476
Figure 182	show ip mroute next-hop command output	480
Figure 183	show ip mroute route command output	481
Figure 184	show ip mroute interface command output	482
Figure 185	show ip mroute static-source-group command output	487
Figure 186	show ip mroute-hw group-trace grp command output	489
Figure 187	show ip mroute-hw group-trace src grp command output	489
Figure 188	show ip mroute-hw group-prune-state grp command output	489
Figure 189	config sys mcast-software-forwarding info command output	492
Figure 190	show sys mcast-software-forwarding command output	492
Figure 191	show ip mroute-hw resource-usage command output	495
Figure 192	show ip mroute show-all command output	496
Figure 193	show sys mcast-mlt-distribution command output	502
Figure 194	show vlan info static-mcastmac command output	509
Figure 195	show ip arp static-mcastmac command output	510
Figure 196	show vlan info ports command output	511
Figure 197	show vlan info all command output	512

---

# Tables

---

Table 1	Parts of a routing table entry	55
Table 2	Summary of how PIM-SSM interacts with IGMPv2 and v3	81
Table 3	IGMP tab fields	96
Table 4	Global tab fields	98
Table 5	IGMP tab fields	102
Table 6	Cache tab fields	105
Table 7	IGMP dialog box—Interface tab fields	106
Table 8	MIB definition	108
Table 9	Multicast Router Discovery tab fields	109
Table 10	Snoop tab fields	111
Table 11	Group tab fields	113
Table 12	IGMP, Insert Static dialog box fields	115
Table 13	Policy, Insert Prefix List dialog box fields	117
Table 14	Access Control tab fields	120
Table 15	Sender tab fields	121
Table 16	IGMP dialog box—SsmGlobal tab fields	123
Table 17	IGMP dialog box—SsmChannel tab fields	128
Table 18	IGMP dialog box—StreamLimit tab fields	130
Table 19	IGMP dialog box—StreamLimit Members tab fields	131
Table 20	Port stream limitation fields	135
Table 21	VLAN stream limitation fields	138
Table 22	Globals tab fields	142
Table 23	Port dialog box—DVMRP tab fields	144
Table 24	DVMRP tab fields	148
Table 25	DVMRP Interfaces tab fields	149
Table 26	DVMRP dialog box—Interface Advance tab fields	150
Table 27	Neighbors tab fields	152
Table 28	Routes tab fields	154
Table 29	Next Hops tab fields	155
Table 30	Policy, Insert Prefix List dialog box fields	162
Table 31	Policy, Insert Route Policy dialog box	164
Table 32	PIM Globals tab fields	191

---

Table 33	PIM Static RP tab fields	196
Table 34	PIM tab fields	198
Table 35	VLAN PIM tab fields	201
Table 36	PIM Interfaces tab fields	204
Table 37	PIM Neighbors tab fields	206
Table 38	PIM RP Set tab fields	207
Table 39	PIM Candidate RP tab fields	209
Table 40	Current BSR tab fields	211
Table 41	PIM Globals tab fields	214
Table 42	PGM Globals tab fields	220
Table 43	PGM port tab fields	222
Table 44	IP, VLAN dialog box—PGM tab fields	224
Table 45	PGM Interfaces tab fields	226
Table 46	Interface Spms/Rdata tab fields	229
Table 47	Interface Naks/Nnaks/Ncfs tab fields	232
Table 48	PGM Session tab fields	234
Table 49	Session Spms/Rdata tab fields	236
Table 50	Session Naks/Nnaks/Ncfs tab fields	238
Table 51	PGM Retransmit tab fields	240
Table 52	Routes tab fields	244
Table 53	Next Hops tab fields	245
Table 54	Multicast dialog box—Interfaces tab fields	247
Table 55	Static Source Group tab fields	250
Table 56	Mroute-HW tab fields	254
Table 57	Prunes tab fields	255
Table 58	Sources tab fields	256
Table 59	Egress VLANs tab fields	257
Table 60	Records Usage tab fields	260
Table 61	Mcast MLT Distribution tab fields	265
Table 62	MultiLink Trunks tab fields	267
Table 63	Bridge, VLAN, Insert Multicast fields	272
Table 64	Multicast ARP fields	273
Table 65	show ip igmp access field descriptions	299
Table 66	show ip pim interface parameters	412
Table 67	show ip pim neighbor parameters	414

---

Table 68	show ip pim rp-set parameters	417
Table 69	show ip pim candidate-rp parameters	418
Table 70	show ip pim active-rp <group> parameter	419
Table 71	show ip pim active-rp parameters	420
Table 72	show ip pim bsr parameters	421
Table 73	show vlan ip pim parameters	432
Table 74	show ip pgm global parameters	457
Table 75	show ip pgm retransmit parameters	458
Table 76	show ip pgm session parameters	461
Table 77	show ip pgm interface config parameters	465
Table 78	show ip pgm interface error general parameters	466
Table 79	show ip pgm interface error nak parameters	468
Table 80	show ip pgm interface stat general parameters	469
Table 81	show ip pgm interface stat nak parameters	470
Table 82	show ip pgm interface stat parity parameters	471
Table 83	show ip mroute-hw group-trace and group-prune-state output fields	490



## 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 8000 Series\* 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.

---

<i>italic text</i>	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 <code>show at &lt;valid_route&gt;</code> , <code>valid_route</code> 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: <code>Set Trap Monitor Filters</code>
separator (>)	Shows menu paths. Example: <code>Protocols &gt; IP</code> 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 <code>show ip {alerts routes}</code> , you enter either <code>show ip alerts</code> or <code>show ip routes</code> , but not both.

## Acronyms

This guide uses the following acronyms:

C-BSR	candidate-boot strap router
DVMRP	Distance Vector Multicast Routing Protocol
IGMP	Internet Group Management Protocol
MLT	Multilink Trunking
MRDISC	Multicast Router Discovery Protocol
PIM-SSM	Protocol Independent Multicast-Sparse Mode
PGM	Pragmatic General Multicast

## 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](http://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](http://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](http://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 Passport 8000 Series switches support:

Topic	Page
<a href="#">Overview of IP Multicast</a>	34
<a href="#">Internet Group Management Protocol (IGMP)</a>	39
<a href="#">Multicast Router Discovery Protocol (MRDISC)</a>	51
<a href="#">Distance Vector Multicast Routing Protocol (DVMRP)</a>	52
<a href="#">Protocol Independent Multicast-Sparse Mode (PIM-SM)</a>	65
<a href="#">PIM-SSM (Source Specific Multicast)</a>	75
<a href="#">PIM passive interfaces</a>	82
<a href="#">Pragmatic General Multicast (PGM)</a>	84
<a href="#">Multicast flow distribution over MLT</a>	87
<a href="#">Multicast MAC filtering</a>	91

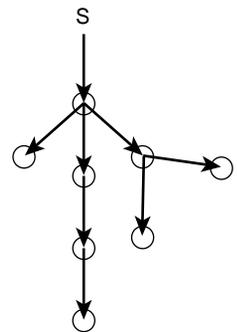
## Overview of IP Multicast

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.

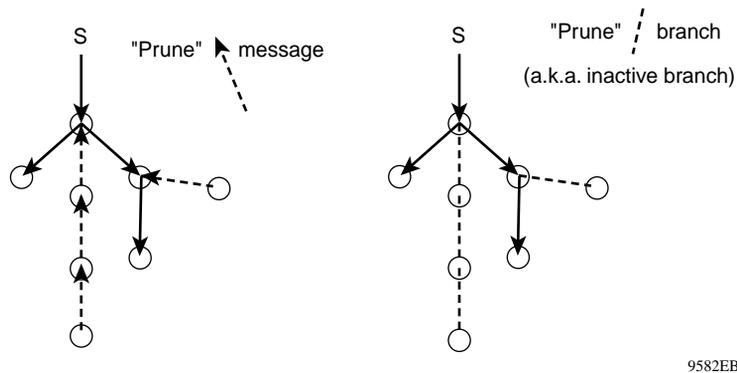


9580EA

*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



9582EB

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 have 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 248](#). For information on configuring static source-groups using the CLI, see [“Configuring multicast static source groups” on page 483](#).

## 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 275](#).

## 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 LMQUI (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 and enabling trap/logs” on page 97](#). For information on configuring fast leave mode using the CLI, see [“Configuring fast leave mode and enabling trap/logs” on page 293](#).

## 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 103](#) and [“Viewing IGMP snooping information” on page 111](#).

For information on configuring IGMP snoop using the CLI, see [“Configuring IGMP on an interface” on page 285](#) or [“Configuring IGMP on a VLAN” on page 320](#).

## 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 100](#) and [“Viewing IGMP snooping information” on page 111](#).

For information on configuring IGMP proxy using the CLI, see [“Configuring IGMP on an interface” on page 285](#) or [“Configuring IGMP on a VLAN” on page 320](#).

## 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:

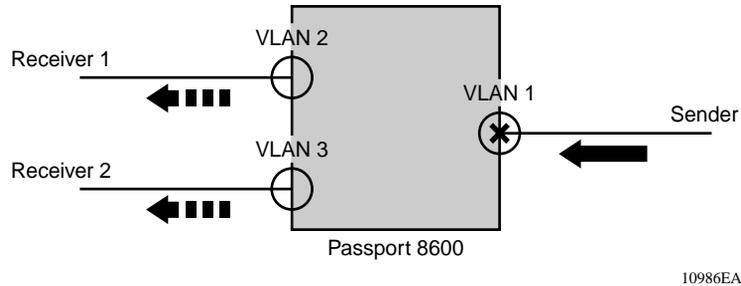
- deny-tx
- deny-rx
- deny-both
- allow-only-tx
- allow-only rx
- allow-only-both

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.

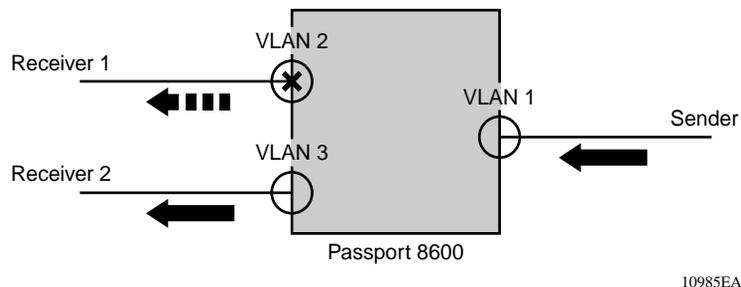
For example, in the following diagram, a deny-tx access policy is configured on VLAN 1 (the ingress VLAN to the Passport 8600). The deny-tx access policy prevents multicast traffic sent by Sender from being forwarded from VLAN 1 to any receiver, consequently preventing Receiver 1 and Receiver 2 from 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



## 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 116](#). For information on configuring multicast access control using the CLI, see [“Configuring multicast access control for an IGMP interface” on page 296](#).

## 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 129](#). For information on configuring multicast stream limitation using the CLI, see [“Configuring multicast stream limitation” on page 332](#).

## 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 109](#). For information on configuring MRDISC using the CLI, see [“Configuring IGMP multicast router discovery options” on page 300](#) and [“Configuring IGMP multicast router discovery on a VLAN” on page 328](#).

## 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:

Topic	Page
<a href="#">Reverse path forwarding</a>	53
<a href="#">Pruning and grafting</a>	53
<a href="#">DVMRP concepts and terminology</a>	54
<a href="#">DVMRP static source groups</a>	56
<a href="#">DVMRP routing policies</a>	57
<a href="#">8000 Series implementation of DVMRP</a>	64

## 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.

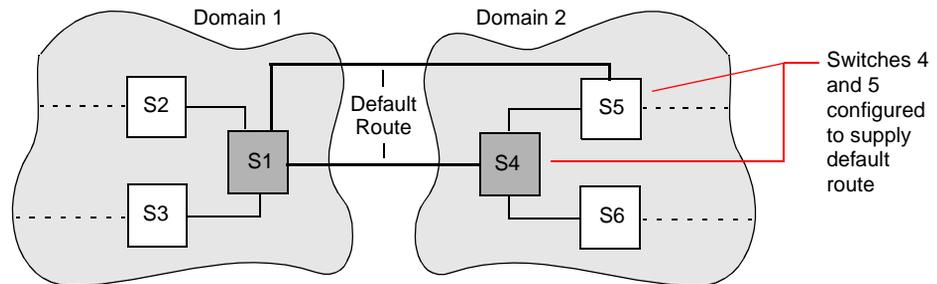
When supplying a default route, you must consider the following:

- 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.

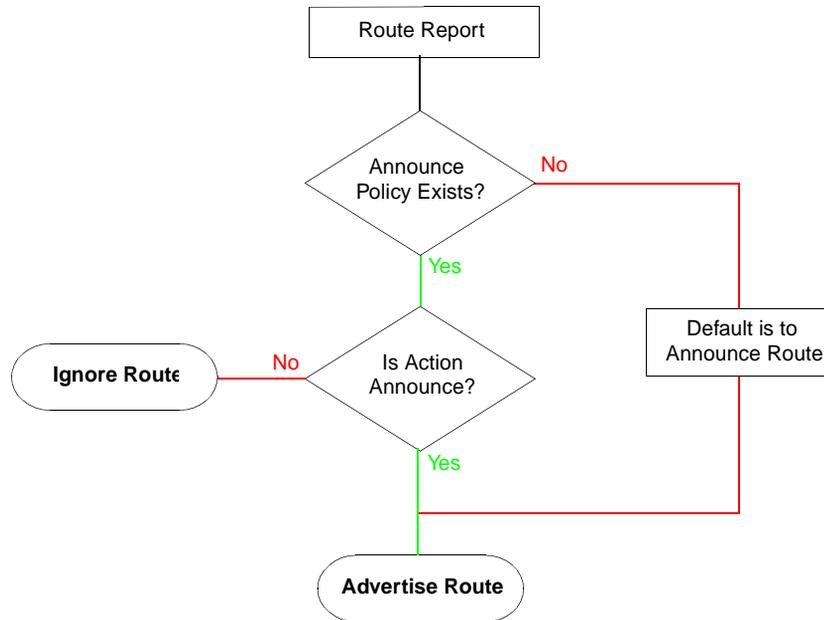
Refer to [Figure 8 on page 61](#) and [Figure 10 on page 63](#) for configuration examples that show the application of the DVMRP announce and accept policies to the same network configuration shown in [Figure 6 on page 58](#).

## **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.

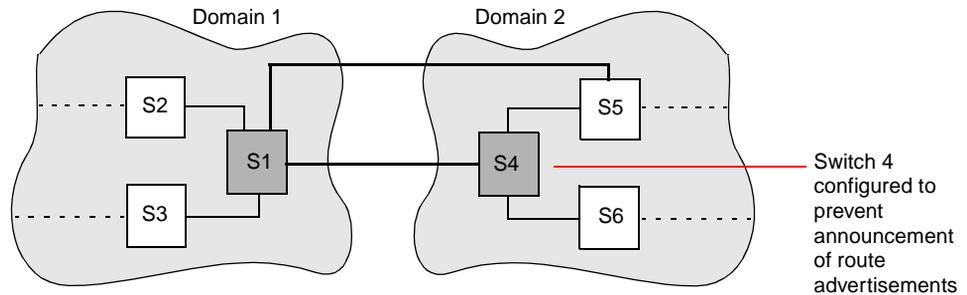
The announce policies are applied to the outgoing advertisements to the other neighbors/peers in the protocol domain. These policies determine whether or not to announce specific route information. Announce policies allow you to selectively announce routes. You can configure a policy to apply to any 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

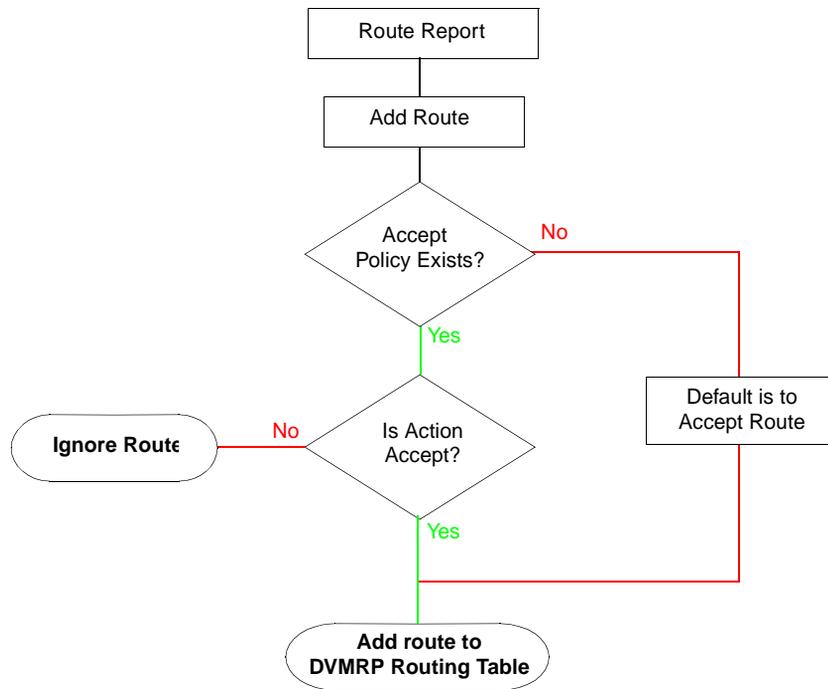
**Figure 8** Announce policy configuration example

## 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.

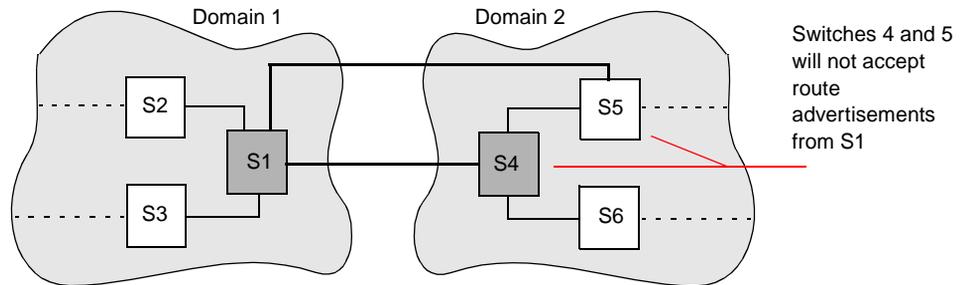
Accept policies allow injecting routes into the DVMRP routing table and can be applied to a single or all interfaces of a switch. These policies allow you to selectively accept routes and you can configure a policy to apply for any route. If there is no policy configured or no matching policy for a given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

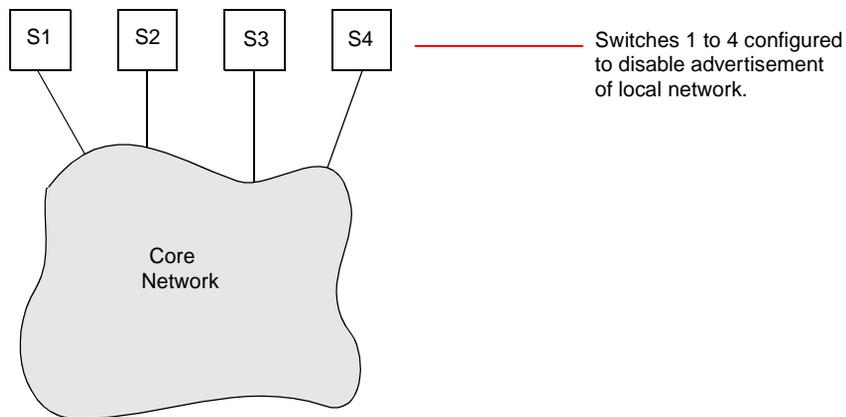
**Figure 10** Accept policy configuration example

### 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 156](#). For information on configuring routing policies using the CLI, see [“Configuring DVMRP routing policies” on page 361](#).

## 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 199](#). For information on configuring a candidate BSR using the CLI, see [“Configuring a candidate BSR on an interface” on page 415](#), [“Configuring a candidate BSR on an Ethernet port” on page 428](#) or [“Configuring a candidate BSR on a VLAN” on page 433](#).

## 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

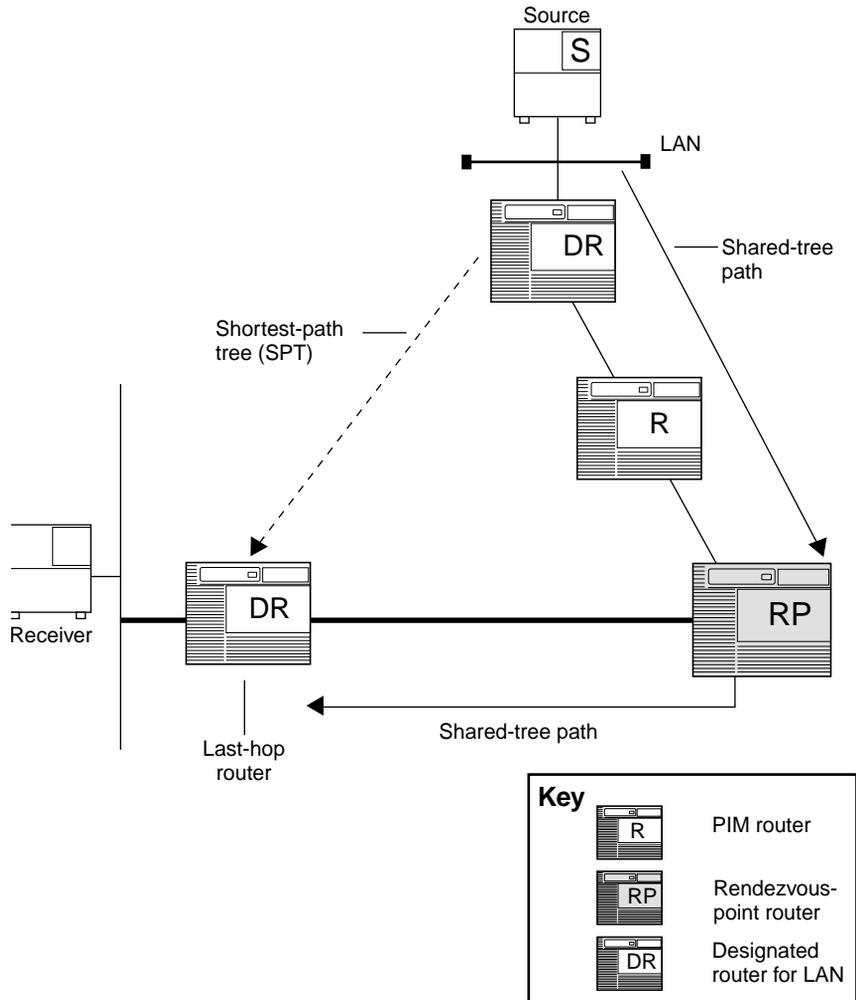
Group members in a PIM-SM domain receive the first packet of data from sources across a shared tree. A *shared tree* consists of a set of paths that connect all members of a multicast group to the RP. PIM creates a shared tree when sources and receivers send messages toward the RP.

### 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



IP00092A

## 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:

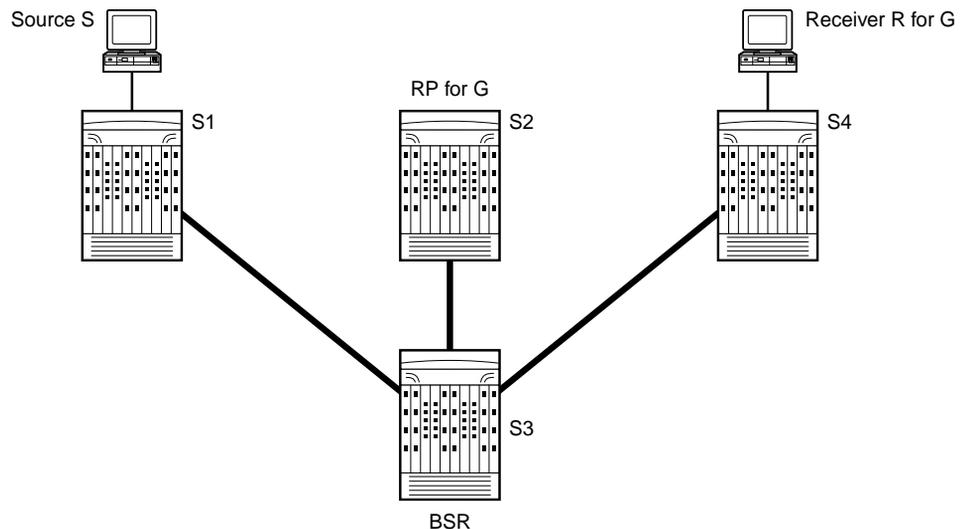
- An underlying unicast routing protocol must be enabled for the switch to provide routing table information to PIM-SM
- In a PIM-SM domain, an active BSR must be in place to send bootstrap messages to all PIM-V2 configured switches and routers to enable them to learn group-to-RP mapping. If several 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



10534EA

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-encapsulates 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.

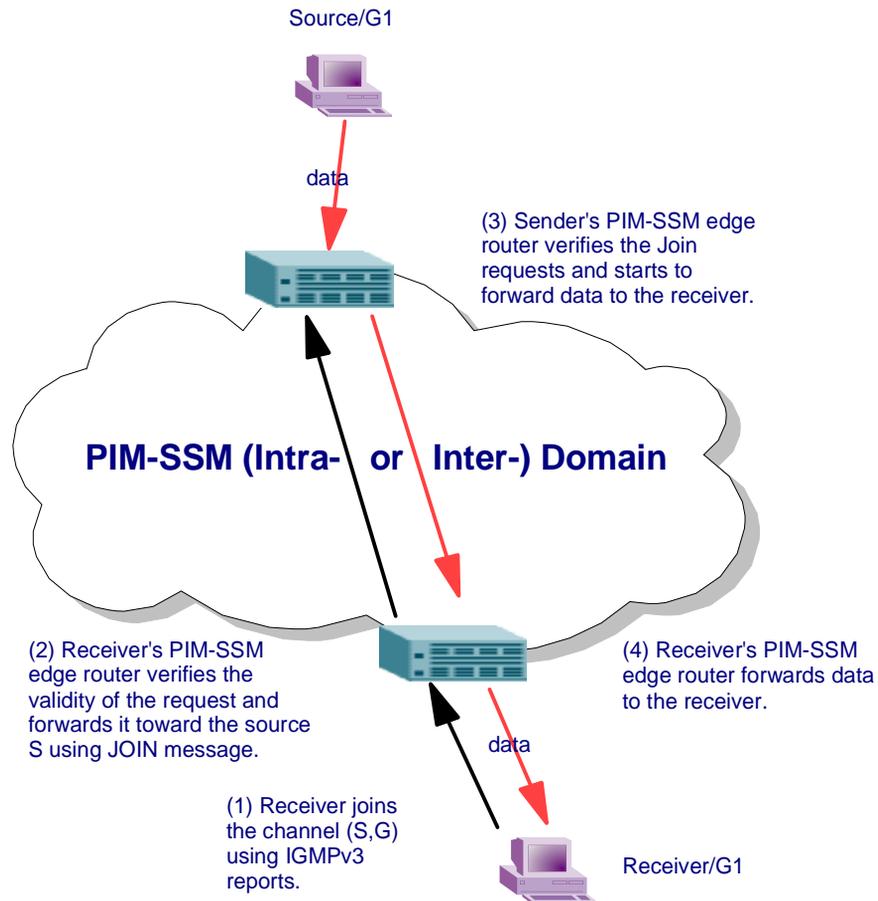
## PIM-SSM architecture

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 122](#). For information on configuring the SSM range using the CLI, see [“Configuring SSM dynamic learning and range group” on page 306](#).

## 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 126](#). For information on configuring the SSM channel table using the CLI, see [“Configuring the SSM channel table” on page 309](#).

## 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<sup>1</sup>

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.

<sup>1</sup> References to any matching static SSM channel entry assumes that the entry is enabled. If an entry is disabled, it will be 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 203](#). For information on configuring PIM passive interfaces using the CLI, see [“Changing the interface type” on page 411](#), [“Changing the port interface type” on page 428](#) or [“Changing the VLAN interface type” on page 431](#).

## 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 217](#) or [“Configuring PGM using the CLI” on page 451](#).

## 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 =:

$$\begin{aligned} &((( ( ( ( ( G[0] \text{ AND } GM[0] ) \text{ xor } ( S[0] \text{ AND } SM[0] ) ) \text{ xor } ( ( G[1] \text{ AND } GM[0] ) \\ & \text{ xor } ( S[1] \text{ AND } SM[1] ) ) ) \text{ xor } ( ( G[2] \text{ AND } GM[2] ) \text{ xor } ( S[2] \text{ AND } SM[2] ) \\ & \text{ xor } ( ( G[3] \text{ AND } GM[3] ) \text{ xor } ( S[3] \text{ AND } SM[3] ) ) ) \text{ MOD (active ports} \\ & \text{of the MLT)} \end{aligned}$$

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 497.](#)”

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 261.](#)”

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 503.](#)”

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 269.](#)”

---

## 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:

Topic	Page
<a href="#">Configuration prerequisites and notes</a>	94
<a href="#">Configuring IGMP parameters on a brouter port</a>	94
<a href="#">Configuring fast leave mode and enabling trap/logs</a>	97
<a href="#">Configuring IGMP parameters on a VLAN</a>	100
<a href="#">Enabling IGMP snooping on a VLAN</a>	103
<a href="#">Viewing IGMP cache information</a>	104
<a href="#">Viewing and editing the IGMP interface table</a>	106
<a href="#">Viewing multicast router discovery information</a>	109
<a href="#">Viewing IGMP snooping information</a>	111
<a href="#">Viewing IGMP group information</a>	112
<a href="#">Creating and viewing IGMP static information</a>	114
<a href="#">Configuring multicast access control</a>	116
<a href="#">Configuring IGMP sender entries</a>	121
<a href="#">Configuring the SSM range and global parameters</a>	122
<a href="#">Configuring the SSM channel table</a>	126
<a href="#">Configuring multicast stream limitation</a>	129

## 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

192.168.151.163 - Port 1/9

IGMP	OSPF	RIP	PIM	PGM	VRRP	Router Discovery			IPX BRouter		
Remote Mirroring		Mroute Stream Limit			Fdb Protect		IP Address		ARP	DHCP	DVMR
<b>Interface</b>	VLAN	STG	MAC Learning	Rate Limiting	Test	SMLT	PCAP	EAPOL	LACP	VLA	

Index: 72  
Name:   
Descr: 10/100BaseTX Port 1/9 Name  
Type: rc100BaseTX  
Mtu: 1950  
PhysAddress: 00:04:38:7e:84:08  
VendorDescr:

AdminStatus:  up  down  testing  
OperStatus: down  
LastChange: 18h:34m:56s  
LinkTrap:  enabled  disabled

AutoNegotiate:  true  false  
AdminDuplex:  half  full  
OperDuplex: half

Apply Refresh Close Help...

**3** Click the IGMP tab.

The IGMP tab opens (Figure 16).

**Figure 16** Port dialog box—IGMP tab

The screenshot shows a window titled "192.168.151.163 - Port 1/3" with a tabbed interface. The "IGMP" tab is selected. The configuration fields are as follows:

- QueryInterval: 125 (1..65535) sec
- QueryMaxResponseTime: 100 0..255 (1/10sec)
- Robustness: 2 2..255
- LastMembQueryIntvl: 10 0..255 (1/10sec)
- Version:  version1  version2  version3
- FastLeaveEnable
- StreamLimitEnable:  enable  disable
- Maximum Number Of Stream: 0 (number)
- Current Number Of Stream: 0

Buttons at the bottom: Apply, Refresh, Close, Help...

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). <b>Note:</b> This value must be less than the QueryInterval.

**Table 3** 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) 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 and enabling trap/logs

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.

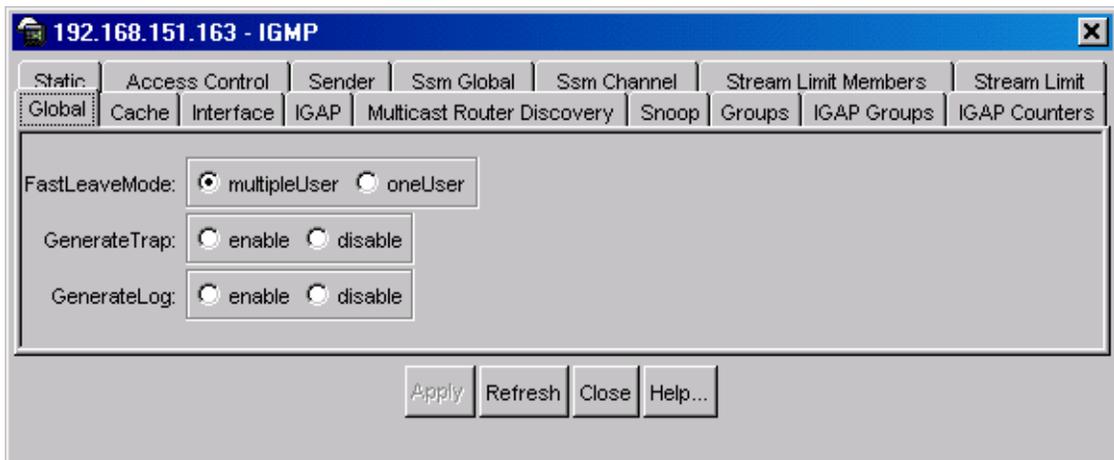


**Note:** Fast leave mode applies only to fast-leave enabled IGMP interfaces. It does not apply to IGAP interfaces, which ignore this mode.

To configure the fast leave mode:

- 1 From the Device Manager menu bar, choose IP Routing > IGMP.  
The IGMP dialog box opens with the Global tab displayed.  
The Global tab opens (Figure 17).

**Figure 17** IGMP dialog box— Global tab



- 2 Click on the mode you want, if not already selected.
- 3 Click Apply.
- 4 Click Enable in Generate trap and Generate Log fields.

[Table 4](#) describes the Global tab fields.

**Table 4** Global tab fields

<b>fast-leave-mode</b>	
multipleUser	Removes from the group <i>only</i> 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.

**Table 4** Global tab fields

<b>generate-trap</b>	
enable	Enabling this command on this switch will trigger trap for the following IGMP events: <ul style="list-style-type: none"> <li>• New IGMP membership for a group</li> <li>• IGMP membership removed for a group</li> <li>• When a querier is changed or new querier comes up on a particular interface</li> </ul>
disable	The switch will not send any IGMP trap events.
<b>generate-log</b>	
enable	Enabling this command on this switch will cause the following IGMP events to be logged: <ul style="list-style-type: none"> <li>• New IGMP membership for a group</li> <li>• IGMP membership removed for a group</li> <li>• When a querier is changed or new querier comes up on a particular interface</li> </ul>
disable	The switch will not log any IGMP events.

## 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

The screenshot shows a window titled "192.168.151.163 - IP, VLAN 1" with a close button (X) in the top right corner. The window contains a tabbed interface with the following tabs: PIM, PGM, VRRP, Router Discovery, Direct Broadcast, RSMLT, IP Address, ARP, DHCP, DVMRP, IGMP (selected), OSPF, and RIP. The IGMP tab is active and displays the following configuration options:

- QueryInterval: 125 (1.65535) sec
- QueryMaxResponseTime: 100 0..255 (1/10sec)
- Robustness: 2 2..255
- LastMembQueryIntvl: 10 0..255 (1/10sec)
- SnoopEnable
- SsmSnoopEnable
- ProxySnoopEnable
- IgapEnable:  enable  disable
- AccntEnable:  enable  disable
- AuthEnable:  enable  disable
- Version:  version1  version2  version3
- FastLeaveEnable
- StreamLimitEnable:  enable  disable
- Maximum Number Of Stream: 0 (number)
- Current Number Of Stream: 0
- FastLeavePortMembers: [ ] ...

At the bottom of the dialog box, there are four buttons: Apply, Refresh, Close, and Help...

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). <b>Note:</b> 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.
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.

**Table 5** IGMP tab fields (continued)

Field	Description
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.
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

The cache display for static joins provides to display static joins configured on a switch for a particular multicast group. You will be able to see all the static members in the IGMP cache table.

To view IGMP cache information:

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

The IGMP dialog box opens with the Global tab displayed (see Figure 17 on page 98).

- 1 Click the Cache tab. The Cache tab displays (Figure 19).

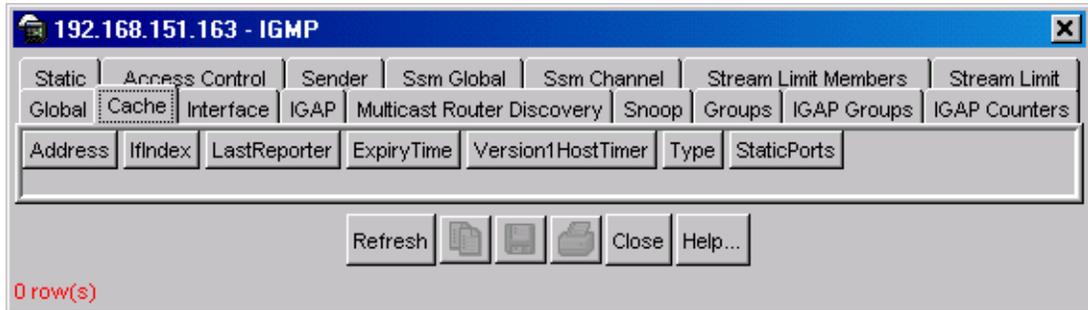
**Figure 19** IGMP dialog box—Cache tab

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.
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.
Static Ports	This field displays the static ports for the static joins, it is null for the dynamic entry.
Type	This field takes either of the two values, dynamic or static.

## 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 Global tab displayed.
- 2 Click the Interface tab.  
The Interface tab opens (Figure 20).

**Figure 20** IGMP dialog box—Interface tab

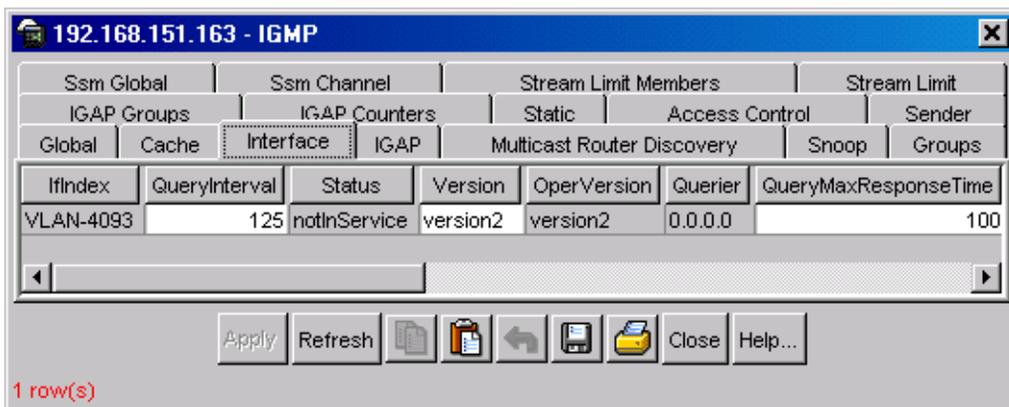


Table 7 describes the Interface tab fields.

**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.

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

Field	Description
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.
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). <b>Note:</b> 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.

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

Field	Description
LastMembQueryIntvl	<p>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.</p> <p>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).</p>
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.
FlushAction	<ul style="list-style-type: none"> <li>• none</li> <li>• flushGrpMem</li> <li>• flushMrouter</li> <li>• flushSender</li> </ul>
RouterAlertEnable	<p>When enabled, this parameter instructs the router to process packets not directly addressed to it.</p> <p><b>Note:</b> To maximize your network performance, Nortel Networks recommends that you set this parameter according to the version of IGMP currently in use.</p> <ul style="list-style-type: none"> <li>• IGMPv1 - Disable</li> <li>• IGMPv2 - Enable</li> <li>• IGMPv3 - Enable</li> </ul>
SsmSnoopEnable	<p>Enables (true) or disables (false) support for PIM source-specific multicast (SSM) on the snooping interface.</p> <ul style="list-style-type: none"> <li>• Enable SSM</li> </ul>

**Table 8** MIB definition

Field	Description
rclgmpInterfaceExtnSsmEnable	Enables Ssm.

## 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 Global 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

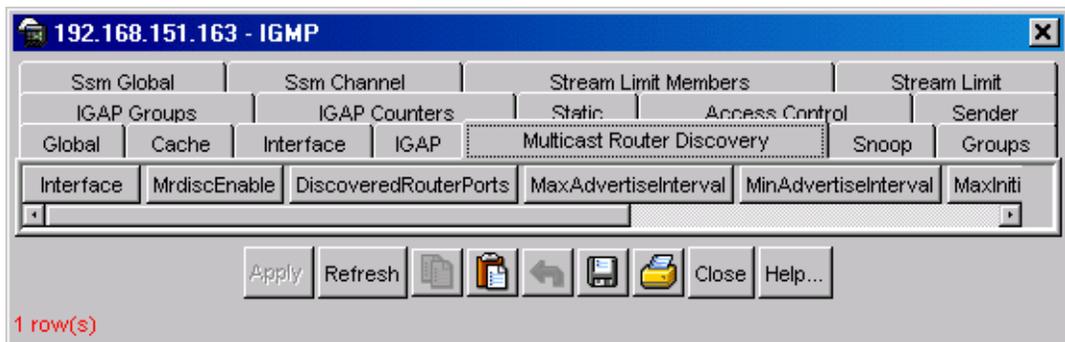


Table 9 describes the Multicast Router Discovery tab fields.

**Table 9** 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. <b>Note:</b> The Multicast Router Discovery protocol is not supported on brouter ports.

**Table 9** Multicast Router Discovery tab fields (continued)

<b>Field</b>	<b>Description</b>
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 not 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 Global tab displayed.
- 2 Click the Snoop tab.  
The Snoop tab opens (Figure 22).

**Figure 22** IGMP dialog box—Snoop tab

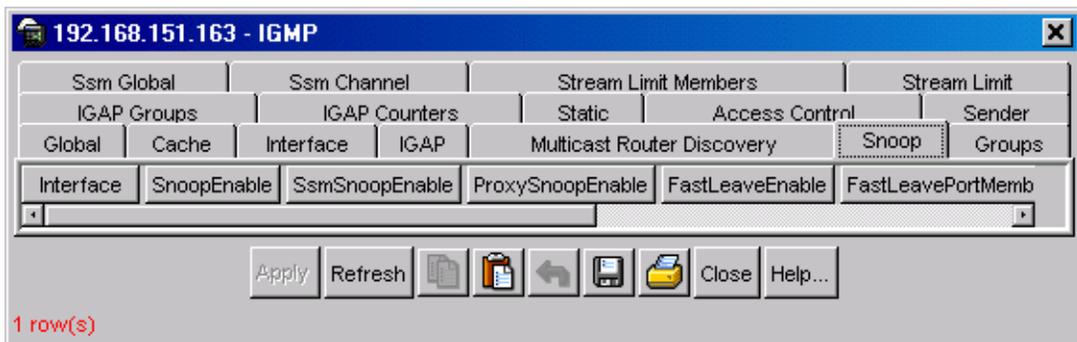


Table 10 describes the Snoop tab fields.

**Table 10** Snoop tab fields

Field	Description
Interface	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 10** 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. <b>Caution:</b> 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.
Ssmsnoopenable	Enables or disables support for PIM source-specific multicast (SSM) on the snooping interface. <ul style="list-style-type: none"> <li>• Enable SSM</li> </ul>

## 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 Global tab displayed.

- 2 Click the Groups tab.

The Groups tab opens ([Figure 23](#)).

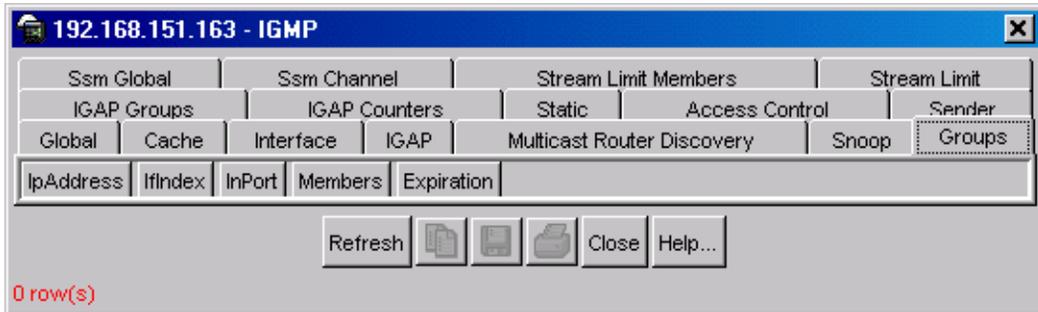
**Figure 23** IGMP dialog box—Groups tab

Table 11 describes the Groups tab fields.

**Table 11** 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 Global 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.

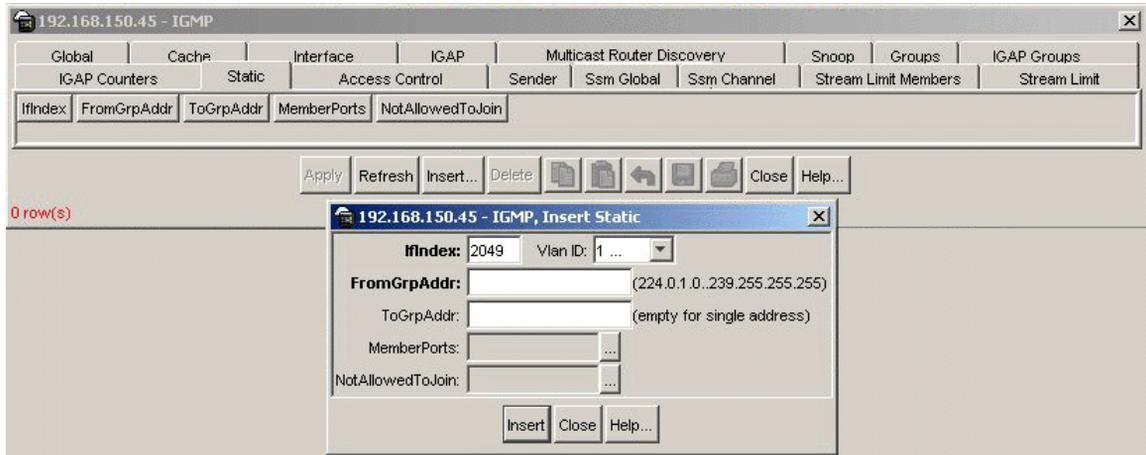
**Figure 24** IGMP and IGMP, Insert Static dialog boxes

Table 12 describes the fields in the IGMP, Insert Static dialog box.

**Table 12** IGMP, Insert Static dialog box fields

Field	Description
Ifindex	<b>The interface on which IGMP entry is enabled.</b>
FromGrpAddr	The starting address of the range. 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 Multicast addresses. If you try to select them, you will receive an invalid message.
ToGrpAddr	The end address of the range. 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 Multicast 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:

Topic	Page
<a href="#">Configuring a prefix list</a>	116
<a href="#">Configuring multicast access control for an interface</a>	118

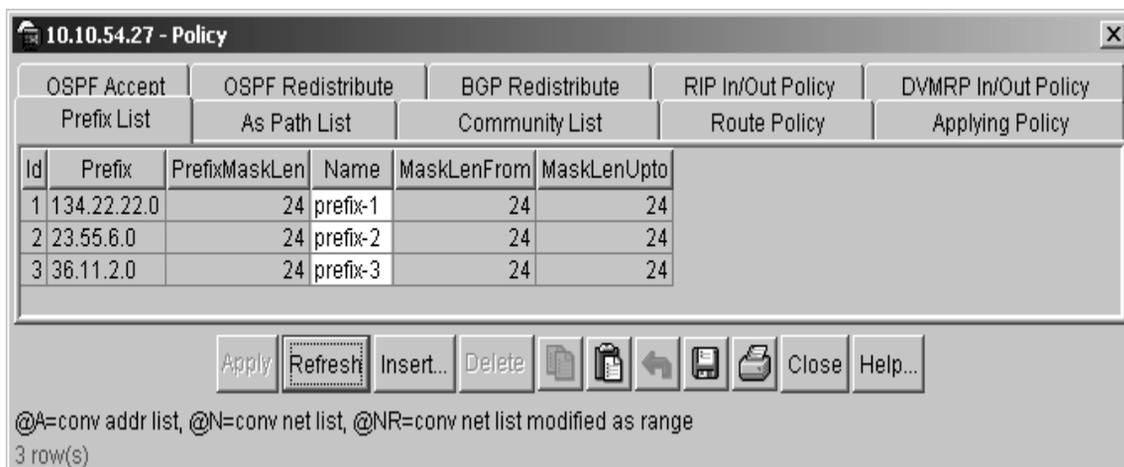
### Configuring a prefix list

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 13 describes the Policy, Insert Prefix List dialog box fields.

**Table 13** Policy, Insert Prefix List dialog box fields

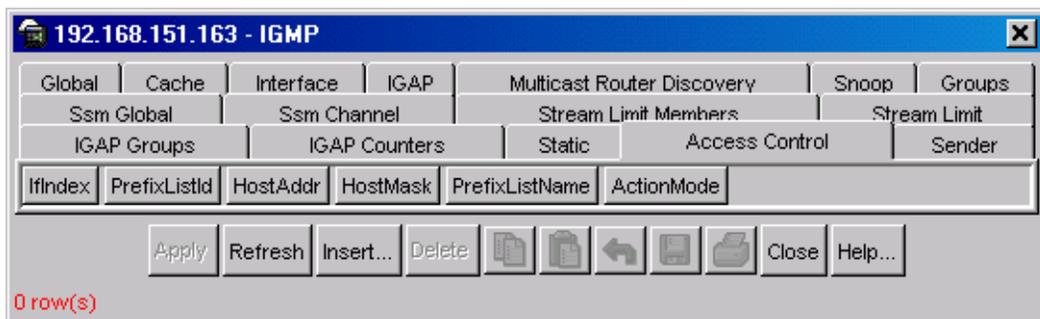
Field	Description
ID	The list identifier.
Prefix	The IP address.
PrefixMaskLen	This is the specified length of the prefix mask. <b>Note:</b> You must enter the full 32-bit mask in order to exact a full match of a specific IP address (for example, such as when creating a policy to match on next-hop).
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.
<b>Note:</b> 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 Global tab displayed.
- 2 Click the Access Control tab.  
The Access Control tab opens ([Figure 27](#)).

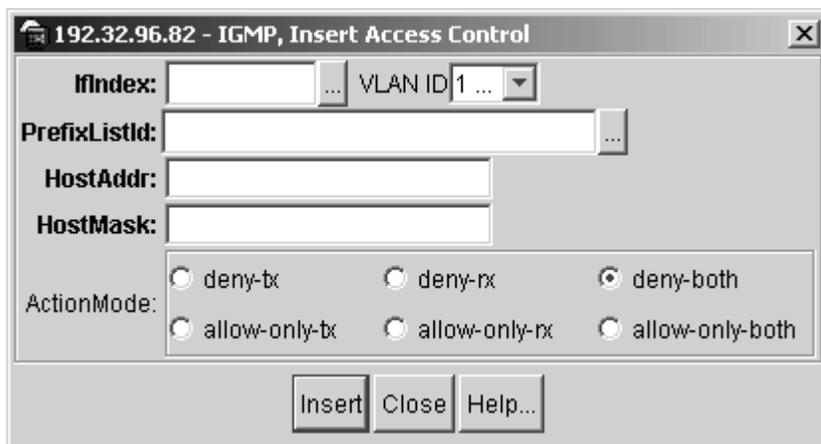
**Figure 27** IGMP dialog box —Access Control tab



- 3 Click Insert.

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

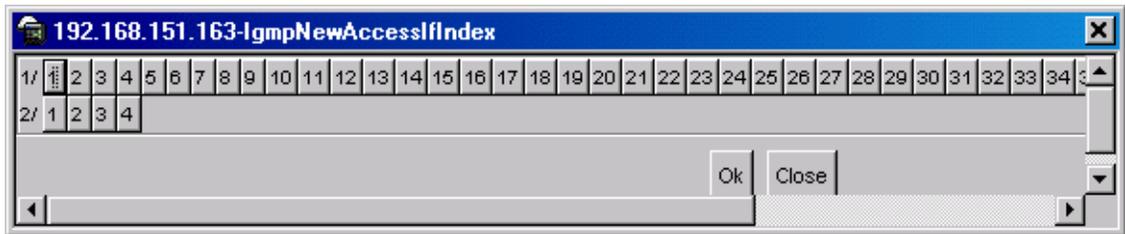
**Figure 28** IGMP, Insert Access Control dialog box



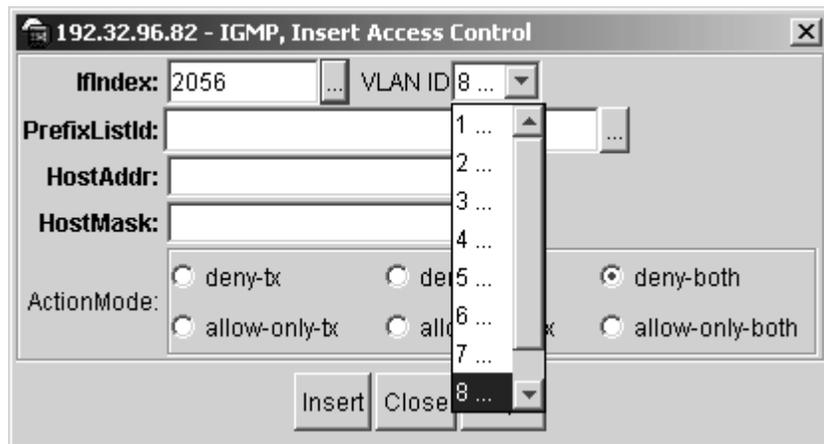
- 4 If you're configuring multicast access control for an IGMP interface, click the ellipsis button (...) next to IfIndex (Figure 29). Select the interface on which the IGMP entry is enabled.

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** IcmpNewAccessIfIndex 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 14](#) describes the Access Control tab fields.

**Table 14** Access Control tab fields

Field	Description
IfIndex	The interface on which the IGMP entry is enabled. The default value is between 2049-6141.
VLAN ID	Identifies the VLAN on which you want to configure multicast access control (1-4093).
PrefixListId	A numeric string that identifies the prefix list. See <a href="#">"Configuring a prefix list" on page 116</a> for more information about prefix lists.
HostAddr	The IP address of the host. See <a href="#">"Specifying host addresses and masks"</a> 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 <a href="#">"Specifying host addresses and masks"</a> for more information.
PrefixListName	The name of the prefix list. See <a href="#">"Configuring a prefix list" on page 116</a> for more information about prefix lists.
ActionMode	Used to specify whether the host identified by HostAddr should be: <ul style="list-style-type: none"><li>• Denied IP multicast transmitted traffic (deny-tx).</li><li>• Denied IP multicast received traffic (deny-rx).</li><li>• Denied both IP multicast transmitted and received traffic (deny-both).</li><li>• Allowed IP multicast transmitted traffic (allow-only-tx).</li><li>• Allowed IP multicast received traffic (allow-only-rx).</li><li>• Allowed both IP multicast transmitted and received traffic (allow-only-both).</li></ul>

## 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 Global tab displayed.
- 2 Click the Sender tab.  
The Sender tab opens (Figure 31).

**Figure 31** IGMP dialog box —Sender tab

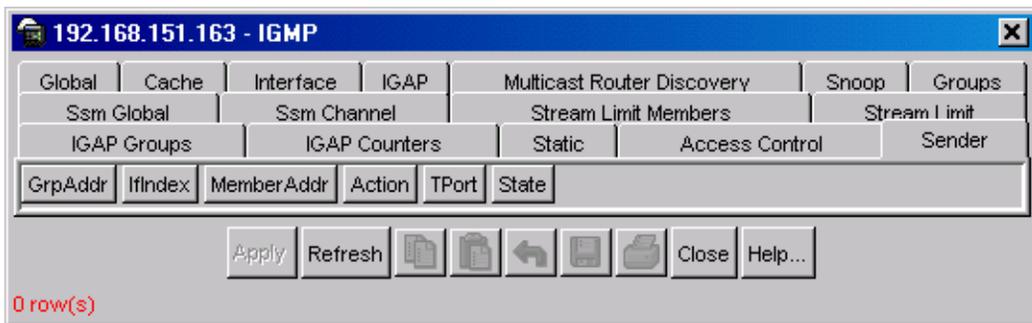


Table 15 describes the Sender tab fields.

**Table 15** 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 15** 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 Global tab displayed.
- 2 Click the SsmGlobal tab.  
The SsmGlobal tab opens ([Figure 32](#)).

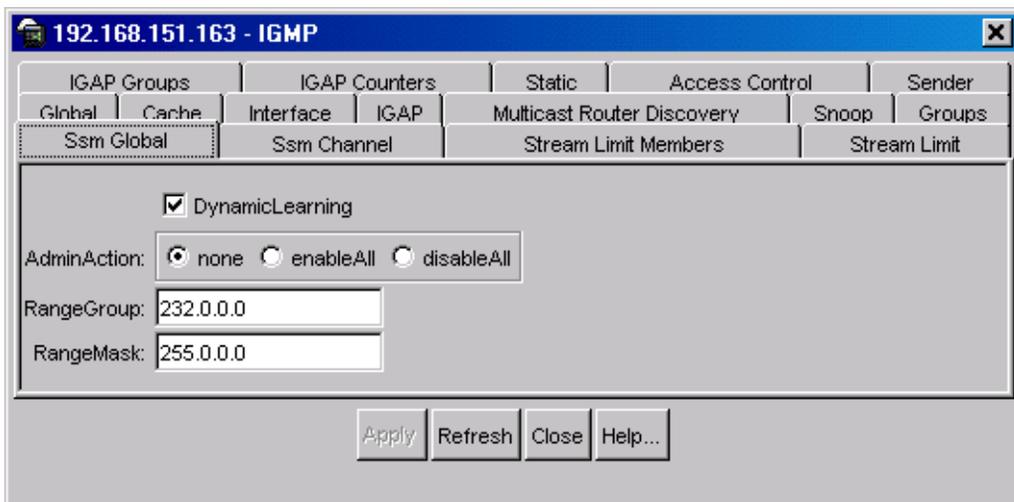
**Figure 32** IGMP dialog box—SsmGlobal tab

Table 16 describes the SsmGlobal tab fields.

**Table 16** 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 <a href="#">“Configuring the SSM channel table.”</a>
AdminAction	Sets the admin state, which determines whether or not the switch uses the table entries. <ul style="list-style-type: none"> <li>• none (default) - Does not set the admin state globally so that you can set it for individual SSM channel table entries.</li> <li>• enableAll - Globally activates all the static entries in the SSM channel table. This setting does not affect the dynamically learned entries.</li> <li>• disableAll - Globally inactivates all the static entries in the SSM channel table. This setting does not affect the dynamically learned entries.</li> </ul> For information on how this setting affects the switch’s behavior, see <a href="#">“Configuring the SSM channel table.”</a>

**Table 16** IGMP dialog box—SsmGlobal tab fields (continued)

Field	Description
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. <b>Note:</b> Before changing this setting, see <a href="#">“Changing the SSM range group.”</a>
RangeMask	Sets the address mask of the multicast group. The default is 255.0.0.0.

## Changing the SSM range group

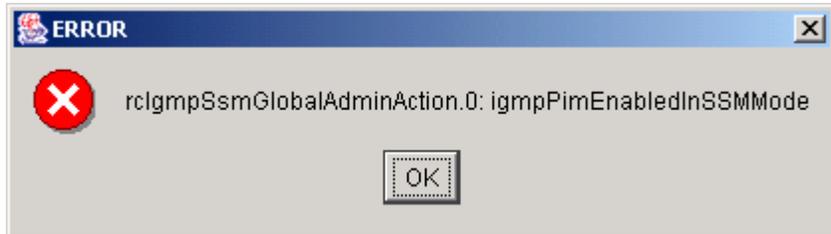


**Note:** This procedure re-initializes PIM and temporarily stops all PIM traffic. For those multicast groups out of SSM range (i.e. under PIM-SM behavior), it also causes an RP relearn delay of up to 60 seconds. This delay can be longer if the BSR is local.

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.



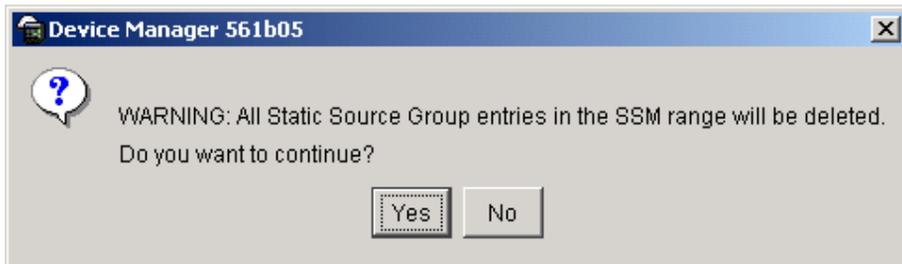
- 2 Open the SsmChannel tab and delete all of the entries in the SSM channel table.

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.

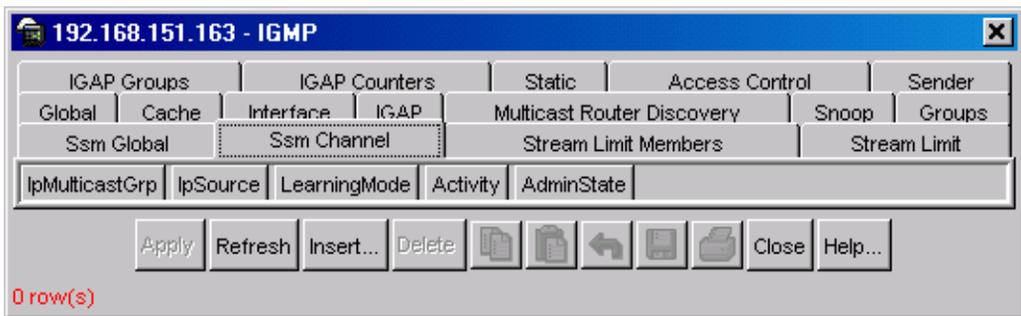
When you disable an SSM channel, the Passport 8600 stops any multicast traffic from the specified source to the specified group. If desired, you can use this static setting as a security feature to block traffic from a certain source to a specific group.

For more information, refer to [“Configuring multicast static source groups” on page 248](#).

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 Global tab displayed.
- 2 Click the SsmChannel tab.  
The SsmChannel tab opens (Figure 33).

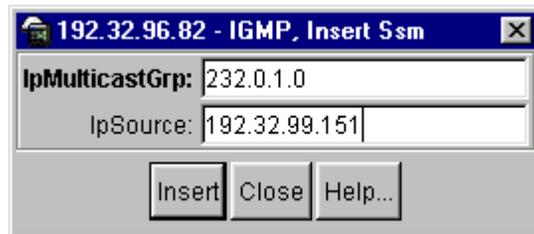
**Figure 33** IGMP dialog box—SsmChannel tab



- 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.

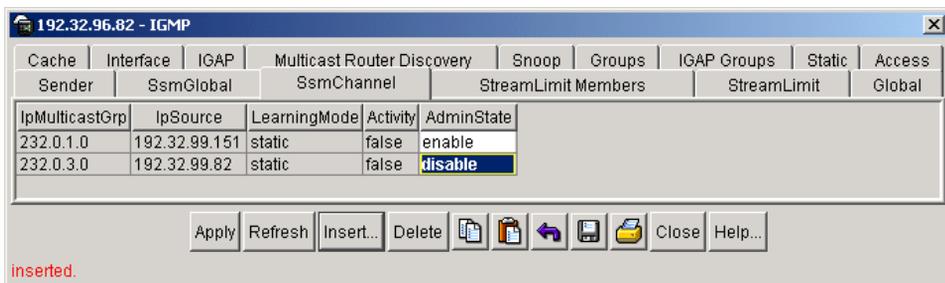
**Figure 35** IGMP dialog box—SsmChannel tab

Table 17 describes the SsmChannel table entry fields.

**Table 17** 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. <b>True</b> indicates that traffic is flowing to the switch, otherwise it should display <b>false</b> . 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 <b>enable</b> (default) to use the entry or <b>disable</b> 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:

Topic	Page
<a href="#">Configuring multicast stream limitation on an interface</a>	129
<a href="#">Configuring multicast stream limitation members</a>	131
<a href="#">Configuring multicast stream limitation on an Ethernet port</a>	134
<a href="#">Configuring multicast stream limitation on a VLAN</a>	136

### Configuring multicast stream limitation on an interface

To configure stream limitation on a specific interface:

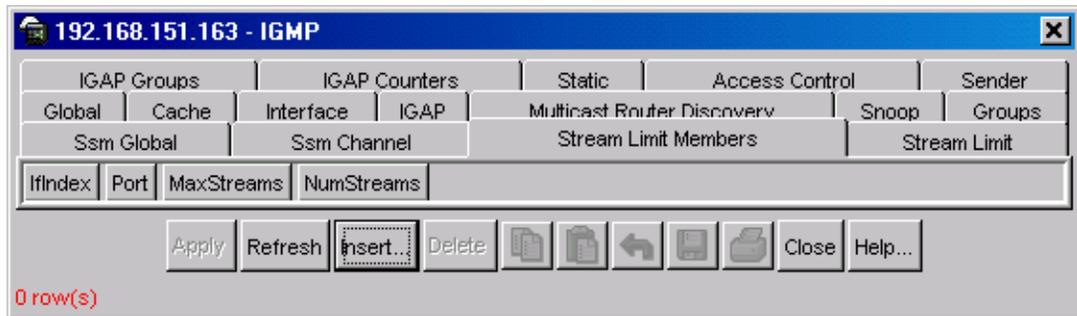
- 1 From the Device Manager menu bar, choose IP Routing > IGMP.

The IGMP dialog box opens with the Global 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 18](#) describes the StreamLimit tab fields.

**Table 18** 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 Global tab displayed.
- 2 Click the StreamLimit Members tab.

The StreamLimit Members tab opens (Figure 37).

**Figure 37** IGMP dialog box—StreamLimit Members tab

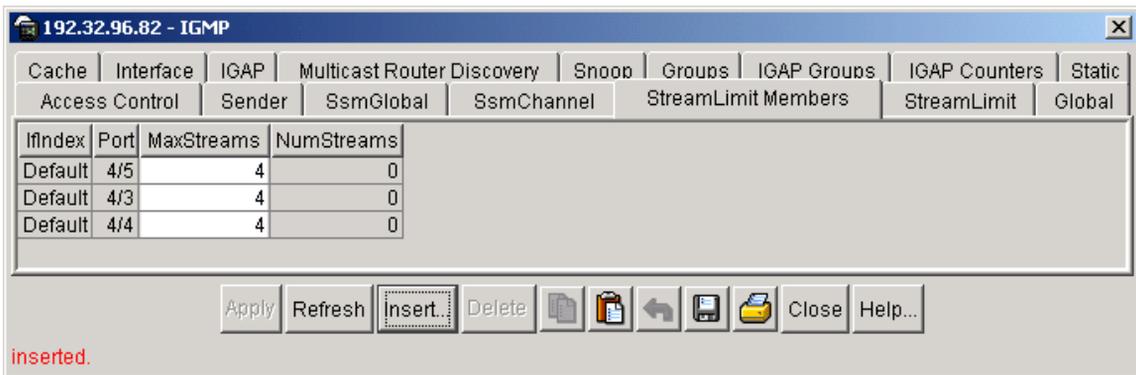


Table 19 describes the StreamLimit Members tab fields.

**Table 19** 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 Global 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.

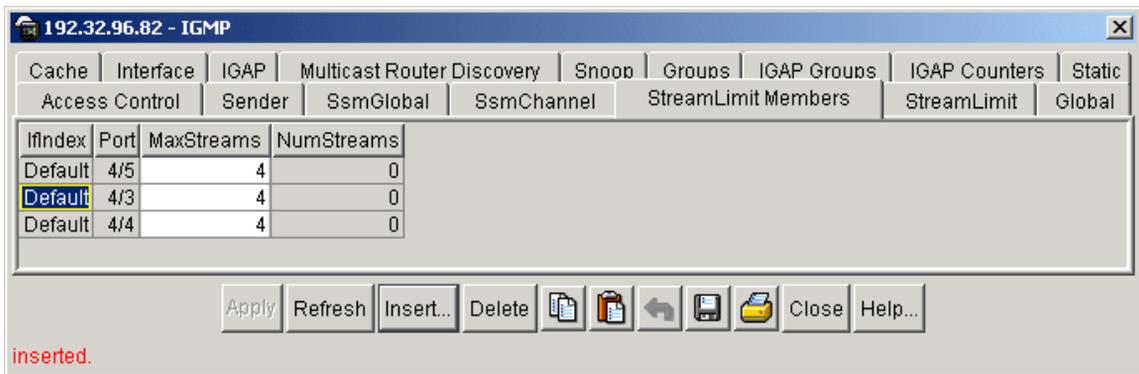
- 6 Enter a maximum number of streams or accept the default of 4.
- 7 Click Insert.

## 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 Global 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.

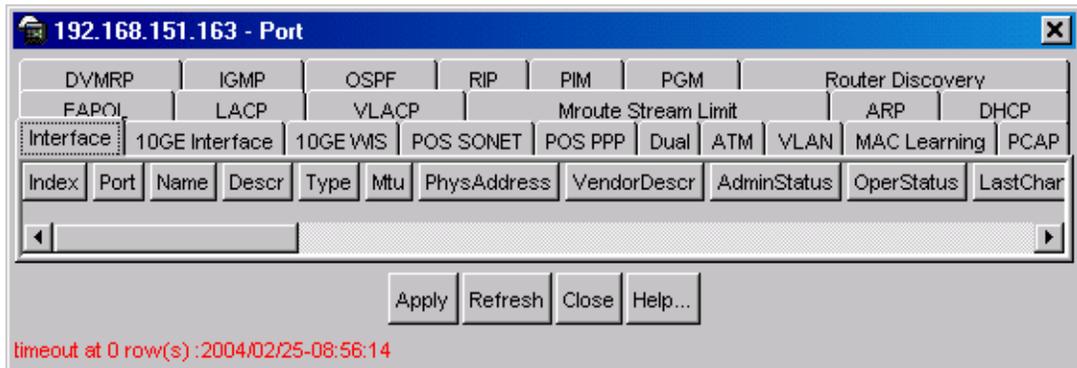
## Configuring multicast stream limitation on an Ethernet port

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 40).

**Figure 40** Port dialog box—Interface tab



- 3 Click the IGMP tab.

The IGMP tab opens (Figure 41).

**Figure 41** Port dialog box—IGMP tab

The screenshot shows a configuration window for IGMP on port 1/3 of interface 192.168.151.163. The window has a menu bar with tabs: Remote Mirroring, Mroute Stream Limit, Fdb Protect, IP Address, ARP, DHCP, DVMPRP, Interface, VLAN, STG, MAC Learning, Rate Limiting, Test, SMLT, PCAP, EAPOL, LACP, VLACP, IGMP, OSPF, RIP, PIM, PGM, VRRP, Router Discovery, and IPX BRouter. The IGMP tab is active, showing the following settings:

- QueryInterval: 125 (1..65535) sec
- QueryMaxResponseTime: 100 0..255 (1/10sec)
- Robustness: 2 2..255
- LastMembQueryIntvl: 10 0..255 (1/10sec)
- Version:  version1  version2  version3
- FastLeaveEnable
- StreamLimitEnable:  enable  disable
- Maximum Number Of Stream: 0 (number)
- Current Number Of Stream: 0

Buttons at the bottom: Apply, Refresh, Close, Help...

[Table 20](#) 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 20** 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 42](#)).

Figure 42 IP, VLAN dialog box—IGMP tab

The screenshot shows a window titled "192.168.151.163 - IP, VLAN 1" with a close button in the top right corner. The window contains a tabbed interface with the following tabs: PIM, PGM, VRRP, Router Discovery, Direct Broadcast, RSMLT, IP Address, ARP, DHCP, DVMRP, IGMP (selected), OSPF, and RIP. The IGMP tab is active and displays the following configuration options:

- QueryInterval: 125 (1.65535) sec
- QueryMaxResponseTime: 100 0..255 (1/10sec)
- Robustness: 2 2..255
- LastMembQueryIntvl: 10 0..255 (1/10sec)
- SnoopEnable
- SsmSnoopEnable
- ProxySnoopEnable
- IgapEnable:  enable  disable
- AccntEnable:  enable  disable
- AuthEnable:  enable  disable
- Version:  version1  version2  version3
- FastLeaveEnable
- StreamLimitEnable:  enable  disable
- Maximum Number Of Stream: 0 (number)
- Current Number Of Stream: 0
- FastLeavePortMembers: [ ] ...

At the bottom of the dialog box, there are four buttons: Apply, Refresh, Close, and Help...

[Table 21](#) 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 21** 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:

Topic	Page
<a href="#">Configuration prerequisites</a>	140
<a href="#">Enabling DVMRP globally</a>	141
<a href="#">Enabling DVMRP on a brouter port</a>	143
<a href="#">Enabling DVMRP on a VLAN</a>	146
<a href="#">Viewing and editing DVMRP interface parameters</a>	149
<a href="#">Viewing and editing DVMRP interface advance parameters</a>	150
<a href="#">Viewing DVMRP neighbor parameters</a>	152
<a href="#">Viewing DVMRP learned routes</a>	153
<a href="#">Viewing DVMRP next hop information</a>	154
<a href="#">Configuring DVMRP routing policies</a>	156

## 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 a 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

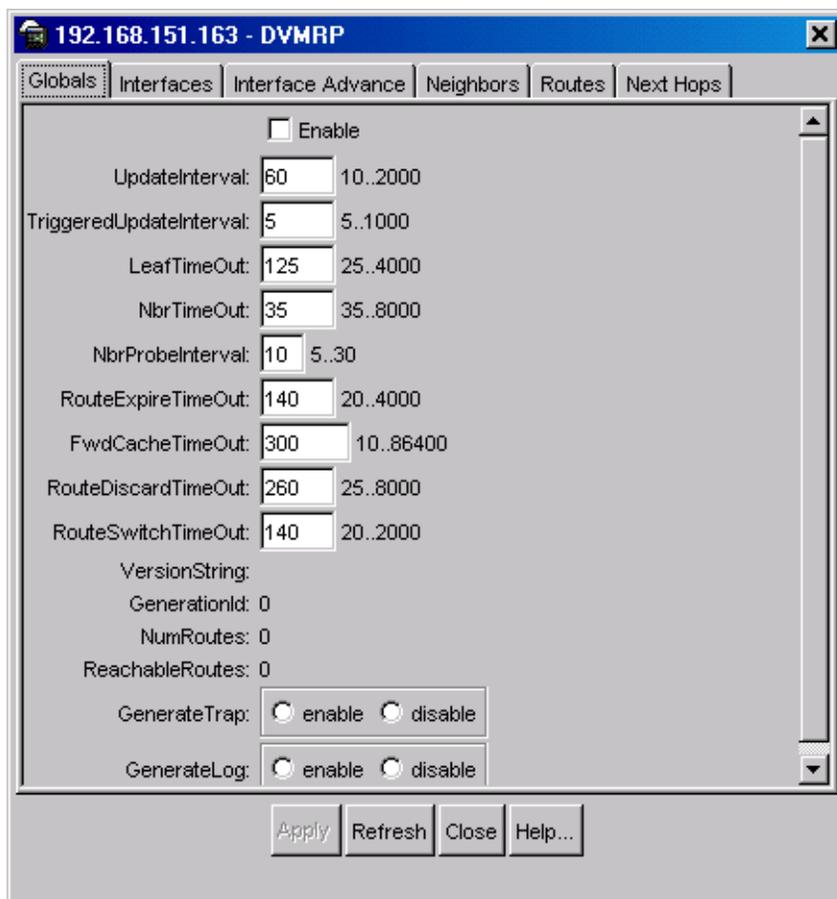
When you enable DVMRP globally and on a particular interface, the IGMP parameters automatically take effect.

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 22](#) describes the Globals tab fields.

**Table 22** 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 DMVPR 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 22** 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.
Generate Trap	Enabling this command on the switch triggers trap for the following DVMRP events: <ul style="list-style-type: none"> <li>• Neighborhood is established</li> <li>• Neighborhood is lost</li> <li>• Enable/Disable DVMRP on an interface</li> </ul>
Generate Log	Enabling this command on the switch logs the following DVMRP events: <ul style="list-style-type: none"> <li>• Neighborhood is established</li> <li>• Neighborhood is lost</li> <li>• Enable/Disable DVMRP on an interface</li> </ul>

## Enabling DVMRP on a router port

To configure DVMRP on a router 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

192.168.151.163 - Port 1/9

Remote Mirroring | Mroute Stream Limit | Fdb Protect | IP Address | ARP | DHCP

Interface | VLAN | STG | MAC Learning | Rate Limiting | Test | SMLT | PCAP | EAPOL | LACP | VLACP

DVMRP | IGMP | OSPF | RIP | PIM | PGM | VRRP | Router Discovery | IPX BRouter

LocalAddr: 0.0.0.0

Enable

Metric: 1 1..31

InterfaceType:  active  passive

DefaultListen

DefaultSupply

DefaultRouteMetric: 1 (number)

AdvertiseSelf

InPolicy:  ...

OutPolicy:  ...

Apply Refresh Close Help...

- 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 23](#) describes the Globals tab fields.

**Table 23** 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) DVMRP on the port.

**Table 23** Port dialog box—DVMRP tab fields (continued)

Field	Description
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

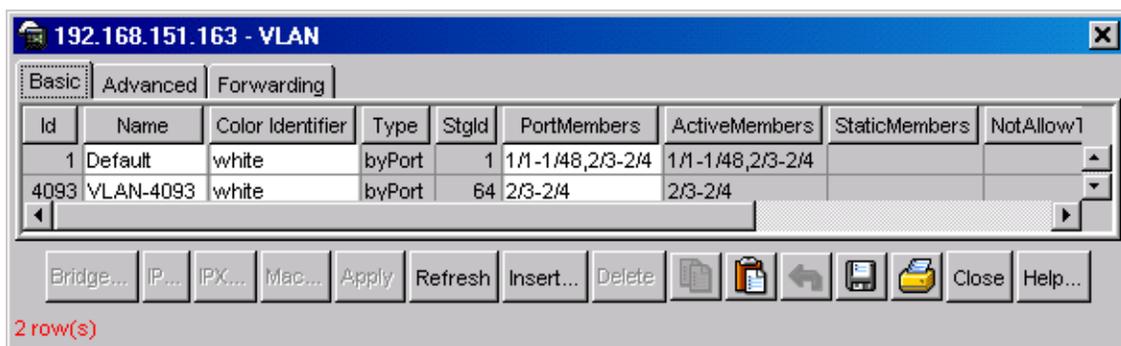
You must enable DVMRP on a VLAN before you configure IGMP on a VLAN.

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).

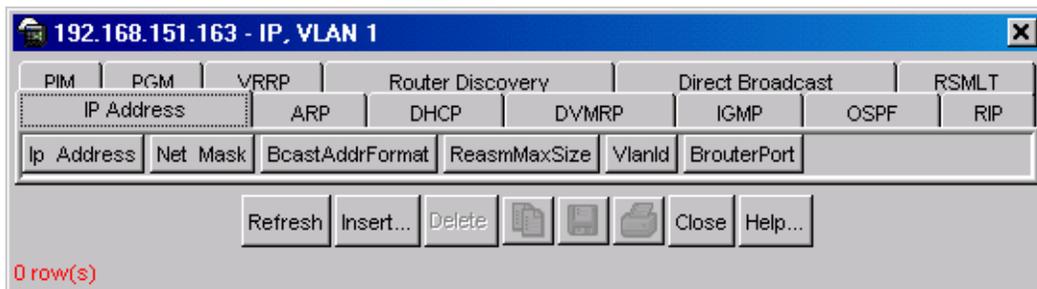
**Figure 45** VLAN dialog box—Basic tab



- 2 Select a VLAN.
- 3 Click IP.

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

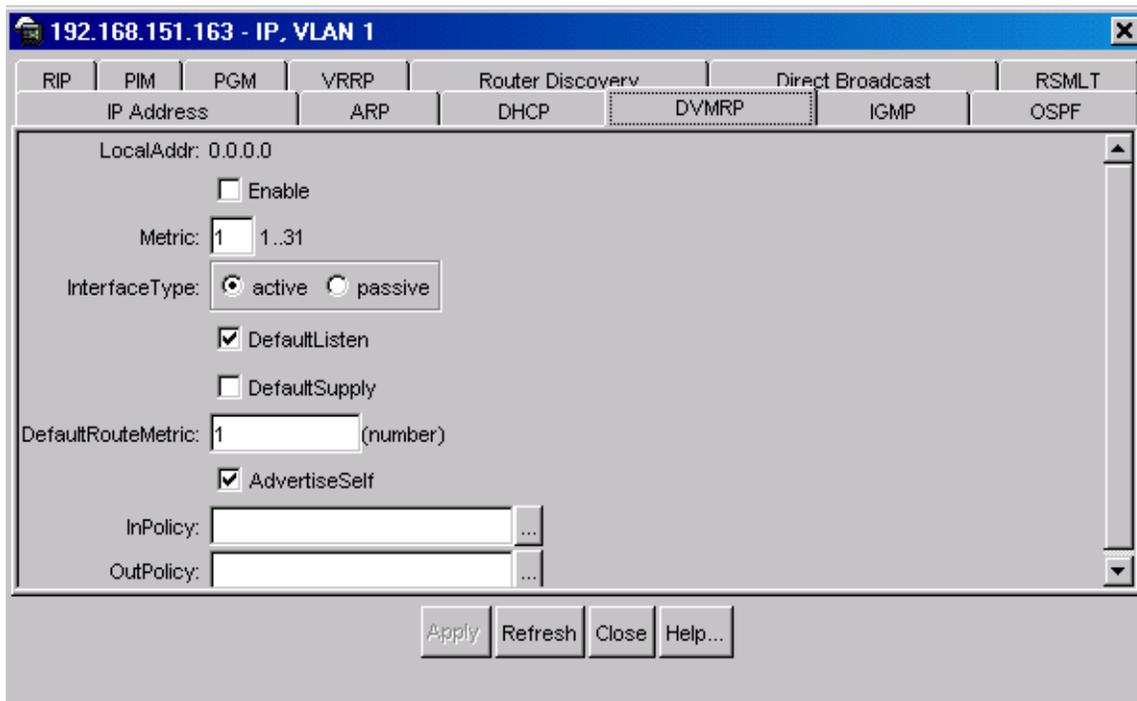
**Figure 46** IP, VLAN dialog box—IP Address tab



- 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 24 describes the DVMRP tab fields

**Table 24** DVMRP tab fields

Field	Description
LocalAddress	Provides the IP address of the DVMRP router interface.
Enable	Enables (checkbox selected) or disables (checkbox not selected) DVMRP 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

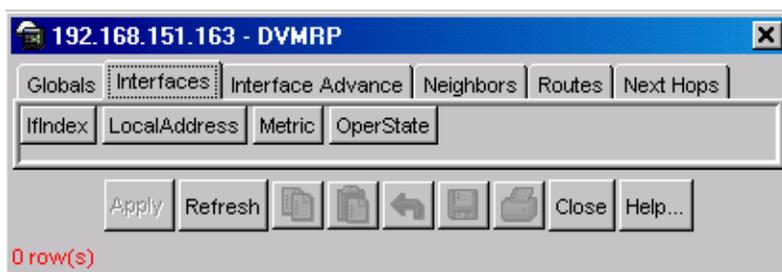


Table 25 describes the DVMRP Interfaces tab fields.

**Table 25** 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 26 provides a description of the fields in this dialog box.

**Figure 49** DVMRP dialog box—Interface Advance tab



Table 26 describes the DVMRP Interface Advance tab fields.

**Table 26** 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) DVMRP on the interface.

**Table 26** DVMRP dialog box—Interface Advance tab fields (continued)

Field	Description
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 for 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

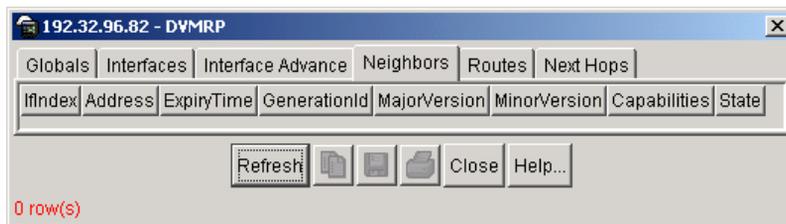


Table 27 describes the Neighbors tab fields.

**Table 27** 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 27** Neighbors tab fields (continued)

Field	Description
Capabilities	<p>The neighboring router's capabilities. The probe flag is 1 byte long with the lower 4 bits containing the following information:</p> <ul style="list-style-type: none"> <li>• The leaf bit (0) indicates that the neighbor has only one interface with neighbors.</li> <li>• The prune bit (1) indicates that the neighbor supports pruning.</li> <li>• The generationID bit (2) indicates that the neighbor sends its generation ID in probe messages.</li> <li>• The mtrace bit (3) indicates that the neighbor can handle mtrace requests.</li> </ul>
State	<p>The state of neighbor adjacency:</p> <ul style="list-style-type: none"> <li>• oneway—The switch sees a packet from the neighbor but no adjacency has been established.</li> <li>• active—Adjacency exists in both directions.</li> <li>• ignoring</li> <li>• down—The interface is not enabled.</li> </ul>

## 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 28](#) describes the fields in the Routes tab.

**Table 28** 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.
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

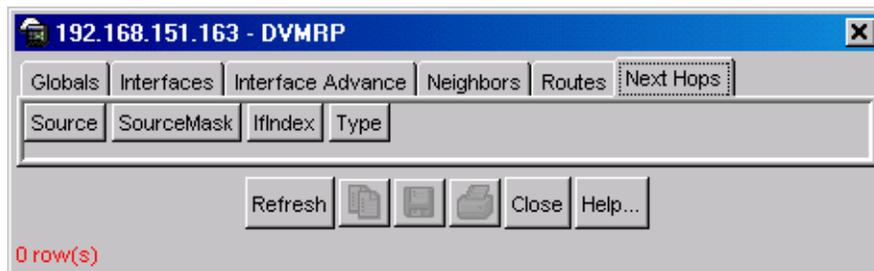


Table 29 describes the fields in the Next Hops tab.

**Table 29** 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:

Topic	Page
<a href="#">Configuring default route policies</a>	156
<a href="#">Configuring DVMRP announce policies</a>	160
<a href="#">Configuring DVMRP accept policies</a>	170
<a href="#">Configuring the advertisement of local network policies</a>	176
<a href="#">Configuring a DVMRP interface type</a>	180
<a href="#">Displaying DVMRP routing policy information</a>	184

### Configuring default route policies

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

Topic	Page
<a href="#">Applying the default route policy to an interface</a>	157
<a href="#">Applying the default route policy to a VLAN</a>	158
<a href="#">Applying the default route policy to a port</a>	159

Before you apply the default route policy to the switch, you must perform the procedures provided in [“Configuration prerequisites” on page 140](#).

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:

Task	Page
<a href="#">Creating a DVMRP announce policy</a>	160
<a href="#">Applying a DVMRP announce policy to an interface</a>	167
<a href="#">Applying a DVMRP announce policy to a VLAN</a>	168
<a href="#">Applying a DVMRP announce policy to a port</a>	169

Before you create and apply a DVMRP announce policy to the switch, you must perform the procedures provided in [“Configuration prerequisites”](#) on page 140.

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.”](#)

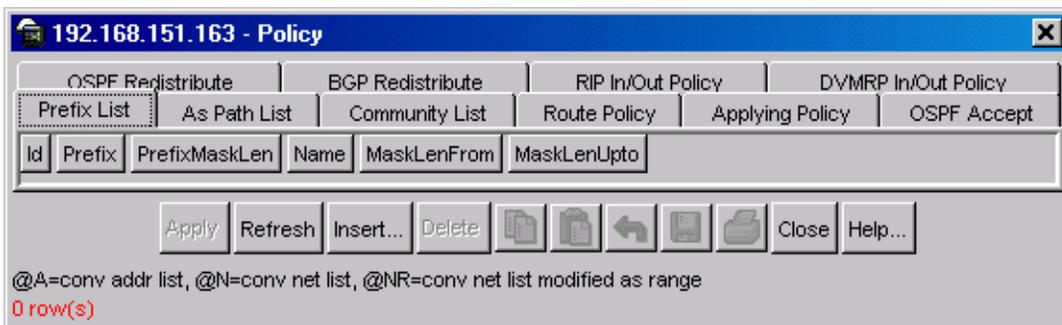
### Creating a DVMRP announce policy

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.

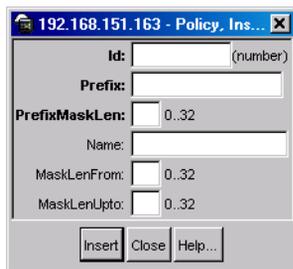
To create a DVMRP announce policy:

- 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).

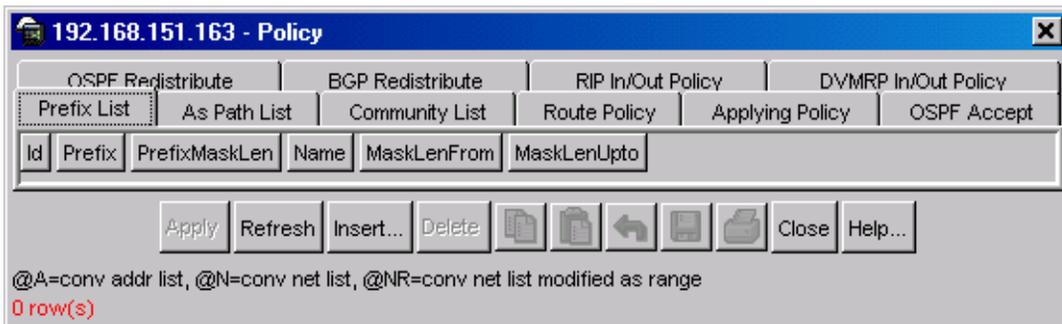
**Figure 54** Prefix List tab—Policy, Insert Prefix List dialog box

- 3 Create a prefix list for the new policy by entering the following information in the Policy, Insert Prefix List dialog box. (Table 30 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 30** 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 31](#) 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 31** Policy, Insert Route Policy dialog box

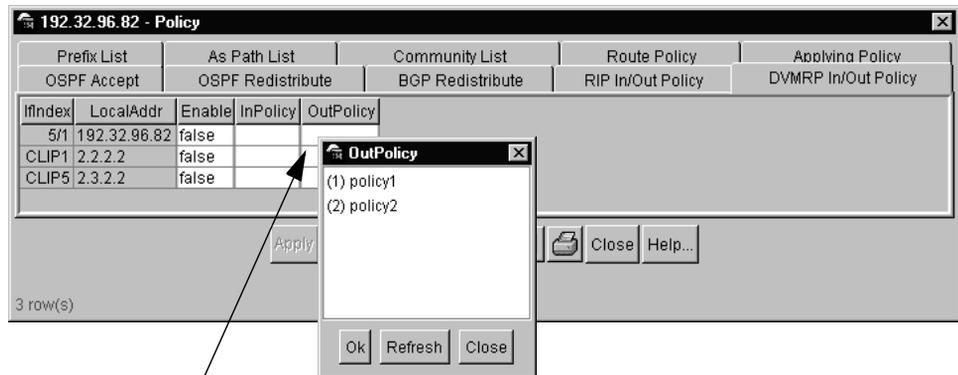
Field	Description
Id	The ID of an entry in the Prefix list table.
SequenceNumber	A second index used to identify a specific policy within a route policy group.
Name	The name of the route policy.
MatchProtocol	Selects the appropriate protocol. Matches the protocol through which the route is learned, if 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 (1 to 65535). If 0, then this field is ignored, if configured. The default is 0.

**Table 31** 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 is 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). Externaltyp1, and Externaltyp2 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. <ul style="list-style-type: none"> <li>• &lt;as-list&gt; specifies the list id of up to four defined as-lists separated by a comma.</li> <li>• [clear] when presents, the as-list configured will be removed.</li> </ul>

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

Double click in the OutPolicy name field to open the OutPolicy dialog box

- 10** Double 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.

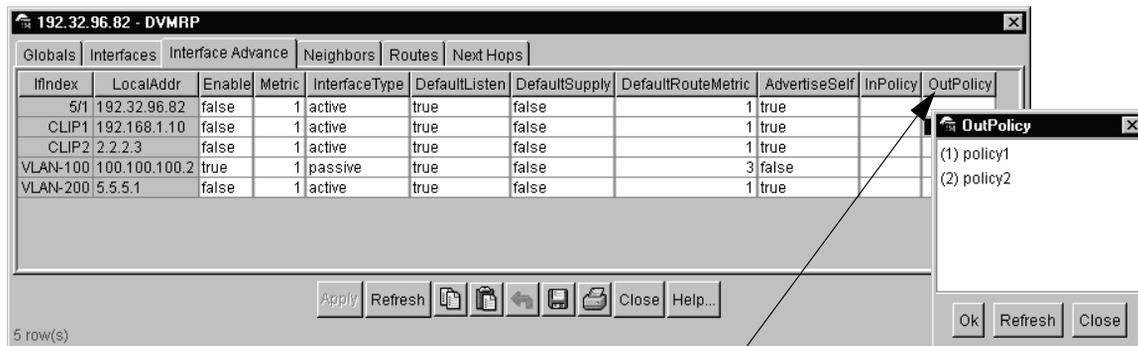
- 2 Select the Interface Advance tab.

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



Double click in the OutPolicy name field to open the 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.

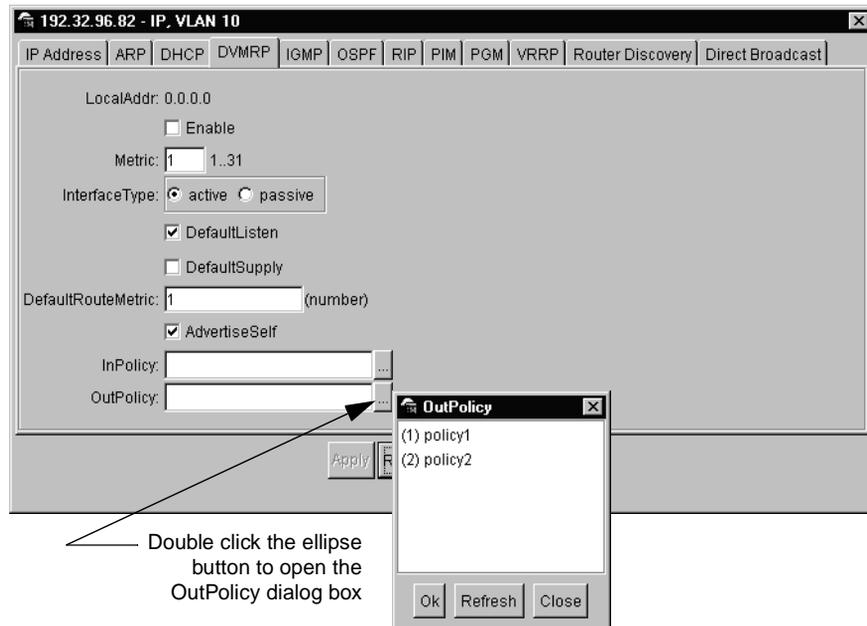
- 3 Click the DVMRP tab.

The DVMRP tab opens and displays the DVMRP configuration options.

- 4 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:

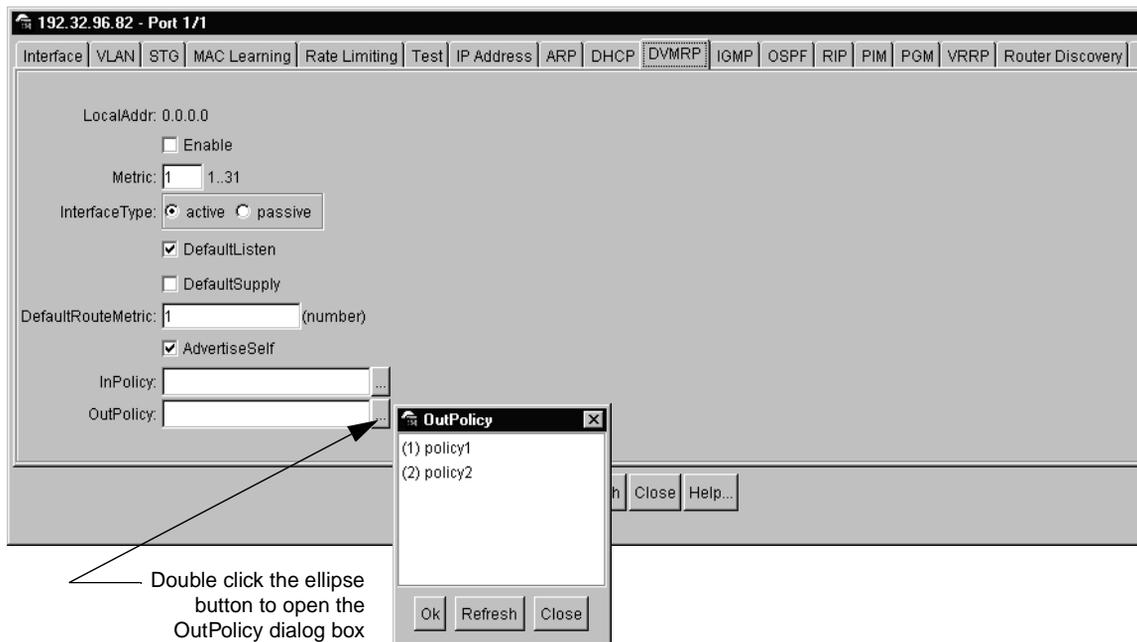
- 1 On the Device Manager, select a port.
- 2 From the Device Manager menu bar, choose Edit > Port.  
The Port dialog box opens with the Interface tab displayed.
- 3 Click the DVMRP tab.

The DVMRP tab opens and displays the DVMRP configuration options.

- 4 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:

Task	Page
<a href="#">Creating a DVMRP accept policy</a>	171
<a href="#">Applying a DVMRP accept policy to an interface</a>	173
<a href="#">Applying a DVMRP accept policy to a VLAN</a>	174
<a href="#">Applying a DVMRP accept policy to a port</a>	175

Before you create and apply a DVMRP accept policy to the switch, you must perform the procedures provided in [“Configuration prerequisites”](#) on page 140.

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 30](#) 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 30](#).
  - 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 31 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 CTRL 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 Double 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.

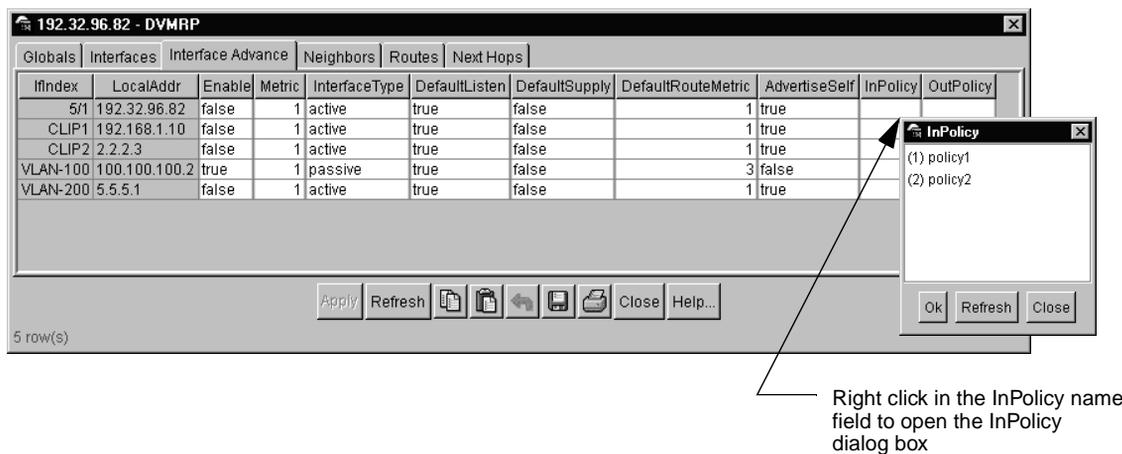
- 2 Select the Interface Advance tab.

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

- 3 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.

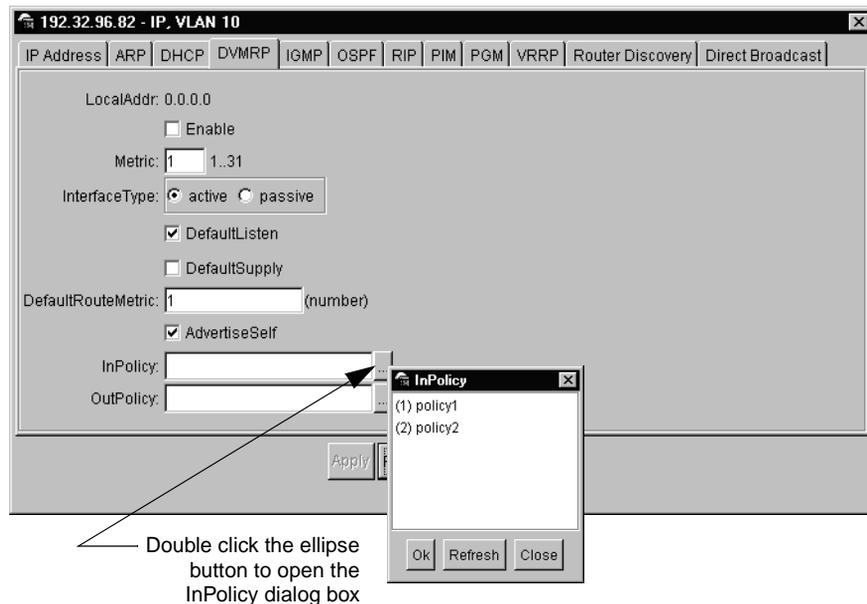
- 3 Click the DVMRP tab.

The DVMRP tab opens and displays the DVMRP configuration options.

- 4 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:

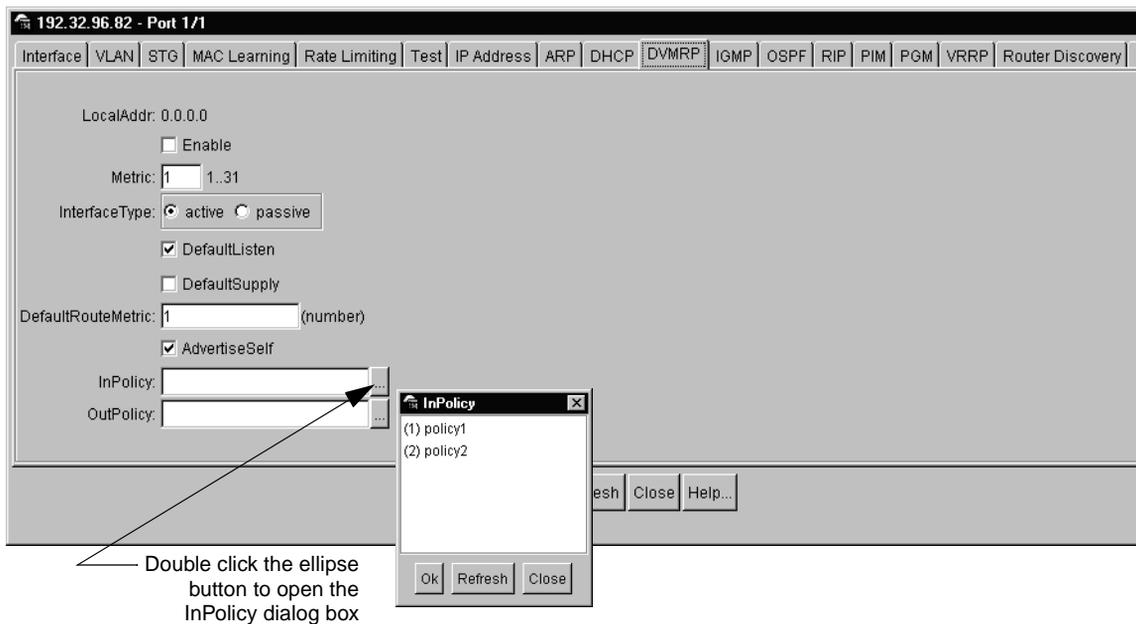
- 1 On the Device Manager, select a port.
- 2 From the Device Manager menu bar, choose Edit > Port.  
The Port dialog box opens with the Interface tab displayed.
- 3 Click the DVMRP tab.

The DVMRP tab opens and displays the DVMRP configuration options.

- 4 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
<a href="#">Apply the advertisement of local networks policy over an interface</a>	177
<a href="#">Apply the advertisement of local networks policy over a VLAN</a>	178
<a href="#">Apply the advertisement of local networks policy over a port</a>	179

Before you apply the advertisement of local networks policy to the switch, you must perform the procedures provided in [“Configuration prerequisites” on page 140](#).

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
<a href="#">Configuring an active or passive interface type</a>	181
<a href="#">Configuring an active or passive VLAN type</a>	182
<a href="#">Configuring an active or passive port type</a>	183

Before you apply the DVMRP passive interface policy to the switch, you must perform the procedures provided in [“Configuration prerequisites” on page 140](#).

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:

Task	Page
<a href="#">Displaying DVMRP routing policy information for an interface</a>	184
<a href="#">Displaying DVMRP routing policy information for a VLAN</a>	185
<a href="#">Displaying DVMRP routing policy information for a port</a>	185

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 211](#).

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:

<b>Topic</b>	<b>Page</b>
<a href="#">Configuration prerequisites</a>	189
<a href="#">Enabling PIM-SM globally</a>	190
<a href="#">Enabling static RP</a>	193
<a href="#">Enabling PIM on a brouter port</a>	197
<a href="#">Configuring a candidate bootstrap router (C-BSR)</a>	199
<a href="#">Enabling PIM on a VLAN interface</a>	200
<a href="#">Viewing and editing PIM interface parameters</a>	203
<a href="#">Viewing PIM-SM neighbor parameters</a>	206
<a href="#">Viewing the RP Set parameters</a>	207
<a href="#">Configuring a candidate RP</a>	208
<a href="#">Viewing the current bootstrap router (BSR)</a>	210
<a href="#">Configuring Source Specific Multicast (SSM)</a>	211

## 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.



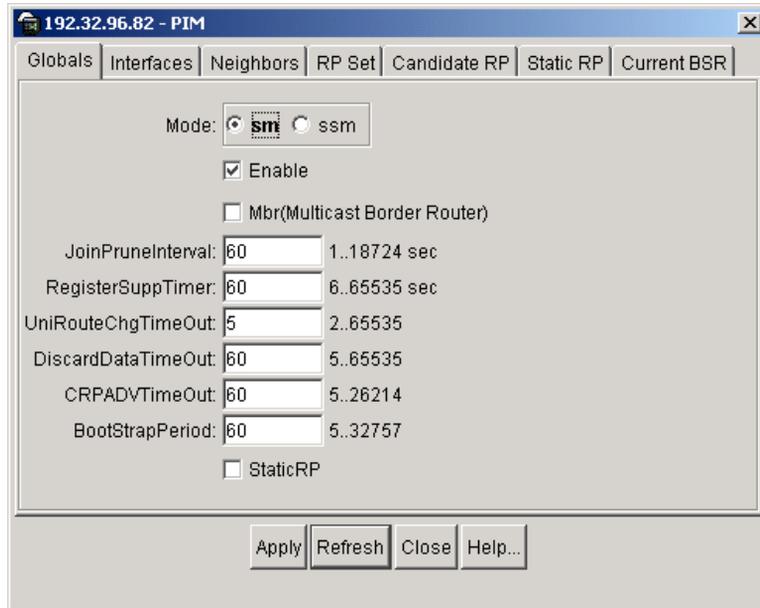
**Note:** To enable PIM-SSM globally, see [“Enabling Source Specific Multicast \(SSM\) globally.”](#) Also note that when you change from one mode to another, an information message pops up to remind you that traffic will not stop immediately.

---

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 32 describes the PIM Globals tab fields.

**Table 32** 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 32** 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. <b>Note:</b> 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.

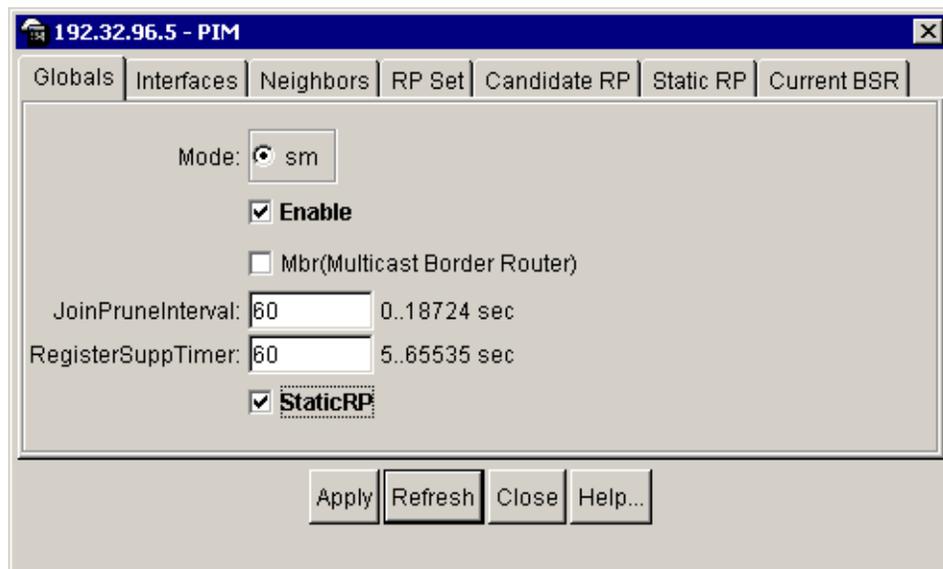
## Enabling static RP procedure

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

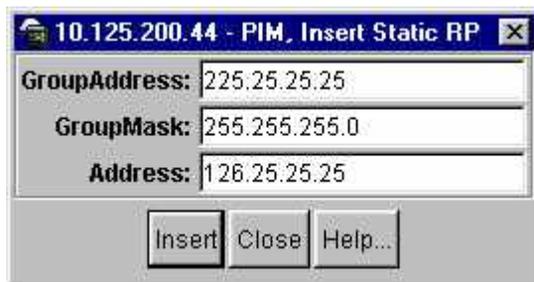


Table 33 describes the PIM Static RP fields.

**Table 33** 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 <b>valid</b> when the switch has a unicast route to the static RP's network and <b>invalid</b> otherwise.

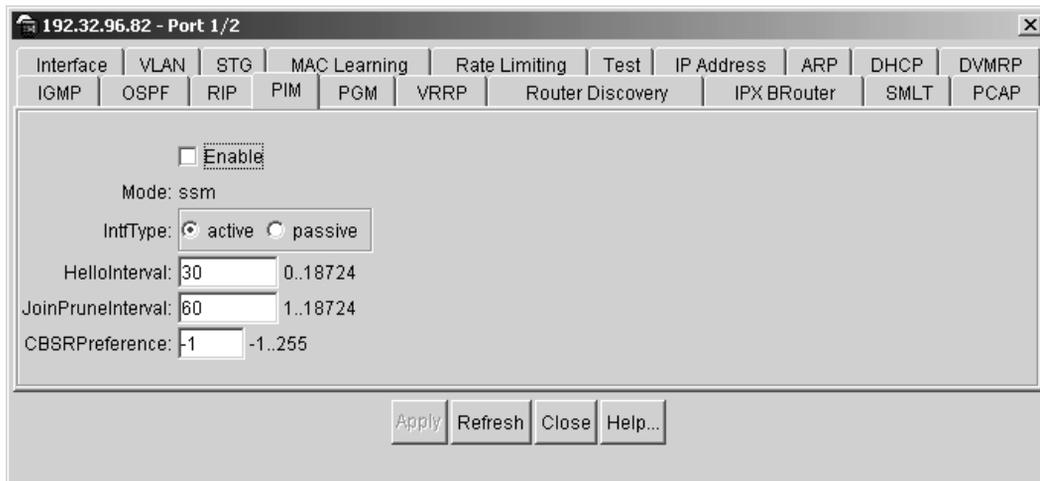
## Enabling PIM on a router port

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 190](#).

To enable PIM on a router 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 34 describes the PIM tab fields.

**Table 34** PIM tab fields

Field	Description
Enable	Enables (true) or disables (false) PIM for the specified router 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 router 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 router 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 router 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 190.

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.

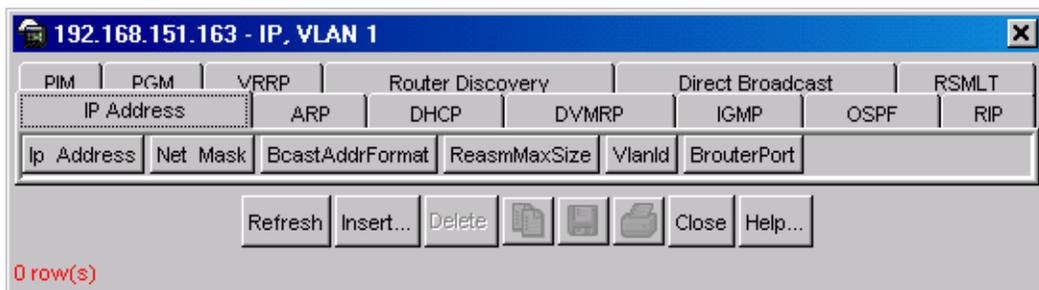
- 2 Select the VLAN ID that you want to configure with PIM.

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



- 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 35 describes the VLAN PIM tab fields.

**Table 35** 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.

**Table 35** VLAN PIM tab fields (continued)

Field	Description
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 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

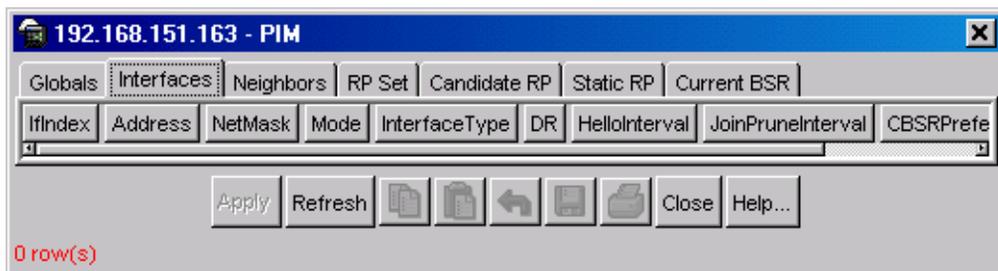


Table 36 describes the PIM Interfaces tab fields.



**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.

**Note:** For instructions on disabling PIM on a router port and changing the state of a PIM interface, see [“Changing the interface type” on page 198](#).

**Note:** For instructions on disabling PIM on a VLAN interface and changing the state of PIM interface, see [“Changing the VLAN interface type” on page 202](#).

**Table 36** 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. <b>Note:</b> 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.

**Table 36** PIM Interfaces tab fields (continued)

<b>Field</b>	<b>Description</b>
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

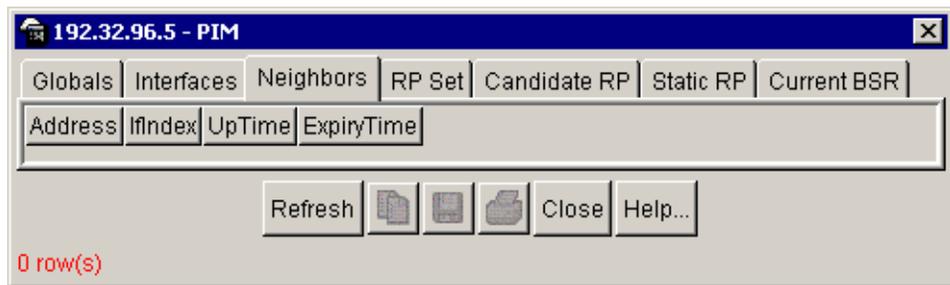


Table 37 describes the PIM Neighbors tab fields.

**Table 37** 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

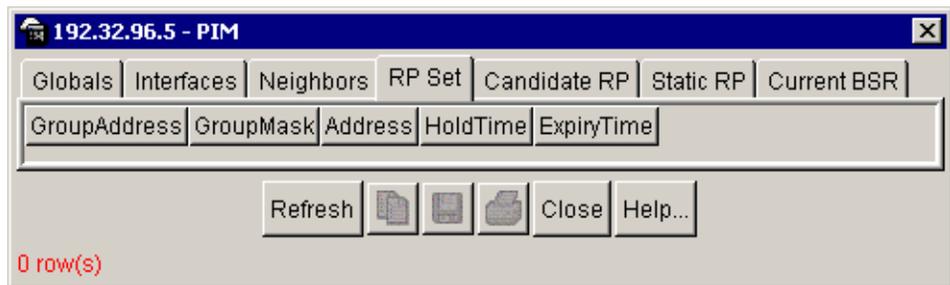


Table 38 describes the PIM RP Set tab fields.

**Table 38** 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 38** PIM RP Set tab fields (continued)

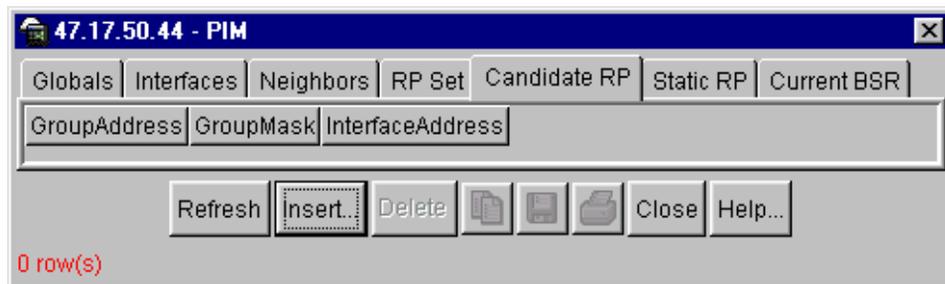
Field	Description
HoldTime	The time specified in a C-RP advertisement that the BSR uses to time out the RP. When the BSR receives an advertisement for the RP, it restarts the timer. If no advertisement arrives before the timer expires, the BSR removes that RP from the RP set.
ExpiryTime	The time remaining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

## Configuring a candidate RP

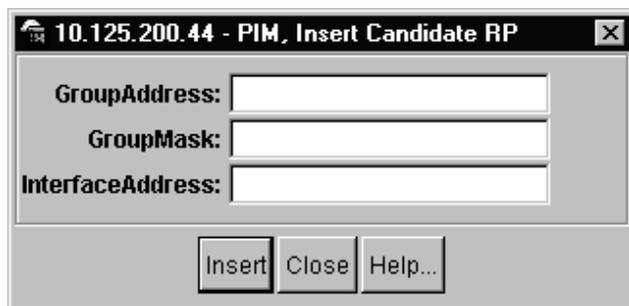
The following steps describe how to add a candidate rendezvous point (C-RP) to the RP Set.

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 39](#) describes the PIM Candidate RP fields.

**Table 39** 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

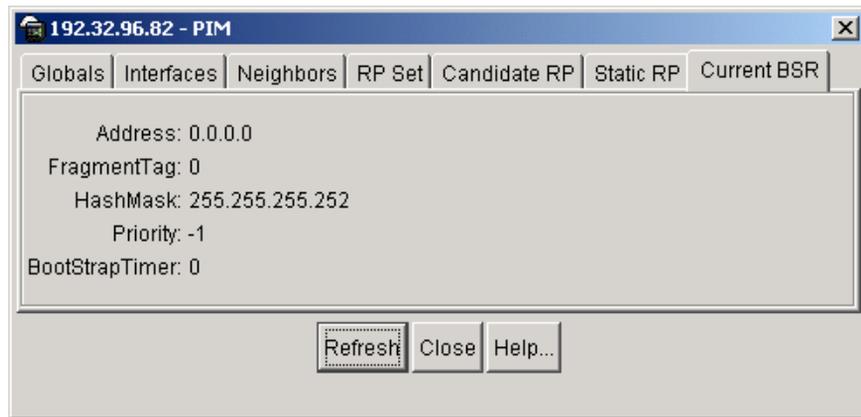


Table 40 describes the Current BSR tab fields.

**Table 40** 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 (RPF) 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.

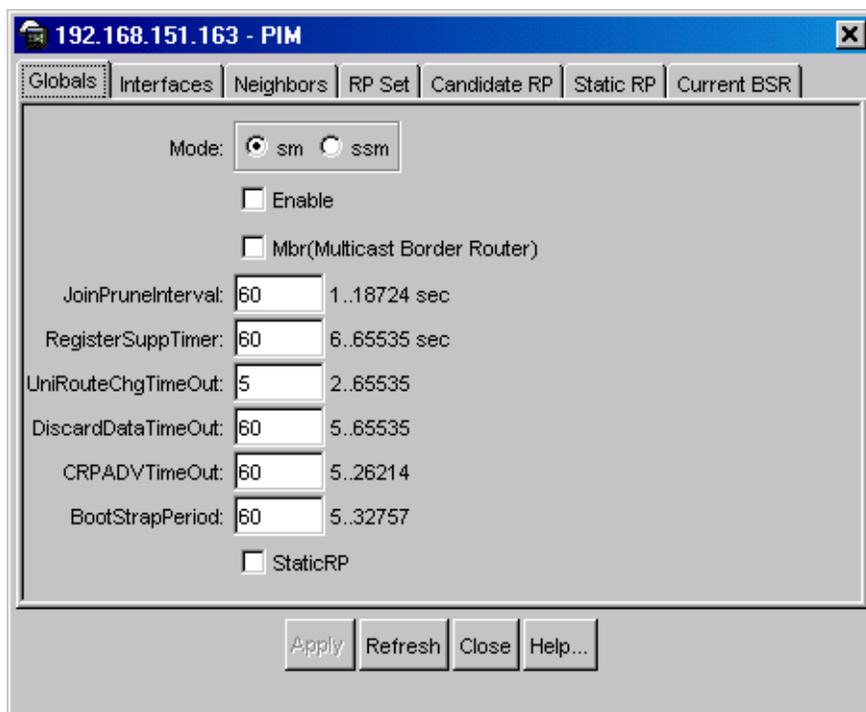
- 3 Enable PIM globally.

## 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 100.](#)”

For information on configuring the SSM group range and channel table, refer to [“Configuring the SSM range and global parameters” on page 122](#) or [“Configuring the SSM channel table” on page 126.](#)”

Table 41 describes the PIM Globals tab fields.

**Table 41** 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. <b>Note:</b> 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.

**Table 41** PIM Globals tab fields (continued)

Field	Description
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.



---

## 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:

Topic	Page
<a href="#">Configuration prerequisites</a>	218
<a href="#">Enabling PGM globally</a>	219
<a href="#">Enabling PGM on an interface</a>	221
<a href="#">Configuring VLANs with PGM</a>	223
<a href="#">Viewing and editing PGM interface parameters</a>	226
<a href="#">Graphing PGM interface statistics</a>	227
<a href="#">Graphing SPM and RDATA statistics for an interface</a>	228
<a href="#">Graphing NAK, NNAK, and NCF statistics for an interface</a>	230
<a href="#">Viewing PGM session parameters</a>	233
<a href="#">Graphing PGM session statistics</a>	234
<a href="#">Graphing SPM statistics for a session</a>	235
<a href="#">Graphing NAK statistics for a session</a>	237
<a href="#">Viewing the Retransmit parameters</a>	240

## 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.

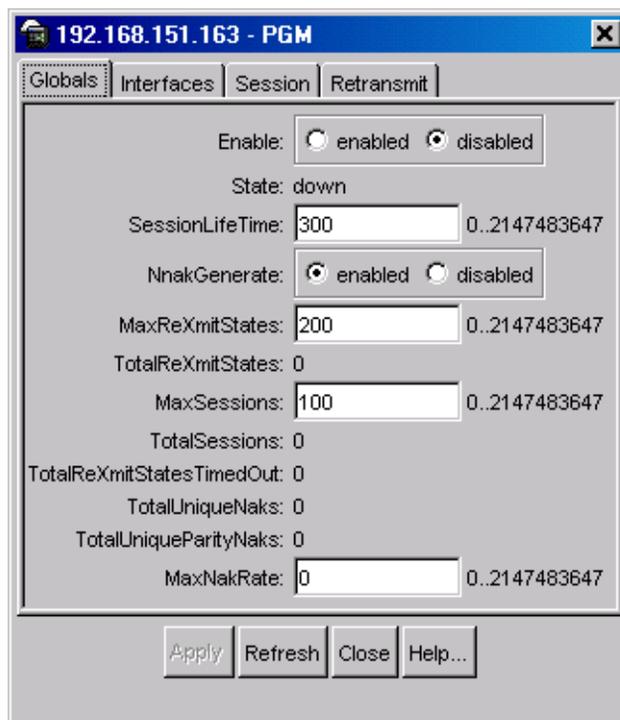
## Enabling PGM globally

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 42 describes the PGM Globals tab fields.

**Table 42** PGM Globals tab fields

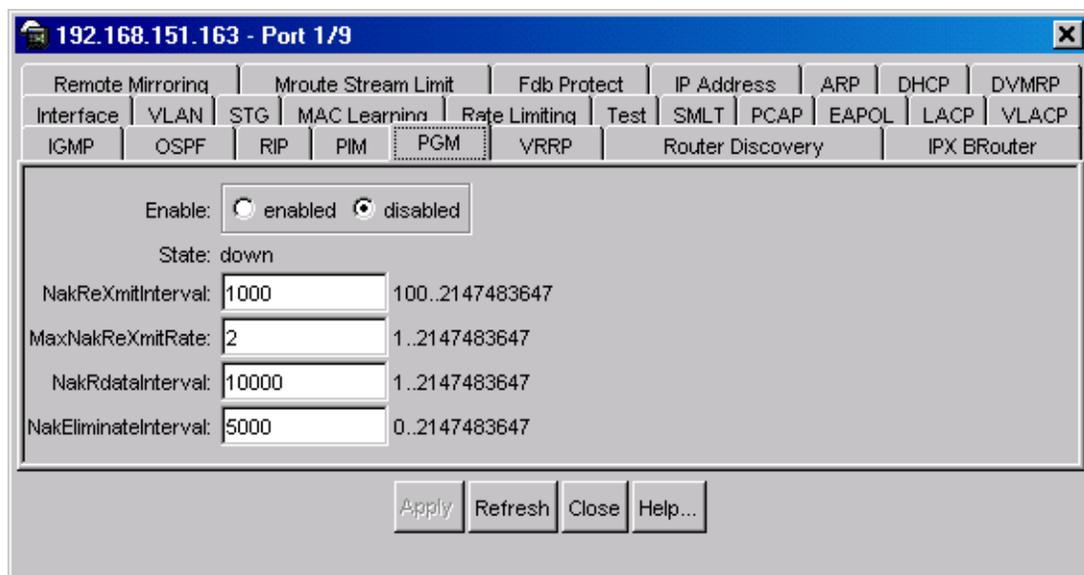
Field	Description
Enable	Enables or disables PGM globally.
State	Displays the current state (up or down) of PGM.
SessionLifeTime	Specifies the length of idle time (in seconds) after which a session times out. Idle time is when no SPMs are received from the upstream. The default is 300 seconds.
NnakGenerate	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 43](#) describes the PGM tab fields.

**Table 43** PGM port tab fields

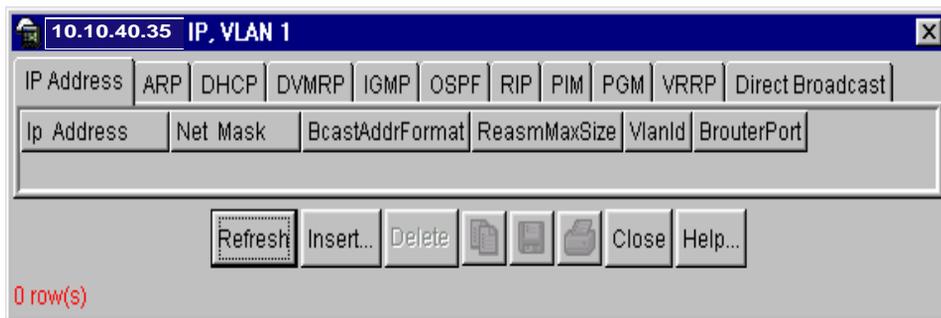
Field	Description
Enable	Enables or disables PGM on this interface.
State	Indicates the current state (up or down) of PGM.
NakReXmitInterval	Specifies how long to wait for an NCF (in milliseconds) before retransmitting the NAK. The default is 1000 milliseconds.
MaxNakReXmitRate	Configures the maximum 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

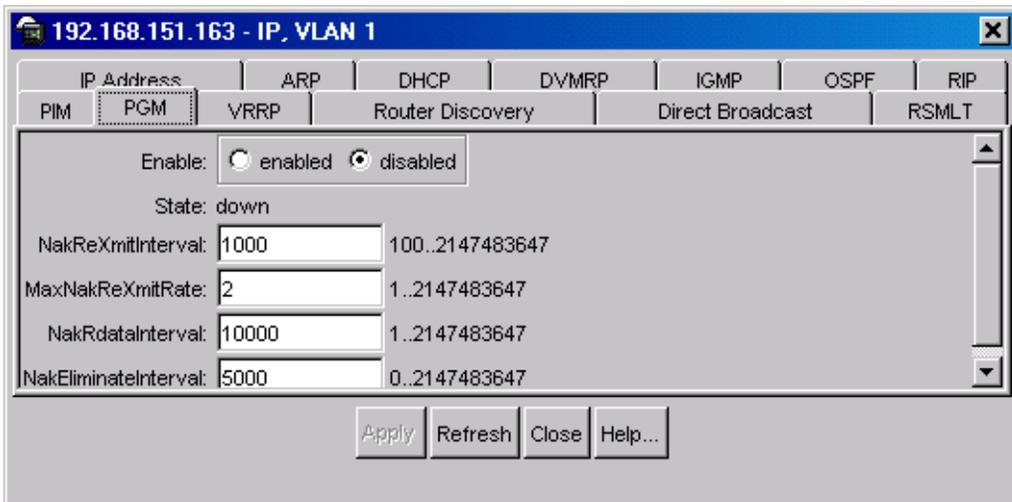
To enable PGM on a VLAN:

- 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 44 describes the PGM VLAN tab fields.

**Table 44** 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.

**Table 44** IP, VLAN dialog box—PGM 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.

## Viewing and editing PGM interface parameters

To view or edit PGM interface parameters:

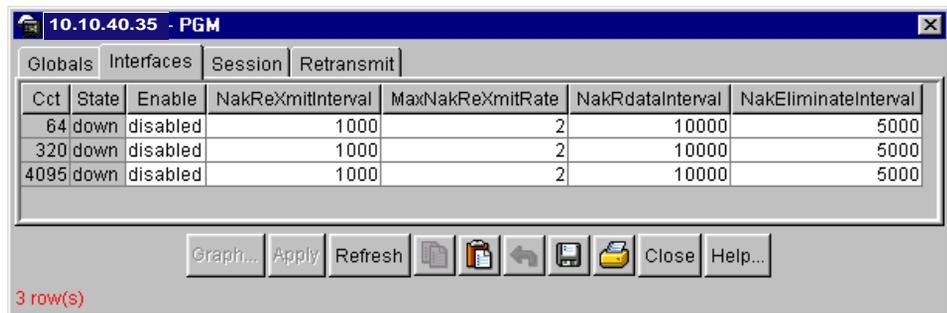
- 1 From the Device Manager menu bar, choose IP Routing > PGM.

The PGM dialog box opens with the Globals tab displayed ([Figure 78 on page 219](#)).

- 2 Click the Interfaces tab.

The Interfaces tab opens ([Figure 82](#)).

**Figure 82** PGM dialog box—Interfaces tab



[Table 45](#) describes the PGM Interfaces tab fields.

**Table 45** 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 45** 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 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 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

	Absolute Value	Cumulative	Average/sec	Minimum/sec	Maximum/sec	LastVal/sec
TotalReXmitStates	0	0	0	0	0	0
TotalReXmitTimedOut	0	0	0	0	0	0
InSpms	0	0	0	0	0	0
OutSpms	0	0	0	0	0	0
InParitySpms	0	0	0	0	0	0
OutParitySpms	0	0	0	0	0	0
InSpmPortErrors	0	0	0	0	0	0
InRdata	0	0	0	0	0	0
OutRdata	0	0	0	0	0	0
InParityRdata	0	0	0	0	0	0
OutParityRdata	0	0	0	0	0	0
InRdataPortErrors	0	0	0	0	0	0
InRdataNoSessionErrors	0	0	0	0	0	0

Table 46 describes the interface Spms/Rdata tab fields.

**Table 46** 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 46** 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](#)).

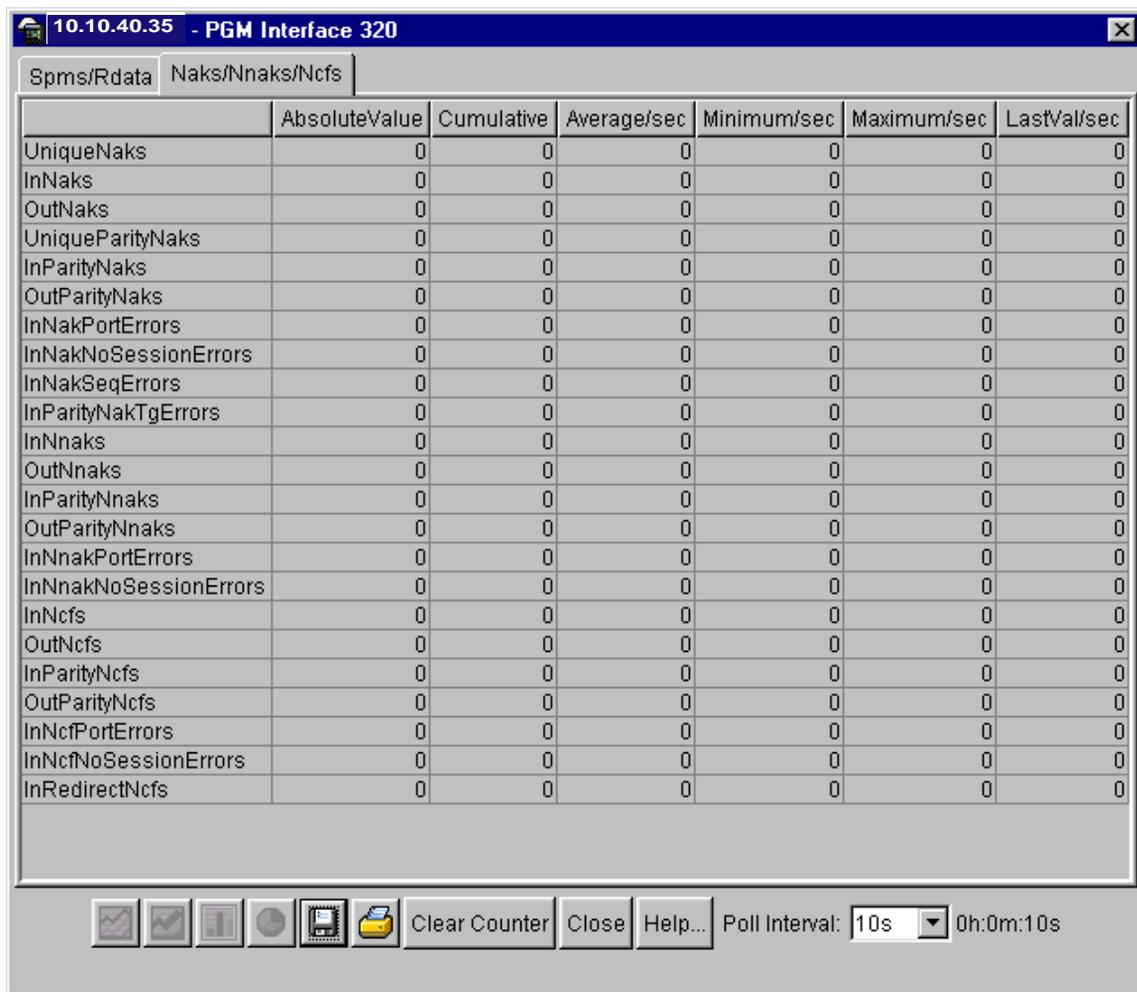
**Figure 84** PGM Interface Graph dialog box—Naks/Nnaks/Ncfs tab

Table 47 describes the interface Naks/Nnaks/Ncfs tab fields.

**Table 47** 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 47** 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

Source	Group	SourcePort	GlobalId	UpstreamAddress	UpstreamIfCct	TrailEdgeSeq	LeadEdgeSeq
155.120.50.201	224.241.241.241	19	9b:78:32:c9:00:00	155.120.50.201	VLAN-50	0	53
155.120.50.201	224.242.242.242	20	9b:78:32:c9:00:00	155.120.50.201	VLAN-50	0	22

2 row(s)

Table 48 describes the PGM Session tab fields.

**Table 48** 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 237



**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

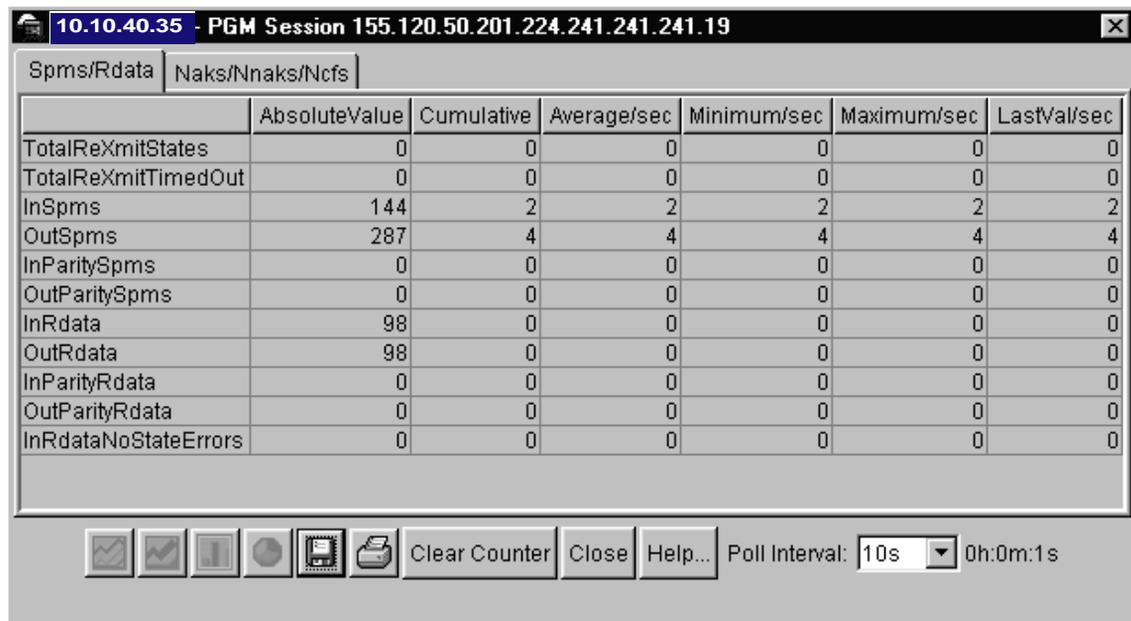


Table 49 describes the session Spms/Rdata tab fields.

**Table 49** Session Spms/Rdata tab fields

<b>Field</b>	<b>Description</b>
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

	AbsoluteValue	Cumulative	Average/sec	Minimum/sec	Maximum/sec	LastVal/sec
UniqueNaks	0	0	0	0	0	0
InNaks	48	0	0	0	0	0
OutNaks	40	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
InNakSeqErrors	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
InNcfs	14	0	0	0	0	0
OutNcfs	48	0	0	0	0	0
InParityNcfs	0	0	0	0	0	0
OutParityNcfs	0	0	0	0	0	0
InRedirectNcfs	0	0	0	0	0	0

Table 50 describes the session Naks/Nnaks/Ncfs tab fields.

**Table 50** 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 50** Session Naks/Nnaks/Ncfs tab fields (continued)

<b>Field</b>	<b>Description</b>
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 51 describes the PGM Retransmit tab fields.

**Table 51** 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:

Topic	Page
<a href="#">Viewing multicast route information</a>	244
<a href="#">Viewing multicast next hop information</a>	245
<a href="#">Viewing and editing multicast interface information</a>	247
<a href="#">Configuring multicast static source groups</a>	248
<a href="#">Troubleshooting DVMRP</a>	253
<a href="#">Configuring IP multicast software forwarding</a>	258

## 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

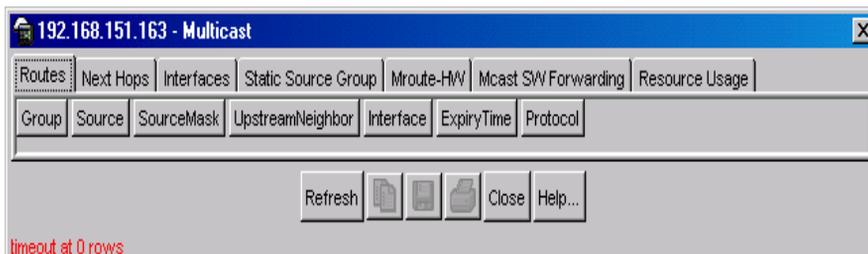


Table 52 describes the Routes tab fields.

**Table 52** 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 52** 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 53 describes the Next Hops tab fields.

**Table 53** 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.

**Table 53** Next Hops tab fields

Field	Description
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

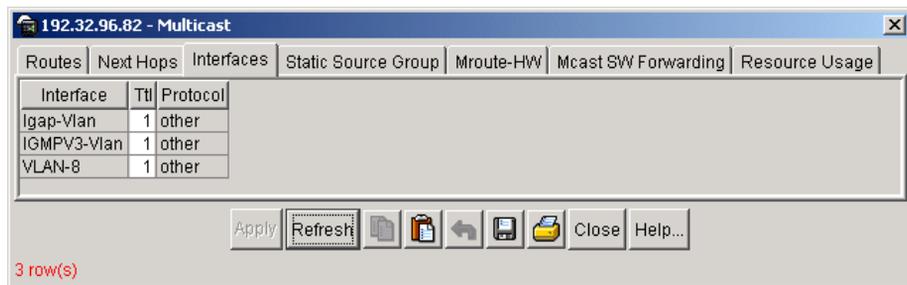


Table 54 describes the Interfaces tab fields.

**Table 54** 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 141.](#)
- PIM Sparse Mode (SM) - To globally enable PIM-SM, refer to [“Enabling PIM-SM globally” on page 190.](#)
- PIM source specific multicast mode (SSM) - To globally enable PIM-SSM, refer to [“Enabling Source Specific Multicast \(SSM\) globally” on page 212.](#)

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 126](#).

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

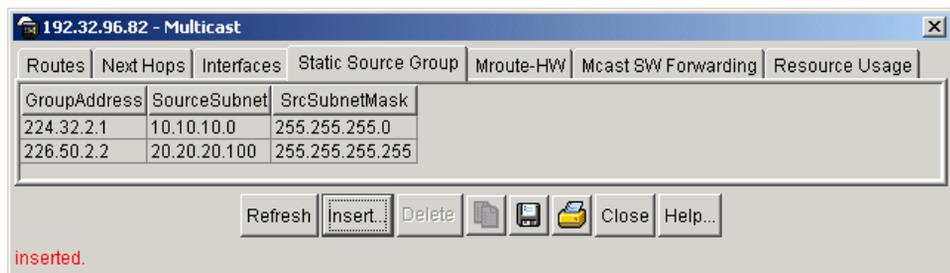


Table 55 describes the Static Source Group tab fields.

**Table 55** 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 <a href="#">“Configuration considerations.”</a>
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.

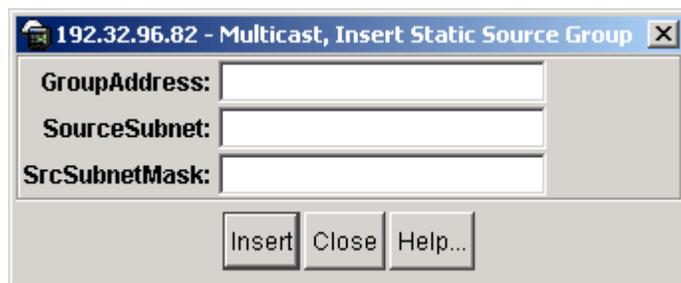
- 2 Click the Static Source Group tab.

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.

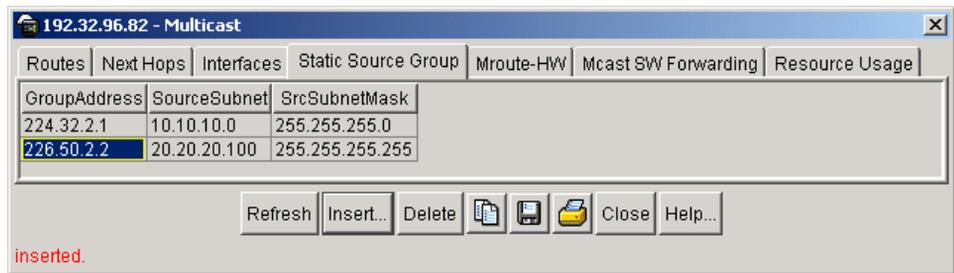


**Note:** To avoid conflicts between the static source group table and the SSM channel table, refer to [“Configuration considerations”](#) before filling out the fields in this dialog box.

## 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 Vlan 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

GroupAddress	Subnet	Invlan	Pruned
224.2.128.119	200.2.10.0	1016	true
224.2.128.119	200.1.10.0	2050	false
224.2.223.173	155.120.59.0	1020	true
224.25.25.25	155.120.51.0	1016	true
224.2.228.209	155.120.52.0	1020	false
224.2.215.39	200.1.10.0	2050	false
237.120.5.4	155.120.50.0	1020	false
224.2.128.119	155.120.60.0	2	false
224.2.157.11	155.120.59.0	1020	true
224.2.128.119	155.120.50.0	1020	false
224.2.206.61	200.1.10.0	2050	false
224.2.128.119	155.120.51.0	1016	true
224.2.215.39	155.120.59.0	1020	false
224.2.206.61	155.120.50.0	1020	false
224.2.228.209	155.120.58.0	1024	false
224.2.215.39	155.120.50.0	1020	false
224.2.215.39	155.120.61.0	1020	false
237.120.5.5	155.120.50.0	1020	false
224.2.228.209	200.2.10.0	1016	true
224.2.228.209	155.120.60.0	2	false

Table 56 describes the fields that appear on the Multicast dialog Mroute-HW tab.

**Table 56** 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. <b>Note:</b> 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

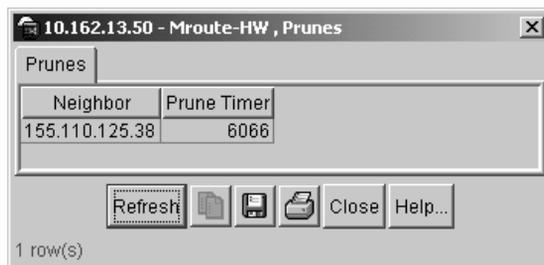


Table 57 describes the fields in the Prunes tab.

**Table 57** 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

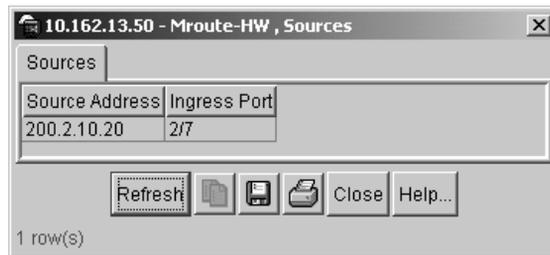


Table 58 describes the fields in the Sources tab.

**Table 58** 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

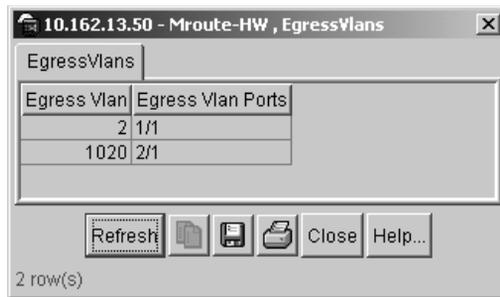


Table 59 describes the Egress VLANs tab fields.

**Table 59** 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.

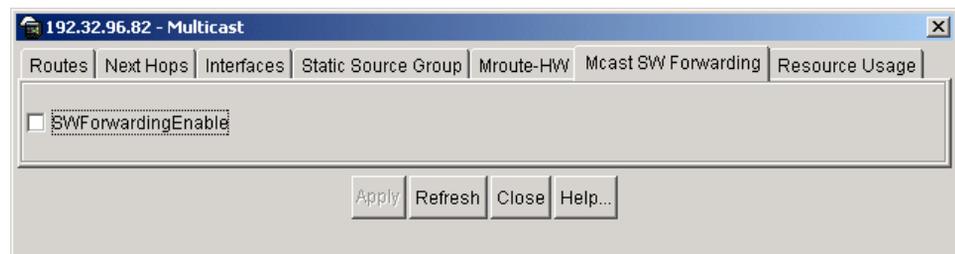


**Note:** To avoid overloading the CPU, Nortel Networks recommends that you do not use the IP multicast software forwarding feature for video multicast applications.

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](#)).

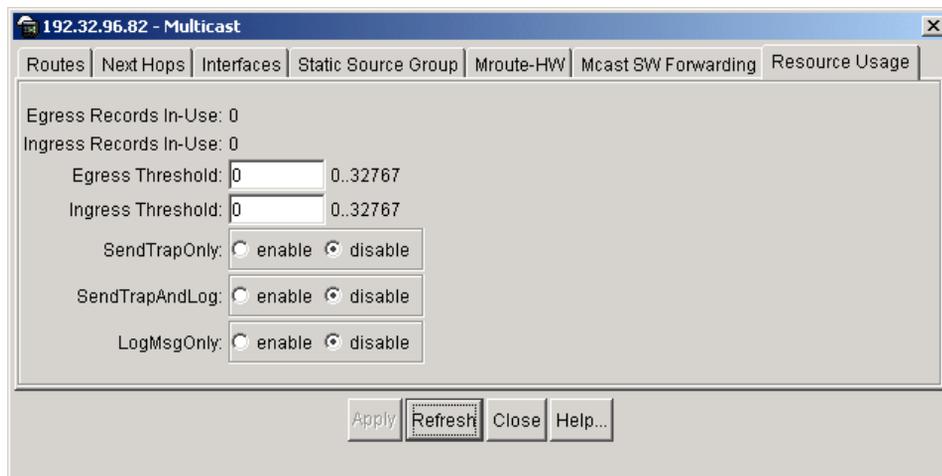
**Figure 100** Multicast Dialog box—Records Usage tab

Table 60 describes the fields in the Resource Usage tab.

**Table 60** 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. <sup>1</sup>
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.

<sup>1</sup> 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:

Topic	Page
<a href="#">Enabling multicast flow distribution globally</a>	262
<a href="#">Enabling multicast flow distribution per MLT</a>	265

## 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 tab

192.168.151.163 - Chassis

1 2 3 Redundancy | Mcast MLT Distribution | Record Reservation | DNS Host | DNS Server

System | Chassis | Boot Config | Trap Sender table | Performance | User Set Time

sysDescr: 0  
 sysUpTime: 0  
 sysContact: abc  
 sysName: A  
 sysLocation: 198.202.189.232  
 VirtualIpAddr:   
 VirtualNetMask:   
 DnsDomainName:

AuthenticationTraps  
 EnableWebServer  
 EnableAccessPolicy  
 MrouteStrLimit

LastChange: 0  
 LastVlanChange: 0  
 LastStatisticsReset: 0  
 LastRunTimeConfigSave: 0  
 LastRunTimeConfigSaveToSlave: 0  
 LastBootConfigSave: 0  
 LastBootConfigSaveOnSlave: 0

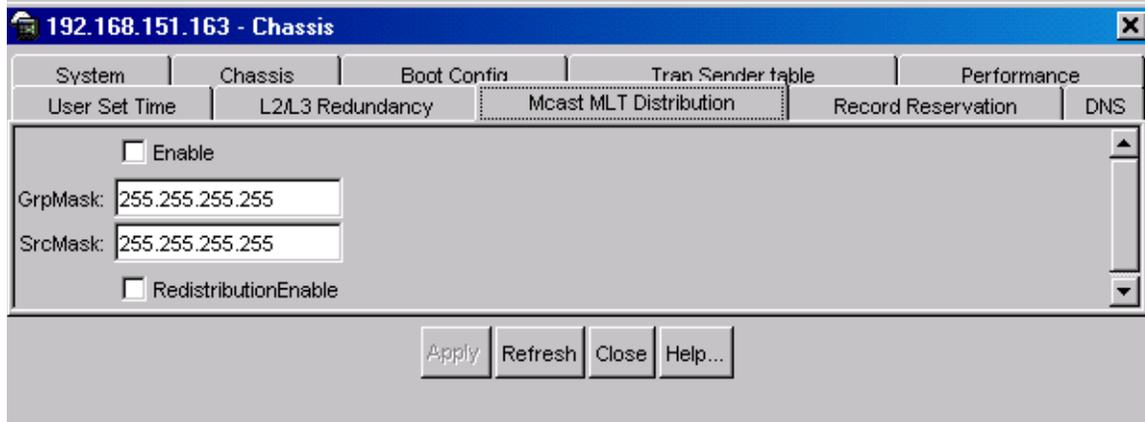
DefaultRuntimeConfigFileName: 0  
 DefaultBootConfigFileName: 0  
 ConfigFileName: Multi.doc

Action:

hardReset       softReset       resetCounters  
 cpuSwitchOver       resetConsole       resetModem  
 saveRuntimeConfig       saveRuntimeConfigToSlave       saveBootCon  
 saveSlaveBootConfig       reset1stStatCounters

2 Click the Mcast MLT Distribution tab.

The Mcast MLT LACP 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 61](#) describes the Mcast MLT Distribution tab fields.

**Table 61** Mcast MLT Distribution tab fields

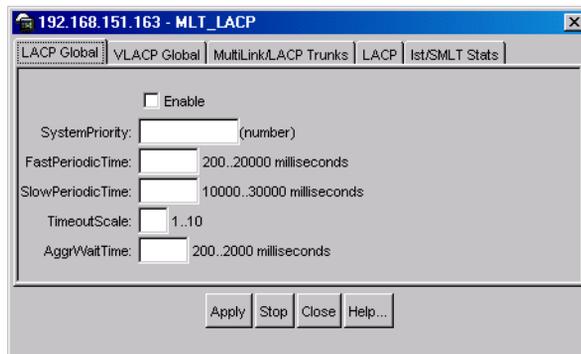
Field	Description
Enable	A check box that allows you to globally enable multicast flow distribution. The default is disabled.
GrpMask	A group mask to use when distributing multicast traffic over an MLT. The default is 255.255.255.255.
SrcMask	A source mask to use when distributing multicast traffic over 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:

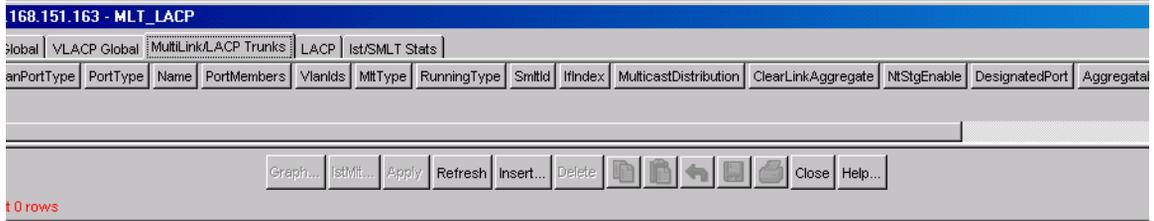
- 1 From the Device Manager menu bar, choose VLAN > MLT/LACP.

The MLT\_LACP dialog box opens with the LACP Globals tab displayed (Figure 103).

**Figure 103** MLT dialog box

- 2 Click on MultiLink/LACP Trunk tab.
- 3 Click Insert.

The MLT, Insert MultiLink Trunks dialog box opens (Figure 104).

**Figure 104** MLT\_LACP Insert Multilink/LACP dialog box

- 4 Type the ID number for the MultiLink Trunk.
- 5 Select a stacked VLAN port type.
- 6 Select Port Type.
- 7 Type a name for the MultiLink Trunk port.
- 8 Select the ports to belong to the SMLT port.
- 9 Select the VLAN IDs to belong to the MultiLink Trunk port.
- 10 Select the MltType.
- 11 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.
- 12 Select enable to activate multicast flow distribution.
- 13 Click Insert.

The MLT dialog box is updated as shown in [\(Figure 105\)](#).

**Figure 105** Updated MLT dialog box

Table 62 describes the MultiLink Trunks tab fields.

**Table 62** 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: <ul style="list-style-type: none"> <li>• normalMLT</li> <li>• istMLT</li> <li>• splitMLT</li> </ul>
SmltId	The split MLT ID.
MulticastDistribution	Enable or disable multicast flow distribution.
ClearLinkAggregate	The clear aggregate.
NtStgEnable	Enabling Stg factors.
DesignatedPorts	Designated Ports.
Aggregatable	Belonging to an aggregate.
IfIndex	Interface index.
AggOperState	The state of operational aggregate.
AggregTimeOfLastOperChange	The aggregate time involved of the last operation.



---

## 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:

Topic	Page
<a href="#">Configuring Layer 2 multicast MAC filtering</a>	270
<a href="#">Configuring Layer 3 multicast MAC filtering</a>	272

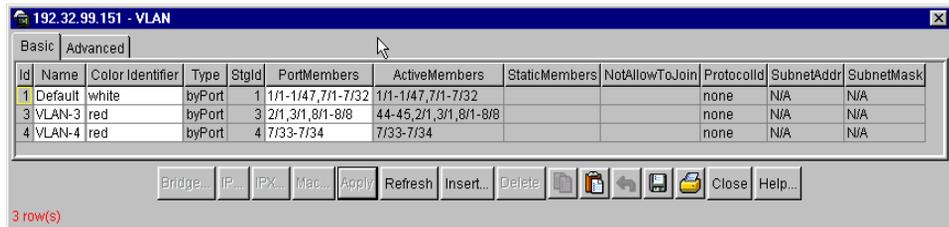
## Configuring Layer 2 multicast MAC filtering

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.

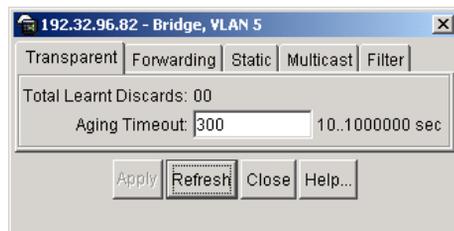
**Figure 106** VLAN dialog box—Basic tab



- 2 From the table, select a VLAN.
- 3 Click the Bridge button.

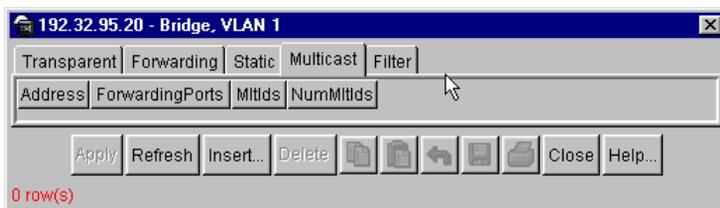
The Bridge dialog box opens with the Transparent tab displayed (Figure 107).

**Figure 107** Bridge, VLAN dialog box—Transparent tab



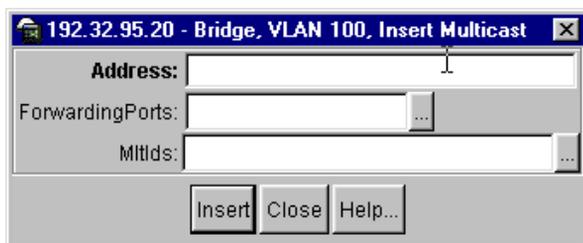
- 4 Click the Multicast tab.

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 63 describes the Bridge, VLAN, Insert Multicast fields.

**Table 63** Bridge, VLAN, Insert Multicast fields

Item	Description
Address	The MAC address for the multicast flooding domain. <sup>1</sup>
ForwardingPorts	The ports to be included in the multicast flooding domain.
MltIds	The MLTs that should be included in the multicast flooding domain.

<sup>1</sup> 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`

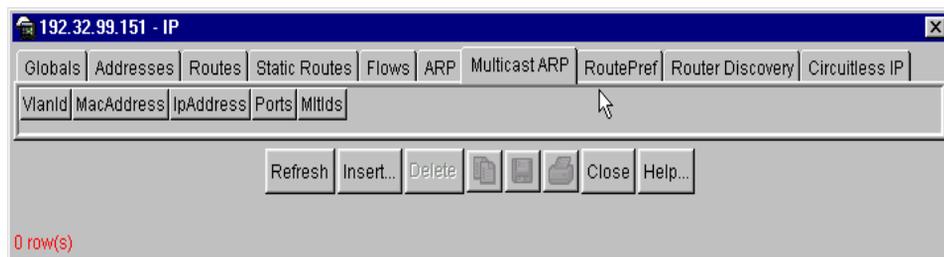
## Configuring Layer 3 multicast MAC filtering

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:

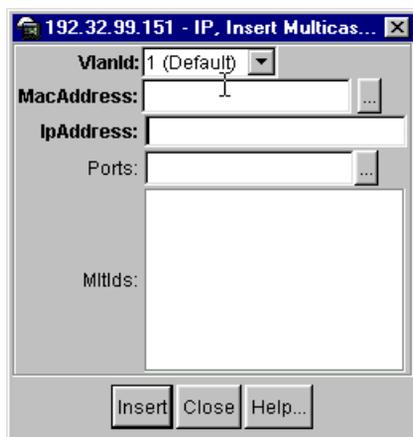
- 1 From the Device Manager menu bar, choose IP Routing > IP > Multicast ARP.

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 64](#) describes the Multicast ARP fields.

**Table 64** 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. <sup>1</sup>
IPAddress	The IP address of the multicast ARP.

**Table 64** 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:

Topic	Page
<a href="#">Roadmap of IGMP commands</a>	277
<a href="#">Configuration prerequisites and notes</a>	278
<a href="#">Configuring IGMP on an interface</a>	285
<a href="#">Configuring fast leave mode and enabling trap/logs</a>	293
<a href="#">Configuring multicast access control for an IGMP interface</a>	296
<a href="#">Configuring IGMP multicast router discovery options</a>	300
<a href="#">Configuring IGMP interface static members</a>	303
<a href="#">Configuring SSM dynamic learning and range group</a>	306
<a href="#">Configuring the SSM channel table</a>	309
<a href="#">Configuring IGMP Ethernet ports</a>	313
<a href="#">Configuring multicast access control for an IGMP Ethernet port</a>	317
<a href="#">Configuring IGMP on a VLAN</a>	320
<a href="#">Configuring multicast access control for a VLAN</a>	325
<a href="#">Configuring IGMP multicast router discovery on a VLAN</a>	328
<a href="#">Configuring IGMP static members on a VLAN</a>	329

<b>Topic</b>	<b>Page</b>
<a href="#">Configuring IGMP fast-leave members on a VLAN</a>	331
<a href="#">Configuring multicast stream limitation</a>	332
<a href="#">Configuring multicast stream limitation members on an interface</a>	334
<a href="#">Configuring multicast stream limitation on an Ethernet port</a>	337
<a href="#">Configuring multicast stream limitation on a VLAN</a>	338
<a href="#">Configuring multicast stream limitation members on a VLAN</a>	339
<a href="#">Displaying all IP IGMP show commands</a>	342

## 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 342](#).



**Note:** 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:

## Configuration prerequisites and notes

Command	Parameter
<code>config ip igmp interface &lt;ipaddr&gt;</code>	<code>info</code> <code>flush &lt;mrouter sender  grp-member&gt;</code> <code>[&lt;SenderAddress&gt;] [&lt;GroupAddress&gt;]</code> <code>last-memb-query-int &lt;1/10 seconds&gt;</code> <code>query-interval &lt;seconds&gt;</code> <code>query-max-resp &lt;1/10 seconds&gt;</code> <code>robustval &lt;integer&gt;</code> <code>router-alert &lt;enable disable&gt;</code> <code>proxy-snoop &lt;enable disable&gt;</code> <code>snoop &lt;enable disable&gt;</code> <code>fast-leave &lt;enable disable&gt;</code> <code>ssm-snoop &lt;enable disable&gt;</code> <code>version &lt;integer&gt;</code>
<code>show ip igmp interface</code>	
<code>show ip igmp cache</code>	
<code>show ip igmp group</code>	
<code>show ip igmp router-alert</code>	
<code>show ip igmp sender</code>	
<code>show ip igmp snoop</code>	
<code>config ip igmp fast-leave-mode</code>	<code>multiple-user</code> <code>one-user</code>
<code>config ip igmp generate-trap</code>	<code>generate-trap &lt;enable disable&gt;</code>
<code>config ip igmp generate-log</code>	<code>generate-log &lt;enable disable&gt;</code>

Command	Parameter
<code>show ip igmp info</code>	
<code>config ip igmp interface &lt;ipaddr&gt; access-control &lt;name&gt;</code>	<p>info</p> <p>delete &lt;HostAddress&gt; &lt;HostMask&gt;</p> <p>create &lt;HostAddress&gt; &lt;HostMask&gt; {deny-tx deny-rx deny-both allow-only-tx allow-only-rx allow-only-both}</p> <p>mode &lt;HostAddress&gt; &lt;HostMask&gt; {deny-tx deny-rx deny-both allow-only-tx allow-only-rx allow-only-both}</p>
<code>show ip igmp access</code>	
<code>config ip igmp interface &lt;ipaddr&gt; mrdisc</code>	<p>info</p> <p>mrdisc-enable &lt;enable disable&gt;</p> <p>max-advertisement-interval [seconds]</p> <p>max-initial-advertisements [integer]</p> <p>max-initial advertisement-interval [seconds]</p> <p>min-advertisement-interval [seconds]</p> <p>neighbor-dead-interval [seconds]</p>
<code>show ip igmp mrdisc</code>	
<code>show ip igmp mrdisc-neighbors</code>	
<code>config ip igmp interface &lt;ipaddr&gt; static-members &lt;GroupAddress&gt;</code>	<p>info</p> <p>add &lt;ports&gt; &lt;static blocked&gt;</p> <p>create &lt;ports&gt; &lt;static blocked&gt;</p> <p>delete</p>

Command	Parameter
<code>show ip igmp static</code>	<code>remove &lt;ports&gt; &lt;static blocked&gt;</code>
<code>config ip igmp ssm</code>	<code>info</code> <code>dynamic-learning &lt;enable disable&gt;</code> <code>ssm-grp-range group &lt;GroupAddress&gt;</code> <code>mask &lt;mask&gt;</code>
<code>show ip igmp ssm-global</code>	
<code>config ip igmp ssm ssm-channel</code>	<code>info</code> <code>create group &lt;GroupAddress&gt; source &lt;SourceAddress&gt;</code> <code>delete group &lt;GroupAddress&gt;</code> <code>disable &lt;all group&gt; [&lt;GroupAddress&gt;]</code> <code>enable &lt;all group&gt; [&lt;GroupAddress&gt;]</code>
<code>show ip igmp ssm-channel</code>	
<code>config ethernet &lt;ports&gt; ip igmp</code>	<code>info</code> <code>flush &lt;mrouter sender  grp-member&gt; [&lt;SenderAddress&gt;] [&lt;GroupAddress&gt;]</code> <code>last-memb-query-int &lt;1/10 seconds&gt;</code> <code>query-interval &lt;seconds&gt;</code> <code>fast-leave &lt;enable disable&gt;</code> <code>query-max-resp &lt;1/10 seconds&gt;</code> <code>robustval &lt;integer&gt;</code> <code>router-alert &lt;enable disable&gt;</code> <code>version &lt;integer&gt;</code>
<code>show ports info igmp [&lt;ports&gt;]</code>	
<code>config ethernet &lt;ports&gt; ip igmp access-control &lt;name&gt;</code>	<code>info</code> <code>create &lt;HostAddress&gt; &lt;HostMask&gt; {deny-tx deny-rx deny-both allow-only-tx allow-only-rx allow-only-both}</code> <code>delete &lt;HostAddress&gt; &lt;HostMask&gt;</code>

Command	Parameter
	<pre>mode &lt;HostAddress&gt; &lt;HostMask&gt; {deny-tx deny-rx deny-both allow-on ly-tx allow-only-rx allow-only-both }</pre>
<pre>config vlan &lt;vid&gt; ip igmp</pre>	<pre>info del-mrouter &lt;ports&gt; flush &lt;mrouter sender  grp-member&gt; [&lt;SenderAddress&gt;] [&lt;GroupAddress&gt;] last-memb-query-int &lt;1/10 seconds&gt; mrouter &lt;ports&gt; query-interval &lt;seconds&gt; query-max-resp &lt;1/10 seconds&gt; robustval &lt;integer&gt; router-alert &lt;enable disable&gt; proxy-snoop &lt;enable disable&gt; snoop &lt;enable disable&gt; fast-leave &lt;enable disable&gt; ssm-snoop &lt;enable disable&gt; version &lt;integer&gt;</pre>
<pre>show vlan info igmp [&lt;vid&gt;]</pre>	
<pre>config vlan &lt;vid&gt; ip igmp access-control &lt;name&gt;</pre>	<pre>info create &lt;HostAddress&gt; &lt;HostMask&gt; {deny-tx deny-rx deny-both allow-on ly-tx allow-only-rx allow-only-both } delete &lt;HostAddress&gt; &lt;HostMask&gt; mode &lt;HostAddress&gt; &lt;HostMask&gt; {deny-tx deny-rx deny-both allow-on ly-tx allow-only-rx allow-only-both }</pre>

Command	Parameter
<code>config vlan &lt;vid&gt; ip igmp mrdisc</code>	<code>info</code> <code>mrdisc-enable &lt;enable disable&gt;</code> <code>max-advertisement- interval</code> <code>&lt;seconds&gt;</code> <code>max-initial- advertisements</code> <code>&lt;integer&gt;</code> <code>max-initial- advertisement-interval</code> <code>&lt;seconds&gt;</code> <code>min-advertisement- interval</code> <code>&lt;seconds&gt;</code> <code>neighbor-dead-interval &lt;seconds&gt;</code>
<code>config vlan &lt;vid&gt; ip igmp</code> <code>static-members</code> <code>&lt;FromGroupAddress-ToGroupAddress&gt;</code>	<code>info</code> <code>add &lt;ports&gt; &lt;static blocked&gt;</code> <code>create &lt;ports&gt; &lt;static blocked&gt;</code> <code>delete</code> <code>remove &lt;ports&gt; &lt;static blocked&gt;</code>
<code>config vlan &lt;vid&gt; ip igmp</code> <code>fast-leave-members</code>	<code>info</code> <code>enable &lt;ports&gt;</code> <code>disable &lt;ports&gt;</code>
<code>config ip igmp interface &lt;ipaddr&gt;</code> <code>stream-limit</code>	<code>info</code> <code>enable</code> <code>disable</code> <code>max-streams &lt;integer&gt;</code>

Command	Parameter
<code>config ip igmp interface &lt;ipaddr&gt; stream-limit-members</code>	<code>info</code> <code>enable &lt;ports&gt; max-streams &lt;value&gt;</code> <code>disable &lt;ports&gt;</code> <code>set &lt;ports&gt; max-streams &lt;value&gt;</code>
<code>show ip igmp stream-limit-interface</code> <code>show ip igmp stream-limit-port</code>	
<code>config ethernet &lt;ports&gt; ip igmp stream-limit</code>	<code>info</code> <code>enable</code> <code>disable</code> <code>max-streams &lt;integer&gt;</code>
<code>config vlan &lt;vid&gt; ip igmp stream-limit</code>	<code>info</code> <code>enable</code> <code>disable</code> <code>max-streams &lt;integer&gt;</code>
<code>config vlan &lt;vid&gt; ip igmp stream-limit-members</code>	<code>info</code> <code>enable &lt;ports&gt; max-streams &lt;value&gt;</code> <code>disable &lt;ports&gt;</code> <code>set &lt;ports&gt; max-streams &lt;value&gt;</code>
<code>show ip igmp show-all [file &lt;value&gt;]</code>	

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:

<b>config ip igmp interface</b> <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>	<p>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.</p> <p>Decreasing the value reduces the time to detect the loss of the last member of a group.</p> <ul style="list-style-type: none"> <li><i>seconds</i> 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).</li> </ul>
query-interval <seconds>	<p>Sets the frequency (in seconds) at which host query packets are transmitted on the interface.</p> <ul style="list-style-type: none"> <li><i>seconds</i> is the range from 1 to 65535 with a default of 125.</li> </ul>
generate-trap <enable disable>	<p>Enabling this command on this switch will trigger trap for the following IGMP events:</p> <ul style="list-style-type: none"> <li>New IGMP membership for a group</li> <li>IGMP membership removed for a group</li> <li>When a querier is changed or new querier comes up on a particular interface.</li> </ul>

<b>config ip igmp interface &lt;ipaddr&gt;</b> followed by:	
<code>generate-log &lt;enable   disable&gt;</code>	Enabling this command on this switch will cause the following IGMP events to be logged: <ul style="list-style-type: none"> <li>• New IGMP membership for a group</li> <li>• IGMP membership removed for a group</li> <li>• When a querier is changed or new querier comes up on a particular interface.</li> </ul>
<code>query-max-resp &lt;1/10 seconds&gt;</code>	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. <ul style="list-style-type: none"> <li>• <i>integer</i> is an integer value with a range of 0 to 255, and the default is 100 tenth seconds (equal to 10 seconds).</li> </ul> <p><b>Note:</b> This value must be less than the query-interval.</p>
<code>robustval &lt;integer&gt;</code>	Allows tuning for the expected packet loss of a network. <i>integer</i> 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.
<code>router-alert &lt;enable   disable&gt;</code>	Enables or disables the router alert option. When enabled, this parameter instructs the router to process packets not directly addressed to it. <b>Note:</b> To maximize your network performance, Nortel Networks recommends that you set this parameter according to the version of IGMP currently in use. <ul style="list-style-type: none"> <li>• IGMPv1 - Disable</li> <li>• IGMPv2 - Enable</li> <li>• IGMPv3 - Enable</li> </ul>
<code>proxy-snoop &lt;enable   disable&gt;</code>	Enables or disables the layer-3 proxy-snoop option.
<code>snoop &lt;enable   disable&gt;</code>	Enables or disables the layer-3 snoop option.
<code>fast-leave &lt;enable   disable&gt;</code>	Enables or disables the fast-leave option on the interface.

<b>config ip igmp interface &lt;ipaddr&gt;</b>	
followed by:	
<code>ssm-snoop</code> <code>&lt;enable   disable&gt;</code>	Enables or disables support for PIM source-specific multicast (SSM) on the snooping interface.
<code>version &lt;integer&gt;</code>	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. <ul style="list-style-type: none"> <li><code>integer</code> is an integer value with a value of 1, 2 or 3. The default value is 2 (IGMPv2).</li> </ul>

### *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  MAXRSPT  QUERY  JOINS  ROBUST  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      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

```
PP8600:5# show ip igmp cache
=====
                                Igmp Cache
=====
GRPADDR  INTERFACE  LASTREPORTER  EXPIRATION  V1HOSTTIMER  STATICPORTS  TYPE
-----
224.1.1.1 Vlan2      0.0.0.0       0           0             1/15         STATIC
224.1.1.2 Vlan2      0.0.0.0       0           0             1/15         STATIC
```

## 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

```
PP8600:5# show ip ig static
=====
                                Igmp Static
=====
GRPADDR  TO-GRPADDR  INTERFACE  STATICPORTS  BLOCKEDPORTS
-----
230.1.1.1 230.1.1.50  Vlan2     1/15
224.1.1.1 224.1.1.100 Vlan2     1/15
```

## 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   ENABLE PORTS   PORTS    TIME
-----
V3       false  false  false
V4       false  false  false
V8       false  false  false
=====

```

## Configuring fast leave mode and enabling trap/logs

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:

<b>config ip igmp fast-leave-mode</b>	
followed by:	
multiple-user	Removes from the group <i>only</i> 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.

To enable the switch to trap IGMP events, use the following command:

```
config ip igmp generate-trap
```

This command includes the following parameters:

<b>config ip igmp generate-trap</b> followed by:	
enable	Enabling this command on this switch will trigger trap for the following IGMP events: <ul style="list-style-type: none"><li>• New IGMP membership for a group</li><li>• IGMP membership removed for a group</li><li>• When a querier is changed or new querier comes up on a particular interface</li></ul>
disable	The switch will not send any IGMP trap events.

To enable the switch to log IGMP events, use the following command:

```
config ip igmp generate-log
```

This command includes the following parameters:

<b>config ip igmp generate-log</b> followed by:	
enable	Enabling this command on this switch will cause the following IGMP events to be logged: <ul style="list-style-type: none"><li>• New IGMP membership for a group</li><li>• IGMP membership removed for a group</li><li>• When a querier is changed or new querier comes up on a particular interface</li></ul>
disable	The switch will not log any IGMP events.

### 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

```
PP8600:5# conf ip igmp info

Sub-Context: clear config dump monitor show test trace wsm asfm
sam
Current Context:

fast-leave-mode : multiple-users
generate-trap : disable
generate-log : disable
```

## 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:

<b>config ip igmp interface &lt;ipaddr&gt; access-control &lt;name&gt;</b> 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. <ul style="list-style-type: none"> <li>• <i>HostAddress</i> is the IP address of the host. See <a href="#">“Specifying host addresses and masks”</a> for more information.</li> <li>• <i>HostMask</i> 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 <a href="#">“Specifying host addresses and masks”</a> for more information.</li> <li>• 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.</li> </ul>

<pre>config ip igmp interface &lt;ipaddr&gt; access-control &lt;name&gt;</pre> <p>followed by:</p>	
<pre>delete &lt;HostAddress&gt; &lt;HostMask&gt;</pre>	<p>Deletes the access control group entry for the specified IGMP interface.</p> <ul style="list-style-type: none"> <li>• <i>HostAddress</i> is the IP address of the host.</li> <li>• <i>HostMask</i> is the subnet mask used to determine the host or hosts covered by this configuration.</li> </ul>
<pre>mode &lt;HostAddress&gt; &lt;HostMask&gt; {deny-tx deny-rx deny-both  allow-only-tx allow-only- rx allow-only-both}</pre>	<p>Changes the access control group configuration.</p> <ul style="list-style-type: none"> <li>• <i>HostAddress</i> is the IP address of the host.</li> <li>• <i>HostMask</i> is the subnet mask used to determine the host or hosts covered by this configuration.</li> <li>• <i>deny-tx deny-rx deny-both allow-only-tx allow-only-rx allow-only-both</i> indicates the action you want for the specified IGMP interface. For example, if you specify <i>deny-both</i>, the interface will deny both transmitted and received traffic.</li> </ul>

### *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 65 shows the field descriptions for the `show ip igmp access` command.

**Table 65** 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 <a href="#">“Specifying host addresses and masks”</a> for more information.

**Table 65** 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 <a href="#">"Specifying host addresses and masks"</a> for more information.
ACCESSMODE	Specifies the action of the access policy. The options are: <ul style="list-style-type: none"> <li>deny-tx – deny IP multicast transmitted traffic.</li> <li>deny-rx – deny IP multicast received traffic.</li> <li>deny-both – deny both IP multicast transmitted and received traffic.</li> <li>allow-only-rx – allow IP multicast transmitted traffic.</li> <li>allow-only-rx – allow IP multicast received traffic.</li> <li>allow-only-both – allow both IP multicast transmitted and received traffic.</li> </ul>

## 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:

<b>config ip igmp interface &lt;ipaddr&gt; mrdisc</b> 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.

<pre>config ip igmp interface &lt;ipaddr&gt; mrdisc</pre> <p>followed by:</p>	
<pre>max-advertisement-interval [seconds]</pre>	<p>Sets the maximum number (in seconds) of multicast advertisements that can be configured on the switch.</p> <p><b>Note:</b> To take effect, save the configuration and reset the switch.</p>
<pre>max-initial-advertisements [integer]</pre>	<p>Used to set the maximum number of initial multicast advertisements that can be configured on the switch.</p> <p><b>Note:</b> To take effect, save the configuration and reset the switch.</p>
<pre>max-initial advertisement-interval [seconds]</pre>	<p>Used to set the maximum number (in seconds) of multicast advertisement intervals that can be configured on the switch.</p> <p><b>Note:</b> To take effect, save the configuration and reset the switch.</p>
<pre>min-advertisement-interval [seconds]</pre>	<p>Used to set the minimum number (in seconds) of multicast advertisements that can be configured on the switch.</p> <p><b>Note:</b> To take effect, save the configuration and reset the switch.</p>
<pre>neighbor-dead-interval [seconds]</pre>	<p>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.</p> <ul style="list-style-type: none"> <li>• <i>seconds</i> is a value from 1 to 59. The default is 30.</li> </ul>

## 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:

<b>config ip igmp interface &lt;ipaddr&gt; static-members &lt;GroupAddress&gt;</b> 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. <ul style="list-style-type: none"> <li>• <i>ports</i> is the port or list of ports to which you want to redirect the multicast stream for this multicast group.</li> <li>• <i>static blocked</i> sets the route to static or blocked.</li> </ul>
create <ports> <static blocked>	Creates static-members on the interface. <ul style="list-style-type: none"> <li>• <i>ports</i> is the port or list of ports to which you want to redirect the multicast stream for this multicast group.</li> <li>• <i>static blocked</i> sets the route to static or blocked.</li> </ul>
delete	Deletes the static-members on the interface.
remove <ports> <static blocked>	Removes slots/ports from the static-members of a protocol-based VLAN. <ul style="list-style-type: none"> <li>• <i>ports</i> the port or list of ports you want to remove from the multicast stream.</li> <li>• <i>static blocked</i> sets the multicast entry to static or blocked.</li> </ul>
<Grp_addr1>-<grp_addr2>	To configure a range of multicast groups for static joins.

### *Configuration Example*

The following configuration example uses the above command to:

- Create static member entry to the IGMP interface
- Add static member entry to the IGMP interface
- Delete static member entry to the IGMP interface
- Configure a range of multicast groups for static joins

After configuring the parameters, use the **info** command to show a summary of the results.

```
config ip igmp interface 5.1.5.136 static-members 236.0.0.1 create
1/1 static
```

```
config ip igmp interface 5.1.5.136 static-members
234.0.0.0-234.0.0.5 create 1/1 static
```

```
config ip igmp interface 5.1.5.136 static-members
234.0.0.0-234.0.0.5 add 1/2 static
```

```
config ip igmp interface 5.1.5.136 static-members
234.0.0.0-234.0.0.5 remove 1/2 static
```

### **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

```
=====
                                Icmp 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:

<b>config ip igmp ssm</b> 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 <a href="#">“Configuring the SSM channel table.”</a>
ssm-grp-range group <GroupAddress> mask <mask>	<p>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.</p> <p><b>Note:</b> Before changing this setting, see <a href="#">“Changing the SSM range group.”</a></p> <ul style="list-style-type: none"> <li>• <i>GroupAddress</i> 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.</li> <li>• <i>mask</i> is the IP address mask of the multicast group. The default is 255.0.0.0.</li> </ul>

### 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.

## Showing SSM group range and dynamic learning status

```
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#
```

To display the SSM group range and the status of dynamic learning, use the following command:

```
show ip igmp ssm-global
```

[Figure 123](#) 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 483](#).

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:

<b>config ip igmp ssm ssm-channel</b>	
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. <ul style="list-style-type: none"> <li>• <i>GroupAddress</i> is any IP multicast address within the SSM range defined by <code>ssm-grp-range group</code>.</li> <li>• <i>SourceAddress</i> is any IP host address that will be sending traffic to the group.</li> </ul>
delete group <GroupAddress>	Deletes the SSM channel table entry that you specify. <ul style="list-style-type: none"> <li>• <i>GroupAddress</i> is the IP multicast address of the table entry you want to delete.</li> </ul>

<b>config ip igmp ssm ssm-channel</b>	
followed by:	
<code>disable &lt;all group&gt; [&lt;GroupAddress&gt;]</code>	<p>Disables the admin state for all static entries in the SSM channel table (<i>all</i>) or for a specific entry (<i>group</i>). This setting does not affect the dynamically learned entries.</p> <p>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.</p> <ul style="list-style-type: none"> <li>• <i>all</i> refers to all the static entries in the SSM channel table.</li> <li>• <i>group</i> requires the <i>GroupAddress</i> of the entry you want to disable.</li> </ul>
<code>enable &lt;all group&gt; [&lt;GroupAddress&gt;]</code>	<p>Enables the admin state for all static entries in the SSM channel table (<i>all</i>) or for a specific entry (<i>group</i>). This setting does not affect the dynamically learned entries.</p> <p>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.</p> <ul style="list-style-type: none"> <li>• <i>all</i> refers to all the static entries in the SSM channel table.</li> <li>• <i>group</i> requires the <i>GroupAddress</i> of the entry you want to disable.</li> </ul>

### 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 124](#) 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

<b>config ethernet &lt;ports&gt; ip igmp</b> 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. <ul style="list-style-type: none"> <li><i>seconds</i> 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).</li> </ul>
query-interval <seconds>	Sets the frequency (in seconds) at which host query packets are transmitted on the port. <ul style="list-style-type: none"> <li><i>seconds</i> is the range of 1 to 65535 seconds. The default value is 125 seconds.</li> </ul>
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.

<b>config ethernet &lt;ports&gt; ip igmp</b> followed by:	
<code>query-max-resp</code> <code>&lt;1/10 seconds&gt;</code>	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. <ul style="list-style-type: none"> <li><i>integer</i> is an integer value with a range of 0 to 255, and the default is 100 tenth seconds (equal to 10 seconds).</li> </ul> <p><b>Note:</b> This value must be less than the query-interval.</p>
<code>robustval &lt;integer&gt;</code>	Allows tuning for the expected packet loss of a network. <ul style="list-style-type: none"> <li><i>integer</i> is the range of 2 to 255 with a default of 2. Increase the value if you expect the network to experience packet loss.</li> </ul>
<code>router-alert</code> <code>&lt;enable   disable&gt;</code>	Enables or disables the router alert option. When enabled, this parameter instructs the router to process packets not directly addressed to it. <p><b>Note:</b> To maximize your network performance, Nortel Networks recommends that you set this parameter according to the version of IGMP currently in use.</p> <ul style="list-style-type: none"> <li>IGMPv1 - Disable</li> <li>IGMPv2 - Enable</li> <li>IGMPv3 - Enable</li> </ul>
<code>version &lt;integer&gt;</code>	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. <ul style="list-style-type: none"> <li><i>integer</i> is an integer value with a value of 1, 2 or 3. The default value is 2 (IGMPv2).</li> </ul>

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.



## 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:

<b>config ethernet &lt;ports&gt; ip igmp access-control &lt;name&gt;</b>	
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}	<p>Creates an access control group entry for a specific IGMP Ethernet port.</p> <ul style="list-style-type: none"> <li><i>HostAddress</i> is the IP address of the host. See <a href="#">“Specifying host addresses and masks”</a> for more information.</li> <li><i>HostMask</i> 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 <a href="#">“Specifying host addresses and masks”</a> for more information.</li> <li>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.</li> </ul>

<pre>config ethernet &lt;ports&gt; ip igmp access-control &lt;name&gt;</pre> followed by:	
<pre>delete &lt;HostAddress&gt; &lt;HostMask&gt;</pre>	Deletes the access control group entry for the specified IGMP interface. <ul style="list-style-type: none"> <li>• <i>HostAddress</i> is the IP address of the host.</li> <li>• <i>HostMask</i> is the subnet mask used to determine the host or hosts covered by this configuration.</li> </ul>
<pre>mode &lt;HostAddress&gt; &lt;HostMask&gt; {deny-tx deny-rx deny-both  allow-only-tx allow-only- rx allow-only-both}</pre>	Changes the access control group configuration. <ul style="list-style-type: none"> <li>• <i>HostAddress</i> is the IP address of the host.</li> <li>• <i>HostMask</i> is the subnet mask used to determine the host or hosts covered by this configuration.</li> <li>• 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.</li> </ul>

### 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:

<b>config vlan &lt;vid&gt; ip igmp</b> 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>	<p>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.</p> <p>Decreasing the value reduces the time to detect the loss of the last member of a group.</p> <ul style="list-style-type: none"> <li><i>seconds</i> 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).</li> </ul>
mrouter <ports>	Adds multicast router ports.
query-interval <seconds>	<p>Sets the frequency (in seconds) at which host query packets are transmitted on the VLAN.</p> <ul style="list-style-type: none"> <li><i>seconds</i> is the range from 1 to 65535. The default value is 125 seconds.</li> </ul>

<b>config vlan &lt;vid&gt; ip igmp</b> followed by:	
<code>query-max-resp</code> <code>&lt;1/10 seconds&gt;</code>	<p>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.</p> <ul style="list-style-type: none"> <li><code>seconds</code> is an integer value with a range of 0 to 255, and the default is 100 tenth seconds (equal to 10 seconds).</li> </ul> <p><b>Note:</b> This value must be less than the <code>query-interval</code>.</p>
<code>robustval &lt;integer&gt;</code>	<p>Allows tuning for the expected packet loss of a network.</p> <ul style="list-style-type: none"> <li><code>integer</code> 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.</li> </ul>
<code>router-alert</code> <code>&lt;enable   disable&gt;</code>	<p>Enables or disables the router alert option. When enabled, this parameter instructs the router to process packets not directly addressed to it.</p> <p><b>Note:</b> To maximize your network performance, Nortel Networks recommends that you set this parameter according to the version of IGMP currently in use.</p> <ul style="list-style-type: none"> <li>IGMPv1 - Disable</li> <li>IGMPv2 - Enable</li> <li>IGMPv3 - Enable</li> </ul>
<code>proxy-snoop</code> <code>&lt;enable   disable&gt;</code>	<p>Enables or disables the proxy-snoop option globally for the VLAN.</p>
<code>snoop &lt;enable   disable&gt;</code>	<p>Enables or disables the snoop option for the VLAN.</p>
<code>fast-leave</code> <code>&lt;enable   disable&gt;</code>	<p>Removes a given port from receiving a leave message from any member of any given group, and the normal IGMP behavior is skipped.</p>
<code>ssm-snoop</code> <code>&lt;enable   disable&gt;</code>	<p>Enables or disables support for PIM source-specific multicast (SSM) on the snooping interface.</p>
<code>version &lt;integer&gt;</code>	<p>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.</p> <ul style="list-style-type: none"> <li><code>integer</code> is an integer value with a value of 1, 2 or 3. The default value is 2 (IGMPv2).</li> </ul>

### *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.

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    RESP          MEMB  SNOOP  ENABLE SNOOP LEAVE LEAVE
                                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:

<b>config vlan &lt;vid&gt; ip igmp access-control &lt;name&gt;</b>	
followed by:	
info	Displays the settings for the access-control parameter.
<pre>create &lt;HostAddress&gt; &lt;HostMask&gt; {deny-tx deny-rx deny-both allow-only-tx allow-only-rx allow-only-both}</pre>	<p>Creates an access control group entry for a specified VLAN.</p> <ul style="list-style-type: none"> <li>• <i>HostAddress</i> is the IP address of the host. See <a href="#">“Specifying host addresses and masks”</a> for more information.</li> <li>• <i>HostMask</i> 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 <a href="#">“Specifying host addresses and masks”</a> for more information.</li> <li>• 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.</li> </ul>

<pre>config vlan &lt;vid&gt; ip igmp access-control &lt;name&gt;</pre> <p>followed by:</p>	
<pre>delete &lt;HostAddress&gt; &lt;HostMask&gt;</pre>	<p>Deletes the access control group entry for the specified VLAN.</p> <ul style="list-style-type: none"> <li>• <i>HostAddress</i> is the IP address of the host.</li> <li>• <i>HostMask</i> is the subnet mask used to determine the host or hosts covered by this configuration.</li> </ul>
<pre>mode &lt;HostAddress&gt; &lt;HostMask&gt; {deny-tx deny-rx deny-both allow-only-tx allow-only-rx allow-only-both}</pre>	<p>Changes the access control group configuration.</p> <ul style="list-style-type: none"> <li>• <i>HostAddress</i> is the IP address of the host.</li> <li>• <i>HostMask</i> is the subnet mask used to determine the host or hosts covered by this configuration.</li> <li>• <i>deny-tx deny-rx deny-both allow-only-tx allow-only-rx allow-only-both</i> indicates the action you want for the specified VLAN. For example, if you specify <i>deny-both</i>, the VLAN will deny both transmitted and received traffic.</li> </ul>

### 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:

<b>config vlan &lt;vid&gt; ip igmp mrdisc</b>	
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
<FromGroupAddress-ToGroupAddress>
```

where:

*vid* is a VLAN ID from 1 to 4092 and

*FromGroupAddress-ToGroupAddress* indicates the range of the static group added.

This command includes the following parameters:

<pre>config vlan &lt;vid&gt; ip igmp static-members &lt;FromGroupAddress&gt;-&lt;ToGroupAddress&gt;</pre> <p>followed by:</p>	
<pre>info</pre>	<p>Displays information about the static members of the VLAN.</p> <p><i>GroupAddress</i> is the multicast group address of the multicast stream.</p>
<pre>add &lt;ports&gt; &lt;static blocked&gt;</pre>	<p>Adds a static-member entry to the VLAN.</p> <ul style="list-style-type: none"> <li>• <i>GroupAddress</i> is the multicast group address of the multicast stream.</li> <li>• <i>ports</i> is the port or list of ports to which you want to redirect the multicast stream for this multicast group.</li> <li>• <i>static blocked</i> sets the route to static or blocked.</li> </ul>
<pre>create &lt;ports&gt; &lt;static blocked&gt;</pre>	<p>Creates a static-member entry to the VLAN.</p> <ul style="list-style-type: none"> <li>• <i>GroupAddress</i> is the multicast group address of the multicast stream.</li> <li>• <i>ports</i> is the port or list of ports to which you want to redirect the multicast stream for this multicast group.</li> <li>• <i>static blocked</i> sets the route to static or blocked.</li> </ul>

<pre>config vlan &lt;vid&gt; ip igmp static-members &lt;FromGroupAddress&gt;-&lt;ToGroupAddress&gt;</pre> <p>followed by:</p>	
delete	<p>Deletes a static-member entry to the VLAN.</p> <ul style="list-style-type: none"> <li>• <i>GroupAddress</i> is the multicast group address of the multicast stream.</li> </ul>
remove <ports> <static   blocked>	<p>Removes a port from the static-member entry to the VLAN.</p> <ul style="list-style-type: none"> <li>• <i>GroupAddress</i> is the multicast group address of the multicast stream.</li> <li>• <i>ports&gt;</i> is the port or list of ports to which you want to redirect the multicast stream for this multicast group.</li> <li>• <i>static   blocked</i> sets the route to static or blocked.</li> </ul>

### Configuration example

This configuration example uses the commands described above to perform the following tasks:

- Create a static member entry to a VLAN
- Add a static member entry to a VLAN
- Delete a static member entry to a VLAN
- Remove a port from the static member entry to the VLAN

After configuring the parameters, use the **info** command to show a summary of the results.

## 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:

<b>config vlan &lt;vid&gt; ip igmp fast-leave-members</b> followed by:	
<code>info</code>	Displays information about the fast-leave members of the VLAN.
<code>enable &lt;ports&gt;</code>	Enables members to join a fast-leave group on a given port on the VLAN. <ul style="list-style-type: none"> <li><i>ports</i> is the port or list of ports to which you want to join the fast-leave group.</li> </ul>
<code>disable &lt;ports&gt;</code>	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:

Topic	Page
<a href="#">Configuring multicast stream limitation on an interface</a>	332
<a href="#">Configuring multicast stream limitation members on an interface</a>	334
<a href="#">Showing multicast stream limitations per interface</a>	335
<a href="#">Showing multicast stream limitations per port</a>	336
<a href="#">Configuring multicast stream limitation on an Ethernet port</a>	337
<a href="#">Configuring multicast stream limitation on a VLAN</a>	338
<a href="#">Configuring multicast stream limitation members on a VLAN</a>	339

### 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:

<b>config ip igmp interface &lt;ipaddr&gt; stream-limit</b>	
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:

<b>config ip igmp interface &lt;ipaddr&gt; stream-limit-members</b> followed by:	
<code>info</code>	Displays information about the stream limit members set on individual ports for this interface.
<code>enable &lt;ports&gt; max-streams &lt;value&gt;</code>	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.
<code>disable &lt;ports&gt;</code>	Disables stream limitation for the specified ports on this interface.
<code>set &lt;ports&gt; max-streams &lt;value&gt;</code>	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 128](#) 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:

<b>config ethernet &lt;ports&gt; ip igmp stream-limit</b> followed by:	
<code>info</code>	Displays information about the stream limits set on this port.
<code>enable</code>	Enables stream limitation on this port.
<code>disable</code>	Disables stream limitation on this port.
<code>max-streams &lt;integer&gt;</code>	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:

<b>config vlan &lt;vid&gt; ip igmp stream-limit</b>	
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:

<b>config vlan &lt;vid&gt; ip igmp stream-limit-members</b> followed by:	
<code>info</code>	Displays information about the stream limit members set on individual ports for this VLAN.
<code>enable &lt;ports&gt;</code> <code>max-streams &lt;value&gt;</code>	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.
<code>disable &lt;ports&gt;</code>	Disables stream limitation for the specified ports on this VLAN.
<code>set &lt;ports&gt; max-streams &lt;value&gt;</code>	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:

Topic	Page
<a href="#">Roadmap of DVMRP commands</a>	344
<a href="#">Configuration prerequisites</a>	348
<a href="#">Configuring DVMRP globally</a>	349
<a href="#">Configuring DVMRP on an interface</a>	352
<a href="#">Configuring DVMRP on Ethernet ports</a>	357
<a href="#">Configuring DVMRP on a VLAN</a>	359
<a href="#">Configuring DVMRP routing policies</a>	361
<a href="#">Displaying all IP DVMRP show commands</a>	396

## 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 396](#).

Use this list as a quick reference or click on any entry for more information:

Command	Parameter
<code>config ip dvmrp</code>	<code>info</code> <code>disable</code> <code>enable</code> <code>leaf-timeout &lt;integer&gt;</code> <code>nbr-timeout &lt;integer&gt;</code> <code>nbr-probe-interval &lt;integer&gt;</code> <code>triggered-update- interval &lt;integer&gt;</code> <code>update-interval &lt;integer&gt;</code> <code>fwd-cache-timeout &lt;integer&gt;</code> <code>route-expiration-timeout &lt;integer&gt;</code> <code>route-discard-timeout &lt;integer&gt;</code> <code>route-switch-timeout &lt;integer&gt;</code> <code>show-next-hop-table &lt;enable disable&gt;</code> <code>generate-trap &lt;enable disable&gt;</code> <code>generate-log &lt;enable disable&gt;</code>
<code>config ip dvmrp interface &lt;ipaddr&gt;</code>	<code>info</code> <code>advertise-self &lt;enable disable&gt;</code>

Command	Parameter
<pre>show ip dvmrp info show ip dvmrp interface show ip dvmrp neighbor show ip dvmrp next-hop show ip dvmrp route</pre>	<pre>create &lt;active passive&gt; default-listen &lt;enable disable&gt; default-supply &lt;enable disable&gt; default-supply-metric &lt;cost&gt; disable enable in-policy &lt;policy name&gt; interface-type &lt;active passive&gt; metric &lt;cost&gt; out-policy &lt;policy name&gt;</pre>
<pre>config ethernet &lt;ports&gt; ip dvmrp</pre>	<pre>info advertise-self &lt;enable disable&gt; create &lt;active passive&gt; default-listen &lt;enable disable&gt; default-supply &lt;enable disable&gt; default-supply-metric &lt;cost&gt; disable enable in-policy &lt;policy name&gt; interface-type &lt;active passive&gt; metric &lt;cost&gt; out-policy &lt;policy name&gt;</pre>
<pre>config vlan &lt;vid&gt; ip dvmrp</pre>	<pre>info</pre>

Command	Parameter
	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 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>

**Command****Parameter**`name <policy name>``set-metric <metric-value>``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:

<b>config ip dvmrp</b> 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>	<p>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.</p> <ul style="list-style-type: none"> <li>• <i>integer</i> is the range of 25 to 4000 seconds. The default value is 125 seconds.</li> </ul>
nbr-timeout <integer>	<p>Sets the length of time (in seconds) the router waits to receive a report from a neighbor before considering the connection inactive.</p> <ul style="list-style-type: none"> <li>• <i>integer</i> is the range of 35 to 8000 seconds. The default value is 35 seconds.</li> </ul>
nbr-probe-interval <integer>	<p>Sets the time interval (in seconds) for the DVMRP router to send a neighbor probe message on its interface.</p> <ul style="list-style-type: none"> <li>• <i>integer</i> is the range of 5 to 30 seconds. The default value is 10 seconds.</li> </ul>
triggered-update-interval <integer>	<p>Sets the time interval (in seconds) between triggered update messages sent when routing information changes.</p> <ul style="list-style-type: none"> <li>• <i>integer</i> is the range of 5 to 1000 seconds. The default value is 5 seconds.</li> </ul>
update-interval <integer>	<p>Sets the time interval (in seconds) between DVMRP router update messages.</p> <ul style="list-style-type: none"> <li>• &lt;integer&gt; is the range of 10 to 2000 seconds. The default value is 60 seconds.</li> </ul>
fld-cache-timeout <integer>	<p>Sets the forward cache timeout (in seconds).</p> <ul style="list-style-type: none"> <li>• &lt;integer&gt; is the range of 300 to 86400 seconds. The default value is 300 seconds.</li> </ul>

<b>config ip dvmrp</b>	
followed by:	
<code>route-expiration-timeout &lt;integer&gt;</code>	Sets the route expiration timeout (in seconds). <ul style="list-style-type: none"> <li>• <i>&lt;integer&gt;</i> is the range of 20 to 4000 seconds. The default value is 140 seconds.</li> </ul>
<code>route-discard-timeout &lt;integer&gt;</code>	Sets the route discard timeout (in seconds). <ul style="list-style-type: none"> <li>• <i>&lt;integer&gt;</i> is the range of 40 to 8000. The default value is 260 seconds.</li> </ul>
<code>route-switch-timeout &lt;integer&gt;</code>	Sets the route switch timeout (in seconds). <ul style="list-style-type: none"> <li>• <i>&lt;integer&gt;</i> is the range of 20 to 2000. The default value is 140 seconds.</li> </ul>
<code>show-next-hop-table &lt;enable   disable&gt;</code>	Enables or disables showing information about the DVMRP next hops. <a href="#">See “Showing DVMRP next hops” on page 355.</a>
<code>generate-trap &lt;enable   disable&gt;</code>	Enabling this command on this switch will trigger trap for the following DVMRP events: <ul style="list-style-type: none"> <li>• Neighborhood is established</li> <li>• Neighborhood is lost</li> <li>• Enable/Disable DVMRP on an interface</li> </ul>
<code>generate-log &lt;enable   disable&gt;</code>	Enabling this command on this switch will cause the following DVMRP events to be logged: <ul style="list-style-type: none"> <li>• Establish a neighborhood.</li> <li>• Loss of neighborhood.</li> <li>• Enable/Disable DVMRP on an interface.</li> </ul>

Figure 131 shows sample output for the `config ip dvmrp info` command.

**Figure 131** config ip dvmrp info command output

```
PP8600:5# conf ip dv inf

Sub-Context: clear config dump monitor show test trace wsm asfm
sam
Current Context:
                enable : false
                update-interval : 60
    triggered-update-interval : 5
                leaf-timeout : 125
                nbr-timeout : 35
                nbr-probe-interval : 10
                fwd-cache-timeout : 300
    route-expire-timeout : 140
                route-disc-timeout : 260
    route-switch-timeout : 140
                show-next-hop-table : disable
                generate-trap : disable
                generate-log : disable
```

## 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:

<b>config ip dvmrp interface &lt;ipaddr&gt;</b> 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 <a href="#">“Applying the advertisement of local networks policy to an interface” on page 384</a>
create <active   passive>	Sets the interface type: active or passive. See <a href="#">“Creating a passive interface” on page 388</a> .
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 <a href="#">“Applying the default route policy to an interface” on page 362</a> .
default-supply <enable   disable>	Generates and advertises the default route when enabled on the interface. The default setting is disable. See <a href="#">“Applying the default route policy to an interface” on page 362</a> .
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 <a href="#">“Applying the default route policy to an interface” on page 362</a> .
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 <a href="#">“Applying a DVMRP accept policy to an interface” on page 381</a> .
interface-type <active   passive>	Configure an interface as active or passive. See <a href="#">“Configuring an active or passive interface type” on page 389</a> .

<b>config ip dvmrp interface &lt;ipaddr&gt;</b> followed by:	
<code>metric &lt;cost&gt;</code>	Sets the cost metric (maximum number of hops) for the router interface. <i>cost</i> is the range of 1 to 31.
<code>out-policy &lt;policy name&gt;</code>	Applies a DVMRP accept policy. See <a href="#">“Applying a DVMRP announce policy to an interface” on page 373</a> .

## 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 349](#).

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:

<b>config ethernet &lt;ports&gt; ip dvmrp</b>	
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 <a href="#">“Applying the advertisement of local networks policy over a port” on page 386</a> .
create <active   passive>	Sets the interface type: active or passive. See <a href="#">“Configuring an active or passive port type” on page 392</a> .
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 <a href="#">“Applying the default route policy to a port” on page 366</a> .
default-supply <enable   disable>	Generates and advertises the default route when enabled on the port. The default setting is disable. See <a href="#">“Applying the default route policy to a port” on page 366</a> .
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 <a href="#">“Applying the default route policy to a port” on page 366</a> .
disable	Disables DVMRP on the port.
enable	Enables DVMRP on the port.
in-policy <policy name>	Applies a DVMRP accept policy. See <a href="#">“Applying a DVMRP accept policy to a port” on page 383</a> .

<b>config ethernet &lt;ports&gt; ip dvmrp</b> followed by:	
interface-type <active passive>	Configure an interface as active or passive. See <a href="#">“Configuring an active or passive port type” on page 392.</a>
metric <cost>	Sets the DVMRP route metric. <i>cost</i> is the maximum number of hops with a value of 1 to 31.
out-policy <policy name>	Applies a DVMRP accept policy. See <a href="#">“Applying a DVMRP announce policy to a port” on page 375.</a>

[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
```

### *Configuration example*

This configuration example uses the commands described above to perform the following tasks:

- Create a passive interface

After configuring the parameters, use the **info** command to show a summary of the results.

## 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:

<b>config vlan &lt;vid&gt; ip dvmrp</b>	
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 <a href="#">“Applying the advertisement of local networks policy over a VLAN” on page 385</a> .
create <active   passive>	Sets the interface type: active or passive. See <a href="#">“Configuring an active or passive VLAN type” on page 391</a> .
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 <a href="#">“Applying the default route policy to a VLAN” on page 364</a> .
default-supply <enable   disable>	Generates and advertises the default route when enabled on the VLAN. The default setting is disable. See <a href="#">“Applying the default route policy to a VLAN” on page 364</a> .
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 <a href="#">“Applying the default route policy to a VLAN” on page 364</a> .
disable	Disables DVMRP on the VLAN.
enable	Enables DVMRP on the VLAN.
in-policy <policy name>	Applies a DVMRP accept policy. See <a href="#">“Applying a DVMRP accept policy to a VLAN” on page 382</a> .
interface-type <active   passive>	Configure an interface as active or passive. See <a href="#">“Configuring an active or passive VLAN type” on page 391</a> .

<b>config vlan &lt;vid&gt; ip dvmrp</b> followed by:	
<code>metric &lt;cost&gt;</code>	Sets the DVMRP route metric. <i>cost</i> is the maximum number of hops with a value of 1 to 31.
<code>out-policy &lt;policy name&gt;</code>	Applies a DVMRP accept policy. See <a href="#">“Applying a DVMRP announce policy to a VLAN”</a> on page 374.

[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:

Topic	Page
<a href="#">Configuring default route policies</a>	361
<a href="#">Configuring DVMRP announce policies</a>	368
<a href="#">Configuring DVMRP accept policies</a>	376
<a href="#">Configuring the advertisement of local network policies</a>	384
<a href="#">Configuring a DVMRP interface type</a>	388
<a href="#">Displaying DVMRP routing policy information</a>	393

## 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:

Topic	Page
<a href="#">Applying the default route policy to an interface</a>	362
<a href="#">Applying the default route policy to a VLAN</a>	364
<a href="#">Applying the default route policy to a port</a>	366

Before you apply the default route policy to the switch, you must perform the procedures provided in [“Configuration prerequisites” on page 348](#).

To display DVMRP default route configuration information for an interface, VLAN, or port, refer to [“Displaying DVMRP routing policy information” on page 393](#).

## 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:

<b>config ip dvmrp interface &lt;ipaddr&gt;</b> 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:

<b>config vlan &lt;vlanid&gt; ip dvmrp</b> 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:

<b>config ethernet &lt;ports&gt; ip dvmrp</b> 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:

Task	Page
<a href="#">Creating a DVMRP announce policy</a>	368
<a href="#">Applying a DVMRP announce policy to an interface</a>	373
<a href="#">Deleting a DVMRP announce policy from an interface</a>	373
<a href="#">Applying a DVMRP announce policy to a VLAN</a>	374
<a href="#">Deleting a DVMRP announce policy from a VLAN</a>	374
<a href="#">Applying a DVMRP announce policy to a port</a>	375
<a href="#">Deleting a DVMRP announce policy from a port</a>	375

Before you create and apply a DVMRP announce policy to the switch, you must perform the procedures provided in [“Configuration prerequisites”](#) on page 348.



**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 393.

### 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:

<b>config ip prefix-list &lt;prefix-list-name&gt;</b>	
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. <i>maskLenFrom &lt;value&gt;</i> is the lower bound of mask length. The default is the mask length. <i>maskLenTo &lt;value&gt;</i> is the higher bound mask length. The default is the mask length. <b>Note:</b> 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. <i>ipaddr/mask&gt;</i> 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:

<b>config ip route-policy &lt;policy name&gt; seq &lt;seq number&gt;</b> followed by:	
<code>action &lt;permit/deny&gt;</code>	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.
<code>create</code>	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.
<code>disable</code>	Disables a route policy with a policy name and a sequence number.
<code>enable</code>	Enables a route policy with a policy name and a sequence number.
<code>match-protocol &lt;protocol name&gt;</code>	Matches the protocol through which the route is learned, if configured.

<b>config ip route-policy &lt;policy name&gt; seq &lt;seq number&gt;</b> followed by:	
<code>match-metric &lt;metric&gt;</code>	Matches the metric of the incoming advertisement or existing route against the specified value, if configured. If 0, then this field is ignored. <ul style="list-style-type: none"> <li>• <code>&lt;metric&gt;</code> is 1 to 65535. The default is 0.</li> </ul>
<code>match-network &lt;prefix-list&gt;</code>	Matches the destination network against the contents of the specified prefix list(s), if configured. <ul style="list-style-type: none"> <li>• <code>&lt;prefix-list&gt;</code> specify the name of up to four defined prefix list by name separated by a comma.</li> </ul>
<code>match-next-hop &lt;prefix-list&gt;</code>	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. <ul style="list-style-type: none"> <li>• <code>&lt;prefix-list&gt;</code> specify the name of up to four defined prefix list by name separated by a comma.</li> </ul>
<code>match-route-src &lt;prefix-list&gt;</code>	Matches the previous hop IP address for DVMRP routes against the contents of the specified prefix list, if configured. <ul style="list-style-type: none"> <li>• <code>&lt;prefix-list&gt;</code> specify the name of up to four defined prefix list by name separated by a comma.</li> </ul>
<code>name &lt;policy name&gt;</code>	Renames a policy once it has been created. This command changes the name field for all sequence numbers under the given policy.
<code>set-metric &lt;metric-value&gt;</code>	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:

Task	Page
<a href="#">Creating a DVMRP accept policy</a>	376
<a href="#">Applying a DVMRP accept policy to an interface</a>	381
<a href="#">Deleting a DVMRP accept policy from an interface</a>	381
<a href="#">Applying a DVMRP accept policy to a VLAN</a>	382
<a href="#">Deleting a DVMRP accept policy from a VLAN</a>	382
<a href="#">Applying a DVMRP accept policy to a port</a>	383
<a href="#">Deleting a DVMRP accept policy from a port</a>	383

Before you create and apply a DVMRP accept policy to the switch, you must perform the procedures provided in [“Configuration prerequisites”](#) on page 348.



**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 393.

### 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:

<b>config ip prefix-list &lt;prefix-list-name&gt;</b>	
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. <i>maskLenFrom &lt;value&gt;</i> is the lower bound of mask length. The default is the mask length. <i>maskLenTo &lt;value&gt;</i> is the higher bound mask length. The default is the mask length. <b>Note:</b> 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. <i>ipaddr/mask</i> 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:

<b>config ip route-policy &lt;policy name&gt; seq &lt;seq number&gt;</b> followed by:	
<code>action &lt;permit/deny&gt;</code>	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.
<code>create</code>	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.
<code>disable</code>	Disables a route policy with a policy name and a sequence number.
<code>enable</code>	Enables a route policy with a policy name and a sequence number.
<code>match-protocol &lt;protocol name&gt;</code>	Matches the protocol through which the route is learned, if configured.

<b>config ip route-policy &lt;policy name&gt; seq &lt;seq number&gt;</b> followed by:	
<code>match-metric &lt;metric&gt;</code>	Matches the metric of the incoming advertisement or existing route against the specified value, if configured. If 0, then this field is ignored. <ul style="list-style-type: none"> <li>• <code>&lt;metric&gt;</code> is 1 to 65535. The default is 0.</li> </ul>
<code>match-network &lt;prefix-list&gt;</code>	Matches the destination network against the contents of the specified prefix list(s), if configured. <ul style="list-style-type: none"> <li>• <code>&lt;prefix-list&gt;</code> specify the name of up to four defined prefix list by name separated by a comma.</li> </ul>
<code>match-next-hop &lt;prefix-list&gt;</code>	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. <ul style="list-style-type: none"> <li>• <code>&lt;prefix-list&gt;</code> specify the name of up to four defined prefix list by name separated by a comma.</li> </ul>
<code>match-route-src &lt;prefix-list&gt;</code>	Matches the previous hop IP address for DVMRP routes against the contents of the specified prefix list, if configured. <ul style="list-style-type: none"> <li>• <code>&lt;prefix-list&gt;</code> specify the name of up to four defined prefix list by name separated by a comma.</li> </ul>
<code>name &lt;policy name&gt;</code>	Renames a policy once it has been created. This command changes the name field for all sequence numbers under the given policy.
<code>set-metric &lt;metric-value&gt;</code>	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:

Task	Page
<a href="#">Applying the advertisement of local networks policy to an interface</a>	384
<a href="#">Applying the advertisement of local networks policy over a VLAN</a>	385
<a href="#">Applying the advertisement of local networks policy over a port</a>	386

Before you apply the advertisement of local networks policy to the switch, you must execute the procedures provided in [“Configuration prerequisites” on page 348](#).

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 393](#).

### 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:

<code>config ip dvmrp interface &lt;ipaddr&gt; advertise-self</code> 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:

<b>config vlan &lt;vid&gt; ip dvmrp advertise-self</b>	
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:

<b>config ether &lt;port&gt; ip dvmrp advertise-self</b> 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:

Task	Page
<a href="#">Creating a passive interface</a>	388
<a href="#">Configuring an active or passive interface type</a>	389
<a href="#">Configuring an active or passive VLAN type</a>	391
<a href="#">Configuring an active or passive port type</a>	392

Before you apply the DVMRP passive interface policy to the switch, you must execute the procedures provided in [“Configuration prerequisites”](#) on page 348.

To display DVMRP interface type configuration information for an interface, VLAN, or port, refer to [“Displaying DVMRP routing policy information”](#) on page 393.

### 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:

<b>config ip dvmrp interface &lt;ipaddr&gt; create</b> 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:

<b>config ip dvmrp interface &lt;ipaddr&gt; interface-type</b>	
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:

<b>config vlan &lt;vid&gt; ip dvmrp interface-type</b>	
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:

<b>config ethernet &lt;port&gt; ip dvmrp interface-type</b>	
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
=====
```

IF	ADDR	METRIC	OPERSTAT	DEFAULT LISTEN	DEFAULT SUPPLY	DEFAULT METRIC	ADVERTISE 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 444](#).

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:

Topic	Page
<a href="#">Roadmap of PIM commands</a>	401
<a href="#">PIM-SM configuration prerequisites</a>	405
<a href="#">Configuring PIM-SM globally</a>	406
<a href="#">Configuring a PIM multicast border router (PMBR)</a>	409
<a href="#">Configuring PIM on an interface</a>	410
<a href="#">Configuring a candidate BSR on an interface</a>	415
<a href="#">Configuring a candidate rendezvous point (C-RP)</a>	416
<a href="#">Configuring a static rendezvous point (RP)</a>	423
<a href="#">Configuring PIM on an Ethernet (brouter) port</a>	427
<a href="#">Configuring a candidate BSR on an Ethernet port</a>	428
<a href="#">Configuring PIM on a VLAN</a>	429
<a href="#">Configuring a candidate BSR on a VLAN</a>	433
<a href="#">Configuring PIM debug trace commands</a>	434
<a href="#">Configuring Source Specific Multicast (SSM)</a>	444
<a href="#">Displaying all IP PIM show commands</a>	448

## 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 448](#).

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
<code>config ip pim interface &lt;ipaddr&gt;</code>	<code>info</code> <code>create &lt;active passive&gt;</code> <code>disable</code> <code>enable</code> <code>hellointerval &lt;seconds&gt;</code> <code>interface-type &lt;active passive&gt;</code> <code>joinprune-interval &lt;seconds&gt;</code>
<code>show ip pim interface</code>	
<code>show ip pim neighbor</code>	
<code>config ip pim candbsr interface &lt;ipaddr&gt;</code>	<code>info</code> <code>enable preference &lt;value&gt;</code> <code>disable</code>
<code>config ip pim candrp</code>	<code>info</code> <code>add grp &lt;ipaddr&gt; mask &lt;ipmask&gt; rp &lt;ipaddr&gt;</code> <code>delete grp &lt;ipaddr&gt; mask &lt;ipmask&gt;</code>
<code>show ip pim rp-set</code>	
<code>show ip pim candidate-rp</code>	
<code>show ip pim active-rp &lt;group&gt;</code>	
<code>show ip pim active-rp</code>	
<code>show ip pim bsr</code>	
<code>show ip pim mroute</code>	
<code>config ip pim static-rp</code>	<code>info</code> <code>add grp &lt;ipaddr&gt; mask &lt;ipmask&gt; rp &lt;ipaddr&gt;</code> <code>delete grp &lt;ipaddr&gt; mask &lt;ipmask&gt; rp &lt;ipaddr&gt;</code>

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**

`config ip pim debug-pimmsg`

**Parameter**

`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 a 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:

<b>config ip pim</b>	
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/ssp>	The configured mode of this interface: sparse or ssm (source-specific multicast). <sup>1</sup>
bootstrap-period <integer>	Specifies the interval (in seconds) that the elected BSR waits between originating bootstrap messages. <ul style="list-style-type: none"> <li><i>integer</i> is a number in the range from 5 to 32757. The default is 60.</li> </ul>
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. <ul style="list-style-type: none"> <li><i>integer</i> is a number in the range from 5 to 26214. The default is 60.</li> </ul>

<b>config ip pim</b> followed by:	
<code>disc-data-timeout &lt;integer&gt;</code>	<p>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.</p> <ul style="list-style-type: none"> <li><i>integer</i> is a number in the range from 5 to 65535. The default is 60.</li> </ul>
<code>activity-chk-interval &lt;integer&gt;</code>	<p>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.</p> <ul style="list-style-type: none"> <li><i>integer</i> is 15, 30 or 210. The default is 30.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>Before you can change the activity-chk-interval, you have to disable PIM globally.</li> <li>Nortel Networks recommends an activity check interval of 30 seconds.</li> <li>On IGAP-enabled interfaces, set the activity check interval to 30 seconds or less.</li> <li>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.</li> </ul>
<code>joinprune-interval &lt;integer&gt;</code>	<p>Specifies how long to wait (in seconds) before the PIM router sends out the next join/prune message to its upstream neighbors.</p> <ul style="list-style-type: none"> <li><i>integer</i> is a number in the range from 1 to 18724. The default is 60.</li> </ul>
<code>register-suppression-timeout &lt;integer&gt;</code>	<p>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.</p> <ul style="list-style-type: none"> <li><i>integer</i> is a number in the range from 6 to 65535. The default is 60.</li> </ul>
<code>unicast-route-change-timeout &lt;integer&gt;</code>	<p>Specifies how often (in seconds) the switch polls the routing table manager (RTM) for unicast routing information updates to be used by PIM.</p> <p><b>Note:</b> 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.</p> <ul style="list-style-type: none"> <li><i>integer</i> is a number in the range from 2 to 65535. The default is 5.</li> </ul>

- 1 To enable PIM-SSM globally, see [“Configuring PIM-SSM globally” on page 446.](#) 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:

<b>config ip pim mbr</b>	
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 406](#).

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:

<b>config ip pim interface &lt;ipaddr&gt;</b> 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 <a href="#">create &lt;active passive&gt;</a> for a description of active and passive interfaces. <code>interface-type</code> 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

```

Passport-8603:3# show ip pim interface

                                Pim Interface
=====
IF      ADDR      MASK      MODE      DR      HLINT JPIN
T CBSPR      OPSTAT INTF TYPE

```

[Table 66](#) describes the `show ip pim interface` parameters.

**Table 66** 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.

**Table 66** show ip pim interface parameters (continued)

<b>Field</b>	<b>Description</b>
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 67 describes the Pim Neighbor parameters.

**Table 67** 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:

<b>config ip pim candbsr interface &lt;ipaddr&gt;</b>	
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:

<b>config ip pim candrp</b> followed by:	
info	Displays current RP configuration settings on the local router interface.
add grp <ipaddr> mask <ipmask> rp <ipaddr>	<p>Adds a candidate RP to the RP set.</p> <ul style="list-style-type: none"> <li>• <b>add grp &lt;ipaddr&gt;</b> - 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.</li> <li>• <b>mask &lt;ipmask&gt;</b> - 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.</li> <li>• <b>rp &lt;ipaddr&gt;</b> - The IP address of the C-RP. This address has to be one of the local PIM-SM enabled interfaces.</li> </ul>
delete grp <ipaddr> mask <ipmask>	<p>Deletes a candidate RP from the RP set.</p> <ul style="list-style-type: none"> <li>• <b>delete</b></li> <li>• <b>grp &lt;ipaddr&gt;</b> - 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.</li> <li>• <b>mask &lt;ipmask&gt;</b> - 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.</li> </ul>

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 68 describes the Pim RPSet parameters.

**Table 68** 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 69 describes the Pim Candidate RP Table parameters.

**Table 69** 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 70 describes the Pim Grp->RP Active RP Table parameters.

**Table 70** 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 71 describes the Pim Grp->RP Active RP Table parameters.

**Table 71** 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 72 describes the Current BootStrap Router Info parameters.

**Table 72** 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:

<b>config ip pim static-rp</b> 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. <ul style="list-style-type: none"> <li>• grp &lt;ipaddr&gt; - 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.</li> <li>• mask &lt;ipmask&gt; - 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.</li> <li>• rp &lt;ipaddr&gt; - The IP address of the static RP.</li> </ul>
delete grp <ipaddr> mask <ipmask> rp <ipaddr>	Deletes a static RP entry from the RP set. <ul style="list-style-type: none"> <li>• grp &lt;ipaddr&gt; - 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.</li> <li>• mask &lt;ipmask&gt; - 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.</li> <li>• rp &lt;ipaddr&gt; - The IP address of the static RP.</li> </ul>
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#
```

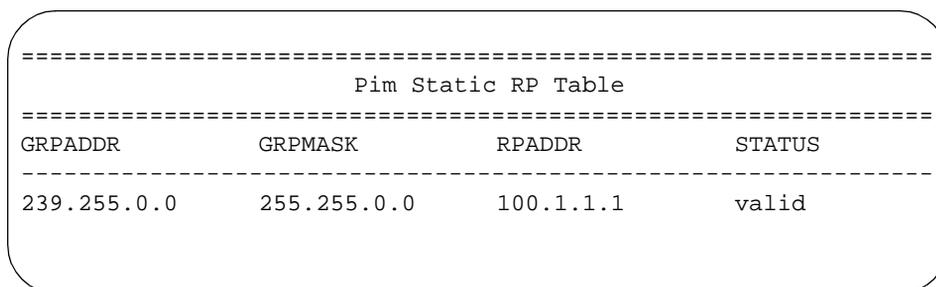
## Showing the static RP table

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 406](#).

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:

<b>config ethernet &lt;ports&gt; ip pim</b>	
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 <a href="#">create &lt;active passive&gt;</a> for a description of active and passive ports. <code>interface-type</code> 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:

<b>config ethernet &lt;ports&gt; ip pim candbsr</b> 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 406](#).

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:

<b>config vlan &lt;vid&gt; ip pim</b>	
followed by:	
<code>info</code>	Displays current PIM configuration settings on the selected VLAN.
<code>disable</code>	Disables PIM on the selected VLAN.
<code>create</code> <code>&lt;active passive&gt;</code>	Enables PIM on a specific VLAN with a specific type. <ul style="list-style-type: none"> <li><code>active</code> allows PIM control traffic to be transmitted and received.</li> <li><code>passive</code> 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.</li> </ul>
<code>enable</code>	Enables PIM on the selected VLAN.
<code>hellointerval</code> <code>&lt;seconds&gt;</code>	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.
<code>interface-type</code> <code>&lt;active passive&gt;</code>	Specifies whether the selected interface is active or passive. See <code>create &lt;active passive&gt;</code> for a description of active and passive interfaces. <code>interface-type</code> 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
<code>joinprune-interval</code> <code>&lt;seconds&gt;</code>	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
jpaint        : 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 73](#) describes the `show vlan ip pim` parameters.

**Table 73** 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:

<b>config vlan &lt;vid&gt; ip pim candbsr</b>	
followed by:	
info	Displays the candidate BSR preference setting for this interface ( <a href="#">Figure 158</a> ).
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).

<b>config ip pim debug-pimmsg</b> 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.

<b>config ip pim debug-pimmsg</b>	
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 437](#).

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,” next](#)
- [“Bootstrap debug trace send/receive output” on page 439](#)
- [“Hello debug trace send/receive output” on page 440](#)
- [“Joinprune debug trace send/receive output” on page 441](#)
- [“Register debug trace send/receive output” on page 442](#)
- [“Regstop debug trace send/receive output” on page 443](#)
- [“Rp-adv debug trace send/receive output” on page 444](#)

## 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 (RPF) 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 285](#) or [“Configuring IGMP on a VLAN” on page 320](#).”

For information on configuring the SSM group range and channel table, refer to [“Showing SSM group range and dynamic learning status” on page 308](#) or [“Configuring the SSM channel table” on page 309](#).”

---

The `config ip pim` command includes the following parameters:

<b>config ip pim</b> followed by:	
info	Displays current PIM settings on the switch.
disable	Globally disables PIM on the switch.
enable	Globally enables PIM on the switch.

<b>config ip pim</b> followed by:	
mode < <i>sparse/ssm</i> >	The configured mode of this interface: sparse or ssm (source-specific multicast).
bootstrap-period < <i>integer</i> >	Specifies the interval (in seconds) that the elected BSR waits between originating bootstrap messages. <ul style="list-style-type: none"> <li><i>integer</i> is a number in the range from 5 to 32757. The default is 60.</li> </ul>
c-rp-adv-timeout < <i>integer</i> >	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. <ul style="list-style-type: none"> <li><i>integer</i> is a number in the range from 5 to 26214. The default is 60.</li> </ul>
disc-data-timeout < <i>integer</i> >	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. <ul style="list-style-type: none"> <li><i>integer</i> is a number in the range from 5 to 65535. The default is 60.</li> </ul>
activity-chk-interval	15, 30 or 210
joinprune-interval < <i>integer</i> >	Specifies how long to wait (in seconds) before the PIM router sends out the next join/prune message to its upstream neighbors. <ul style="list-style-type: none"> <li><i>integer</i> is a number in the range from 1 to 18724. The default is 60.</li> </ul>
register-suppression-timeout < <i>integer</i> >	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. <ul style="list-style-type: none"> <li><i>integer</i> is a number in the range from 6 to 65535. The default is 60.</li> </ul>
unicast-route-change-timeout < <i>integer</i> >	Specifies how often (in seconds) the switch polls the routing table manager (RTM) for unicast routing information updates to be used by PIM. <p><b>Note:</b> 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.</p> <ul style="list-style-type: none"> <li><i>integer</i> is a number in the range from 2 to 65535. The default is 5.</li> </ul>

### 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:

Topic	Page
<a href="#">Roadmap of PGM commands</a>	<a href="#">452</a>
<a href="#">Configuration considerations and prerequisites</a>	<a href="#">454</a>
<a href="#">Configuring PGM globally</a>	<a href="#">455</a>
<a href="#">Configuring PGM on an interface</a>	<a href="#">463</a>
<a href="#">Configuring PGM on Ethernet ports</a>	<a href="#">472</a>
<a href="#">Configuring PGM on a VLAN</a>	<a href="#">474</a>
<a href="#">Displaying all IP PGM show commands</a>	<a href="#">476</a>

## 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 476](#).

Use this list as a quick reference or click on any entry for more information:

Command	Parameter
<code>config ip pgm</code>	<code>info</code> <code>state &lt;enable disable&gt;</code> <code>session-life-time &lt;integer&gt;</code> <code>nnak-generate &lt;enable disable&gt;</code> <code>max-rexmit-state &lt;integer&gt;</code> <code>max-sessions &lt;integer&gt;</code>
<code>show ip pgm global</code>	
<code>show ip pgm retransmit</code>	
<code>show ip pgm session</code>	
<code>config ip pgm interface &lt;ipaddr&gt;</code>	<code>info</code> <code>state &lt;enable disable&gt;</code> <code>nak-re-xmit-int &lt;integer&gt;</code> <code>max-nak-re-xmit-cnt &lt;integer&gt;</code> <code>max-nak-rdata-int &lt;integer&gt;</code> <code>nak-eliminate-int &lt;integer&gt;</code>
<code>show ip pgm interface config</code>	
<code>show ip pgm interface error general</code>	
<code>show ip pgm interface error nak</code>	

Command	Parameter
<code>show ip pgm interface stat general</code>	
<code>show ip pgm interface stat nak</code>	
<code>show ip pgm interface stat parity</code>	
<code>config ethernet &lt;ports&gt; ip pgm</code>	<code>info</code> <code>state &lt;enable disable&gt;</code> <code>nak-re-xmit-int &lt;integer&gt;</code> <code>max-nak-re-xmit-cnt &lt;integer&gt;</code> <code>max-nak-rdata-int &lt;integer&gt;</code> <code>nak-eliminate-int &lt;integer&gt;</code>
<code>config vlan &lt;vid&gt; ip pgm</code>	<code>info</code> <code>state &lt;enable disable&gt;</code> <code>nak-re-xmit-int &lt;integer&gt;</code> <code>max-nak-re-xmit-cnt &lt;integer&gt;</code> <code>max-nak-rdata-int &lt;integer&gt;</code> <code>nak-eliminate-int &lt;integer&gt;</code>
<code>show ip pgm show-all [file &lt;value&gt;]</code>	

## 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:

<b>config ip pgm</b> 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 74 describes the `show ip pgm global` parameters.

**Table 74** 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 75 describes the `show ip pgm retransmit` parameters.

**Table 75** 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              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
-----

SOURCE  GLOBAL          IN    OUT   IN_RDATA  UNIQUE  IN    OUT   IN_NAK
PORT    ID              RDATA RDATA NO_STATE  NAKS    NAKS  NAKS  SEQ
                               ERRORS
-----

SOURCE  GLOBAL          IN    OUT   IN    OUT   IN    OUT   IN_REDIRECTED
PORT    ID              NNAKS NNAKS NCFS   NCFS   NCFS  NCFS
-----

SOURCE  GLOBAL          IN    OUT   IN    OUT   IN    OUT
PORT    ID              PARITY PARITY PARITY PARITY PARITY PARITY
                               NAK    NAK    RDATA RDATA NCF    NCF
-----

SOURCE  GLOBAL          IN    OUT   UNIQUE
PORT    ID              PARITY PARITY PARITY
                               SPM    SPM    NAKS
-----

```

SOURCE PORT	GLOBAL ID	SOURCE	GROUP	UPSTREAM ADDRESS	UPSTRM IF_CCT
19	9b:78:32:c9:0:0	155.120.50.201	224.241.241.241	155.120.50.201	2050

SOURCE PORT	GLOBAL ID	TRAIL EDGE SEQ	LEAD EDGE SEQ	IN SPMS	OUT SPMS	TOTAL RE_XMIT STATES	TOTAL RE_XMIT TIMEOUT
19	9b:78:32:c9:0:0	0	237	407	813	0	0

SOURCE PORT	GLOBAL ID	IN RDATA	OUT RDATA	IN_RDATA NO_STATE ERRORS	UNIQUE NAKS	IN NAKS	OUT NAKS	IN_NAK SEQ ERRORS
19	9b:78:32:c9:0:0	98	98	0	0	48	40	0

SOURCE PORT	GLOBAL ID	IN NNAKS	OUT NNAKS	IN NCFS	OUT NCFS	IN REDIRECTED NCFS
19	9b:78:32:c9:0:0	0	0	2	0	0

SOURCE PORT	GLOBAL ID	IN PARITY NAK	OUT PARITY NAK	IN PARITY RDATA	OUT PARITY RDATA	IN PARITY NCF	OUT PARITY NCF
19	9b:78:32:c9:0:0	0	0	2	3	0	0

SOURCE PORT	GLOBAL ID	IN PARITY SPM	OUT PARITY SPM	UNIQUE PARITY NAKS
19	9b:78:32:c9:0:0	3	0	8

Table 76 describes the `show ip pgm session` parameters.

**Table 76** 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 ERRORS	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 76** show ip pgm session parameters (continued)

<b>Field</b>	<b>Description</b>
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:

<b>config ip pgm interface &lt;ipaddr&gt;</b> followed by:	
<code>info</code>	Displays current PGM settings on the selected interface.
<code>state</code> <code>&lt;enable   disable&gt;</code>	Indicates the current state (enable or disable) of PGM on the selected interface.
<code>nak-re-xmit-int</code> <code>&lt;integer&gt;</code>	Specifies how long to wait for an NCF (in milliseconds) before retransmitting the NAK. The default value is 1000 milliseconds.
<code>max-nak-re-xmit-cnt</code> <code>&lt;integer&gt;</code>	Configures the maximum number of NAK retransmission packets allowed per second. The default value is 2 pps.
<code>max-nak-rdata-int</code> <code>&lt;integer&gt;</code>	Specifies how long to wait for RDATA (in milliseconds) after receiving an NCF. The default value is 10000 milliseconds.
<code>nak-eliminate-int</code> <code>&lt;integer&gt;</code>	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 <code>max-nak-rdata-int</code> . 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 466](#)  
[“Showing PGM interface NAK errors” on page 467](#)
- Interface statistics  
[“Showing PGM interface statistics” on page 468](#)  
[“Showing PGM interface NAK statistics” on page 470](#)  
[“Showing PGM interface parity statistics” on page 471](#)

## 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 77](#) describes the `show ip pgm interface config` parameters.

**Table 77** 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 78 describes the `show ip pgm interface error general` parameters.

**Table 78** 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 78** 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 PORT ERRORS	IN_NAK NO_SESSION ERRORS	IN_NAK SEQ ERRORS	IN_NNAK PORT ERRORS	IN_NNAK NO_SESSION ERRORS	PARITY NAK_TG ERRORS
Port1/1	0	0	0	0	0	0
Port5/1	0	0	0	0	0	0

Table 79 describes the `show ip pgm interface error nak` parameters.

**Table 79** 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
-----
Port1/1  0         0         274    273    9        0        2        0        0
Port5/1  0         0         109    110    14       0        2        0        0

```

[Table 80](#) describes the `show ip pgm interface stat general` parameters.

**Table 80** 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 81 describes the `show ip pgm interface stat nak` parameters.

**Table 81** 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 SPMS	OUT SPMS	IN RDATA	OUT RDATA	IN NCFS	OUT NCFS	IN NAKS	OUT NAKS	UNIQUE NAKS
Port1/1	86	87	2	0	2	0	0	0	0
Port5/1	211	212	6	0	2	0	0	0	0

Table 82 describes the `show ip pgm interface stat parity` parameters.

**Table 82** 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 82** 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:

<b>config ethernet &lt;ports&gt; ip pgm</b> 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.

<b>config ethernet &lt;ports&gt; ip pgm</b> 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:

<b>config vlan &lt;vid&gt; ip pgm</b> followed by:	
<code>info</code>	Displays current pgm settings on the selected VLAN.
<code>state</code> <code>&lt;enable   disable&gt;</code>	Indicates the current state (enable or disable) of PGM on the selected VLAN.
<code>nak-re-xmit-int</code> <code>&lt;integer&gt;</code>	Specifies how long to wait for an NCF (in milliseconds) before retransmitting the NAK. The default value is 1000 milliseconds.
<code>max-nak-re-xmit-cnt</code> <code>&lt;integer&gt;</code>	Configures the maximum number of NAK retransmission packets allowed per second. The default value is 2.
<code>max-nak-rdata-int</code> <code>&lt;integer&gt;</code>	Specifies how long to wait for RDATA (in milliseconds) after receiving an NCF. The default value is 10000 milliseconds.
<code>nak-eliminate-int</code> <code>&lt;integer&gt;</code>	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 <code>max-nak-rdata-int</code> . 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  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:

Topic	Page
<a href="#">Roadmap of multicast route commands</a>	478
<a href="#">Displaying multicast routes</a>	480
<a href="#">Showing a multicast route's next hop</a>	480
<a href="#">Showing multicast route information</a>	481
<a href="#">Configuring a multicast route on an interface</a>	481
<a href="#">Showing multicast routes on an interface</a>	482
<a href="#">Configuring multicast static source groups</a>	483
<a href="#">Showing DVMRP troubleshooting information</a>	488
<a href="#">Showing DVMRP troubleshooting information</a>	488
<a href="#">Configuring IP multicast software forwarding</a>	491
<a href="#">Showing the software forwarding configuration</a>	492
<a href="#">Configuring the resource usage counter for multicast streams</a>	493
<a href="#">Showing the hardware resource usage output</a>	495
<a href="#">Displaying all IP mroute show commands</a>	496

## 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 496](#).

Use this list as a quick reference or click on any entry for more information:

Command	Parameter
<code>config ip mroute</code>	<code>info</code>
<code>config ip mroute interface &lt;ipaddr&gt;</code>	<code>info</code> <code>ttl &lt;ttl&gt;</code>
<code>config ip mroute static-source-group &lt;GroupSubnet&gt;</code>	<code>info</code> <code>create &lt;SourceSubnet&gt;</code> <code>&lt;SrcSubnetMask&gt;</code> <code>delete &lt;SourceSubnet&gt;</code> <code>&lt;SrcSubnetMask&gt;</code>
<code>config sys mcast-software-forwarding</code>	<code>info</code> <code>disable</code> <code>enable</code>
<code>show ip mroute interface</code>	
<code>show ip mroute next-hop</code>	
<code>show ip mroute route</code>	
<code>show ip mroute static-source-group [&lt;GroupAddress&gt;]</code>	

Command	Parameter
<code>show ip mroute-hw group-trace</code>	
<code>show ip mroute-hw group-prune-state</code>	
<code>show sys mcast-software-forwarding</code>	
<code>config ip mroute resource-usage</code>	<code>info</code> <code>egress-Threshold &lt;integer&gt;</code> <code>ingress-Threshold &lt;integer&gt;</code> <code>send-Trap-And-Log &lt;enable disable&gt;</code> <code>trap-Msg-Only &lt;enable disable&gt;</code> <code>log-Msg-Only &lt;enable disable&gt;</code>
<code>show ip mroute-hw resource-usage</code>	
<code>show ip mroute show-all [file &lt;value&gt;]</code>	

## 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:

<b>config ip mroute</b>	
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:

<b>config ip mroute interface &lt;ipaddr&gt;</b>	
followed by:	
<code>info</code>	Displays information about the multicast route interface.
<code>ttl &lt;ttl&gt;</code>	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 349.](#)
- PIM Sparse Mode (SM) - To globally enable PIM-SM, refer to [“Configuring PIM-SM globally” on page 406.](#)
- PIM Source Specific Multicast mode (SSM) - To globally enable PIM-SSM, refer to [“Configuring Source Specific Multicast \(SSM\)” on page 444.](#)

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 306](#).

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:

<b>config ip mroute static-source-group &lt;GroupSubnet&gt;</b> followed by:	
<code>info</code>	Displays information about the source-group entry.
<code>create &lt;SourceSubnet&gt; &lt;SrcSubnetMask&gt;</code>	Creates a new static multicast source-group entry. You cannot create duplicate groups. <sup>1</sup> <ul style="list-style-type: none"> <li><i>SourceSubnet</i> 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 <a href="#">“Configuration considerations.”</a></li> <li><i>SrcSubnetMask</i> is the source’s subnet mask for this static source-group entry.</li> </ul>
<code>delete &lt;SourceSubnet&gt; &lt;SrcSubnetMask&gt;</code>	Deletes the source-group entry from the static source-group table.

<sup>1</sup> 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.

<b>show ip mroute-hw</b> followed by:	
<code>group-trace [src &lt;value&gt;] [grp &lt;value&gt;]</code>	<p>You use the <code>show ip mroute-hw group-trace</code> command as follows:</p> <ul style="list-style-type: none"> <li>• When you use it by itself, the output includes all the group entries found in the hardware records.</li> <li>• When you follow the command with <code>grp &lt;value&gt;</code>, the output includes all the entries corresponding to the specified Group Address (<a href="#">Figure 186</a>).</li> <li>• When you follow the command with <code>src &lt;value&gt;</code> and <code>grp &lt;value&gt;</code>, the output includes only the specified Source-Group pair (<a href="#">Figure 187</a>).</li> </ul>
<code>group-prune-state [grp &lt;value&gt;]</code>	<p>You use the <code>show ip mroute-hw group-prune-state</code> command as follows:</p> <ul style="list-style-type: none"> <li>• When you use it by itself, the output includes all the group entries found in the hardware records.</li> <li>• When you follow the command with <code>grp &lt;value&gt;</code>, the output includes all the entries corresponding to the specified Group Address (<a href="#">Figure 188</a>).</li> </ul>

**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 83 describes the output fields that appear in Figure 186, Figure 187, and Figure 188.

**Table 83** 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. <b>Note:</b> 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:

<b>config sys mcast-software-forwarding</b> followed by:	
info	Displays the current <code>config sys mcast-software-forwarding</code> 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:

<b>config ip mroute resource-usage</b> followed by:	
<code>info</code>	Displays the record usage counter's current configuration.
<code>egress-Threshold</code> <code>&lt;integer&gt;</code>	Sets the egress record threshold (S,G). A notification message is sent if this value is exceeded. <i>integer</i> is a value between 0 and 32767.
<code>ingress-Threshold</code> <code>&lt;integer&gt;</code>	Sets the ingress record threshold (peps). A notification message is sent if this value is exceeded. <i>integer</i> is a value between 0 and 32767.
<code>send-Trap-And-Log</code> <code>&lt;enable disable&gt;</code>	Sets the notification method to sending both a trap message and a log message when the threshold level is exceeded. <sup>1</sup>

<b>config ip mroute resource-usage</b> 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 VLANs, Spanning Tree, and Link Aggregation*.

This chapter includes the following topics:

Topic	Page
<a href="#">Roadmap of multicast MLT commands</a>	498
<a href="#">Configuring multicast flow distribution globally</a>	499
<a href="#">Configuring multicast flow distribution per MLT</a>	501
<a href="#">Showing the multicast MLT distribution show command</a>	502

## 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:

<b>Command</b>	<b>Parameter</b>
<code>config sys mcast-mlt-distribution</code>	<code>info</code> <code>enable</code> <code>disable</code> <code>grp-mask &lt;grp-mask&gt;</code> <code>src-mask &lt;src-mask&gt;</code> <code>redistribution &lt;enable disable&gt;</code>
<code>config mlt &lt;mltid&gt;</code> <code>mcast-distribution</code>	<code>enable</code>  <code>disable</code>
<code>show sys mcast-mlt-distribution</code>	

## 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:

<b>config sys mcast-mlt-distribution</b> 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 <i>grp-mask</i> and <i>src-mask</i> 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:

<b>config mlt &lt;mltid&gt; mcast-distribution</b> 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:

Topic	Page
<a href="#">Roadmap of multicast MAC filtering commands</a>	504
<a href="#">Configuring Layer 2 multicast MAC filtering</a>	505
<a href="#">Configuring Layer 3 multicast MAC filtering</a>	507
<a href="#">Showing the Layer 2 multicast MAC filters</a>	509
<a href="#">Showing the Layer 3 multicast MAC ARP data</a>	510
<a href="#">Showing VLAN port data</a>	511
<a href="#">Showing the multicast VLAN information</a>	512

## 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
<code>config vlan &lt;vid&gt; static-mcastmac</code>	<code>info</code> <code>add mac &lt;value&gt; [port &lt;value&gt;] [mlt &lt;value&gt;]</code> <code>add-mlt &lt;mid&gt; mac &lt;value&gt;</code> <code>add-ports &lt;ports&gt; mac &lt;value&gt;</code> <code>delete mac &lt;value&gt;</code> <code>delete-mlt &lt;mid&gt; mac &lt;value&gt;</code> <code>delete-ports &lt;ports&gt; mac &lt;value&gt;</code>
<code>config ip arp static-mcastmac</code>	<code>info</code> <code>add mac &lt;value&gt; ip &lt;value&gt; vlan &lt;value&gt; [port &lt;value&gt;] [mlt &lt;value&gt;]</code> <code>delete &lt;ipaddr&gt;</code>
<code>show vlan info static-mcastmac &lt;vid&gt;</code>	
<code>show ip arp static-mcastmac</code>	
<code>show vlan info ports &lt;vid&gt;</code>	
<code>show vlan info all &lt;vid&gt; [by &lt;value&gt;]</code>	

## 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:

<b>config vlan &lt;vid&gt; static-mcastmac</b>	
followed by:	
info	Displays current settings.
add mac <value> [port <value>] [mlt <value>]	Adds VLAN static multicast MAC entries, where: <ul style="list-style-type: none"> <li>• mac &lt;value&gt; is the MAC address.<sup>1</sup></li> <li>• port &lt;value&gt; is the port to receive the multicast flooding.</li> <li>• mlt &lt;value&gt; is the MID.</li> </ul>
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.

<sup>1</sup> 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:

<b>config ip arp static-mcastmac</b>	
followed by:	
info	Displays current settings.
add mac <value> ip <value> vlan <value> [port <value>] [mlt <value>]	Adds static multicast MAC entries, where: <ul style="list-style-type: none"> <li>• mac &lt;value&gt; is the MAC address.<sup>1</sup></li> <li>• ip &lt;value&gt; is the IP address.</li> <li>• vlan &lt;value&gt; is the VLAN ID number.</li> <li>• port &lt;value&gt; is the port to receive the multicast flooding.</li> <li>• mlt &lt;value&gt; is the MID.</li> </ul>
delete <ipaddr>	Deletes static multicast MAC entries.

<sup>1</sup> 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

---

## A

accounting  
  enabling 102  
acronyms 31  
activity check interval 407  
authentication  
  enabling 102  
Auto-RP 68

## B

bootstrap router 69  
broadcast 35, 52  
BSR, configuring 199  
BSR, viewing 210

## C

candidate bootstrap router 69  
candidate RP router 68  
C-BSR, configuring a port with the CLI 428  
C-BSR, configuring a VLAN with the CLI 433  
C-BSR, configuring an interface with the CLI 415  
C-BSR, configuring with Device Manager 199  
C-BSR, setting a preference with Device Manager 198  
C-BSR, setting a preference with the CLI 415, 429, 433  
Cisco Auto-RP 68  
config ip commands 370, 378  
config ip igmp interface commands 285, 306, 309

config ip route-policy seq command 370, 378  
config sys mcast-software-forwarding info  
  command output 492  
config vlan ip igmp commands 320  
configuring IP multicast software forwarding  
  using the CLI 491  
    config sys mcast-software-forwarding  
      command 491  
    show sys mcast-software-forwarding  
      command 492  
  using the DM 258  
conventions, text 30  
C-RP  
  configuring 208  
customer support 32

## D

designated router. *See* DR  
Distance Vector Multicast Routing Protocol. *See* DVMRP  
distribution tree 34  
DLR (designated local repairer) 217  
DR  
  (designated router), describing 67  
DVMRP 52  
  broadcast 52  
  configuration prerequisites 140, 348  
  description 343  
  enabling a port 143  
  enabling a VLAN 146  
  enabling globally 141, 349  
  IGMP host membership 65

- IP subnet-based VLAN 64
- leaf network 56
- metric cost 144, 147
- multicast tree 53
- neighbors 54, 152
- next hops 154
- port-based VLAN 64
- prune 52
- reports 54
- reverse path forwarding 53
- route metric 55
- route selection 55
- routes 153
- routing table 53, 55
- shortest-path tree 56
- source distribution tree 52
- source networks 52, 54
- source route advertisement 54
- upstream neighbor 55
- DVMRP CLI commands
  - config ethernet ip dvmrp 357
  - config ip dvmrp 349
  - config ip dvmrp interface 352
  - config vlan ip dvmrp 359
  - roadmap of all commands 344
  - show ip dvmrp info 353
  - show ip dvmrp interface 393
  - show ip dvmrp neighbor 354
  - show ip dvmrp next-hop 355
  - show ip dvmrp route 356
  - show ports info dvmrp 394
  - show vlan info dvmrp 394
- DVMRP Device Manager commands
  - Capabilities 153
  - ExpiryTime 152
  - GenerationId 143, 152
  - LeafTimeOut 142
  - MajorVersion 152
  - MinorVersion 152
  - NbrProbeInterval 142
  - NbrTimeOut 142
  - NumRoutes 143
  - ReachableRoutes 143
  - State 153
  - TriggeredUpdateInterval 142
  - Type (leaf or branch) 155
  - UpdateInterval 142
  - UpstreamNeighbor 154
  - VersionString 142
- DVMRP troubleshooting
  - using the CLI
    - show ip mroute-hw group trace (usage) 488
    - show ip mroute-hw group-prune-state (usage) 488
- DVMRP troubleshooting, Mroute-HW tab 253
- F**
  - fast leave mode 41
  - fast-leave mode, IGMP 313
- H**
  - host addresses and masks, specifying 49
  - host group 36
- I**
  - ID field 117, 162
  - IfIndex field
    - DVMRP Interfaces tab 150
  - IGAP
    - enabling 102
  - IGAP CLI commands
    - config ip igmp interface igap configuration example 486, 494
  - IGAP Device Manager fields
    - AccntEnable 102
    - AuthEnable 102
    - IgapEnable 102
  - IGMP 37
    - cache information 104
    - configuration prerequisites 94, 284
    - description 39
    - DVMRP 65

- electd querier 39
  - fast leave feature 41
  - host leave message 41
  - host reports 40
  - interface table 106
  - maximum response time 40
  - Multicast Router Discovery Protocol 51
  - multicast stream limitation 129, 332
  - PIM-SSM 214
  - proxy 43
  - queries 39, 42
  - router alert option 94, 284
  - snoop 43
  - snooping 42, 43, 51, 94, 103
  - static entry 114
  - stream limitation members 131
  - versions 44
- IGMP CLI commands**
- config ethernet ip igmp 313
  - config ethernet ip igmp access-control 317
  - config ethernet ip igmp access-control
    - configuration example 318
  - config ethernet ip igmp stream-limit 337
  - config ip igmp info 275
  - config ip igmp interface access-control 296
  - config ip igmp interface access-control
    - configuration example 298
  - config ip igmp interface mrdisc 300
  - config ip igmp interface static-members 303
  - config ip igmp interface stream-limit 332
  - config ip igmp interface
    - stream-limit-member 334
  - config vlan ip igmp access-control 325
  - config vlan ip igmp access-control configuration example 327
  - config vlan ip igmp fast-leave-members 331
  - config vlan ip igmp mrdisc 328
  - config vlan ip igmp static-members 329
  - config vlan ip igmp stream-limit 338
  - config vlan ip igmp stream-limit-members 339
  - roadmap of all commands 277
  - show ip igmp access 299
  - show ip igmp cache 290
  - show ip igmp group 290
  - show ip igmp interface 288
  - show ip igmp mrdisc 302
  - show ip igmp mrdisc-neighbors 302
  - show ip igmp router-alert 291
  - show ip igmp sender 291
  - show ip igmp snoop 292
  - show ip igmp static 304
  - show ip igmp stream-limit-interface 335
  - show ip igmp stream-limit-port 336
  - show ports info igmp 308, 311, 315
  - show vlan info igmp 324
- IGMP Device Manager commands**
- AcctEnable 102
  - AuthEnable 102
  - Current Number Of Stream 130, 135, 138
  - DiscoveredRouterPorts 109
  - FastLeaveEnable 103
  - FastLeavePortMembers 103
  - FlushAction 108
  - IfIndex 131
  - IgapEnable 102
  - Interface 130
  - Join messages 107
  - LastMembQueryIntvl 102, 108
  - LastReporter 105
  - MaxAdvertiseInterval 110
  - Maximum Number Of Stream 130, 135, 138
  - MaxInitialAdvertisements 110
  - MaxInitialAdvertisementInterval 110
  - MaxStreams 131
  - MinAdvertiseInterval 110
  - MrdiscEnable 109
  - NeighborDeadInterval 110
  - NotAllowedToJoin 115
  - NumStreams 131
  - OtherQuerierPresentTimeout 108
  - Port 131
  - ProxySnoopEnable 102
  - QueryInterval 102
  - QueryMaxResponseTime 102
  - Robustness 102
  - RouterAlertEnable 108
  - SnoopEnable 102
  - SnoopMRouterPorts 103

- SsmSnoopEnable 102
- Stream Limit Enable 130
- StreamLimitEnable 135, 138
- Version 103
- Version1Host Timer 105
- WrongVersionQueries 107

IGMP snoop commands 286

IGMPv1

- description 44
- host reports 40

IGMPv2

- control packets 94, 284
- description 44
- host reports 40

IGMPv3

- description 44
- host reports 40

Internet Group Management Protocol. *See* IGMP

IP commands

- configure 370, 378

IP multicast software forwarding

- default setting 258, 491
- hardware considerations 258, 491

## L

- leaf timeout, DVMRP 349
- local router interface, DVMRP 352
- LocalAddress field 144, 148, 150

## M

MAC filtering

- configuration command 92
- configuring Layer 2 multicast 270, 505
- configuring Layer 3 multicast 272, 507
- creating VLANs 91
- defining a flooding domain 91
- description 91, 269, 503
- Layer 2, description 91
- Layer 3, description 91
- max number of MAC addresses 91

MAC filtering CLI commands

- config ip arp static-mcastmac 507
- config ip arp static-mcastmac configuration example 508
- config vlan static-mcastmac 505
- config vlan static-mcastmac configuration example 506
- roadmap of all commands 504
- show ip arp static-mcastmac 510
- show vlan info all 512
- show vlan info ports 511
- show vlan info static-mcastmac 509

MAC filtering configuration example 506, 508

MAC filtering Device Manager commands

- Address 272
- ForwardingPorts 272
- IPAddress 273
- MacAddress 273
- MltIDs 274
- MltIds 272
- Ports 274
- VlanID 273

MaskLenFrom field 117, 162

MaskLenUpto field 117, 162

MatchInterface field 165

MatchMetric field 164

MatchProtocol field 164

MatchRouteType field 165

Metric field

- DVMRP Interfaces tab 145, 148, 151

MLT

- description 87, 261, 497
- distribution algorithm 87
- E-module support 87
- enabling multicast flow distribution globally 262, 499
- enabling multicast flow distribution per MLT 265, 501

MLT CLI commands

- config mlt mcast-distribution 501
- config sys mcast-mlt-distribution 499

- config sys mcast-mlt-distribution configuration
    - example 499
    - roadmap of all commands 498
    - show sys mcast-mlt-distribution 502
  - MLT configuration example 499
  - MLT Device Manager commands
    - MltType 267
    - MulticastDistribution 267
    - PortMembers 267
    - PortType 267
    - RedistributionEnable 265
    - SmltId 267
    - SvlanPortType 267
    - VlanIds 267
  - multicast
    - address range 37
    - broadcast 35
    - class D address 37
    - distribution tree 34
    - DVMRP 52
    - E-module support for MLT 87
    - flow distribution over MLT 87
    - flow distribution over MLT configuration
      - command 90
    - flow distribution over MLT configuration example 88
    - flow distribution over MLT traffic
      - redistribution 89
    - IGMP 37
    - interfaces 247
    - MAC filtering 91
    - MLT distribution algorithm 87
    - next hops 245
    - permanent host group 36
    - PGM 84
    - PGM terms 85
    - PIM-SM 65
    - PIM-SM domain 66
    - PIM-SM hosts 66
    - prune 35
    - reverse path 35
    - routes 244
    - static source group 248, 483
    - stream 114
    - transient host group 36
  - multicast access control
    - configuring
      - using Device Manager 116, 118
    - configuring on IGMP Ethernet port
      - using the CLI 317
    - configuring on IGMP interface
      - using the CLI 296
    - configuring on VLAN
      - using the CLI 325
    - displaying control groups 299
    - overview of 44
    - policy types
      - allow-only-both 49
      - allow-only-rx 49
      - allow-only-tx 48
      - deny-both 48
      - deny-rx 47
      - deny-tx 46
    - tab fields 120
  - multicast border router 66
  - Multicast CLI commands
    - config ip igmp fast-leave-mode 293
    - config ip mroute 480
    - config ip mroute interface 481
    - config ip mroute static-source-group 485
    - roadmap of all commands 478
    - show ip igmp info 295
    - show ip mroute interface 482
    - show ip mroute next-hop 480
    - show ip mroute route 481
    - show ip mroute static-source-group 487
  - Multicast Device Manager commands
    - ClosestMemberHops 246
    - ExpiryTime 245
    - Group 244
    - Interface 244
    - multipleUser 98
    - oneUser 98
    - Protocol 245
    - Source 244
    - SourceMask 244
-

- static source group 248, 483
- UpstreamNeighbor 244
- Multicast dialog box- Mcast SW Forwarding tab 258
- Multicast dialog box- Mroute-HW tab 254
- Multicast dialog box- Mroute-HW tab- Egress VLANs tab 257
- Multicast dialog box- Mroute-HW tab- Prunes tab 255
- Multicast dialog box- Mroute-HW tab- Sources tab 256
- multicast flow distribution over MLT. *See* MLT
- multicast MAC filtering. *See* MAC filtering
- multicast route discovery 300, 328
- Multicast Router Discovery Protocol 51
- multicast stream limitation
  - adding a member 132
  - deleting a member 133
  - description 50
  - using Device Manager 129
  - using the CLI 332
- multicast stream limitation members
  - using Device Manager 131

## N

- Name field 117, 162
- neighbor timeout, DVMRP 349

## P

- passive interface, PIM 82

### PGM

- as a DLR 217
- configuration prerequisites 218, 454
- description 84, 217, 451
- designated local repairers (DLRs) 86
- DVMRP 218, 454
- editing interface parameters 226
- enabling globally 219, 455
- enabling on a VLAN 223

- enabling on an interface 221
- graphing interface statistics 227
- graphing session statistics 234
- IGMP snooping 218, 454
- NAK confirmations (NCFs) 86
- negative acknowledgements (NAKs) 85
- PIM-SM 218, 454
- source path messages (SPMs) 85
- terms 85
- transport session identifiers (TSIs) 85
- viewing retransmit parameters 240
- viewing session parameters 233

### PGM CLI commands

- config ethernet ip pgm 472
- config ip pgm 455
- config ip pgm interface 463
- config vlan ip pgm 474
- roadmap of all commands 452
- show ip pgm global 456
- show ip pgm interface config 464
- show ip pgm interface error general 466
- show ip pgm interface error nak 467
- show ip pgm interface stat general 468
- show ip pgm interface stat nak 470
- show ip pgm interface stat parity 471
- show ip pgm retransmit 458
- show ip pgm session 459

### PGM Device Manager commands

- LeadEdgeSeq 234
- MaxNakRate 220
- MaxNakReXmitRate 222
- MaxReXmitStates 220
- MaxSessions 220
- NAK 232
- NakEliminateInterval 222
- NakRdataInterval 222
- NakReXmitInterval 222
- NCF 232
- NNAK 232
- NnakGenerate 220
- RDATA 229
- SessionLifeTime 220
- SPM 229

- TotalReXmitStates 220
  - TotalReXmitStatesTimedOut 220
  - TotalSessions 220
  - TotalUniqueNaks 220
  - TotalUniqueParityNaks 220
  - TrailEdgeSeq 234
  - UpstreamAddress 234
  - UpstreamIfCct 234
- PIM**
- active interface 82
  - activity check interval 407
  - changing on a VLAN interface type 202
  - changing the interface type 198
  - changing the interface type using the CLI 428
  - changing the VLAN interface type using the CLI 431
  - configuring on a brouter port using the CLI 427
  - configuring on a VLAN using the CLI 429
  - configuring on an interface using the CLI 410
- C-RP**
- configuring 208
- debug messages** 434
- DR**
- showing 204
- enabling on a brouter port using Device Manager 197
- enabling on a VLAN using Device Manager 200
- neighbor parameters 206
- passive interface 82
- showing interface information 411
- viewing and editing interface parameters using Device Manager 203
- viewing current BSR 210
- viewing RP Set parameters 207
- PIM CLI commands**
- config ethernet ip pim 427
  - config ip pim candrp 416
  - config ip pim debug-pimmsg 434
  - config ip pim interface 410
  - config ip pim static-rp 424
  - config ip pim static-rp configuration example 425
  - config vlan ip pim 429
  - show ip pim active-rp 419
  - show ip pim bsr 421
  - show ip pim candidate-rp 418
  - show ip pim info 408
  - show ip pim interface 411, 431
  - show ip pim mroute 422
  - show ip pim neighbor 414
  - show ip pim rp-set 417
  - show ip pim static-rp 426
- PIM Device Manager commands**
- CBSRPreference 198
  - Component 208
- DR**
- showing 204
- ExpiryTime 206
- HelloInterval 198
- HoldTime 208
- UpTime 206
- PIM-SM**
- BSR**
- (bootstrap router), description 69
  - configuring 199
- C-BSR**
- (candidate bootstrap router), description 69
  - configuring 199
- Cisco Auto-RP 68
- configuration prerequisites 189
- C-RP**
- (candidate RP), description 68
  - description 65, 399
  - domain 66
- DR**
- (designated router), description 67
- DVMRP, configuring with 140, 189, 348, 405
- enabling globally 190, 406
- enabling static RP 194
- hosts 66
- IGMP, configuring with 190
- join/prune messages 69
- MBR**
- configuring 409
- OSPF, configuring with 189

**PMBR**

(PIM Multicast Border Router),

description 66

configuring 409

receiver join process 72

receiver leave process 72

register messages 70

register-stop messages 70

required elements 73

Reverse Path Forwarding 189

RIP, configuring with 189

**RP**

(rendezvous-point), description 67

shared tree 70

shortest-path tree 70

source sending packets to group 72

static RP router 68

**PIM-SM CLI commands**

config ip pim 406

config ip pim mbr 409

roadmap of all commands 401

**PIM-SSM**

configuration example using the CLI 448

configuring 211

description 211

enabling globally 212

enabling globally with the CLI 446

IGMPv3 214, 446

**PMBR 66**

Pragmatic General Multicast. *See* PGM

Prefix field 117, 162

prefix lists

configuring 116

PrefixMaskLen field 117, 162

product support 32

Protocol Independent Multicast-Sparse Mode. *See*  
PIM-SM

proxy-snoop option, IGMP 321

prune 35, 52

publications

hard copy 32

**R**

rendezvous-point router 67

resource usage

using Device Manager 259

using the CLI 493

Reverse Path Forwarding 189

reverse path multicast 35

router alert option 94, 284

router update messages, DVMRP 349

RP Set parameters 207

**S**

shortest-path tree 56

show ip dvmrp show-all command 396

show ip igmp show-all command 342

show ip mroute show-all command 496

show ip mroute-hw group trace grp command  
output 489

show ip mroute-hw group-prune-state grp  
command output 489

show ip mroute-hw group-trace src grp command  
output 489

show ip pgm show-all command 476

show ip pim show-all command 448

show sys mcast-software-forwarding command  
output 492

snoop option, IGMP 321

source distribution tree 52

static RP

active RP election algorithm 194

configuration considerations 193

configuration example 425

configuring with the CLI 424

description 193

enabling 194

static RP router 68

static source group

- adding a new group 251
- configuration considerations 248, 483
- definition 248, 483
- deleting a group 252
  - SSM channel conflict 249, 484
- stream limitation 50, 129, 332
- stream limitation members 131
- support, Nortel Networks 32

## T

- technical publications 32
- technical support 32
- text conventions 30
- time-to-live, multicast 481

## V

- VLAN
  - DVMRP 64

