IP Multicast: PIM Configuration Guide

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2017 Cisco Systems, Inc. All rights reserved.

CONTENTS

CHAPTER 1 **Read Me First** 1

CHAPTER 2 **IP Multicast Technology Overview** 3

- Finding Feature Information 3
- Information About IP Multicast Technology 4
  - Role of IP Multicast in Information Delivery 4
  - Multicast Group Transmission Scheme 4
  - IP Multicast Routing Protocols 6
  - IP Multicast Group Addressing 8
    - IP Class D Addresses 8
  - IP Multicast Address Scoping 8
  - Layer 2 Multicast Addresses 10
  - IP Multicast Delivery Modes 10
    - Any Source Multicast 10
    - Source Specific Multicast 11
  - Protocol Independent Multicast Overview 11
    - PIM Dense Mode 11
    - PIM Sparse Mode 12
    - Sparse-Dense Mode 13
    - Bidirectional PIM 13
  - Multicast Group Modes 14
    - Bidirectional Mode 14
    - Sparse Mode 14
    - Dense Mode 14
  - Rendezvous Points 15
    - Auto-RP 15
    - Sparse-Dense Mode for Auto-RP 16
    - Bootstrap Router 16

Multicast Source Discovery Protocol 16
Anycast RP 17
Multicast Forwarding 18
Multicast Distribution Source Tree 18
Multicast Distribution Shared Tree 19
Source Tree Advantage 19
Shared Tree Advantage 20
Reverse Path Forwarding 20
RPF Check 21
PIM Dense Mode Fallback 22
Guidelines for Choosing a PIM Mode 23
Where to Go Next 23
Additional References 24
Feature Information for IP Multicast Technology Overview 25
Glossary 25

CHAPTER 3 **Configuring Basic IP Multicast** 29
Finding Feature Information 29
Prerequisites for Configuring Basic IP Multicast 29
Information About Configuring Basic IP Multicast 30
Auto-RP Overview 30
The Role of Auto-RP in a PIM Network 30
IP Multicast Boundary 30
Benefits of Auto-RP in a PIM Network 31
Anycast RP Overview 31
BSR Overview 32
BSR Election and Functionality 32
BSR Border Interface 32
Static RP Overview 32
SSM Overview 33
SSM Components 33
How SSM Differs from Internet Standard Multicast 33
SSM Operations 34
IGMPv3 Host Signaling 35
Benefits of Source Specific Multicast 35

Bidir-PIM Overview 36
Multicast Group Modes 36
Bidirectional Shared Tree 36
DF Election 38
Bidirectional Group Tree Building 38
Packet Forwarding 38
Benefits of Bidirectional PIM 39
How to Configure Basic IP Multicast 39
Configuring Sparse Mode with Auto-RP(CLI) 39
What to Do Next 44
Configuring Sparse Mode with Anycast RP 44
What to Do Next 47
Configuring Sparse Mode with a Bootstrap Router 47
What to Do Next 52
Configuring Sparse Mode with a Single Static RP(CLI) 52
What to Do Next 54
Configuring Source Specific Multicast 54
What to Do Next 56
Configuring Bidirectional PIM 57
Configuration Examples for Basic IP Multicast 59
Example: Sparse Mode with Auto-RP 59
Sparse Mode with Anycast RP Example 59
Sparse Mode with Bootstrap Router Example 61
BSR and RFC 2362 Interoperable Candidate RP Example 61
Example: Sparse Mode with a Single Static RP 62
SSM with IGMPv3 Example 63
SSM Filtering Example 63
Bidir-PIM Example 63
Additional References 64
Feature Information for Configuring Basic IP Multicast in IPv4 Networks 65

CHAPTER 4 **Configuring Basic IP Multicast in IPv6 Networks 69**
Finding Feature Information 69
Prerequisites for Configuring Basic IP Multicast 69
Information About Configuring Basic IP Multicast in IPv6 Networks 70

IPv6 Multicast 70
IPv6 Multicast Overview 70
IPv6 Multicast Addressing 70
IPv6 Multicast Groups 72
IPv6 Multicast Address Group Range Support 72
Scoped Address Architecture 72
MRIB 73
IPv6 Multicast Process Switching and Fast Switching 73
IPv6 Anycast RP Solution 74
PIMv6 Anycast RP Solution Overview 74
PIMv6 Anycast RP Normal Operation 74
PIMv6 Anycast RP Failover 75
IPv6 BSR 76
IPv6 BSR 76
IPv6 BSR: Configure RP Mapping 76
IPv6 BSR: Scoped Zone Support 77
IPv6 Multicast: RPF Flooding of BSR Packets 77
IPv6 Multicast Groups 77
IPv6 Multicast Address Group Range Support 78
How to Configure Basic IP Multicast in IPv6 Networks 78
Enabling IPv6 Multicast Routing 78
Disabling the Device from Receiving Unauthenticated Multicast Traffic 79
Troubleshooting IPv6 Multicast 80
Configuring PIMv6 Anycast RP 82
Configuring a BSR and Verifying BSR Information 85
Sending PIM RP Advertisements to the BSR 86
Configuring BSR for Use Within Scoped Zones 87
Configuring BSR Devices to Announce Scope-to-RP Mappings 89
Configuration Examples for Configuring IP Multicast Basic in IPv6 Networks 90
Example: Enabling IPv6 Multicast Routing 90
Examples: Disabling IPv6 Multicast Address Group Range Support 90
Example: Verifying IPv6 MRIB Information 90
Example: Configuring PIMv6 Anycast RP 91
Example: Configuring a BSR 91
Additional References 91

Feature Information for Configuring Basic IP Multicast in IPv6 Networks 92

CHAPTER 5 **Using MSDP to Interconnect Multiple PIM-SM Domains 97**

Finding Feature Information 97

Prerequisites for MSDP 97

Information About Using MSDP to Interconnect Multiple PIM-SM Domains 98

Benefits of Using MSDP to Interconnect Multiple PIM-SM Domains 98

Use of MSDP to Interconnect Multiple PIM-SM Domains 98

MSDP Message Types 100

SA Messages 101

SA Request Messages 101

SA Response Messages 101

Keepalive Messages 101

SA Message Origination Receipt and Processing 101

SA Message Origination 101

SA Message Receipt 102

How RPF Check Rules Are Applied to SA Messages 102

How the Software Determines the Rule to Apply to RPF Checks 102

Rule 1 of RPF Checking of SA Messages in MSDP 103

Implications of Rule 1 of RPF Checking on MSDP 103

Rule 2 of RPF Checking of SA Messages in MSDP 103

Implications of Rule 2 of RPF Checking on MSDP 104

Rule 3 of RPF Checking of SA Messages in MSDP 104

SA Message Processing 104

MSDP Peers 105

MSDP MD5 Password Authentication 105

How MSDP MD5 Password Authentication Works 105

Benefits of MSDP MD5 Password Authentication 105

SA Message Limits 105

MSDP Keepalive and Hold-Time Intervals 106

MSDP Connection-Retry Interval 106

MSDP Compliance with IETF RFC 3618 106

Benefits of MSDP Compliance with RFC 3618 107

Default MSDP Peers 107

MSDP Mesh Groups 108

Benefits of MSDP Mesh Groups 109
SA Origination Filters 109
Use of Outgoing Filter Lists in MSDP 109
Use of Incoming Filter Lists in MSDP 110
TTL Thresholds in MSDP 111
SA Request Messages 111
SA Request Filters 112
MSDP MIB 112
How to Use MSDP to Interconnect Multiple PIM-SM Domains 112
Configuring an MSDP Peer 112
Shutting Down an MSDP Peer 114
Configuring MSDP MD5 Password Authentication Between MSDP Peers 115
Troubleshooting Tips 116
Preventing DoS Attacks by Limiting the Number of SA Messages Allowed in the SA Cache from Specified MSDP Peers 116
Adjusting the MSDP Keepalive and Hold-Time Intervals 118
Adjusting the MSDP Connection-Retry Interval 119
Configuring MSDP Compliance with IETF RFC 3618 120
Configuring a Default MSDP Peer 121
Configuring an MSDP Mesh Group 122
Controlling SA Messages Originated by an RP for Local Sources 123
Controlling the Forwarding of SA Messages to MSDP Peers Using Outgoing Filter Lists 124
Controlling the Receipt of SA Messages from MSDP Peers Using Incoming Filter Lists 125
Using TTL Thresholds to Limit the Multicast Data Sent in SA Messages 127
Requesting Source Information from MSDP Peers 128
Controlling the Response to Outgoing SA Request Messages from MSDP Peers Using SA Request Filters 129
Including a Bordering PIM Dense Mode Region in MSDP 130
Configuring an Originating Address Other Than the RP Address 131
Monitoring MSDP 132
Clearing MSDP Connections Statistics and SA Cache Entries 134
Enabling SNMP Monitoring of MSDP 135
Troubleshooting Tips 137
Configuration Examples for Using MSDP to Interconnect Multiple PIM-SM Domains 137

Example: Configuring an MSDP Peer 137
Example: Configuring MSDP MD5 Password Authentication 137
Configuring MSDP Compliance with IETF RFC 3618 Example 138
Configuring a Default MSDP Peer Example 138
Example: Configuring MSDP Mesh Groups 140
Additional References 140
Feature Information for Using MSDP to Interconnect Multiple PIM-SM Domains 141

CHAPTER 6 **PIM Allow RP** 145
Finding Feature Information 145
Restrictions for PIM Allow RP 145
Information About PIM Allow RP 146
Rendezvous Points 146
PIM Allow RP 146
How to Configure PIM Allow RP 147
Configuring RPs for PIM-SM 147
Enabling PIM Allow RP 150
Displaying Information About PIM-SM and RPs 151
Configuration Examples for PIM Allow RP 152
Example: IPv4 PIM Allow RP 152
Example: IPv6 PIM Allow RP 153
Additional References for PIM Allow RP 154
Feature Information for PIM Allow RP 155

CHAPTER 7 **Configuring Source Specific Multicast** 157
Finding Feature Information 157
Restrictions for Source Specific Multicast 157
Information About Source Specific Multicast 159
SSM Overview 159
SSM Components Overview 159
How SSM Differs from Internet Standard Multicast 160
SSM Operations 160
IGMPv3 Host Signaling 161
Benefits of SSM 161
IGMP v3lite Host Signalling 162

URD Host Signalling 163
How to Configure Source Specific Multicast 165
Configuring SSM 165
Monitoring SSM 166
Configuration Examples of Source Specific Multicast 166
SSM with IGMPv3 Example 166
SSM with IGMP v3lite and URD Example 167
SSM Filtering Example 167
Additional References 167
Feature Information for Source Specific Multicast 169

CHAPTER 8 **Tunneling to Connect Non-IP Multicast Areas 171**
Finding Feature Information 171
Prerequisites for Tunneling to Connect Non-IP Multicast Areas 171
Information About Tunneling to Connect Non-IP Multicast Areas 172
Benefits of Tunneling to Connect Non-IP Multicast Areas 172
IP Multicast Static Route 172
How to Connect Non-IP Multicast Areas 173
Configuring a Tunnel to Connect Non-IP Multicast Areas 173
Configuration Examples for Tunneling to Connect Non-IP Multicast Areas 175
Tunneling to Connect Non-IP Multicast Areas Example 175
Additional References 178
Feature Information for Tunneling to Connect Non-IP Multicast Areas 179

CHAPTER 9 **Automatic Multicast Tunneling 181**
Finding Feature Information 181
Restrictions for Automatic Multicast Tunneling 181
Information About Automatic Multicast Tunneling 182
Overview 182
Automatic Multicast Tunneling Message Exchanges 182
AMT Tunnel and Traffic Types 183
Advantages of Automatic Multicast Tunneling 183
Prerequisites for AMT 183
Configuration Recommendations for AMT 184
How to Configure Automatic Multicast Tunneling 184

Enabling and Configuring Automatic Multicast Tunneling on a Relay 184
Enabling and Configuring Automatic Multicast Tunneling on Gateway 187
Displaying and Verifying AMT Configuration 190
Displaying and Verifying AMT Relay Configuration 192
Displaying and Verifying AMT Gateway Configuration 195
Configuration Examples for Automatic Multicast Tunneling 197
Example: AMT Relay Configuration 197
Example: AMT Gateway Configuration 197
Additional References for Automatic Multicast Tunneling 198
Feature Information for Automatic Multicast Tunneling 198

CHAPTER 10 **BFD Support for Multicast (PIM)** 201
Restrictions for BFD Support for Multicast (PIM) 201
Information About BFD Support for Multicast (PIM) 201
PIM BFD 201
How to Configure BFD Support for Multicast (PIM) 202
Enabling BFD PIM on an Interface 202
Configuration Examples for BFD Support for Multicast (PIM) 204
Additional References for BFD Support for Multicast (PIM) 204
Feature Information for BFD Support for Multicast (PIM) 204

CHAPTER 11 **HSRP Aware PIM** 207
Finding Feature Information 207
Restrictions for HSRP Aware PIM 207
Information About HSRP Aware PIM 208
HSRP 208
HSRP Aware PIM 209
How to Configure HSRP Aware PIM 209
Configuring an HSRP Group on an Interface 209
Configuring PIM Redundancy 211
Configuration Examples for HSRP Aware PIM 212
Example: Configuring an HSRP Group on an Interface 212
Example: Configuring PIM Redundancy 213
Additional References for HSRP Aware PIM 213
Feature Information for HSRP Aware PIM 214

CHAPTER 12 VRRP Aware PIM 215

Finding Feature Information 215

Restrictions for VRRP Aware PIM 216

Information About VRRP Aware PIM 216

Overview of VRRP Aware PIM 216

How to Configure VRRP Aware PIM 217

Configuring VRRP Aware PIM 217

Configuration Examples for VRRP Aware PIM 219

Example: VRRP Aware PIM 219

Additional References for VRRP Aware PIM 219

Feature Information for VRRP Aware PIM 220

CHAPTER 13 Verifying IP Multicast Operation 221

Finding Feature Information 221

Prerequisites for Verifying IP Multicast Operation 221

Restrictions for Verifying IP Multicast Operation 222

Information About Verifying IP Multicast Operation 222

Guidelines for Verifying IP Multicast Operation in a PIM-SM and PIM-SSM Network Environment 222

Common Commands Used to Verify IP Multicast Operation on the Last Hop Router for PIM-SM and PIM-SSM 222

Common Commands Used to Verify IP Multicast Operation on Routers Along the SPT for PIM-SM and PIM-SSM 224

Common Commands Used to Verify IP Multicast Operation on the First Hop Router for PIM-SM and PIM-SSM 224

How to Verify IP Multicast Operation 225

Using PIM-Enabled Routers to Test IP Multicast Reachability 225

Configuring Routers to Respond to Multicast Pings 225

Pinging Routers Configured to Respond to Multicast Pings 226

Verifying IP Multicast Operation in a PIM-SM or a PIM-SSM Network 227

Verifying IP Multicast Operation on the Last Hop Router 227

Verifying IP Multicast on Routers Along the SPT 231

Verifying IP Multicast on the First Hop Router 232

Configuration Examples for Verifying IP Multicast Operation 233

Verifying IP Multicast Operation in a PIM-SM or PIM-SSM Network Example 233
Verifying IP Multicast on the Last Hop Router Example 234
Verifying IP Multicast on Routers Along the SPT Example 237
Verifying IP Multicast on the First Hop Router Example 237
Additional References 238
Feature Information for Verifying IP Multicast Operation 239

CHAPTER 14 **Monitoring and Maintaining IP Multicast** 241
Finding Feature Information 242
Prerequisites for Monitoring and Maintaining IP Multicast 242
Information About Monitoring and Maintaining IP Multicast 242
IP Multicast Heartbeat 242
Session Announcement Protocol (SAP) 243
PIM MIB Extensions for SNMP Traps for IP Multicast 243
Benefits of PIM MIB Extensions 244
How to Monitor and Maintain IP Multicast 244
Displaying Multicast Peers Packet Rates and Loss Information and Tracing a Path 244
Displaying IP Multicast System and Network Statistics 245
Clearing IP Multicast Routing Table or Caches 246
Monitoring IP Multicast Delivery Using IP Multicast Heartbeat 248
Advertising Multicast Multimedia Sessions Using SAP Listener 249
Disabling Fast Switching of IP Multicast 250
Enabling PIM MIB Extensions for IP Multicast 251
Configuration Examples for Monitoring and Maintaining IP Multicast 253
Displaying IP Multicast System and Network Statistics Example 253
Monitoring IP Multicast Delivery Using IP Multicast Heartbeat Example 254
Advertising Multicast Multimedia Sessions Using SAP Listener Example 254
Displaying IP Multicast System and Network Statistics Example 255
Enabling PIM MIB Extensions for IP Multicast Example 256
Additional References 256
Feature Information for Monitoring and Maintaining IP Multicast 257

CHAPTER 15 **Multicast User Authentication and Profile Support** 259
Finding Feature Information 259
Restrictions for Multicast User Authentication and Profile Support 259

Information About Multicast User Authentication and Profile Support 260
IPv6 Multicast User Authentication and Profile Support 260
How to Configure Multicast User Authentication and Profile Support 260
Enabling AAA Access Control for IPv6 Multicast 260
Specifying Method Lists and Enabling Multicast Accounting 261
Disabling the Device from Receiving Unauthenticated Multicast Traffic 262
Configuration Examples for Multicast User Authentication and Profile Support 263
Example: Enabling AAA Access Control, Specifying Method Lists, and Enabling Multicast Accounting for IPv6 263
Additional References for IPv6 Services: AAAA DNS Lookups 263
Feature Information for Multicast User Authentication and Profile Support 265

CHAPTER 16 **IPv6 Multicast: Bootstrap Router** 267
Finding Feature Information 267
Information About IPv6 Multicast: Bootstrap Router 267
IPv6 BSR 267
IPv6 BSR: Configure RP Mapping 268
IPv6 BSR: Scoped Zone Support 268
IPv6 Multicast: RPF Flooding of BSR Packets 269
How to Configure IPv6 Multicast: Bootstrap Router 269
Configuring a BSR and Verifying BSR Information 269
Sending PIM RP Advertisements to the BSR 270
Configuring BSR for Use Within Scoped Zones 271
Configuring BSR Devices to Announce Scope-to-RP Mappings 273
Configuration Examples for IPv6 Multicast: Bootstrap Router 274
Example: Configuring a BSR 274
Additional References 274
Feature Information for IPv6 Multicast: Bootstrap Router 275

CHAPTER 17 **IPv6 Multicast: PIM Sparse Mode** 279
Finding Feature Information 279
Information About IPv6 Multicast PIM Sparse Mode 279
Protocol Independent Multicast 279
PIM-Sparse Mode 280
Designated Router 280

Rendezvous Point 281
PIM Shared Tree and Source Tree (Shortest-Path Tree) 282
Reverse Path Forwarding 284
How to Configure IPv6 Multicast PIM Sparse Mode 284
Enabling IPv6 Multicast Routing 284
Configuring PIM-SM and Displaying PIM-SM Information for a Group Range 285
Configuring PIM Options 287
Resetting the PIM Traffic Counters 289
Turning Off IPv6 PIM on a Specified Interface 290
Configuration Examples for IPv6 Multicast PIM Sparse Mode 291
Example: Enabling IPv6 Multicast Routing 291
Example: Configuring PIM 291
Example: Displaying IPv6 PIM Topology Information 291
Example: Displaying PIM-SM Information for a Group Range 292
Example: Configuring PIM Options 292
Example: Displaying Information About PIM Traffic 293
Additional References 293
Feature Information for IPv6 Multicast PIM Sparse Mode 294

CHAPTER 18 **IPv6 Multicast: Static Multicast Routing for IPv6** 297
Finding Feature Information 297
Information About IPv6 Static Mroutes 297
How to Configure IPv6 Static Multicast Routes 298
Configuring Static Mroutes 298
Configuration Examples for IPv6 Static Multicast Routes 299
Example: Configuring Static Mroutes 299
Additional References 300
Feature Information for IPv6 Multicast: Static Multicast Routing for IPv6 301

CHAPTER 19 **IPv6 Multicast: PIM Source-Specific Multicast** 303
Finding Feature Information 303
Prerequisites for IPv6 Multicast: PIM Source-Specific Multicast 303
Information About IPv6 Multicast: PIM Source-Specific Multicast 304
IPv6 Multicast Routing Implementation 304
Protocol Independent Multicast 304

PIM-Source Specific Multicast 305
PIM Shared Tree and Source Tree (Shortest-Path Tree) 305
Reverse Path Forwarding 307
How to Configure IPv6 Multicast: PIM Source-Specific Multicast 308
Configuring PIM Options 308
Resetting the PIM Traffic Counters 309
Clearing the PIM Topology Table to Reset the MRIB Connection 310
Configuration Examples for IPv6 Multicast: PIM Source-Specific Multicast 312
Example: Displaying IPv6 PIM Topology Information 312
Example: Configuring Join/Prune Aggregation 313
Example: Displaying Information About PIM Traffic 313
Additional References 314
Feature Information for IPv6 Multicast: PIM Source-Specific Multicast 315

CHAPTER 20 **IPv6 Source Specific Multicast Mapping** 317
Finding Feature Information 317
Information About IPv6 Source Specific Multicast Mapping 317
How to Configure IPv6 Source Specific Multicast Mapping 318
Configuring IPv6 SSM 318
Configuration Examples for IPv6 Source Specific Multicast Mapping 319
Example: IPv6 SSM Mapping 319
Additional References 320
Feature Information for IPv6 Source Specific Multicast Mapping 321

CHAPTER 21 **IPv6 Multicast: Explicit Tracking of Receivers** 323
Finding Feature Information 323
Information About IPv6 Multicast Explicit Tracking of Receivers 323
Explicit Tracking of Receivers 323
How to Configure IPv6 Multicast Explicit Tracking of Receivers 324
Configuring Explicit Tracking of Receivers to Track Host Behavior 324
Configuration Examples for IPv6 Multicast Explicit Tracking of Receivers 325
Example: Configuring Explicit Tracking of Receivers 325
Additional References 325
Feature Information for IPv6 Multicast: Explicit Tracking of Receivers 326

CHAPTER 22 **IPv6 Bidirectional PIM** 327

Finding Feature Information 327

Restrictions for IPv6 Bidirectional PIM 327

Information About IPv6 Bidirectional PIM 328

Bidirectional PIM 328

How to Configure IPv6 Bidirectional PIM 328

Configuring Bidirectional PIM and Displaying Bidirectional PIM Information 328

Configuration Examples for IPv6 Bidirectional PIM 330

Example: Configuring Bidirectional PIM and Displaying Bidirectional PIM Information 330

Additional References 330

Feature Information for IPv6 Bidirectional PIM 331

CHAPTER 23 **IPv6 PIM Passive Mode** 333

Finding Feature Information 333

Information About IPv6 PIM Passive Mode 333

How to Configure IPv6 PIM Passive Mode 334

Additional References 335

Feature Information for IPv6 PIM Passive 336

CHAPTER 24 **IPv6 Multicast: Routable Address Hello Option** 337

Finding Feature Information 337

Information About the Routable Address Hello Option 337

How to Configure IPv6 Multicast: Routable Address Hello Option 338

Configuring the Routable Address Hello Option 338

Configuration Example for the Routable Address Hello Option 339

Additional References 339

Feature Information for IPv6 Multicast: Routable Address Hello Option 340

CHAPTER 25 **PIMv6 Anycast RP Solution** 343

Finding Feature Information 343

Information About the PIMv6 Anycast RP Solution 343

PIMv6 Anycast RP Solution Overview 343

PIMv6 Anycast RP Normal Operation 344

PIMv6 Anycast RP Failover 345

How to Configure the PIMv6 Anycast RP Solution 345
Configuring PIMv6 Anycast RP 345
Configuration Examples for the PIMv6 Anycast RP Solution 349
Example: Configuring PIMv6 Anycast RP 349
Additional References 349
Feature Information for PIMv6 Anycast RP Solution 350

CHAPTER 26 **MTR in VRF** 351
Finding Feature Information 351
Information About MTR in VRF 351
MTR in VRF Overview 351
How to Configure VRF in MTR 352
Configuring MTR in VRF 352
Configuring Examples for MTR in VRF 355
Example for MTR in VRF 355
Additional References for MTR in VRF 355
Feature Information for MTR in VRF 356

CHAPTER 1

Read Me First

Important Information about Cisco IOS XE 16

Effective Cisco IOS XE Release 3.7.0E (for Catalyst Switching) and Cisco IOS XE Release 3.17S (for Access and Edge Routing) the two releases evolve (merge) into a single version of converged release—the Cisco IOS XE 16—providing one release covering the extensive range of access and edge products in the Switching and Routing portfolio.

Feature Information

Use Cisco Feature Navigator to find information about feature support, platform support, and Cisco software image support. An account on Cisco.com is not required.

Related References

- Cisco IOS Command References, All Releases

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. RSS feeds are a free service.

CHAPTER 2

IP Multicast Technology Overview

IP multicast is a bandwidth-conserving technology that reduces traffic by delivering a single stream of information simultaneously to potentially thousands of businesses and homes. Applications that take advantage of multicast include video conferencing, corporate communications, distance learning, and distribution of software, stock quotes, and news.

This module contains a technical overview of IP multicast. IP multicast is an efficient way to use network resources, especially for bandwidth-intensive services such as audio and video. Before beginning to configure IP multicast, it is important that you understand the information presented in this module.

- Finding Feature Information, page 3
- Information About IP Multicast Technology, page 4
- Where to Go Next, page 23
- Additional References, page 24
- Feature Information for IP Multicast Technology Overview, page 25
- Glossary, page 25

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About IP Multicast Technology

Role of IP Multicast in Information Delivery

IP multicast is a bandwidth-conserving technology that reduces traffic by delivering a single stream of information simultaneously to potentially thousands of businesses and homes. Applications that take advantage of multicast include video conferencing, corporate communications, distance learning, and distribution of software, stock quotes, and news.

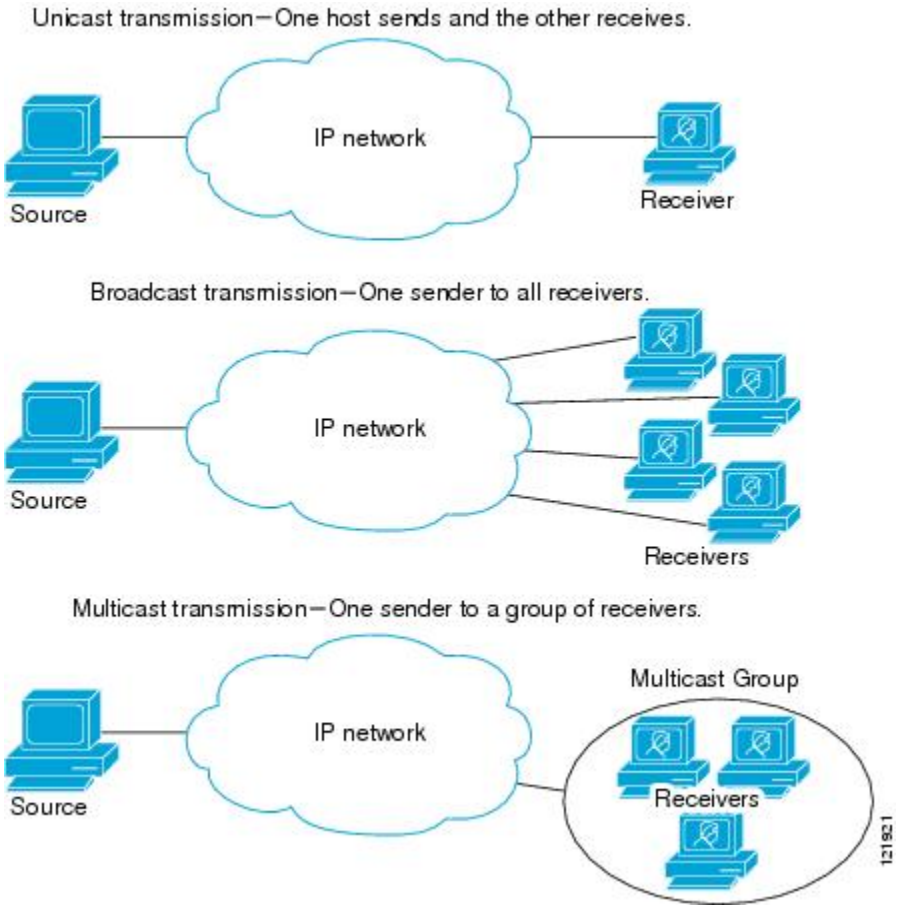
IP multicast routing enables a host (source) to send packets to a group of hosts (receivers) anywhere within the IP network by using a special form of IP address called the IP multicast group address. The sending host inserts the multicast group address into the IP destination address field of the packet and IP multicast routers and multilayer switches forward incoming IP multicast packets out all interfaces that lead to the members of the multicast group. Any host, regardless of whether it is a member of a group, can send to a group. However, only the members of a group receive the message.

Multicast Group Transmission Scheme

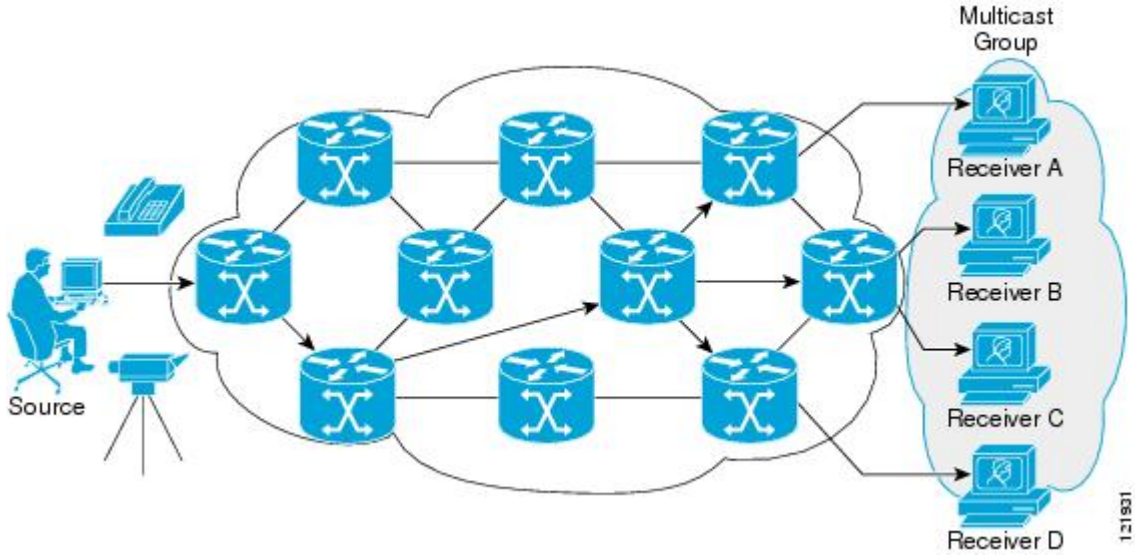
IP communication consists of hosts that act as senders and receivers of traffic as shown in the first figure. Senders are called sources. Traditional IP communication is accomplished by a single host source sending packets to another single host (unicast transmission) or to all hosts (broadcast transmission). IP multicast provides a third scheme, allowing a host to send packets to a subset of all hosts (multicast transmission). This subset of receiving hosts is called a multicast group. The hosts that belong to a multicast group are called group members.

Multicast is based on this group concept. A multicast group is an arbitrary number of receivers that join a group in order to receive a particular data stream. This multicast group has no physical or geographical boundaries--the hosts can be located anywhere on the Internet or on any private internetwork. Hosts that are interested in receiving data from a source to a particular group must join that group. Joining a group is accomplished by a host receiver by way of the Internet Group Management Protocol (IGMP).

In a multicast environment, any host, regardless of whether it is a member of a group, can send to a group. However, only the members of a group can receive packets sent to that group. Multicast packets are delivered to a group using best-effort reliability, just like IP unicast packets.



In the next figure, the receivers (the designated multicast group) are interested in receiving the video data stream from the source. The receivers indicate their interest by sending an IGMP host report to the routers in the network. The routers are then responsible for delivering the data from the source to the receivers. The routers use Protocol Independent Multicast (PIM) to dynamically create a multicast distribution tree. The video data stream will then be delivered only to the network segments that are in the path between the source and the receivers.



IP Multicast Routing Protocols

The software supports the following protocols to implement IP multicast routing:

- IGMP is used between hosts on a LAN and the routers (and multilayer switchescontrollersdevices) on that LAN to track the multicast groups of which hosts are members. To participate in IP multicasting, multicast hosts, routers, and multilayer switchescontrollersdevices must have the Internet Group Management Protocol (IGMP) operating.
- Protocol Independent Multicast (PIM) is used between routers so that they can track which multicast packets to forward to each other and to their directly connected LANs.
- Distance Vector Multicast Routing Protocol (DVMRP) is used on the MBONE (the multicast backbone of the Internet). The software supports PIM-to-DVMRP interaction.
- IGMP Snooping is used for multicasting in a Layer 2 switching environment. It helps reduce the flooding of multicast traffic by dynamically configuring Layer 2 interfaces so that multicast traffic is forwarded to only those interfaces associated with IP multicast devices.
- Multicast VLAN Registration (MVR) is used to prevent data from being multicast on multiple VLANs. It allows a single VLAN to be selected as the carrier for multicast traffic, which then feeds the appropriate subscribers in other separate VLANs.

This figure shows where these protocols operate within the IP multicast environment.

Figure 1: IP Multicast Routing Protocols

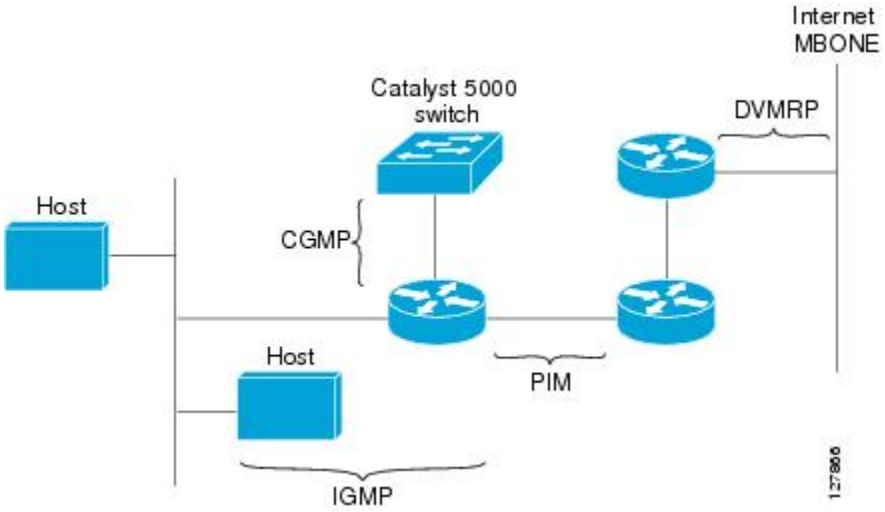


Figure 2: IP Multicast Routing Protocols

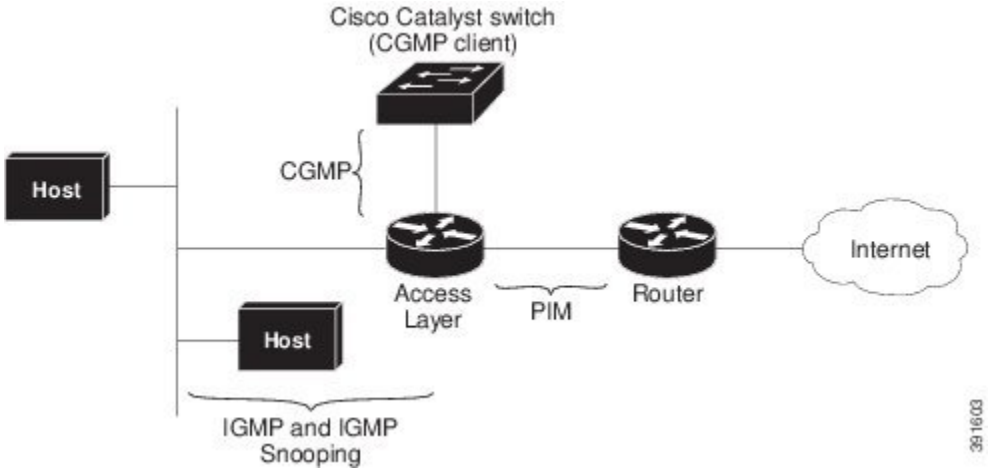
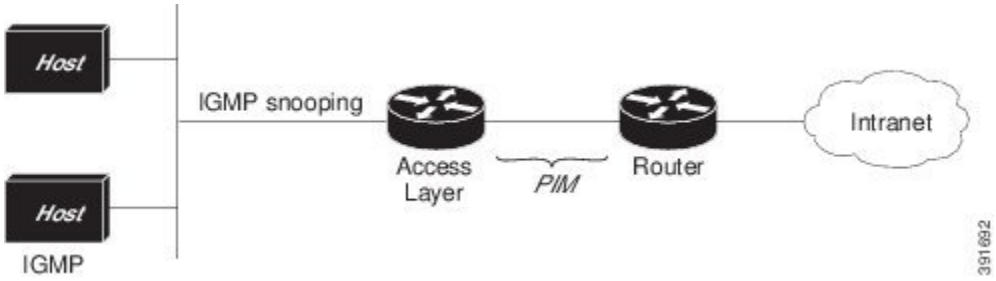


Figure 3: IP Multicast Routing Protocols



According to IPv4 multicast standards, the MAC destination multicast address begins with 0100:5e and is appended by the last 23 bits of the IP address. For example, if the IP destination address is 239.1.1.39, the MAC destination address is 0100:5e01:0127.

A multicast packet is unmatched when the destination IPv4 address does not match the destination MAC address. The switchcontrollerdevice forwards the unmatched packet in hardware based upon the MAC address table. If the destination MAC address is not in the MAC address table, the switchcontrollerdevice floods the packet to the all port in the same VLAN as the receiving port.

IP Multicast Group Addressing

A multicast group is identified by its multicast group address. Multicast packets are delivered to that multicast group address. Unlike unicast addresses that uniquely identify a single host, multicast IP addresses do not identify a particular host. To receive the data sent to a multicast address, a host must join the group that address identifies. The data is sent to the multicast address and received by all the hosts that have joined the group indicating that they wish to receive traffic sent to that group. The multicast group address is assigned to a group at the source. Network administrators who assign multicast group addresses must make sure the addresses conform to the multicast address range assignments reserved by the Internet Assigned Numbers Authority (IANA).

IP Class D Addresses

IP multicast addresses have been assigned to the IPv4 Class D address space by IANA. The high-order four bits of a Class D address are 1110. Therefore, host group addresses can be in the range 224.0.0.0 to 239.255.255.255. A multicast address is chosen at the source (sender) for the receivers in a multicast group.

Note The Class D address range is used only for the group address or destination address of IP multicast traffic. The source address for multicast datagrams is always the unicast source address.

IP Multicast Address Scoping

The multicast address range is subdivided to provide predictable behavior for various address ranges and for address reuse within smaller domains. The table provides a summary of the multicast address ranges. A brief summary description of each range follows.

Table 1: Multicast Address Range Assignments

Name	Range	Description
Reserved Link-Local Addresses	224.0.0.0 to 224.0.0.255	Reserved for use by network protocols on a local network segment.
Globally Scoped Addresses	224.0.1.0 to 238.255.255.255	Reserved to send multicast data between organizations and across the Internet.

Name	Range	Description
Source Specific Multicast	232.0.0.0 to 232.255.255.255	Reserved for use with the SSM datagram delivery model where data is forwarded only to receivers that have explicitly joined the group.
GLOP Addresses	233.0.0.0 to 233.255.255.255	Reserved for statically defined addresses by organizations that already have an assigned autonomous system (AS) domain number.
Limited Scope Address	239.0.0.0 to 239.255.255.255	Reserved as administratively or limited scope addresses for use in private multicast domains.

Reserved Link-Local Addresses

The IANA has reserved the range 224.0.0.0 to 224.0.0.255 for use by network protocols on a local network segment. Packets with an address in this range are local in scope and are not forwarded by IP routers. Packets with link local destination addresses are typically sent with a time-to-live (TTL) value of 1 and are not forwarded by a router.

Within this range, reserved link-local addresses provide network protocol functions for which they are reserved. Network protocols use these addresses for automatic router discovery and to communicate important routing information. For example, Open Shortest Path First (OSPF) uses the IP addresses 224.0.0.5 and 224.0.0.6 to exchange link-state information.

IANA assigns single multicast address requests for network protocols or network applications out of the 224.0.1.xxx address range. Multicast routers forward these multicast addresses.

Globally Scoped Addresses

Addresses in the range 224.0.1.0 to 238.255.255.255 are called globally scoped addresses. These addresses are used to send multicast data between organizations across the Internet. Some of these addresses have been reserved by IANA for use by multicast applications. For example, the IP address 224.0.1.1 is reserved for Network Time Protocol (NTP).

Source Specific Multicast Addresses

Addresses in the range 232.0.0.0/8 are reserved for Source Specific Multicast (SSM) by IANA. In Cisco IOS software, you can use the **ip pim ssm**command to configure SSM for arbitrary IP multicast addresses also. SSM is an extension of Protocol Independent Multicast (PIM) that allows for an efficient data delivery mechanism in one-to-many communications. SSM is described in the IP Multicast Delivery Modes, on page 10 section.

GLOP Addresses

GLOP addressing (as proposed by RFC 2770, GLOP Addressing in 233/8) proposes that the 233.0.0.0/8 range be reserved for statically defined addresses by organizations that already have an AS number reserved. This practice is called GLOP addressing. The AS number of the domain is embedded into the second and third octets of the 233.0.0.0/8 address range. For example, AS 62010 is written in hexadecimal format as F23A.

Separating the two octets F2 and 3A results in 242 and 58 in decimal format. These values result in a subnet of 233.242.58.0/24 that would be globally reserved for AS 62010 to use.

Limited Scope Addresses

The range 239.0.0.0 to 239.255.255.255 is reserved as administratively or limited scoped addresses for use in private multicast domains. These addresses are constrained to a local group or organization. Companies, universities, and other organizations can use limited scope addresses to have local multicast applications that will not be forwarded outside their domain. Routers typically are configured with filters to prevent multicast traffic in this address range from flowing outside an autonomous system (AS) or any user-defined domain. Within an AS or domain, the limited scope address range can be further subdivided so that local multicast boundaries can be defined.

Note Network administrators may use multicast addresses in this range, inside a domain, without conflicting with others elsewhere in the Internet.

Layer 2 Multicast Addresses

Historically, network interface cards (NICs) on a LAN segment could receive only packets destined for their burned-in MAC address or the broadcast MAC address. In IP multicast, several hosts need to be able to receive a single data stream with a common destination MAC address. Some means had to be devised so that multiple hosts could receive the same packet and still be able to differentiate between several multicast groups. One method to accomplish this is to map IP multicast Class D addresses directly to a MAC address. Using this method, NICs can receive packets destined to many different MAC address.

Cisco Group Management Protocol (CGMP) is used on routers connected to Catalyst switches to perform tasks similar to those performed by IGMP. CGMP is necessary for those Catalyst switches that cannot distinguish between IP multicast data packets and IGMP report messages, both of which are addressed to the same group address at the MAC level.

IP Multicast Delivery Modes

IP multicast delivery modes differ only for the receiver hosts, not for the source hosts. A source host sends IP multicast packets with its own IP address as the IP source address of the packet and a group address as the IP destination address of the packet.

Any Source Multicast

For the Any Source Multicast (ASM) delivery mode, an IP multicast receiver host can use any version of IGMP to join a multicast group. This group is notated as G in the routing table state notation. By joining this group, the receiver host is indicating that it wants to receive IP multicast traffic sent by any source to group G. The network will deliver IP multicast packets from any source host with the destination address G to all receiver hosts in the network that have joined group G.

ASM requires group address allocation within the network. At any given time, an ASM group should only be used by a single application. When two applications use the same ASM group simultaneously, receiver hosts of both applications will receive traffic from both application sources. This may result in unexpected

excess traffic in the network. This situation may cause congestion of network links and malfunction of the application receiver hosts.

Source Specific Multicast

Source Specific Multicast (SSM) is a datagram delivery model that best supports one-to-many applications, also known as broadcast applications. SSM is a core network technology for the Cisco implementation of IP multicast targeted for audio and video broadcast application environments.

For the SSM delivery mode, an IP multicast receiver host must use IGMP Version 3 (IGMPv3) to subscribe to channel (S,G). By subscribing to this channel, the receiver host is indicating that it wants to receive IP multicast traffic sent by source host S to group G. The network will deliver IP multicast packets from source host S to group G to all hosts in the network that have subscribed to the channel (S, G).

SSM does not require group address allocation within the network, only within each source host. Different applications running on the same source host must use different SSM groups. Different applications running on different source hosts can arbitrarily reuse SSM group addresses without causing any excess traffic on the network.

Protocol Independent Multicast Overview

The Protocol Independent Multicast (PIM) protocol maintains the current IP multicast service mode of receiver-initiated membership. PIM is not dependent on a specific unicast routing protocol; it is IP routing protocol independent and can leverage whichever unicast routing protocols are used to populate the unicast routing table, including Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), and static routes. PIM uses unicast routing information to perform the multicast forwarding function.

Although PIM is called a multicast routing protocol, it actually uses the unicast routing table to perform the reverse path forwarding (RPF) check function instead of building up a completely independent multicast routing table. Unlike other routing protocols, PIM does not send and receive routing updates between routers.

PIM is defined in RFC 4601, Protocol Independent Multicast - Sparse Mode (PIM-SM)

PIM can operate in dense mode or sparse mode. The router can also handle both sparse groups and dense groups at the same time (sparse-dense mode). The mode determines how the router populates its multicast routing table and how the router forwards multicast packets it receives from its directly connected LANs.

PIM is supported only on 3560-CX switches.

For information about PIM forwarding (interface) modes, see the following sections:

PIM Dense Mode

PIM dense mode (PIM-DM) uses a push model to flood multicast traffic to every corner of the network. This push model is a method for delivering data to the receivers without the receivers requesting the data. This method is efficient in certain deployments in which there are active receivers on every subnet in the network.

In dense mode, a router assumes that all other routers want to forward multicast packets for a group. If a router receives a multicast packet and has no directly connected members or PIM neighbors present, a prune message is sent back to the source. Subsequent multicast packets are not flooded to this router on this pruned branch. PIM builds source-based multicast distribution trees.

PIM-DM initially floods multicast traffic throughout the network. Routers that have no downstream neighbors prune back the unwanted traffic. This process repeats every 3 minutes.

Routers accumulate state information by receiving data streams through the flood and prune mechanism. These data streams contain the source and group information so that downstream routers can build up their multicast forwarding table. PIM-DM supports only source trees--that is, (S,G) entries--and cannot be used to build a shared distribution tree.

Note Dense mode is not often used and its use is not recommended. For this reason it is not specified in the configuration tasks in related modules.

PIM Sparse Mode

PIM sparse mode (PIM-SM) uses a pull model to deliver multicast traffic. Only network segments with active receivers that have explicitly requested the data will receive the traffic.

Unlike dense mode interfaces, sparse mode interfaces are added to the multicast routing table only when periodic Join messages are received from downstream routers, or when a directly connected member is on the interface. When forwarding from a LAN, sparse mode operation occurs if an RP is known for the group. If so, the packets are encapsulated and sent toward the RP. When no RP is known, the packet is flooded in a dense mode fashion. If the multicast traffic from a specific source is sufficient, the first hop router of the receiver may send Join messages toward the source to build a source-based distribution tree.

PIM-SM distributes information about active sources by forwarding data packets on the shared tree. Because PIM-SM uses shared trees (at least, initially), it requires the use of a rendezvous point (RP). The RP must be administratively configured in the network. See the Rendezvous Points, on page 15 section for more information.

In sparse mode, a router assumes that other routers do not want to forward multicast packets for a group, unless there is an explicit request for the traffic. When hosts join a multicast group, the directly connected routers send PIM Join messages toward the RP. The RP keeps track of multicast groups. Hosts that send multicast packets are registered with the RP by the first hop router of that host. The RP then sends Join messages toward the source. At this point, packets are forwarded on a shared distribution tree. If the multicast traffic from a specific source is sufficient, the first hop router of the host may send Join messages toward the source to build a source-based distribution tree.

Sources register with the RP and then data is forwarded down the shared tree to the receivers. The edge routers learn about a particular source when they receive data packets on the shared tree from that source through the RP. The edge router then sends PIM (S,G) Join messages toward that source. Each router along the reverse path compares the unicast routing metric of the RP address to the metric of the source address. If the metric for the source address is better, it will forward a PIM (S,G) Join message toward the source. If the metric for the RP is the same or better, then the PIM (S,G) Join message will be sent in the same direction as the RP. In this case, the shared tree and the source tree would be considered congruent.

If the shared tree is not an optimal path between the source and the receiver, the routers dynamically create a source tree and stop traffic from flowing down the shared tree. This behavior is the default behavior in software. Network administrators can force traffic to stay on the shared tree by using the **ip pim spt-threshold infinity** command.

PIM-SM scales well to a network of any size, including those with WAN links. The explicit join mechanism prevents unwanted traffic from flooding the WAN links.

Sparse-Dense Mode

If you configure either sparse mode or dense mode on an interface, then sparseness or denseness is applied to the interface as a whole. However, some environments might require PIM to run in a single region in sparse mode for some groups and in dense mode for other groups.

An alternative to enabling only dense mode or only sparse mode is to enable sparse-dense mode. In this case, the interface is treated as dense mode if the group is in dense mode; the interface is treated in sparse mode if the group is in sparse mode. You must have an RP if the interface is in sparse-dense mode and you want to treat the group as a sparse group.

If you configure sparse-dense mode, the idea of sparseness or denseness is applied to the groups for which the router is a member.

Another benefit of sparse-dense mode is that Auto-RP information can be distributed in a dense mode; yet, multicast groups for user groups can be used in a sparse mode manner. Therefore there is no need to configure a default RP at the leaf routers.

When an interface is treated in dense mode, it is populated in the outgoing interface list of a multicast routing table when either of the following conditions is true:

- Members or DVMRP neighbors are on the interface.
- There are PIM neighbors and the group has not been pruned.

When an interface is treated in sparse mode, it is populated in the outgoing interface list of a multicast routing table when either of the following conditions is true:

- Members or DVMRP neighbors are on the interface.
- An explicit Join message has been received by a PIM neighbor on the interface.

Bidirectional PIM

Bidirectional PIM (bidir-PIM) is an enhancement of the PIM protocol that was designed for efficient many-to-many communications within an individual PIM domain. Multicast groups in bidirectional mode can scale to an arbitrary number of sources with only a minimal amount of additional overhead.

The shared trees that are created in PIM sparse mode are unidirectional. This means that a source tree must be created to bring the data stream to the RP (the root of the shared tree) and then it can be forwarded down the branches to the receivers. Source data cannot flow up the shared tree toward the RP--this would be considered a bidirectional shared tree.

In bidirectional mode, traffic is routed only along a bidirectional shared tree that is rooted at the RP for the group. In bidir-PIM, the IP address of the RP acts as the key to having all routers establish a loop-free spanning tree topology rooted in that IP address. This IP address need not be a router address, but can be any unassigned IP address on a network that is reachable throughout the PIM domain.

Bidir-PIM is derived from the mechanisms of PIM sparse mode (PIM-SM) and shares many of the shared tree operations. Bidir-PIM also has unconditional forwarding of source traffic toward the RP upstream on the shared tree, but no registering process for sources as in PIM-SM. These modifications are necessary and sufficient to allow forwarding of traffic in all routers solely based on the (*, G) multicast routing entries. This feature eliminates any source-specific state and allows scaling capability to an arbitrary number of sources.

Multicast Group Modes

In PIM, packet traffic for a multicast group is routed according to the rules of the mode configured for that multicast group. The Cisco implementation of PIM supports four modes for a multicast group:

- PIM Bidirectional mode
- PIM Sparse mode
- PIM Dense mode
- PIM Source Specific Multicast (SSM) mode

A router can simultaneously support all four modes or any combination of them for different multicast groups.

Bidirectional Mode

In bidirectional mode, traffic is routed only along a bidirectional shared tree that is rooted at the rendezvous point (RP) for the group. In bidir-PIM, the IP address of the RP acts as the key to having all routers establish a loop-free spanning tree topology rooted in that IP address. This IP address need not be a router, but can be any unassigned IP address on a network that is reachable throughout the PIM domain. This technique is the preferred configuration method for establishing a redundant RP configuration for bidir-PIM.

Membership to a bidirectional group is signalled via explicit Join messages. Traffic from sources is unconditionally sent up the shared tree toward the RP and passed down the tree toward the receivers on each branch of the tree.

Sparse Mode

Sparse mode operation centers around a single unidirectional shared tree whose root node is called the rendezvous point (RP). Sources must register with the RP to get their multicast traffic to flow down the shared tree by way of the RP. This registration process actually triggers a shortest path tree (SPT) Join by the RP toward the source when there are active receivers for the group in the network.

A sparse mode group uses the explicit join model of interaction. Receiver hosts join a group at a rendezvous point (RP). Different groups can have different RPs.

Multicast traffic packets flow down the shared tree to only those receivers that have explicitly asked to receive the traffic.

Dense Mode

Dense mode operates using the broadcast (flood) and prune model.

In populating the multicast routing table, dense mode interfaces are always added to the table. Multicast traffic is forwarded out all interfaces in the outgoing interface list to all receivers. Interfaces are removed from the outgoing interface list in a process called pruning. In dense mode, interfaces are pruned for various reasons including that there are no directly connected receivers.

A pruned interface can be reestablished, that is, grafted back so that restarting the flow of multicast traffic can be accomplished with minimal delay.

Rendezvous Points

A rendezvous point (RP) is a role that a device performs when operating in Protocol Independent Multicast (PIM) Sparse Mode (SM). An RP is required only in networks running PIM SM. In the PIM-SM model, only network segments with active receivers that have explicitly requested multicast data will be forwarded the traffic. This method of delivering multicast data is in contrast to PIM Dense Mode (PIM DM). In PIM DM, multicast traffic is initially flooded to all segments of the network. Routers that have no downstream neighbors or directly connected receivers prune back the unwanted traffic.

An RP acts as the meeting place for sources and receivers of multicast data. In a PIM-SM network, sources must send their traffic to the RP. This traffic is then forwarded to receivers down a shared distribution tree. By default, when the first hop device of the receiver learns about the source, it will send a Join message directly to the source, creating a source-based distribution tree from the source to the receiver. This source tree does not include the RP unless the RP is located within the shortest path between the source and receiver.

In most cases, the placement of the RP in the network is not a complex decision. By default, the RP is needed only to start new sessions with sources and receivers. Consequently, the RP experiences little overhead from traffic flow or processing. In PIM version 2, the RP performs less processing than in PIM version 1 because sources must only periodically register with the RP to create state.

Auto-RP

In the first version of PIM-SM, all leaf routers (routers directly connected to sources or receivers) were required to be manually configured with the IP address of the RP. This type of configuration is also known as static RP configuration. Configuring static RPs is relatively easy in a small network, but it can be laborious in a large, complex network.

Following the introduction of PIM-SM version 1, Cisco implemented a version of PIM-SM with the Auto-RP feature. Auto-RP automates the distribution of group-to-RP mappings in a PIM network. Auto-RP has the following benefits:

- Configuring the use of multiple RPs within a network to serve different groups is easy.
- Auto-RP allows load splitting among different RPs and arrangement of RPs according to the location of group participants.
- Auto-RP avoids inconsistent, manual RP configurations that can cause connectivity problems.

Multiple RPs can be used to serve different group ranges or serve as backups to each other. For Auto-RP to work, a router must be designated as an RP-mapping agent, which receives the RP-announcement messages from the RPs and arbitrates conflicts. The RP-mapping agent then sends the consistent group-to-RP mappings to all other routers. Thus, all routers automatically discover which RP to use for the groups they support.

Note If you configure PIM in sparse mode or sparse-dense mode and do not configure Auto-RP, you must statically configure an RP.

Note If router interfaces are configured in sparse mode, Auto-RP can still be used if all routers are configured with a static RP address for the Auto-RP groups.

To make Auto-RP work, a router must be designated as an RP mapping agent, which receives the RP announcement messages from the RPs and arbitrates conflicts. The RP mapping agent then sends the consistent group-to-RP mappings to all other routers by dense mode flooding. Thus, all routers automatically discover which RP to use for the groups they support. The Internet Assigned Numbers Authority (IANA) has assigned two group addresses, 224.0.1.39 and 224.0.1.40, for Auto-RP. One advantage of Auto-RP is that any change to the RP designation must be configured only on the routers that are RPs and not on the leaf routers. Another advantage of Auto-RP is that it offers the ability to scope the RP address within a domain. Scoping can be achieved by defining the time-to-live (TTL) value allowed for the Auto-RP advertisements.

Each method for configuring an RP has its own strengths, weaknesses, and level of complexity. In conventional IP multicast network scenarios, we recommend using Auto-RP to configure RPs because it is easy to configure, well-tested, and stable. The alternative ways to configure an RP are static RP, Auto-RP, and bootstrap router.

Sparse-Dense Mode for Auto-RP

A prerequisite of Auto-RP is that all interfaces must be configured in sparse-dense mode using the **ip pim sparse-dense-mode** interface configuration command. An interface configured in sparse-dense mode is treated in either sparse mode or dense mode of operation, depending on which mode the multicast group operates. If a multicast group has a known RP, the interface is treated in sparse mode. If a group has no known RP, by default the interface is treated in dense mode and data will be flooded over this interface. (You can prevent dense-mode fallback; see the module “Configuring Basic IP Multicast.”)

To successfully implement Auto-RP and prevent any groups other than 224.0.1.39 and 224.0.1.40 from operating in dense mode, we recommend configuring a “sink RP” (also known as “RP of last resort”). A sink RP is a statically configured RP that may or may not actually exist in the network. Configuring a sink RP does not interfere with Auto-RP operation because, by default, Auto-RP messages supersede static RP configurations. We recommend configuring a sink RP for all possible multicast groups in your network, because it is possible for an unknown or unexpected source to become active. If no RP is configured to limit source registration, the group may revert to dense mode operation and be flooded with data.

Bootstrap Router

Another RP selection model called bootstrap router (BSR) was introduced after Auto-RP in PIM-SM version 2. BSR performs similarly to Auto-RP in that it uses candidate routers for the RP function and for relaying the RP information for a group. RP information is distributed through BSR messages, which are carried within PIM messages. PIM messages are link-local multicast messages that travel from PIM router to PIM router. Because of this single hop method of disseminating RP information, TTL scoping cannot be used with BSR. A BSR performs similarly as an RP, except that it does not run the risk of reverting to dense mode operation, and it does not offer the ability to scope within a domain.

Multicast Source Discovery Protocol

In the PIM sparse mode model, multicast sources and receivers must register with their local rendezvous point (RP). Actually, the router closest to a source or a receiver registers with the RP, but the key point to note is that the RP “knows” about all the sources and receivers for any particular group. RPs in other domains have no way of knowing about sources that are located in other domains. Multicast Source Discovery Protocol (MSDP) is an elegant way to solve this problem.

MSDP is a mechanism that allows RPs to share information about active sources. RPs know about the receivers in their local domain. When RPs in remote domains hear about the active sources, they can pass on that information to their local receivers. Multicast data can then be forwarded between the domains. A useful

feature of MSDP is that it allows each domain to maintain an independent RP that does not rely on other domains, but it does enable RPs to forward traffic between domains. PIM-SM is used to forward the traffic between the multicast domains.

The RP in each domain establishes an MSDP peering session using a TCP connection with the RPs in other domains or with border routers leading to the other domains. When the RP learns about a new multicast source within its own domain (through the normal PIM register mechanism), the RP encapsulates the first data packet in a Source-Active (SA) message and sends the SA to all MSDP peers. Each receiving peer uses a modified Reverse Path Forwarding (RPF) check to forward the SA, until the SA reaches every MSDP router in the interconnected networks--theoretically the entire multicast internet. If the receiving MSDP peer is an RP, and the RP has a (*, G) entry for the group in the SA (there is an interested receiver), the RP creates (S,G) state for the source and joins to the shortest path tree for the source. The encapsulated data is decapsulated and forwarded down the shared tree of that RP. When the last hop router (the router closest to the receiver) receives the multicast packet, it may join the shortest path tree to the source. The MSDP speaker periodically sends SAs that include all sources within the domain of the RP.

MSDP was developed for peering between Internet service providers (ISPs). ISPs did not want to rely on an RP maintained by a competing ISP to provide service to their customers. MSDP allows each ISP to have its own local RP and still forward and receive multicast traffic to the Internet.

Anycast RP

Anycast RP is a useful application of MSDP. Originally developed for interdomain multicast applications, MSDP used for Anycast RP is an intradomain feature that provides redundancy and load-sharing capabilities. Enterprise customers typically use Anycast RP for configuring a Protocol Independent Multicast sparse mode (PIM-SM) network to meet fault tolerance requirements within a single multicast domain.

In Anycast RP, two or more RPs are configured with the same IP address on loopback interfaces. The Anycast RP loopback address should be configured with a 32-bit mask, making it a host address. All the downstream routers should be configured to “know” that the Anycast RP loopback address is the IP address of their local RP. IP routing automatically will select the topologically closest RP for each source and receiver. Assuming that the sources are evenly spaced around the network, an equal number of sources will register with each RP. That is, the process of registering the sources will be shared equally by all the RPs in the network.

Because a source may register with one RP and receivers may join to a different RP, a method is needed for the RPs to exchange information about active sources. This information exchange is done with MSDP.

In Anycast RP, all the RPs are configured to be MSDP peers of each other. When a source registers with one RP, an SA message will be sent to the other RPs informing them that there is an active source for a particular multicast group. The result is that each RP will know about the active sources in the area of the other RPs. If any of the RPs were to fail, IP routing would converge and one of the RPs would become the active RP in more than one area. New sources would register with the backup RP. Receivers would join toward the new RP and connectivity would be maintained.

Note The RP is normally needed only to start new sessions with sources and receivers. The RP facilitates the shared tree so that sources and receivers can directly establish a multicast data flow. If a multicast data flow is already directly established between a source and the receiver, then an RP failure will not affect that session. Anycast RP ensures that new sessions with sources and receivers can begin at any time.

Multicast Forwarding

Forwarding of multicast traffic is accomplished by multicast-capable routers. These routers create distribution trees that control the path that IP multicast traffic takes through the network in order to deliver traffic to all receivers.

Multicast traffic flows from the source to the multicast group over a distribution tree that connects all of the sources to all of the receivers in the group. This tree may be shared by all sources (a shared tree) or a separate distribution tree can be built for each source (a source tree). The shared tree may be one-way or bidirectional.

Before describing the structure of source and shared trees, it is helpful to explain the notations that are used in multicast routing tables. These notations include the following:

- (S,G) = (unicast source for the multicast group G, multicast group G)
- (*,G) = (any source for the multicast group G, multicast group G)

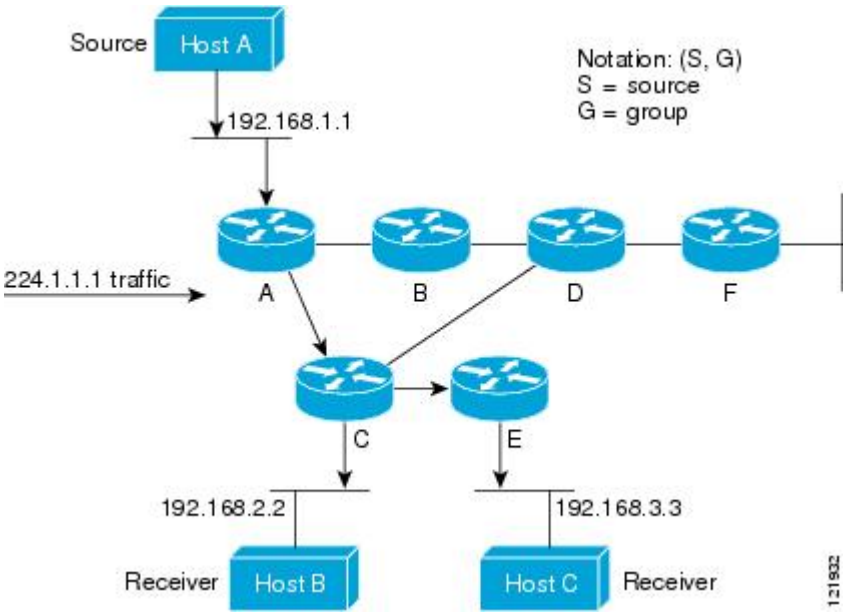
The notation of (S,G), pronounced "S comma G," enumerates a shortest path tree where S is the IP address of the source and G is the multicast group address.

Shared trees are (*,G) and the source trees are (S,G) and always routed at the sources.

Multicast Distribution Source Tree

The simplest form of a multicast distribution tree is a source tree. A source tree has its root at the source host and has branches forming a spanning tree through the network to the receivers. Because this tree uses the shortest path through the network, it is also referred to as a shortest path tree (SPT).

The figure shows an example of an SPT for group 224.1.1.1 rooted at the source, Host A, and connecting two receivers, Hosts B and C.



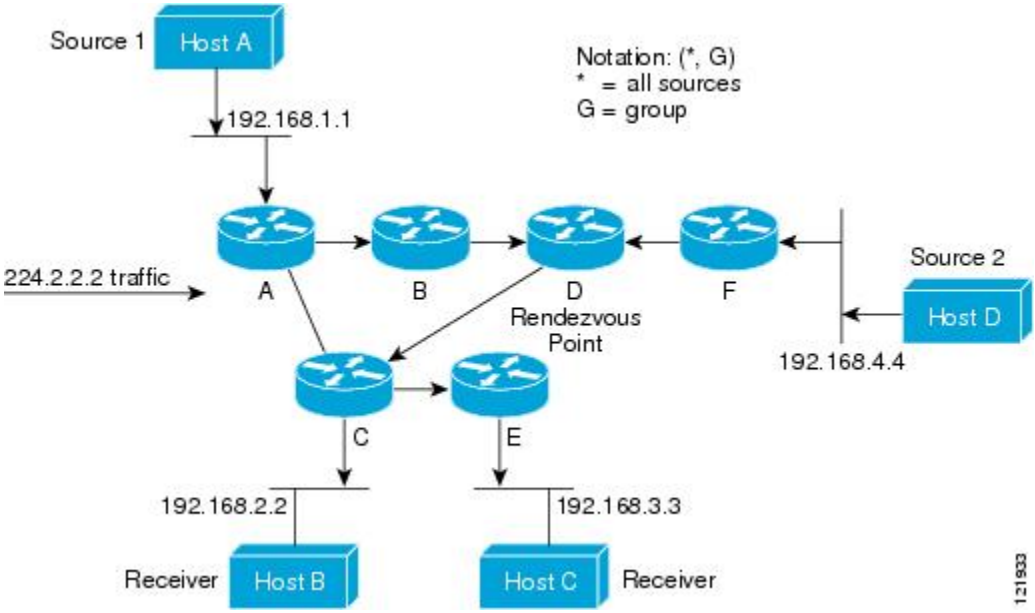
Using standard notation, the SPT for the example shown in the figure would be (192.168.1.1, 224.1.1.1).

The (S,G) notation implies that a separate SPT exists for each individual source sending to each group--which is correct.

Multicast Distribution Shared Tree

Unlike source trees that have their root at the source, shared trees use a single common root placed at some chosen point in the network. This shared root is called a rendezvous point (RP).

Figure 5 shows a shared tree for the group 224.2.2.2 with the root located at Router D. This shared tree is unidirectional. Source traffic is sent towards the RP on a source tree. The traffic is then forwarded down the shared tree from the RP to reach all of the receivers (unless the receiver is located between the source and the RP, in which case it will be serviced directly).



In this example, multicast traffic from the sources, Hosts A and D, travels to the root (Router D) and then down the shared tree to the two receivers, Hosts B and C. Because all sources in the multicast group use a common shared tree, a wildcard notation written as (*, G), pronounced "star comma G," represents the tree. In this case, * means all sources, and G represents the multicast group. Therefore, the shared tree shown in Figure 5 would be written as (*, 224.2.2.2).

Both source trees and shared trees are loop-free. Messages are replicated only where the tree branches. Members of multicast groups can join or leave at any time; therefore the distribution trees must be dynamically updated. When all the active receivers on a particular branch stop requesting the traffic for a particular multicast group, the routers prune that branch from the distribution tree and stop forwarding traffic down that branch. If one receiver on that branch becomes active and requests the multicast traffic, the router will dynamically modify the distribution tree and start forwarding traffic again.

Source Tree Advantage

Source trees have the advantage of creating the optimal path between the source and the receivers. This advantage guarantees the minimum amount of network latency for forwarding multicast traffic. However, this optimization comes at a cost. The routers must maintain path information for each source. In a network

that has thousands of sources and thousands of groups, this overhead can quickly become a resource issue on the routers. Memory consumption from the size of the multicast routing table is a factor that network designers must take into consideration.

Shared Tree Advantage

Shared trees have the advantage of requiring the minimum amount of state in each router. This advantage lowers the overall memory requirements for a network that only allows shared trees. The disadvantage of shared trees is that under certain circumstances the paths between the source and receivers might not be the optimal paths, which might introduce some latency in packet delivery. For example, in the figure above the shortest path between Host A (source 1) and Host B (a receiver) would be Router A and Router C. Because we are using Router D as the root for a shared tree, the traffic must traverse Routers A, B, D and then C. Network designers must carefully consider the placement of the rendezvous point (RP) when implementing a shared tree-only environment.

In unicast routing, traffic is routed through the network along a single path from the source to the destination host. A unicast router does not consider the source address; it considers only the destination address and how to forward the traffic toward that destination. The router scans through its routing table for the destination address and then forwards a single copy of the unicast packet out the correct interface in the direction of the destination.

In multicast forwarding, the source is sending traffic to an arbitrary group of hosts that are represented by a multicast group address. The multicast router must determine which direction is the upstream direction (toward the source) and which one is the downstream direction (or directions) toward the receivers. If there are multiple downstream paths, the router replicates the packet and forwards it down the appropriate downstream paths (best unicast route metric)--which is not necessarily all paths. Forwarding multicast traffic away from the source, rather than to the receiver, is called Reverse Path Forwarding (RPF). RPF is described in the following section.

Reverse Path Forwarding

In unicast routing, traffic is routed through the network along a single path from the source to the destination host. A unicast router does not consider the source address; it considers only the destination address and how to forward the traffic toward that destination. The router scans through its routing table for the destination network and then forwards a single copy of the unicast packet out the correct interface in the direction of the destination.

In multicast forwarding, the source is sending traffic to an arbitrary group of hosts that are represented by a multicast group address. The multicast router must determine which direction is the upstream direction (toward the source) and which one is the downstream direction (or directions) toward the receivers. If there are multiple downstream paths, the router replicates the packet and forwards it down the appropriate downstream paths (best unicast route metric)--which is not necessarily all paths. Forwarding multicast traffic away from the source, rather than to the receiver, is called Reverse Path Forwarding (RPF). RPF is an algorithm used for forwarding multicast datagrams.

Protocol Independent Multicast (PIM) uses the unicast routing information to create a distribution tree along the reverse path from the receivers towards the source. The multicast routers then forward packets along the distribution tree from the source to the receivers. RPF is a key concept in multicast forwarding. It enables routers to correctly forward multicast traffic down the distribution tree. RPF makes use of the existing unicast routing table to determine the upstream and downstream neighbors. A router will forward a multicast packet only if it is received on the upstream interface. This RPF check helps to guarantee that the distribution tree will be loop-free.

RPF Check

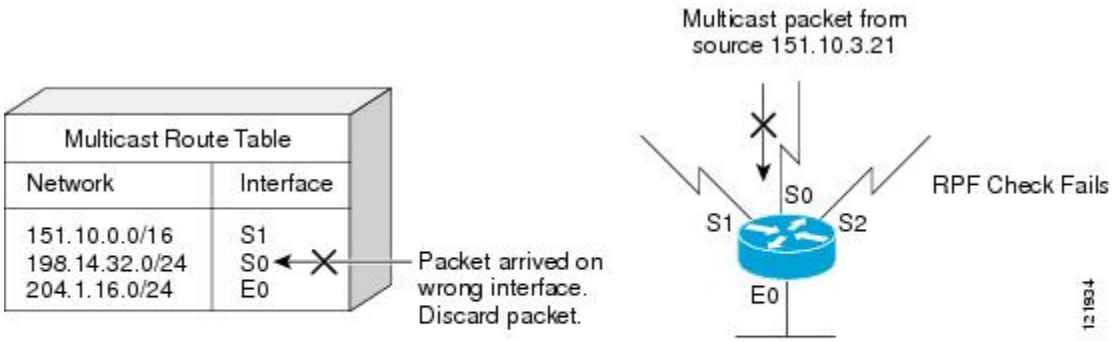
When a multicast packet arrives at a router, the router performs an RPF check on the packet. If the RPF check succeeds, the packet is forwarded. Otherwise, it is dropped.

For traffic flowing down a source tree, the RPF check procedure works as follows:

1. The router looks up the source address in the unicast routing table to determine if the packet has arrived on the interface that is on the reverse path back to the source.
2. If the packet has arrived on the interface leading back to the source, the RPF check succeeds and the packet is forwarded out the interfaces present in the outgoing interface list of a multicast routing table entry.
3. If the RPF check in Step 2 fails, the packet is dropped.

The figure shows an example of an unsuccessful RPF check.

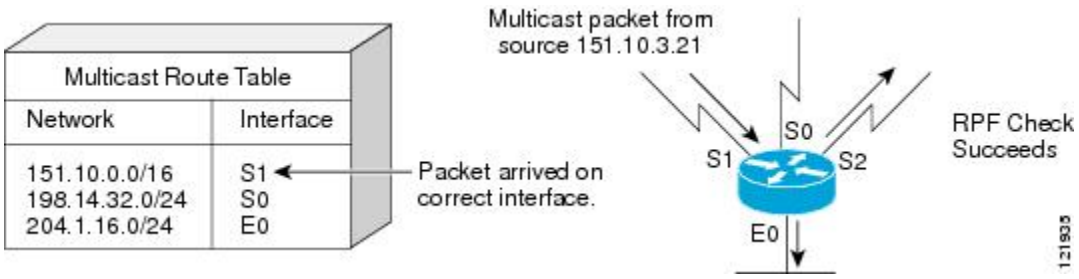
Figure 4: RPF Check Fails



As the figure illustrates, a multicast packet from source 151.10.3.21 is received on serial interface 0 (S0). A check of the unicast route table shows that S1 is the interface this router would use to forward unicast data to 151.10.3.21. Because the packet has arrived on interface S0, the packet is discarded.

The figure shows an example of a successful RPF check.

Figure 5: RPF Check Succeeds



In this example, the multicast packet has arrived on interface S1. The router refers to the unicast routing table and finds that S1 is the correct interface. The RPF check passes, and the packet is forwarded.

PIM uses both source trees and RP-rooted shared trees to forward datagrams. The RPF check is performed differently for each:

- If a PIM router or multilayer switchcontrollerdevice has a source-tree state (that is, an (S, G) entry is present in the multicast routing table), it performs the RPF check against the IP address of the source of the multicast packet.
- If a PIM router or multilayer switchcontrollerdevice has a shared-tree state (and no explicit source-tree state), it performs the RPF check on the RP address (which is known when members join the group).

DVMRP and dense-mode PIM use only source trees and use RPF.

Note DVMRP is not supported on the switchcontrollerdevice.

Sparse-mode PIM uses the RPF lookup function to decide where it needs to send joins and prunes:

- (S, G) joins (which are source-tree states) are sent toward the source.
- (*,G) joins (which are shared-tree states) are sent toward the RP.

PIM Dense Mode Fallback

If you use IP multicast in mission-critical networks, you should avoid the use of PIM-DM (dense mode).

Dense mode fallback describes the event of the PIM mode changing (falling back) from sparse mode (which requires an RP) to dense mode (which does not use an RP). Dense mode fallback occurs when RP information is lost.

If all interfaces are configured with the **ip pim sparse-mode** command, there is no dense mode fallback because dense mode groups cannot be created over interfaces configured for sparse mode.

Cause and Effect of Dense Mode Fallback

PIM determines whether a multicast group operates in PIM-DM or PIM-SM mode based solely on the existence of RP information in the group-to-RP mapping cache. If Auto-RP is configured or a bootstrap router (BSR) is used to distribute RP information, there is a risk that RP information can be lost if all RPs, Auto-RP, or the BSR for a group fails due to network congestion. This failure can lead to the network either partially or fully falling back into PIM-DM.

If a network falls back into PIM-DM and AutoRP or BSR is being used, dense mode flooding will occur. Routers that lose RP information will fallback into dense mode and any new states that must be created for the failed group will be created in dense mode.

Effects of Preventing Dense Mode Fallback

Prior to the introduction of PIM-DM fallback prevention, all multicast groups without a group-to-RP mapping would be treated as dense mode.

With the introduction of PIM-DM fallback prevention, the PIM-DM fallback behavior has been changed to prevent dense mode flooding. By default, if all of the interfaces are configured to operate in PIM sparse mode (using the **ip pim sparse-mode** command), there is no need to configure the **no ip pim dm-fallback** command

(that is, the PIM-DM fallback behavior is enabled by default). If any interfaces are not configured using the **ip pim sparse-mode**command (for example, using the **ip pim sparse-dense-mode** command), then the PIM-DM fallback behavior can be explicit disabled using the **no ip pim dm-fallback**command.

When the **no ip pim dm-fallback** command is configured or when **ip pim sparse-mode** is configured on all interfaces, any existing groups running in sparse mode will continue to operate in sparse mode but will use an RP address set to 0.0.0.0. Multicast entries with an RP address set to 0.0.0.0 will exhibit the following behavior:

- Existing (S, G) states will be maintained.
- No PIM Join or Prune messages for (*, G) or (S, G, RPbit) are sent.
- Received (*, G) or (S, G, RPbit) Joins or Prune messages are ignored.
- No registers are sent and traffic at the first hop is dropped.
- Received registers are answered with register stop.
- Asserts are unchanged.
- The (*, G) outgoing interface list (olist) is maintained only for the Internet Group Management Protocol (IGMP) state.
- Multicast Source Discovery Protocol (MSDP) source active (SA) messages for RP 0.0.0.0 groups are still accepted and forwarded.

Guidelines for Choosing a PIM Mode

Before beginning the configuration process, you must decide which PIM mode needs to be used. This determination is based on the applications you intend to support on your network.

Basic guidelines include the following:

- In general, if the application is one-to-many or many-to-many in nature, then PIM-SM can be used successfully.
- For optimal one-to-many application performance, SSM is appropriate but requires IGMP version 3 support.
- For optimal many-to-many application performance, bidirectional PIM is appropriate but hardware support is limited to Cisco devices and the Catalyst 6000 series switches with Sup720.

Where to Go Next

- To configure basic IP multicast, see the “ Configuring Basic IP Multicast ” module.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IP multicast commands	*Cisco IOS IP Multicast Command Reference*

Standards

Standard	Title
No new or modified standards are supported, and support for existing standards has not been modified.	--

MIBs

MIB	MIBs Link
CISCO-PIM-MIB	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2934	*Protocol Independent Multicast MIB for IPv4*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for IP Multicast Technology Overview

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 2: Feature Information for IP Multicast Technology Overview

Feature Names	Releases	Feature Configuration Information
PIM Dense Mode Fallback Prevention in a Network Following RP Information Loss	12.3(4)T	The PIM Dense Mode Fallback Prevention in a Network Following RP Information Loss feature enables you to prevent PIM-DM fallback when all RPs fail. Preventing the use of dense mode is very important to multicast networks whose reliability is critical. This feature provides a mechanism to keep the multicast groups in sparse mode, thereby preventing dense mode flooding.

Glossary

basic multicast--Interactive intra-domain multicast. Supports multicast applications within an enterprise campus. Also provides an additional integrity in the network with the inclusion of a reliable multicast transport, PGM.

bidir PIM--Bidirectional PIM is an extension to the PIM suite of protocols that implements shared sparse trees with bidirectional flow of data. In contrast to PIM-SM, bidir-PIM avoids keeping source specific state in router and thus allows trees to scale to an arbitrary number of sources.

broadcast--One-to-all transmission where the source sends one copy of the message to all nodes, whether they wish to receive it or not.

Cisco Group Management Protocol (CGMP)--Cisco-developed protocol that allows Layer 2 switches to leverage IGMP information on Cisco routers to make Layer 2 forwarding decisions. It allows the switches to forward multicast traffic to only those ports that are interested in the traffic.

dense mode (DM) (Internet Draft Spec)--Actively attempts to send multicast data to all potential receivers (flooding) and relies upon their self-pruning (removal from group) to achieve desired distribution.

designated router (DR)--The router in a PIM-SM tree that instigates the Join/Prune message cascade upstream to the RP in response to IGMP membership information it receives from IGMP hosts.

distribution tree--Multicast traffic flows from the source to the multicast group over a distribution tree that connects all of the sources to all of the receivers in the group. This tree may be shared by all sources (a shared-tree), or a separate distribution tree can be built for each source (a source-tree). The shared-tree may be one-way or bidirectional.

IGMP messages--IGMP messages are encapsulated in standard IP datagrams with an IP protocol number of 2 and the IP Router Alert option (RFC 2113).

IGMP snooping--IGMP snooping requires the LAN switch to examine, or “snoop,” some Layer 3 information in the IGMP packet sent from the host to the router. When the switch hears an IGMP report from a host for a particular multicast group, the switch adds the host’s port number to the associated multicast table entry. When it hears an IGMP Leave Group message from a host, it removes the host’s port from the table entry.

IGMP unidirectional link routing--Cisco’s other UDLR solution is to use IP multicast routing with IGMP, which has been enhanced to accommodate UDLR. This solution scales very well for many satellite links.

Internet Group Management Protocol v2 (IGMP)--Used by IP routers and their immediately connected hosts to communicate multicast group membership states.

Internet Group Management Protocol v3 (IGMP)--IGMP is the protocol used by IPv4 systems to report their IP multicast group memberships to neighboring multicast routers. Version 3 of IGMP adds support for “source filtering,” that is, the ability for a system to report interest in receiving packets only from specific source addresses, or from all but specific source addresses, sent to a particular multicast address.

multicast--A routing technique that allows IP traffic to be sent from one source or multiple sources and delivered to multiple destinations. Instead of sending individual packets to each destination, a single packet is sent to a group of destinations known as a multicast group, which is identified by a single IP destination group address. Multicast addressing supports the transmission of a single IP datagram to multiple hosts.

multicast routing monitor (MRM)--A management diagnostic tool that provides network fault detection and isolation in a large multicast routing infrastructure. It is designed to notify a network administrator of multicast routing problems in near real time.

Multicast Source Discovery Protocol (MSDP)--A mechanism to connect multiple PIM sparse mode (PIM-SM) domains. MSDP allows multicast sources for a group to be known to all rendezvous point(s) (RPs) in different domains. Each PIM-SM domain uses its own RPs and need not depend on RPs in other domains. An RP runs MSDP over TCP to discover multicast sources in other domains. MSDP is also used to announce sources sending to a group. These announcements must originate at the domain’s RP. MSDP depends heavily on MBGP for interdomain operation.

Protocol Independent Multicast (PIM)--A multicast routing architecture defined by the IETF that enables IP multicast routing on existing IP networks. Its key point is its independence from any underlying unicast protocol such as OSPF or BGP.

prune--Multicast routing terminology indicating that the multicast-enabled router has sent the appropriate multicast messages to remove itself from the multicast tree for a particular multicast group. It will stop receiving the multicast data addressed to that group and, therefore, cannot deliver the data to any connected hosts until it rejoins the group.

query--IGMP messages originating from the router(s) to elicit multicast group membership information from its connected hosts.

rendezvous point (RP)--The multicast router that is the root of the PIM-SM shared multicast distribution tree.

report--IGMP messages originating from the hosts that are joining, maintaining, or leaving their membership in a multicast group.

source tree--A multicast distribution path that directly connects the source's and receivers' designated router (or the rendezvous point) to obtain the shortest path through the network. Results in most efficient routing of data between source and receivers, but may result in unnecessary data duplication throughout the network if built by anything other than the RP.

sparse mode (SM) (RFC 2362)--Relies upon an explicitly joining method before attempting to send multicast data to receivers of a multicast group.

UDLR tunnel--Uses a back channel (another link) so the routing protocols believe the one-way link is bidirectional. The back channel itself is a special, unidirectional, generic route encapsulation (GRE) tunnel through which control traffic flows in the opposite direction of the user data flow. This feature allows IP and its associated unicast and multicast routing protocols to believe the unidirectional link is logically bidirectional. This solution accommodates all IP unicast and multicast routing protocols without changing them. However, it does not scale and no more than 20 tunnels should feed into the upstream router. The purpose of the unidirectional GRE tunnel is to move control packets from a downstream node to an upstream node.

Unicast--Point-to-point transmission requiring the source to send an individual copy of a message to each requester.

unidirectional Link Routing Protocol (UDLR)--A routing protocol that provides a way to forward multicast packets over a physical unidirectional interface (such as a satellite link of high bandwidth) to stub networks that have a back channel.

URL rendezvous directory (URD)--URD is a multicast-lite solution that directly provides the network with information about the specific source of a content stream. It enables the network to quickly establish the most direct distribution path from the source to the receiver, thus significantly reducing the time and effort required in receiving the streaming media. URD allows an application to identify the source of the content stream through a web page link or web directly. When that information is sent back to the application it is then conveyed back to the network using URD.

In this feature, a URD-capable web page provides information about the source, the group, and the application (via media-type) on a web page. An interested host will click on the web page pulling across the information in an HTTP transaction. The last-hop router to receiver would intercept this transaction and send it to a special port allocated by IANA. The last-hop router is also URD capable and uses the information to initiate the PIM source, group (S,G) join on behalf of the host.

CHAPTER 3

Configuring Basic IP Multicast

IP multicast is a bandwidth-conserving technology that reduces traffic by delivering a single stream of information simultaneously to potentially thousands of corporate businesses and homes. Applications that take advantage of multicast include video conferencing, corporate communications, distance learning, and distribution of software, stock quotes, and news. This module describes the tasks used to configure basic IP multicast.

- Finding Feature Information, page 29
- Prerequisites for Configuring Basic IP Multicast, page 29
- Information About Configuring Basic IP Multicast, page 30
- How to Configure Basic IP Multicast, page 39
- Configuration Examples for Basic IP Multicast, page 59
- Additional References, page 64
- Feature Information for Configuring Basic IP Multicast in IPv4 Networks, page 65

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring Basic IP Multicast

- To determine which of the tasks contained in this module you will have to perform, you must decide which Protocol Independent Multicast (PIM) mode will be used. This determination is based on the applications you intend to support on your network.

- All access lists to be used with the tasks in this module should be configured prior to beginning the configuration task. For information about how to configure an access list, see the "Creating an IP Access List and Applying It to an Interface" module of the *Security Configuration Guide: Access Control Lists* guide.

Information About Configuring Basic IP Multicast

Auto-RP Overview

The Role of Auto-RP in a PIM Network

Auto-RP automates the distribution of group-to-rendezvous point (RP) mappings in a PIM network. To make Auto-RP work, a device must be designated as an RP mapping agent, which receives the RP announcement messages from the RPs and arbitrates conflicts. The RP mapping agent then sends the consistent group-to-RP mappings to all other devices by way of dense mode flooding.

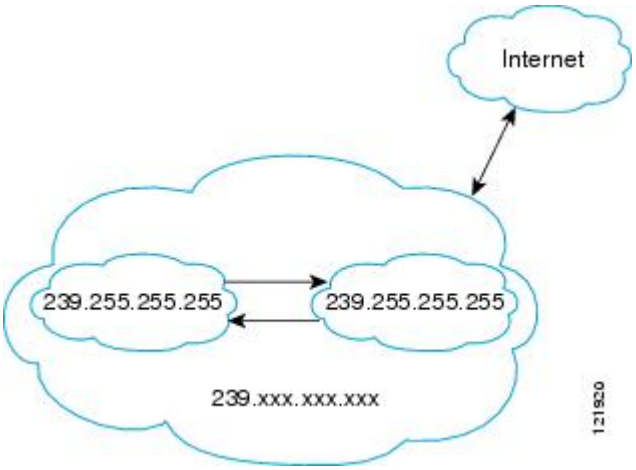
Thus, all routers automatically discover which RP to use for the groups they support. The Internet Assigned Numbers Authority (IANA) has assigned two group addresses, 224.0.1.39 and 224.0.1.40, for Auto-RP.

The mapping agent receives announcements of intention to become the RP from Candidate-RPs. The mapping agent then announces the winner of the RP election. This announcement is made independently of the decisions by the other mapping agents.

IP Multicast Boundary

As shown in the figure, address scoping defines domain boundaries so that domains with RPs that have the same IP address do not leak into each other. Scoping is performed on the subnet boundaries within large domains and on the boundaries between the domain and the Internet.

Figure 6: Address Scoping at Boundaries



You can set up an administratively scoped boundary on an interface for multicast group addresses using the **ip multicast boundary** command with the *access-list* argument. A standard access list defines the range of addresses affected. When a boundary is set up, no multicast data packets are allowed to flow across the boundary from either direction. The boundary allows the same multicast group address to be reused in different administrative domains.

The Internet Assigned Numbers Authority (IANA) has designated the multicast address range 239.0.0.0 to 239.255.255.255 as the administratively scoped addresses. This range of addresses can be reused in domains administered by different organizations. They would be considered local, not globally unique.

You can configure the **filter-autorp** keyword to examine and filter Auto-RP discovery and announcement messages at the administratively scoped boundary. Any Auto-RP group range announcements from the Auto-RP packets that are denied by the boundary access control list (ACL) are removed. An Auto-RP group range announcement is permitted and passed by the boundary only if all addresses in the Auto-RP group range are permitted by the boundary ACL. If any address is not permitted, the entire group range is filtered and removed from the Auto-RP message before the Auto-RP message is forwarded. In order to block all multicast traffic coming in on interface but allow multicast traffic coming out of the interface, use the**{ ip | ipv6 } multicast boundary block sources** command.

Benefits of Auto-RP in a PIM Network

- Auto-RP allows any change to the RP designation to be configured only on the devices that are RPs, not on the leaf routers.
- Auto-RP offers the ability to scope the RP address within a domain.

Anycast RP Overview

Anycast RP is a useful application of MSDP. Originally developed for interdomain multicast applications, MSDP used for Anycast RP is an intradomain feature that provides redundancy and load-sharing capabilities. Enterprise customers typically use Anycast RP for configuring a Protocol Independent Multicast sparse mode (PIM-SM) network to meet fault tolerance requirements within a single multicast domain.

In anycast RP, two or more RPs are configured with the same IP address on loopback interfaces. The anycast RP loopback address should be configured with a 32-bit mask, making it a host address. All the downstream routers should be configured so that the anycast RP loopback address is the IP address of their local RP. IP routing will automatically select the topologically closest RP for each source and receiver. Assuming that the sources are evenly spaced around the network, an equal number of sources will register with each RP. That is, the process of registering the sources will be shared equally by all the RPs in the network.

Because a source may register with one RP and receivers may join to a different RP, a method is needed for the RPs to exchange information about active sources. This information exchange is done with MSDP.

In anycast RP, all the RPs are configured to be MSDP peers of each other. When a source registers with one RP, an SA message will be sent to the other RPs informing them that there is an active source for a particular multicast group. The result is that each RP will know about the active sources in the area of the other RPs. If any of the RPs were to fail, IP routing would converge, and one of the RPs would become the active RP in more than one area. New sources would register with the backup RP. Receivers would join the new RP and connectivity would be maintained.

The RP is normally needed only to start new sessions with sources and receivers. The RP facilitates the shared tree so that sources and receivers can establish a direct multicast data flow. If a multicast data flow is already

established between a source and the receiver, an RP failure will not affect that session. Anycast RP ensures that new sessions with sources and receivers can begin at any time.

BSR Overview

BSR Election and Functionality

PIM uses the BSR to discover and announce RP-set information for each group prefix to all the routers in a PIM domain. This is the same function performed by Auto-RP, but the BSR is part of the PIM Version 2 specification. The BSR mechanism interoperates with Auto-RP on Cisco routers.

To avoid a single point of failure, you can configure several candidate BSRs in a PIM domain. A BSR is elected among the candidate BSRs automatically; they use bootstrap messages to discover which BSR has the highest priority. This router then announces to all PIM routers in the PIM domain that it is the BSR.

Following the election of the BSR, candidate RPs use unicast to announce to the BSR their willingness to be the RP. The BSR advertises the entire group-to-RP mapping set to the router link local address 224.0.0.13. Unlike the RP mapping agent in Auto-RP, which is used by Auto-RP to select the RP, every router in the BSR network is responsible for selecting the RP.

BSR lacks the ability to scope RP advertisements; however, BSR is used when vendor interoperability or open standard adherence is a requirement.

BSR Border Interface

A border interface in a PIM sparse mode domain requires precautions to prevent exchange of certain traffic with a neighboring domain reachable through that interface, especially if that domain is also running PIM sparse mode. BSR and Auto-RP messages should not be exchanged between different domains, because routers in one domain may elect RPs in the other domain, resulting in protocol malfunction or loss of isolation between the domains. Configure a BSR border interface to prevent BSR messages from being sent or received through an interface.

Static RP Overview

If you are configuring PIM sparse mode, you must configure a PIM RP for a multicast group. An RP can either be configured statically in each device, or learned through a dynamic mechanism. This task explains how to statically configure an RP, as opposed to the router learning the RP through a dynamic mechanism such as Auto-RP.

PIM designated routers (DRs) forward data from directly connected multicast sources to the RP for distribution down the shared tree. Data is forwarded to the RP in one of two ways. It is encapsulated in register packets and unicast directly to the RP, or, if the RP has itself joined the source tree, it is multicast forwarded per the RPF forwarding algorithm. Last hop routers directly connected to receivers may, at their discretion, join themselves to the source tree and prune themselves from the shared tree.

A single RP can be configured for multiple groups that are defined by an access list. If no RP is configured for a group, the router treats the group as dense using the PIM dense mode techniques. (You can prevent this occurrence by configuring the **no ip pim dm-fallback**command.)

If dynamic and static group-to-RP mappings are used together and there is an RP address conflict, the RP address configured for a static group-to-RP mapping (with the **ip pim rp-address override**command) will take precedence.

Note If the **override** keyword is not specified and there is RP address conflict, dynamic group-to-RP mappings will take precedence over static group-to-RP mappings.

SSM Overview

Source Specific Multicast (SSM). SSM is an extension of IP multicast where datagram traffic is forwarded to receivers from only those multicast sources that the receivers have explicitly joined. For multicast groups configured for SSM, only source-specific multicast distribution trees (not shared trees) are created.

SSM Components

Source Specific Multicast (SSM) is a datagram delivery model that best supports one-to-many applications, also known as broadcast applications. SSM is a core networking technology for the Cisco implementation of IP multicast solutions targeted for audio and video broadcast application environments and is described in RFC 3569. The following two components together support the implementation of SSM:

- Protocol Independent Multicast source-specific mode (PIM-SSM)
- Internet Group Management Protocol Version 3 (IGMPv3)

Protocol Independent Multicast (PIM) SSM, or PIM-SSM, is the routing protocol that supports the implementation of SSM and is derived from PIM sparse mode (PIM-SM). IGMP is the Internet Engineering Task Force (IETF) standards track protocol used for hosts to signal multicast group membership to routers. IGMP Version 3 supports source filtering, which is required for SSM. In order for SSM to run with IGMPv3, SSM must be supported in the device, the host where the application is running, and the application itself.

How SSM Differs from Internet Standard Multicast

The standard IP multicast infrastructure in the Internet and many enterprise intranets is based on the PIM-SM protocol and Multicast Source Discovery Protocol (MSDP). These protocols have proved to be reliable, extensive, and efficient. However, they are bound to the complexity and functionality limitations of the Internet Standard Multicast (ISM) service model. For example, with ISM, the network must maintain knowledge about which hosts in the network are actively sending multicast traffic. With SSM, this information is provided by receivers through the source addresses relayed to the last-hop devices by IGMPv3. SSM is an incremental response to the issues associated with ISM and is intended to coexist in the network with the protocols developed for ISM. In general, SSM provides IP multicast service for applications that utilize SSM.

ISM service is described in RFC 1112. This service consists of the delivery of IP datagrams from any source to a group of receivers called the multicast host group. The datagram traffic for the multicast host group consists of datagrams with an arbitrary IP unicast source address S and the multicast group address G as the IP destination address. Systems will receive this traffic by becoming members of the host group. Membership in a host group simply requires signaling the host group through IGMP Version 1, 2, or 3.

In SSM, delivery of datagrams is based on (S, G) channels. Traffic for one (S, G) channel consists of datagrams with an IP unicast source address S and the multicast group address G as the IP destination address. Systems

will receive this traffic by becoming members of the (S, G) channel. In both SSM and ISM, no signaling is required to become a source. However, in SSM, receivers must subscribe or unsubscribe to (S, G) channels to receive or not receive traffic from specific sources. In other words, receivers can receive traffic only from (S, G) channels to which they are subscribed, whereas in ISM, receivers need not know the IP addresses of sources from which they receive their traffic. The proposed standard approach for channel subscription signaling utilizes IGMP INCLUDE mode membership reports, which are supported only in IGMP Version 3.

SSM can coexist with the ISM service by applying the SSM delivery model to a configured subset of the IP multicast group address range. The Internet Assigned Numbers Authority (IANA) has reserved the address range from 232.0.0.0 through 232.255.255.255 for SSM applications and protocols. The software allows SSM configuration for an arbitrary subset of the IP multicast address range from 224.0.0.0 through 239.255.255.255. When an SSM range is defined, an existing IP multicast receiver application will not receive any traffic when it tries to use addresses in the SSM range unless the application is modified to use explicit (S, G) channel subscription or is SSM-enabled through a URL Rendezvous Directory (URD).

SSM can coexist with the ISM service by applying the SSM delivery model to a configured subset of the IP multicast group address range. The Internet Assigned Numbers Authority (IANA) has reserved the address range from 232.0.0.0 through 232.255.255.255 for SSM applications and protocols. The software allows SSM configuration for an arbitrary subset of the IP multicast address range from 224.0.0.0 through 239.255.255.255. When an SSM range is defined, an existing IP multicast receiver application will not receive any traffic when it tries to use addresses in the SSM range unless the application is modified to use explicit (S, G) channel subscription or is SSM-enabled.

SSM Operations

An established network in which IP multicast service is based on PIM-SM can support SSM services. SSM can also be deployed alone in a network without the full range of protocols that are required for interdomain PIM-SM. That is, SSM does not require an RP, so there is no need for an RP mechanism such as Auto-RP, MSDP, or bootstrap router (BSR).

If SSM is deployed in a network that is already configured for PIM-SM, then only the last-hop devices must be upgraded to a software image that supports SSM. Routers that are not directly connected to receivers do not have to upgrade to a software image that supports SSM. In general, these non-last-hop devices must only run PIM-SM in the SSM range. They may need additional access control configuration to suppress MSDP signaling, registering, or PIM-SM shared-tree operations from occurring within the SSM range.

The SSM mode of operation is enabled by configuring the SSM range using the **ip pim ssm** global configuration command. This configuration has the following effects:

- For groups within the SSM range, (S, G) channel subscriptions are accepted through IGMPv3 INCLUDE mode membership reports.
- PIM operations within the SSM range of addresses change to PIM-SSM, a mode derived from PIM-SM. In this mode, only PIM (S, G) Join and Prune messages are generated by the device. Incoming messages related to rendezvous point tree (RPT) operations are ignored or rejected, and incoming PIM register messages are immediately answered with Register-Stop messages. PIM-SSM is backward-compatible with PIM-SM unless a device is a last-hop device. Therefore, devices that are not last-hop devices can run PIM-SM for SSM groups (for example, if they do not yet support SSM).
- For groups within the SSM range, no MSDP Source-Active (SA) messages within the SSM range will be accepted, generated, or forwarded.

IGMPv3 Host Signaling

IGMPv3 is the third version of the IETF standards track protocol in which hosts signal membership to last-hop devices of multicast groups. IGMPv3 introduces the ability for hosts to signal group membership that allows filtering capabilities with respect to sources. A host can signal either that it wants to receive traffic from all sources sending to a group except for some specific sources (a mode called EXCLUDE) or that it wants to receive traffic only from some specific sources sending to the group (a mode called INCLUDE).

IGMPv3 can operate with both ISM and SSM. In ISM, both EXCLUDE and INCLUDE mode reports are accepted by the last-hop router. In SSM, only INCLUDE mode reports are accepted by the last-hop router.

Benefits of Source Specific Multicast

IP Multicast Address Management Not Required

In the ISM service, applications must acquire a unique IP multicast group address because traffic distribution is based only on the IP multicast group address used. If two applications with different sources and receivers use the same IP multicast group address, then receivers of both applications will receive traffic from the senders of both applications. Even though the receivers, if programmed appropriately, can filter out the unwanted traffic, this situation would cause generally unacceptable levels of unwanted traffic.

Allocating a unique IP multicast group address for an application is still a problem. Most short-lived applications use mechanisms like Session Description Protocol (SDP) and Session Announcement Protocol (SAP) to get a random address, a solution that does not work well with a rising number of applications in the Internet. The best current solution for long-lived applications is described in RFC 2770, but this solution suffers from the restriction that each autonomous system is limited to only 255 usable IP multicast addresses.

In SSM, traffic from each source is forwarded between devices in the network independent of traffic from other sources. Thus different sources can reuse multicast group addresses in the SSM range.

Denial of Service Attacks from Unwanted Sources Inhibited

In SSM, multicast traffic from each individual source will be transported across the network only if it was requested (through IGMPv3, IGMP v3lite, or URD memberships) from a receiver. In contrast, ISM forwards traffic from any active source sending to a multicast group to all receivers requesting that multicast group. In Internet broadcast applications, this ISM behavior is highly undesirable because it allows unwanted sources to easily disturb the actual Internet broadcast source by simply sending traffic to the same multicast group. This situation depletes bandwidth at the receiver side with unwanted traffic and thus disrupts the undisturbed reception of the Internet broadcast. In SSM, this type of denial of service (DoS) attack cannot be made by simply sending traffic to a multicast group.

Easy to Install and Manage

SSM is easy to install and provision in a network because it does not require the network to maintain which active sources are sending to multicast groups. This requirement exists in ISM (with IGMPv1, IGMPv2, or IGMPv3).

The current standard solutions for ISM service are PIM-SM and MSDP. Rendezvous point (RP) management in PIM-SM (including the necessity for Auto-RP or BSR) and MSDP is required only for the network to learn about active sources. This management is not necessary in SSM, which makes SSM easier than ISM to install and manage, and therefore easier than ISM to operationally scale in deployment. Another factor that contributes to the ease of installation of SSM is the fact that it can leverage preexisting PIM-SM networks and requires only the upgrade of last hop devices to support IGMPv3, IGMP v3lite, or URD.

Ideal for Internet Broadcast Applications

The three benefits previously described make SSM ideal for Internet broadcast-style applications for the following reasons:

- The ability to provide Internet broadcast services through SSM without the need for unique IP multicast addresses allows content providers to easily offer their service (IP multicast address allocation has been a serious problem for content providers in the past).
- The prevention against DoS attacks is an important factor for Internet broadcast services because, with their exposure to a large number of receivers, they are the most common targets for such attacks.
- The ease of installation and operation of SSM makes it ideal for network operators, especially in those cases where content needs to be forwarded between multiple independent PIM domains (because there is no need to manage MSDP for SSM between PIM domains).

Bidir-PIM Overview

Bidir-PIM shares many of its shortest path tree (SPT) operations with PIM-SM. Bidir-PIM also has unconditional forwarding of source traffic toward the RP upstream on the shared tree, but has no registering process for sources as in PIM-SM. These modifications allow forwarding of traffic in all routers based solely on the (*, G) multicast routing entries. This form of forwarding eliminates any source-specific state and allows scaling capability to an arbitrary number of sources.

Multicast Group Modes

In PIM, packet traffic for a multicast group is routed according to the rules of the mode configured for that multicast group. The Cisco implementation of PIM supports four modes for a multicast group:

- PIM bidirectional mode
- PIM dense mode
- PIM sparse mode
- PIM Source Specific Mode (SSM)

A router can simultaneously support all four modes or any combination of them for different multicast groups.

Bidirectional Shared Tree

In bidirectional mode, traffic is routed only along a bidirectional shared tree that is rooted at the rendezvous point (RP) for the group. In bidir-PIM, the IP address of the RP acts as the key to having all routers establish a loop-free spanning tree topology rooted in that IP address. This IP address need not be a router, but can be any unassigned IP address on a network that is reachable throughout the PIM domain. This technique is the preferred configuration method for establishing a redundant RP configuration for bidir-PIM.

Membership in a bidirectional group is signaled by way of explicit Join messages. Traffic from sources is unconditionally sent up the shared tree toward the RP and passed down the tree toward the receivers on each branch of the tree.

The figures below show the difference in state created per router for a unidirectional shared tree and source tree versus a bidirectional shared tree.

Figure 7: Unidirectional Shared Tree and Source Tree

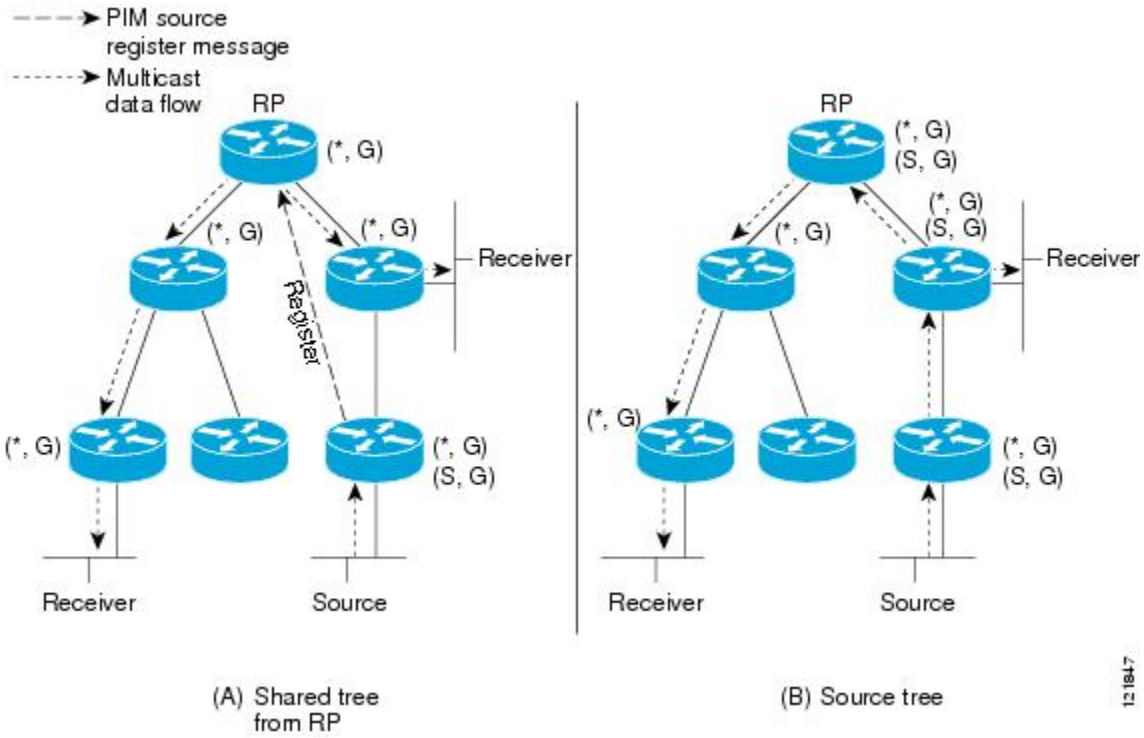
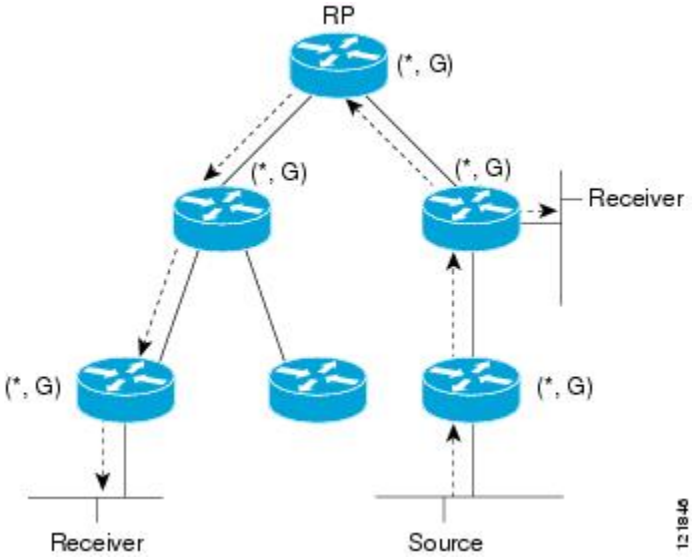


Figure 8: Bidirectional Shared Tree



For packets that are forwarded downstream from the RP toward receivers, there are no fundamental differences between bidir-PIM and PIM-SM. Bidir-PIM deviates substantially from PIM-SM for traffic that is passed from sources upstream toward the RP.

PIM-SM cannot forward traffic in the upstream direction of a tree because it accepts traffic from only one Reverse Path Forwarding (RPF) interface. This interface (for the shared tree) points toward the RP, thus allowing only downstream traffic flow. Upstream traffic is first encapsulated into unicast register messages, which are passed from the designated router (DR) of the source toward the RP. Second, the RP joins an SPT that is rooted at the source. Therefore, in PIM-SM, traffic from sources destined for the RP does not flow upstream in the shared tree, but downstream along the SPT of the source until it reaches the RP. From the RP, traffic flows along the shared tree toward all receivers.

In bidir-PIM, the packet-forwarding rules have been improved over PIM-SM, allowing traffic to be passed up the shared tree toward the RP. To avoid multicast packet looping, bidir-PIM introduces a new mechanism called designated forwarder (DF) election, which establishes a loop-free SPT rooted at the RP.

DF Election

On every network segment and point-to-point link, all PIM routers participate in a procedure called designated forwarder (DF) election. The procedure selects one router as the DF for every RP of bidirectional groups. This router is responsible for forwarding multicast packets received on that network.

The DF election is based on unicast routing metrics. The router with the most preferred unicast routing metric to the RP becomes the DF. Use of this method ensures that only one copy of every packet will be sent to the RP, even if there are parallel equal-cost paths to the RP.

A DF is selected for every RP of bidirectional groups. As a result, multiple routers may be elected as DF on any network segment, one for each RP. Any particular router may be elected as DF on more than one interface.

Bidirectional Group Tree Building

The procedure for joining the shared tree of a bidirectional group is almost identical to that used in PIM-SM. One main difference is that, for bidirectional groups, the role of the DR is assumed by the DF for the RP.

On a network that has local receivers, only the router elected as the DF populates the outgoing interface list (olist) upon receiving Internet Group Management Protocol (IGMP) Join messages, and sends (*, G) Join and Leave messages upstream toward the RP. When a downstream router wishes to join the shared tree, the RPF neighbor in the PIM Join and Leave messages is always the DF elected for the interface that lead to the RP.

When a router receives a Join or Leave message, and the router is not the DF for the receiving interface, the message is ignored. Otherwise, the router updates the shared tree in the same way as in sparse mode.

In a network where all routers support bidirectional shared trees, (S, G) Join and Leave messages are ignored. There is also no need to send PIM assert messages because the DF election procedure eliminates parallel downstream paths from any RP. An RP never joins a path back to the source, nor will it send any register stops.

Packet Forwarding

A router creates (*, G) entries only for bidirectional groups. The olist of a (*, G) entry includes all the interfaces for which the router has been elected DF and that have received either an IGMP or PIM Join message. If a router is located on a sender-only branch, it will also create a (*, G) state, but the olist will not include any interfaces.

If a packet is received from the RPF interface toward the RP, the packet is forwarded downstream according to the olist of the (*, G) entry. Otherwise, only the router that is the DF for the receiving interface forwards the packet upstream toward the RP; all other routers must discard the packet.

Benefits of Bidirectional PIM

- Bidir-PIM removes the performance cost of maintaining a routing state table for a large number of sources.
- Bidir-PIM is designed to be used for many-to-many applications within individual PIM domains. Multicast groups in bidirectional PIM mode can scale to an arbitrary number of sources without incurring overhead due to the number of sources.

How to Configure Basic IP Multicast

The tasks described in this section configure the basic IP multicast modes. No single task in this section is required; however, at least one of the tasks must be performed to configure IP multicast in a network. More than one of the tasks may be needed.

Configuring Sparse Mode with Auto-RP(CLI)

Before You Begin

- An interface configured in sparse-dense mode is treated in either sparse mode or dense mode of operation, depending on the mode in which the multicast group operates. You must decide how to configure your interfaces.
- All access lists that are needed when Auto-RP is configured should be configured prior to beginning the configuration task.

Note

- If a group has no known RP and the interface is configured to be sparse-dense mode, the interface is treated as if it were in dense mode, and data is flooded over the interface. To avoid this data flooding, configure the Auto-RP listener and then configure the interface as sparse mode.
- When configuring Auto-RP, you must either configure the Auto-RP listener feature (Step 5) and specify sparse mode (Step 7) or specify sparse-dense mode (Step 8) .
- When you configure sparse-dense mode, dense mode failover may result in a network dense-mode flood. To avoid this condition, use PIM sparse mode with the Auto-RP listener feature.

Follow this procedure to configure auto-rendezvous point (Auto-RP). Auto-RP can also be optionally used with anycast RP.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip multicast-routing** [**distributed**]
4. Either perform Steps 5 through 7 or perform Steps 6 and 8.
5. **ip pim autorp listener**
6. **interface** *type number*
7. **ip pim sparse-mode**
8. **ip pim sparse-dense-mode**
9. **exit**
10. Repeat Steps 1 through 9 on all PIM interfaces.
11. **ip pim send-rp-announce** {*interface-type interface-number* | *ip-address*} **scope** *ttl-value* [**group-list** *access-list*] [**interval** *seconds*] [**bidir**]
12. **ip pim send-rp-discovery** [*interface-type interface-number*] **scope** *ttl-value* [**interval** *seconds*]
13. **ip pim rp-announce-filter rp-list** *access-list* **group-list** *access-list*
14. **no ip pim dm-fallback**
15. **interface** *type number*
16. **ip multicast boundary** *access-list* [**filter-autorp**]
17. **end**
18. **show ip pim autorp**
19. **show ip pim rp** [**mapping**] [*rp-address*]
20. **show ip igmp groups** [*group-name* | *group-address*| *interface-type interface-number*] [**detail**]
21. **show ip mroute** [*group-address* | *group-name*] [*source-address* | *source-name*] [*interface-type interface-number*] [**summary**] [**count**] [**active** *kbps*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `SwitchControllerDevice> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `SwitchControllerDevice# configure terminal`	Enters global configuration mode.
Step 3	**ip multicast-routing** [**distributed**]	Enables IP multicast routing.

	Command or Action	Purpose
	Example: `SwitchControllerDevice(config)# ip multicast-routing`	• Use the **distributed** keyword to enabled Multicast Distributed Switching.
Step 4	Either perform Steps 5 through 7 or perform Steps 6 and 8.	--
Step 5	**ip pim autorp listener** **Example:** `SwitchControllerDevice(config)# ip pim autorp listener`	Causes IP multicast traffic for the two Auto-RP groups 224.0.1.39 and 224.0.1.40 to be PIM dense mode flooded across interfaces operating in PIM sparse mode. • Skip this step if you are configuring sparse-dense mode in Step 8.
Step 6	**interface** *type number* **Example:** `SwitchControllerDevice(config)# interface Gigabitethernet 1/0/0`	Selects an interface that is connected to hosts on which PIM can be enabled.
Step 7	**ip pim sparse-mode** **Example:** `SwitchControllerDevice(config-if)# ip pim sparse-mode`	Enables PIM sparse mode on an interface. When configuring Auto-RP in sparse mode, you must also configure the Auto-RP listener in the next step. • Skip this step if you are configuring sparse-dense mode in Step 8.
Step 8	**ip pim sparse-dense-mode** **Example:** `SwitchControllerDevice(config-if)# ip pim sparse-dense-mode`	Enables PIM sparse-dense mode on an interface. • Skip this step if you configured sparse mode in Step 7.
Step 9	**exit** **Example:** `SwitchControllerDevice(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.
Step 10	Repeat Steps 1 through 9 on all PIM interfaces.	--
Step 11	**ip pim send-rp-announce** {*interface-type interface-number* | *ip-address*} **scope** *ttl-value* [**group-list** *access-list*] [**interval** *seconds*] [**bidir**]	Sends RP announcements out all PIM-enabled interfaces. • Perform this step on the RP device only. • Use the *interface-type*and *interface-number* arguments to define which IP address is to be used as the RP address.

	Command or Action	Purpose
	Example: `SwitchControllerDevice(config)# ip pim send-rp-announce loopback0 scope 31 group-list 5`	• Use the *ip-address* argument to specify a directly connected IP address as the RP address. **Note** If the *ip-address* argument is configured for this command, the RP-announce message will be sourced by the interface to which this IP address is connected (that is, the source address in the IP header of the RP-announce message is the IP address of that interface). • This example shows that the interface is enabled with a maximum of 31 hops. The IP address by which the device wants to be identified as RP is the IP address associated with loopback interface 0. Access list 5 describes the groups for which this device serves as RP.
Step 12	**ip pim send-rp-discovery** [*interface-type interface-number*] **scope** *ttl-value* [**interval** *seconds*] **Example:** `SwitchControllerDevice(config)# ip pim send-rp-discovery loopback 1 scope 31`	Configures the device to be an RP mapping agent. • Perform this step on RP mapping agent devices or on combined RP/RP mapping agent devices. **Note** Auto-RP allows the RP function to run separately on one device and the RP mapping agent to run on one or multiple devices. It is possible to deploy the RP and the RP mapping agent on a combined RP/RP mapping agent device. • Use the optional *interface-type* and *interface-number* arguments to define which IP address is to be used as the source address of the RP mapping agent. • Use the **scope** keyword and *ttl-value* argument to specify the Time-to-Live (TTL) value in the IP header of Auto-RP discovery messages. • Use the optional **interval** keyword and *seconds* argument to specify the interval at which Auto-RP discovery messages are sent. **Note** Lowering the interval at which Auto-RP discovery messages are sent from the default value of 60 seconds results in more frequent floodings of the group-to-RP mappings. In some network environments, the disadvantages of lowering the interval (more control packet overhead) may outweigh the advantages (more frequent group-to-RP mapping updates). • The example shows limiting the Auto-RP discovery messages to 31 hops on loopback interface 1.
Step 13	**ip pim rp-announce-filter rp-list** *access-list* **group-list** *access-list*	Filters incoming RP announcement messages sent from candidate RPs (C-RPs) to the RP mapping agent.

	Command or Action	Purpose
	Example: `SwitchControllerDevice(config)# ip pim rp-announce-filter rp-list 1 group-list 2`	• Perform this step on the RP mapping agent only.
Step 14	**no ip pim dm-fallback** **Example:** `SwitchControllerDevice(config)# no ip pim dm-fallback`	(Optional) Prevents PIM dense mode fallback. • Skip this step if all interfaces have been configured to operate in PIM sparse mode. **Note** The **no ip pim dm-fallback** command behavior is enabled by default if all the interfaces are configured to operate in PIM sparse mode (using the **ip pim sparse-mode** command).
Step 15	**interface** *type number* **Example:** `SwitchControllerDevice(config)# interface gigabitethernet 1/0/0`	Selects an interface that is connected to hosts on which PIM can be enabled.
Step 16	**ip multicast boundary** *access-list* [**filter-autorp**] **Example:** `SwitchControllerDevice(config-if)# ip multicast boundary 10 filter-autorp`	Configures an administratively scoped boundary. • Perform this step on the interfaces that are boundaries to other devices. • The access list is not shown in this task. • An access list entry that uses the **deny** keyword creates a multicast boundary for packets that match that entry.
Step 17	**end** **Example:** `SwitchControllerDevice(config-if)# end`	Returns to global configuration mode.
Step 18	**show ip pim autorp** **Example:** `SwitchControllerDevice# show ip pim autorp`	(Optional) Displays the Auto-RP information.
Step 19	**show ip pim rp** [**mapping**] [*rp-address*] **Example:** `SwitchControllerDevice# show ip pim rp mapping`	(Optional) Displays RPs known in the network and shows how the device learned about each RP.

	Command or Action	Purpose
Step 20	**show ip igmp groups** [*group-name* | *group-address*| *interface-type interface-number*] [**detail**] **Example:** `SwitchControllerDevice# show ip igmp groups`	(Optional) Displays the multicast groups having receivers that are directly connected to the device and that were learned through Internet Group Management Protocol (IGMP). • A receiver must be active on the network at the time that this command is issued in order for receiver information to be present on the resulting display.
Step 21	**show ip mroute** [*group-address* | *group-name*] [*source-address* | *source-name*] [*interface-type interface-number*] [**summary**] [**count**] [**active** *kbps*] **Example:** `SwitchControllerDevice# show ip mroute cbone-audio`	(Optional) Displays the contents of the IP multicast routing (mroute) table.

What to Do Next

Proceed to the “ Verifying IP Multicast Operation ” module.

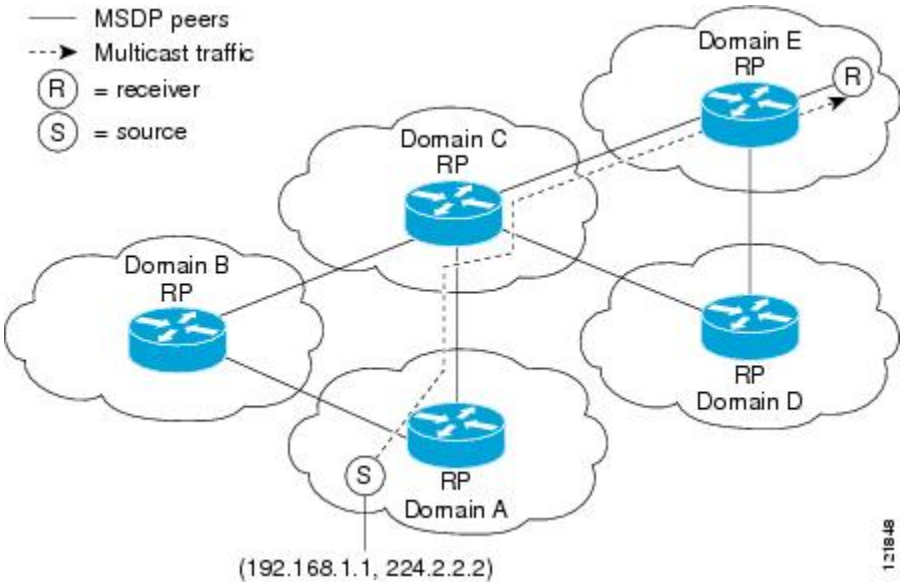
Configuring Sparse Mode with Anycast RP

This section describes how to configure sparse mode with anycast RP for RP redundancy.

Anycast RPs are configured statically, and interfaces are configured to operate in Protocol Independent Multicast-Sparse Mode (PIM-SM). In an anycast RP configuration, two or more RPs are configured with the same IP address on loopback interfaces. The Anycast RP loopback address should be configured with a 32-bit mask, making it a host address. An Anycast RP configuration is easy to configure and troubleshoot because the same host address is used as the RP address regardless of which router it is configured on.

Anycast RP allows two or more rendezvous points (RPs) to share the load for source registration and have the ability to act as hot backup routers for each other. Multicast Source Discovery Protocol (MSDP) is the key protocol that makes anycast RP possible.

Figure 9: MSDP Sharing Source Information Between RPs in Each Domain



SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip multicast-routing** [**distributed**]
4. **interface** *type number*
5. **ip pim sparse-mode**
6. **ip pim rp-address** *rp-address*
7. Repeat Steps 1 through 6 on two or more routers assigning the same RP address to each.
8. **interface loopback** [*interface-number*] **ip address** [*ip-address*] [*mask*]
9. **interface loopback** [*interface-number*] **ip address** [*ip-address*] [*mask*]
10. **exit**
11. **ip msdp peer** {*peer-name* | *peer-address*} [**connect-source** *interface-type* **interface-number**] [**remote-as** *as-number*]
12. **ip msdp originator-id loopback** [*interface*]
13. Repeat Steps 8 through 12 on the redundant RPs.

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip multicast-routing** [**distributed**] **Example:** `Router(config)# ip multicast-routing`	Enables IP multicast routing. • Use the **distributed** keyword to enable Multicast Distributed Switching.
Step 4	**interface** *type number* **Example:** `Router(config)# interface gigabitethernet 1/0/0`	Selects an interface that is connected to hosts on which PIM can be enabled.
Step 5	**ip pim sparse-mode** **Example:** `Router(config-if)# ip pim sparse-mode`	Enables sparse mode.
Step 6	**ip pim rp-address** *rp-address* **Example:** `Router(config-if)# ip pim rp-address 10.0.0.1`	Configures the address of a PIM RP for a particular group.
Step 7	Repeat Steps 1 through 6 on two or more routers assigning the same RP address to each.	--

Step 8	**interface loopback** [*interface-number*] **ip address** [*ip-address*] [*mask*]
	
	Example:
	`Router(config-if)# interface loopback 0`
	
	Example:
	`ip address 10.0.0.1 255.255.255.255`
		Configures the interface loopback IP address for the RP router.
		• Perform this step on the RP routers.

	Command or Action	Purpose

Step 9	**interface loopback** [*interface-number*] **ip address** [*ip-address*] [*mask*]
	
	Example:
	`Router(config-if)# interface loopback 1`
	
	Example:
	`ip address 10.1.1.1 255.255.255.255`
		Configures the interface loopback IP address for MSDP peering.

Step 10	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.
Step 11	**ip msdp peer** {*peer-name* | *peer-address*} [**connect-source** *interface-type* **interface-number**] [**remote-as** *as-number*] **Example:** `Router(config)# ip msdp peer 10.1.1.2 connect-source loopback 1`	Configures an MSDP peer. • Perform this step on the RP routers.
Step 12	**ip msdp originator-id loopback** [*interface*] **Example:** `Router(config)# ip msdp originator-id loopback 1`	Allows an MSDP speaker that originates a SA message to use the IP address of the interface as the RP address in the SA message. • Perform this step on the RP routers.
Step 13	Repeat Steps 8 through 12 on the redundant RPs.	--

What to Do Next

Proceed to the " Verifying IP Multicast Operation " module.

Configuring Sparse Mode with a Bootstrap Router

This section describes how to configure a bootstrap router (BSR), which provides a fault-tolerant, automated RP discovery and distribution mechanism so that routers learn the group-to-RP mappings dynamically.

Note The simultaneous deployment of Auto-RP and BSR is not supported.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip multicast-routing** [**distributed**]
4. **interface** *type number*
5. **ip pim sparse-mode**
6. **end**
7. Repeat Steps 1 through 6 on every multicast-enabled interface on every router.
8. **ip pim bsr-candidate** *interface-type interface-number* [*hash-mask-length* [*priority*]]
9. **ip pim rp-candidate** *interface-type interface-number* [group-list *access-list*] [**interval** seconds] [**priority** *value*]
10. Repeat Steps 8 through 10 on all RP and BSR routers.
11. **interface** *type number*
12. **ip pim bsr-border**
13. **end**
14. Repeat Steps 11 through 13 on all the routers that have boundary interfaces where the messages should not be sent or received.
15. **show ip pim rp** [**mapping**] [*rp-address*]
16. **show ip pim rp-hash** [*group-address*] [*group-name*]
17. **show ip pim bsr-router**
18. **show ip igmp groups** [*group-name* | *group-address*| *interface-type interface-number*] [**detail**]
19. **show ip mroute**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip multicast-routing** [**distributed**] **Example:** `Router(config)# ip multicast-routing`	Enables IP multicast routing. • Use the **distributed** keyword to enable Multicast Distributed Switching.

	Command or Action	Purpose
Step 4	**interface** *type number* **Example:** `Router(config)# interface gigabitethernet 1/0/0`	Selects an interface that is connected to hosts on which PIM can be enabled.
Step 5	**ip pim sparse-mode** **Example:** `Router(config-if)# ip pim sparse-mode`	Enables sparse mode.
Step 6	**end** **Example:** `Router(config-if)# end`	Returns to global configuration mode.
Step 7	Repeat Steps 1 through 6 on every multicast-enabled interface on every router.	--
Step 8	**ip pim bsr-candidate** *interface-type interface-number* [*hash-mask-length* [*priority*]] **Example:** `Router(config)# ip pim bsr-candidate gigibitethernet 0/0/0 0 192`	Configures the router to announce its candidacy as a bootstrap router (BSR). • Perform this step on the RP or on combined RP/BSR routers. **Note** BSR allows the RP function to run separately on one router and the BSR to run on one or multiple routers. It is possible to deploy the RP and the BSR on a combined RP/BSR router. • This command configures the router to send BSR messages to all its PIM neighbors, with the address of the designated interface (configured for the *interface-type* and *interface-number*arguments) as the BSR address. • Use the optional *hash-mask-length* argument to set the length of a mask (32 bits maximum) that is to be ANDed with the group address before the PIMv2 hash function is called. All groups with the same seed hash (correspond) to the same RP. For example, if this value is 24, only the first 24 bits of the group addresses matter. The hash mask length allows one RP to be used for multiple groups. The default hash mask length is 0. • Use the optional *priority* argument (after you set the hash mask length) to specify the priority of the BSR as a C-RP. The priority range is from 0 to 255. The BSR C-RP with the highest priority (the lowest priority value) is preferred. If the priority values are the same, the router with the higher IP address is preferred. The default priority value is 0.

	Command or Action	Purpose
		Note The Cisco IOS and Cisco IOS XE implementation of PIM BSR uses the value 0 as the default priority for candidate RPs and BSRs. This implementation predates the draft-ietf-pim-sm-bsr IETF draft, the first IETF draft to specify 192 as the default priority value. The Cisco IOS and Cisco IOS XE implementation, thus, deviates from the IETF draft. To comply with the default priority value specified in the draft, you must explicitly set the priority value to 192.
Step 9	**ip pim rp-candidate** *interface-type interface-number* [group-list *access-list*] [**interval** seconds] [**priority** *value*] **Example:** `Router(config)# ip pim rp-candidate gigabitethernet 2/0/0 group-list 4 priority 192`	Configures the router to advertise itself as a PIM Version 2 candidate RP to the BSR. • Perform this step on the RP or on combined RP/BSR routers. **Note** BSR allows the RP function to run separately on one router and the BSR to run on one or multiple routers. It is possible to deploy the RP and the BSR on a combined RP/BSR router. • When an interval is specified, the candidate RP advertisement interval is set to the number of seconds specified. The default interval is 60 seconds. Tuning this interval down can reduce the time required to fail over to a secondary RP at the expense of generating more PIMv2 messages. • The Cisco IOS and Cisco IOS XE implementation of PIM BSR selects an RP from a set of candidate RPs using a method that is incompatible with the specification in RFC 2362. See the BSR and RFC 2362 Interoperable Candidate RP Example, on page 61 section for a configuration workaround. See CSCdy56806 using the Cisco Bug Toolkit for more information. **Note** The Cisco IOS and Cisco IOS XE implementation of PIM BSR uses the value 0 as the default priority for candidate RPs and BSRs. This implementation predates the draft-ietf-pim-sm-bsr IETF draft, the first IETF draft to specify 192 as the default priority value. The Cisco IOS and Cisco IOS XE implementation, thus, deviates from the IETF draft. To comply with the default priority value specified in the draft, you must explicitly set the priority value to 192.
Step 10	Repeat Steps 8 through 10 on all RP and BSR routers.	--
Step 11	**interface** *type number* **Example:** `Router(config)# interface gigabitethernet 1/0/0`	Selects an interface that is connected to hosts on which PIM can be enabled.

	Command or Action	Purpose
Step 12	**ip pim bsr-border** **Example:** `Router(config-if)# ip pim bsr-border`	Prevents the bootstrap router (BSR) messages from being sent or received through an interface. • See the BSR Border Interface, on page 32 section for more information.
Step 13	**end** **Example:** `Router(config-if)# end`	Ends the current configuration session and returns to privileged EXEC mode.
Step 14	Repeat Steps 11 through 13 on all the routers that have boundary interfaces where the messages should not be sent or received.	--
Step 15	**show ip pim rp** [**mapping**] [*rp-address*] **Example:** `Router# show ip pim rp`	(Optional) Displays active rendezvous points (RPs) that are cached with associated multicast routing entries.
Step 16	**show ip pim rp-hash** [*group-address*] [*group-name*] **Example:** `Router# show ip pim rp-hash 239.1.1.1`	(Optional) Displays which rendezvous point (RP) is being selected for a specified group.
Step 17	**show ip pim bsr-router** **Example:** `Router# show ip pim bsr-router`	(Optional) Displays the bootstrap router (BSR) information.
Step 18	**show ip igmp groups** [*group-name* | *group-address*| *interface-type interface-number*] [**detail**] **Example:** `Router# show ip igmp groups`	(Optional) Displays the multicast groups having receivers that are directly connected to the router and that were learned through IGMP. • A receiver must be active on the network at the time that this command is issued in order for receiver information to be present on the resulting display.
Step 19	**show ip mroute** **Example:** `Router# show ip mroute cbone-audio`	(Optional) Displays the contents of the IP mroute table.

What to Do Next

Proceed to the " Verifying IP Multicast Operation " module.

Configuring Sparse Mode with a Single Static RP(CLI)

A rendezvous point (RP) is required in networks running Protocol Independent Multicast sparse mode (PIM-SM). In PIM-SM, traffic will be forwarded only to network segments with active receivers that have explicitly requested multicast data.

This section describes how to configure sparse mode with a single static RP.

Before You Begin

All access lists that are needed when sparse mode is configured with a single static RP should be configured prior to beginning the configuration task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip multicast-routing** [**distributed**]
4. **interface** *type number*
5. **ip pim sparse-mode**
6. Repeat Steps 1 through 5 on every interface that uses IP multicast.
7. **exit**
8. **ip pim rp-address** *rp-address* [*access-list*] [**override**]
9. **end**
10. **show ip pim rp** [**mapping**] [*rp-address*]
11. **show ip igmp groups** [*group-name* | *group-address*| *interface-type interface-number*] [**detail**]
12. **show ip mroute**
13. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `SwitchControllerDevice> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `SwitchControllerDevice# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**ip multicast-routing** [**distributed**] **Example:** `SwitchControllerDevice(config)# ip multicast-routing`	Enables IP multicast routing. • Use the **distributed** keyword to enable Multicast Distributed Switching.
Step 4	**interface** *type number* **Example:** `SwitchControllerDevice(config)# interface gigabitethernet 1/0/0`	Selects an interface that is connected to hosts on which PIM can be enabled.
Step 5	**ip pim sparse-mode** **Example:** `SwitchControllerDevice(config-if)# ip pim sparse-mode`	Enables PIM on an interface. You must use sparse mode.
Step 6	Repeat Steps 1 through 5 on every interface that uses IP multicast.	--
Step 7	**exit** **Example:** `SwitchControllerDevice(config-if)# exit`	Returns to global configuration mode.
Step 8	**ip pim rp-address** *rp-address* [*access-list*] [**override**] **Example:** `SwitchControllerDevice(config)# ip pim rp-address 192.168.0.0`	Configures the address of a PIM RP for a particular group. • The optional *access-list* argument is used to specify the number or name a standard access list that defines the multicast groups to be statically mapped to the RP. **Note** If no access list is defined, the RP will map to all multicast groups, 224/4. • The optional **override** keyword is used to specify that if dynamic and static group-to-RP mappings are used together and there is an RP address conflict, the RP address configured for a static group-to-RP mapping will take precedence. **Note** If the **override** keyword is not specified and there is RP address conflict, dynamic group-to-RP mappings will take precedence over static group-to-RP mappings.
Step 9	**end** **Example:** `SwitchControllerDevice(config)# end`	Ends the current configuration session and returns to EXEC mode.

	Command or Action	Purpose
Step 10	**show ip pim rp** [**mapping**] [*rp-address*] **Example:** `SwitchControllerDevice# show ip pim rp mapping`	(Optional) Displays RPs known in the network and shows how the router learned about each RP.
Step 11	**show ip igmp groups** [*group-name* | *group-address*| *interface-type interface-number*] [**detail**] **Example:** `SwitchControllerDevice# show ip igmp groups`	(Optional) Displays the multicast groups having receivers that are directly connected to the router and that were learned through IGMP. • A receiver must be active on the network at the time that this command is issued in order for receiver information to be present on the resulting display.
Step 12	**show ip mroute** **Example:** `SwitchControllerDevice# show ip mroute`	(Optional) Displays the contents of the IP mroute table.
Step 13	**copy running-config startup-config** **Example:** `SwitchControllerDevice# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

What to Do Next

Proceed to the “ Verifying IP Multicast Operation ” module.

Configuring Source Specific Multicast

Follow these steps to configure SSM:

Before You Begin

If you want to use an access list to define the Source Specific Multicast (SSM) range, configure the access list before you reference the access list in the **ip pim ssm** command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip multicast-routing** [**distributed**]
4. **ip pim ssm** {**default** | **range** *access-list*}
5. **interface** *type number*
6. **ip pim sparse-mode**
7. Repeat Steps 1 through 6 on every interface that uses IP multicast.
8. **ip igmp version 3**
9. Repeat Step 8 on all host-facing interfaces.
10. **end**
11. **show ip igmp groups** [*group-name* | *group-address*| *interface-type interface-number*] [**detail**]
12. **show ip mroute**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `SwitchControllerDevice> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `SwitchControllerDevice# configure terminal`	Enters global configuration mode.
Step 3	**ip multicast-routing** [**distributed**] **Example:** `SwitchControllerDevice(config)# ip multicast-routing`	Enables IP multicast routing. • Use the **distributed** keyword to enable Multicast Distributed Switching.
Step 4	**ip pim ssm** {**default** | **range** *access-list*} **Example:** `SwitchControllerDevice(config)# ip pim ssm default`	Configures SSM service. • The **default** keyword defines the SSM range access list as 232/8. • The **range** keyword specifies the standard IP access list number or name that defines the SSM range.

	Command or Action	Purpose
Step 5	**interface** *type number* **Example:** `SwitchControllerDevice(config)# interface gigabitethernet 1/0/0`	Selects an interface that is connected to hosts on which IGMPv3 can be enabled.
Step 6	**ip pim sparse-mode** **Example:** `SwitchControllerDevice(config-if)# ip pim sparse-mode`	Enables PIM on an interface. You must use sparse mode.
Step 7	Repeat Steps 1 through 6 on every interface that uses IP multicast.	--
Step 8	**ip igmp version 3** **Example:** `SwitchControllerDevice(config-if)# ip igmp version 3`	Enables IGMPv3 on this interface. The default version of IGMP is set to Version 2. Version 3 is required by SSM.
Step 9	Repeat Step 8 on all host-facing interfaces.	--
Step 10	**end** **Example:** `SwitchControllerDevice(config-if)# end`	Ends the current configuration session and returns to privileged EXEC mode.
Step 11	**show ip igmp groups** [*group-name* | *group-address*| *interface-type interface-number*] [**detail**] **Example:** `SwitchControllerDevice# show ip igmp groups`	(Optional) Displays the multicast groups having receivers that are directly connected to the device and that were learned through IGMP. • A receiver must be active on the network at the time that this command is issued in order for receiver information to be present on the resulting display.
Step 12	**show ip mroute** **Example:** `SwitchControllerDevice# show ip mroute`	(Optional) Displays the contents of the IP mroute table. • This command displays whether a multicast group is configured for SSM service or a source-specific host report has been received.

What to Do Next

Proceed to the “ Verifying IP Multicast Operation ” module.

Configuring Bidirectional PIM

Follow these steps to configure bidirectional PIM:

Before You Begin

All required access lists must be configured before configuring bidirectional PIM.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip multicast-routing** [**distributed**]
4. **interface** *type number*
5. **ip pim sparse-mode**
6. **exit**
7. **ip pim bidir-enable**
8. **ip pim rp-address** *rp-address* [*access-list*] [**override**] **bidir**
9. **end**
10. Repeat Steps 2 through 9 on every multicast-enabled interface on every router.
11. **show ip pim rp** [**mapping**] [*rp-address*]
12. **show ip mroute**
13. **show ip pim interface** [*type number*] [**df** | **count**] [*rp-address*]
14. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device# enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `SwitchControllerDevice# configure terminal`	Enters global configuration mode.
Step 3	**ip multicast-routing** [**distributed**] **Example:** `SwitchControllerDevice(config)# ip multicast-routing`	Enables IP multicast routing. • Use the **distributed** keyword to enable Multicast Distributed Switching.

	Command or Action	Purpose
Step 4	**interface** *type number* **Example:** `SwitchControllerDevice(config)# interface gigabitethernet 1/0/0`	Selects an interface that is connected to hosts on which PIM can be enabled.
Step 5	**ip pim sparse-mode** **Example:** `SwitchControllerDevice(config-if)# ip pim sparse-mode`	Enables sparse mode.
Step 6	**exit** **Example:** `SwitchControllerDevice(config-if)# exit`	Returns to global configuration mode.
Step 7	**ip pim bidir-enable** **Example:** `SwitchControllerDevice(config)# ip pim bidir-enable`	Enables bidir-PIM on a router. • Perform this step on every router.
Step 8	**ip pim rp-address** *rp-address* [*access-list*] [**override**] **bidir** **Example:** `SwitchControllerDevice(config)# ip pim rp-address 10.0.1.1 45 bidir`	Configures the address of a PIM RP for a particular group. • Perform this step on every router. • This command defines the RP as bidirectional and defines the bidirectional group by way of the access list. • The optional **override** keyword is used to specify that if dynamic and static group-to-RP mappings are used together and there is an RP address conflict, the RP address configured for a static group-to-RP mapping will take precedence. **Note** If the **override** keyword is not specified and there is RP address conflict, dynamic group-to-RP mappings will take precedence over static group-to-RP mappings.
Step 9	**end** **Example:** `SwitchControllerDevice(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.
Step 10	Repeat Steps 2 through 9 on every multicast-enabled interface on every router.	--

	Command or Action	Purpose
Step 11	**show ip pim rp** [**mapping**] [*rp-address*] **Example:** `Device# show ip pim rp`	(Optional) Displays active RPs that are cached with associated multicast routing entries.
Step 12	**show ip mroute** **Example:** `SwitchControllerDevice# show ip mroute`	(Optional) Displays the contents of the IP mroute table.
Step 13	**show ip pim interface** [*type number*] [**df** | **count**] [*rp-address*] **Example:** `Device# show ip pim interface`	(Optional) Displays information about the elected DF for each RP of an interface, along with the unicast routing metric associated with the DF.
Step 14	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Configuration Examples for Basic IP Multicast

Example: Sparse Mode with Auto-RP

The following example configures sparse mode with Auto-RP:

```
ip multicast-routing
ip pim autorp listener
ip pim send-rp-announce Loopback0 scope 16 group-list 1
ip pim send-rp-discovery Loopback1 scope 16
no ip pim dm-fallback
access-list 1 permit 239.254.2.0 0.0.0.255
access-list 1 permit 239.254.3.0 0.0.0.255
.
.
.
access-list 10 permit 224.0.1.39
access-list 10 permit 224.0.1.40
access-list 10 permit 239.254.2.0 0.0.0.255
access-list 10 permit 239.254.3.0 0.0.0.255
```

Sparse Mode with Anycast RP Example

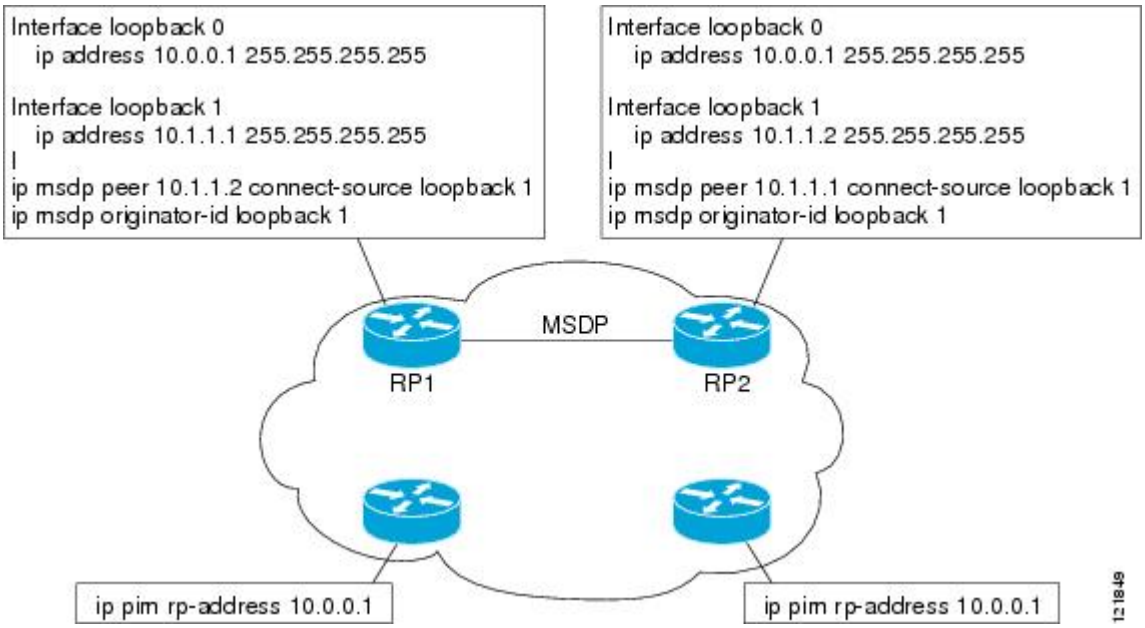
The main purpose of an Anycast RP implementation is that the downstream multicast routers will have just one address for an RP. The example given in the figure below shows how loopback interface 0 of the RPs

(RP1 and RP2) is configured with the 10.0.0.1 IP address. If this 10.0.0.1 address is configured on all RPs as the address for loopback interface 0 and then configured as the RP address, IP routing will converge on the closest RP. This address must be a host route; note the 255.255.255.255 subnet mask.

The downstream routers must be informed about the 10.0.0.1 RP address. In the figure below, the routers are configured statically with the **ip pim rp-address 10.0.0.1**global configuration command. This configuration could also be accomplished using the Auto-RP or bootstrap router (BSR) features.

The RPs in the figure must also share source information using MSDP. In this example, loopback interface 1 of the RPs (RP1 and RP2) is configured for MSDP peering. The MSDP peering address must be different from the anycast RP address.

Figure 10: AnyCast RP Configuration



Many routing protocols choose the highest IP address on loopback interfaces for the router ID. A problem may arise if the router selects the anycast RP address for the router ID. It is recommended that you avoid this problem by manually setting the router ID on the RPs to the same address as the MSDP peering address (for example, the loopback 1 address in the figure above). In Open Shortest Path First (OSPF), the router ID is configured using the **router-id**router configuration command. In Border Gateway Protocol (BGP), the router ID is configured using the **bgp router-id** router configuration command. In many BGP topologies, the MSDP peering address and the BGP peering address must be the same in order to pass the RPF check. The BGP peering address can be set using the **neighbor update-source** router configuration command.

The anycast RP example above uses IP addresses taken from RFC 1918. These IP addresses are normally blocked at interdomain borders and therefore are not accessible to other ISPs. You must use valid IP addresses if you want the RPs to be reachable from other domains.

The following example shows how to perform an Anycast RP configuration.

On RP 1

```
ip pim rp-address 10.0.0.1
interface loopback 0
```

```
 ip address 10.0.0.1 255.255.255.255
!
interface loopback 1
 ip address 10.1.1.1. 255.255.255.255
!
 ip msdp peer 10.1.1.2 connect-source loopback 1
 ip msdp originator-id loopback 1
```

On RP 2

```
ip pim rp-address 10.0.0.1
interface loopback 0
 ip address 10.0.0.1 255.255.255.255
interface loopback 1
 ip address 10.1.1.2. 255.255.255.255
!
 ip msdp peer 10.1.1.1 connect-source loopback 1
 ip msdp originator-id loopback 1
```

All Other Routers

```
ip pim rp-address 10.0.0.1
```

Sparse Mode with Bootstrap Router Example

The following example is a configuration for a candidate BSR, which also happens to be a candidate RP:

```
!
ip multicast-routing
!
interface GigabitEthernet0/0/0
 ip address 172.69.62.35 255.255.255.240
 ip pim sparse-mode
!
interface GigabitEthernet1/0/0
 ip address 172.21.24.18 255.255.255.248
 ip pim sparse-mode
!
interface GigabitEthernet2/0/0
 ip address 172.21.24.12 255.255.255.248
 ip pim sparse-mode
!
ip pim bsr-candidate GigabitEthernet2/0/0 30 10
ip pim rp-candidate GigabitEthernet2/0/0 group-list 5
access-list 5 permit 239.255.2.0 0.0.0.255
```

BSR and RFC 2362 Interoperable Candidate RP Example

When Cisco and non-Cisco routers are being operated in a single PIM domain with PIM Version 2 BSR, care must be taken when configuring candidate RPs because the Cisco implementation of the BSR RP selection is not fully compatible with RFC 2362.

RFC 2362 specifies that the BSR RP be selected as follows (RFC 2362, 3.7):

1. Select the candidate RP with the highest priority (lowest configured priority value).
2. If there is a tie in the priority level, select the candidate RP with the highest hash function value.
3. If there is a tie in the hash function value, select the candidate RP with the highest IP address.

Cisco routers always select the candidate RP based on the longest match on the announced group address prefix before selecting an RP based on priority, hash function, or IP address.

Inconsistent candidate RP selection between Cisco and non-Cisco RFC 2362-compliant routers in the same domain if multiple candidate RPs with partially overlapping group address ranges are configured can occur. Inconsistent candidate RP selection can prevent connectivity between sources and receivers in the PIM domain. A source may register with one candidate RP and a receiver may connect to a different candidate RP even though it is in the same group.

The following example shows a configuration that can cause inconsistent RP selection between a Cisco and a non-Cisco router in a single PIM domain with PIM Version 2 BSR:

```
access-list 10 permit 224.0.0.0  7.255.255.255
ip pim rp-candidate gigabitethernet1/0/0 group-list 10 priority 20
access-list 20 permit 224.0.0.0 15.255.255.255
ip pim rp-candidate gigabitethernet2/0/0 group-list 20 priority 10
```

In this example, a candidate RP on GigabitEthernet interface 1/0/0 announces a longer group prefix of 224.0.0.0/5 with a lower priority of 20. The candidate RP on GigabitEthernet interface 2/0/0 announces a shorter group prefix of 224.0.0.0/4 with a higher priority of 10. For all groups that match both ranges a Cisco router will always select the candidate RP on Ethernet interface 1 because it has the longer announced group prefix. A non-Cisco fully RFC 2362-compliant router will always select the candidate RP on GigabitEthernet interface 2/0/0 because it is configured with a higher priority.

To avoid this interoperability issue, do not configure different candidate RPs to announce partially overlapping group address prefixes. Configure any group prefixes that you want to announce from more than one candidate RP with the same group prefix length.

The following example shows how to configure the previous example so that there is no incompatibility between a Cisco router and a non-Cisco router in a single PIM domain with PIM Version 2 BSR:

```
access-list 10 permit 224.0.0.0  7.255.255.255
ip pim rp-candidate gigabitethernet1/0/0 group-list 10 priority 20
access-list 20 permit 224.0.0.0  7.255.255.255
access-list 20 permit 232.0.0.0  7.255.255.255
ip pim rp-candidate gigabitethernet2/0/0 group-list 20 priority 10
```

In this configuration the candidate RP on Ethernet interface 2 announces group address 224.0.0.0/5 and 232.0.0.0/5 which equal 224.0.0.0/4, but gives the interface the same group prefix length (5) as the candidate RP on Ethernet 1. As a result, both a Cisco router and an RFC 2362-compliant router will select the RP Ethernet interface 2.

Example: Sparse Mode with a Single Static RP

The following example sets the PIM RP address to 192.168.1.1 for all multicast groups and defines all groups to operate in sparse mode:

```
ip multicast-routing
interface gigiabitethernet 1/0/0
 ip pim sparse-mode
ip pim rp-address 192.168.1.1
```

Note The same RP cannot be used for both bidirectional and sparse mode groups.

The following example sets the PIM RP address to 172.16.1.1 for the multicast group 225.2.2.2 only:

```
access list 1 225.2.2.2 0.0.0.0
 ip pim rp-address 172.17.1.1
```

SSM with IGMPv3 Example

The following example shows how to configure a device (running IGMPv3) for SSM:

```
ip multicast-routing
!
interface GigabitEthernet3/1/0
 ip address 172.21.200.203 255.255.255.0
 description backbone interface
 ip pim sparse-mode
!
interface GigabitEthernet3/2/0
 ip address 131.108.1.2 255.255.255.0
 ip pim sparse-mode
 description ethernet connected to hosts
 ip igmp version 3
!
ip pim ssm default
```

SSM Filtering Example

The following example shows how to configure filtering on legacy RP routers running software releases that do not support SSM routing. This filtering will suppress all unwanted PIM-SM and MSDP traffic in the SSM range. Without this filtering, SSM will still operate, but there may be additional RPT traffic if legacy first hop and last hop routers exist in the network.

```
ip access-list extended  no-ssm-range
  deny   ip any 232.0.0.0 0.255.255.255 ! SSM range
  permit ip any any
! Deny registering in SSM range
ip pim accept-register list no-ssm-range
ip access-list extended msdp-nono-list
  deny   ip any 232.0.0.0 0.255.255.255 ! SSM Range
  ! .
  ! .
  ! .
  ! See ftp://ftpeng.cisco.com/ipmulticast/config-notes/msdp-sa-filter.txt for other SA
  ! messages that typically need to be filtered.
  permit ip any any
! Filter generated SA messages in SSM range. This configuration is only needed if there
! are directly connected sources to this router. The “ip pim accept-register” command
! filters remote sources.
ip msdp redistribute list msdp-nono-list
! Filter received SA messages in SSM range. “Filtered on receipt” means messages are
! neither processed or forwarded. Needs to be configured for each MSDP peer.
ip msdp sa-filter in msdp-peer1 list msdp-nono-list
! .
! .
! .
ip msdp sa-filter in msdp-peerN list msdp-nono-list
```

Bidir-PIM Example

By default, a bidirectional RP advertises all groups as bidirectional. An access list on the RP can be used to specify a list of groups to be advertised as bidirectional. Groups with the **deny** keyword will operate in dense mode. A different, nonbidirectional RP address is required for groups that operate in sparse mode because a single access list only allows either a **permit** or **deny** keyword.

The following example shows how to configure an RP for both sparse mode and bidirectional mode groups. The groups identified as 224/8 and 227/8 are bidirectional groups, and 226/8 is a sparse mode group. The RP must be configured to use different IP addresses for the sparse mode and bidirectional mode operations. Two loopback interfaces are used to allow this configuration. The addresses of these loopback interfaces must be routed throughout the PIM domain in such a way that the other routers in the PIM domain can communicate with the RP.

```
ip multicast-routing
!
.
.
.
!
interface loopback 0
 description One loopback address for this router's Bidir Mode RP function
 ip address 10.0.1.1 255.255.255.0
!
interface loopback 1
description One loopback address for this router's Sparse Mode RP function
 ip address 10.0.2.1 255.255.255.0
!
.
.
.
!
ip pim bidir-enable
ip pim rp-address 10.0.1.1 45 bidir
ip pim rp-address 10.0.2.1 46
!
access-list 45 permit 224.0.0.0 0.255.255.255
access-list 45 permit 227.0.0.0 0.255.255.255
access-list 46 permit 226.0.0.0 0.255.255.255
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IP multicast commands	Cisco IOS IP Multicast Command Reference

Standards and RFCs

Standard/RFC	Title
draft-kouvelas-pim-bidir-new-00.txt	A New Proposal for Bi-directional PIM
RFC 1112	Host Extensions for IP Multicasting
RFC 1918	Address Allocation for Private Internets
RFC 2770	GLOP Addressing in 233/8

Standard/RFC	Title
RFC 3569	An Overview of Source-Specific Multicast (SSM)

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Configuring Basic IP Multicast in IPv4 Networks

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 3: Feature Information for Configuring Basic IP Multicast in IPv4 Networks

Feature Name	Releases	Feature Information
Auto RP Enhancements	Cisco IOS XE Release 2.1	Auto-RP automates the distribution of group-to-rendezvous point (RP) mappings in a PIM network. To make Auto-RP work, a router must be designated as an RP mapping agent, which receives the RP announcement messages from the RPs and arbitrates conflicts.
Bidirectional PIM	Cisco IOS XE Release 2.2 Cisco IOS XE Release 3.8S Cisco IOS XE Release 3.9S	Bidirectional PIM is an extension to the PIM suite of protocols that implements shared sparse trees with bidirectional data flow. In contrast to PIM-Sparse Mode, Bidirectional PIM avoids keeping source-specific state in a router and allows trees to scale to an arbitrary number of sources. In Cisco IOS XE Release 3.8S, support was added for the Cisco ISR 4400 Series Routers. In Cisco IOS XE Release 3.9S, support was added for the Cisco CSR 1000V.
PIM Dense Mode Fallback Prevention in a Network Following RP Information Loss	12.3(4)T 12.0(28)S 12.2(33)SRA 12.2(33)SXH Cisco IOS XE Release 2.1 15.0(1)S	The PIM Dense Mode Fallback Prevention in a Network Following RP Information Loss feature enables you to prevent PIM-DM fallback when all RPs fail. Preventing the use of dense mode is very important to multicast networks whose reliability is critical. This feature provides a mechanism to keep the multicast groups in sparse mode, thereby preventing dense mode flooding. The following command was introduced by this feature: **ip pim dm-fallback**.

Feature Name	Releases	Feature Information
Source Specific Multicast (SSM)	12.3(4)T 12.2(25)S 12.0(28)S 12.2(33)SXH 12.2(33)SRA 15.0(1)S Cisco IOS XE Release 2.1 Cisco IOS XE 3.1.0SG Cisco IOS XE Release 3.8S Cisco IOS XE Release 3.9S	SSM is an extension of IP multicast where datagram traffic is forwarded to receivers from only those multicast sources that the receivers have explicitly joined. For multicast groups configured for SSM, only source-specific multicast distribution trees (not shared trees) are created. In Cisco IOS XE Release 3.8S, support was added for the Cisco ISR 4400 Series Routers. In Cisco IOS XE Release 3.9S, support was added for the Cisco CSR 1000V.

CHAPTER 4

Configuring Basic IP Multicast in IPv6 Networks

This module describes how to configure basic IP multicast in an IPv6 network.

- Finding Feature Information, page 69
- Prerequisites for Configuring Basic IP Multicast, page 69
- Information About Configuring Basic IP Multicast in IPv6 Networks, page 70
- How to Configure Basic IP Multicast in IPv6 Networks, page 78
- Configuration Examples for Configuring IP Multicast Basic in IPv6 Networks, page 90
- Additional References, page 91
- Feature Information for Configuring Basic IP Multicast in IPv6 Networks, page 92

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring Basic IP Multicast

- To determine which of the tasks contained in this module you will have to perform, you must decide which Protocol Independent Multicast (PIM) mode will be used. This determination is based on the applications you intend to support on your network.
- All access lists to be used with the tasks in this module should be configured prior to beginning the configuration task. For information about how to configure an access list, see the "Creating an IP Access List and Applying It to an Interface" module of the *Security Configuration Guide: Access Control Lists* guide.

Information About Configuring Basic IP Multicast in IPv6 Networks

IPv6 Multicast

IPv6 Multicast Overview

An IPv6 multicast group is an arbitrary group of receivers that want to receive a particular data stream. This group has no physical or geographical boundaries--receivers can be located anywhere on the Internet or in any private network. Receivers that are interested in receiving data flowing to a particular group must join the group by signaling their local device. This signaling is achieved with the MLD protocol.

Devices use the MLD protocol to learn whether members of a group are present on their directly attached subnets. Hosts join multicast groups by sending MLD report messages. The network then delivers data to a potentially unlimited number of receivers, using only one copy of the multicast data on each subnet. IPv6 hosts that wish to receive the traffic are known as group members.

Packets delivered to group members are identified by a single multicast group address. Multicast packets are delivered to a group using best-effort reliability, just like IPv6 unicast packets.

The multicast environment consists of senders and receivers. Any host, regardless of whether it is a member of a group, can send to a group. However, only the members of a group receive the message.

A multicast address is chosen for the receivers in a multicast group. Senders use that address as the destination address of a datagram to reach all members of the group.

Membership in a multicast group is dynamic; hosts can join and leave at any time. There is no restriction on the location or number of members in a multicast group. A host can be a member of more than one multicast group at a time.

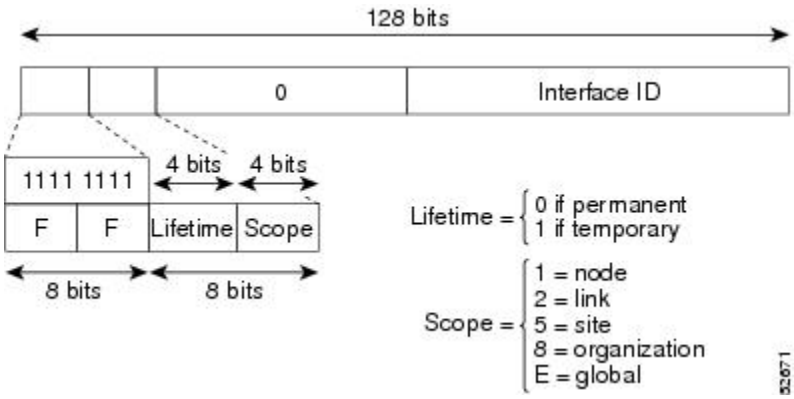
How active a multicast group is, its duration, and its membership can vary from group to group and from time to time. A group that has members may have no activity.

IPv6 Multicast Addressing

An IPv6 multicast address is an IPv6 address that has a prefix of FF00::/8 (1111 1111). An IPv6 multicast address is an identifier for a set of interfaces that typically belong to different nodes. A packet sent to a multicast address is delivered to all interfaces identified by the multicast address. The second octet following the prefix defines the lifetime and scope of the multicast address. A permanent multicast address has a lifetime parameter equal to 0; a temporary multicast address has a lifetime parameter equal to 1. A multicast address that has the scope of a node, link, site, or organization, or a global scope has a scope parameter of 1, 2, 5, 8, or E,

respectively. For example, a multicast address with the prefix FF02::/16 is a permanent multicast address with a link scope. The figure below shows the format of the IPv6 multicast address.

Figure 11: IPv6 Multicast Address Format



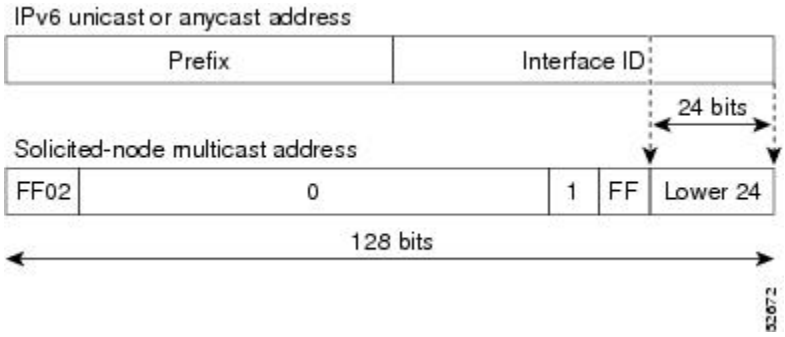
IPv6 nodes (hosts and routers) are required to join (receive packets destined for) the following multicast groups:

- All-nodes multicast group FF02:0:0:0:0:0:0:1 (scope is link-local)
- Solicited-node multicast group FF02:0:0:0:0:1:FF00:0000/104 for each of its assigned unicast and anycast addresses

IPv6 routers must also join the all-routers multicast group FF02:0:0:0:0:0:0:2 (scope is link-local).

The solicited-node multicast address is a multicast group that corresponds to an IPv6 unicast or anycast address. IPv6 nodes must join the associated solicited-node multicast group for every unicast and anycast address to which it is assigned. The IPv6 solicited-node multicast address has the prefix FF02:0:0:0:0:1:FF00:0000/104 concatenated with the 24 low-order bits of a corresponding IPv6 unicast or anycast address (see the figure below). For example, the solicited-node multicast address corresponding to the IPv6 address 2037::01:800:200E:8C6C is FF02::1:FF0E:8C6C. Solicited-node addresses are used in neighbor solicitation messages.

Figure 12: IPv6 Solicited-Node Multicast Address Format



Note There are no broadcast addresses in IPv6. IPv6 multicast addresses are used instead of broadcast addresses.

IPv6 Multicast Groups

An IPv6 address must be configured on an interface before the interface can forward IPv6 traffic. Configuring a site-local or global IPv6 address on an interface automatically configures a link-local address and activates IPv6 for that interface. Additionally, the configured interface automatically joins the following required multicast groups for that link:

- Solicited-node multicast group FF02:0:0:0:0:1:FF00::/104 for each unicast and anycast address assigned to the interface

  Note The solicited-node multicast address is used in the neighbor discovery process.

- All-nodes link-local multicast group FF02::1
- All-routers link-local multicast group FF02::2

IPv6 Multicast Address Group Range Support

This feature provides an access control mechanism for IPv6 multicast edge routing. The ACL specifies the multicast groups or channels that are to be permitted or denied. For groups or channels that are denied, the device ignores protocol traffic and actions (for example, no MLD states are created, no mroute states are created, no PIM joins are forwarded), and drops data traffic on all interfaces in the system, disabling multicast for groups or channels denied by the ACL.

Scoped Address Architecture

IPv6 includes support for global and nonglobal addresses. This section describes the usage of IPv6 addresses of different scopes.

A scope zone, or a simply a zone, is a connected region of topology of a given scope. For example, the set of links connected by devices within a particular site, and the interfaces attached to those links, comprise a single zone of site-local scope.

A zone is a particular instance of a topological region (for example, Zone1's site or Zone2's site), whereas a scope is the size of a topological region (for example, a site or a link). The zone to which a particular nonglobal address pertains is not encoded in the address itself, but rather is determined by context, such as the interface from which it is sent or received. Therefore, addresses of a given nonglobal scope may be reused in different zones of that scope. For example, Zone1's site and Zone2's site may each contain a node with site-local address FEC0::1.

Zones of the different scopes are instantiated as follows:

- Each link, and the interfaces attached to that link, comprises a single zone of link-local scope (for both unicast and multicast).

- There is a single zone of global scope (for both unicast and multicast), comprising all the links and interfaces in the Internet.
- The boundaries of zones of scope other than interface-local, link-local, and global must be defined and configured by network administrators. A site boundary serves as such for both unicast and multicast.

Zone boundaries are relatively static features and do not change in response to short-term changes in topology. Therefore, the requirement that the topology within a zone be "connected" is intended to include links and interfaces that may be connected only occasionally. For example, a residential node or network that obtains Internet access by dialup to an employer's site may be treated as part of the employer's site-local zone even when the dialup link is disconnected. Similarly, a failure of a device, interface, or link that causes a zone to become partitioned does not split that zone into multiple zones; rather, the different partitions are still considered to belong to the same zone.

Zones have the following additional properties:

- Zone boundaries cut through nodes, not links (the global zone has no boundary, and the boundary of an interface-local zone encloses just a single interface.)
- Zones of the same scope cannot overlap; that is, they can have no links or interfaces in common.
- A zone of a given scope (less than global) falls completely within zones of larger scope; that is, a smaller scope zone cannot include more topology than any larger scope zone with which it shares any links or interfaces.
- Each interface belongs to exactly one zone of each possible scope.

MRIB

The Multicast Routing Information Base (MRIB) is a protocol-independent repository of multicast routing entries instantiated by multicast routing protocols (routing clients). Its main function is to provide independence between routing protocols and the Multicast Forwarding Information Base (MFIB). It also acts as a coordination and communication point among its clients.

Routing clients use the services provided by the MRIB to instantiate routing entries and retrieve changes made to routing entries by other clients. Besides routing clients, MRIB also has forwarding clients (MFIB instances) and special clients such as MLD. MFIB retrieves its forwarding entries from MRIB and notifies the MRIB of any events related to packet reception. These notifications can either be explicitly requested by routing clients or spontaneously generated by the MFIB.

Another important function of the MRIB is to allow for the coordination of multiple routing clients in establishing multicast connectivity within the same multicast session. MRIB also allows for the coordination between MLD and routing protocols.

IPv6 Multicast Process Switching and Fast Switching

A unified MFIB is used to provide both fast switching and process switching support for PIM-SM and PIM-SSM in IPv6 multicast. In process switching, the Route Processor must examine, rewrite, and forward each packet. The packet is first received and copied into the system memory. The device then looks up the Layer 3 network address in the routing table. The Layer 2 frame is then rewritten with the next-hop destination address and sent to the outgoing interface. The RP also computes the cyclic redundancy check (CRC). This switching method is the least scalable method for switching IPv6 packets.

IPv6 multicast fast switching allows devices to provide better packet forwarding performance than process switching. Information conventionally stored in a route cache is stored in several data structures for IPv6 multicast switching. The data structures provide optimized lookup for efficient packet forwarding.

In IPv6 multicast forwarding, the first packet is fast-switched if the PIM protocol logic allows it. In IPv6 multicast fast switching, the MAC encapsulation header is precomputed. IPv6 multicast fast switching uses the MFIB to make IPv6 destination prefix-based switching decisions. In addition to the MFIB, IPv6 multicast fast switching uses adjacency tables to prepend Layer 2 addressing information. The adjacency table maintains Layer 2 next-hop addresses for all MFIB entries.

The adjacency table is populated as adjacencies are discovered. Each time an adjacency entry is created (such as through ARP), a link-layer header for that adjacent node is precomputed and stored in the adjacency table. Once a route is determined, it points to a next hop and corresponding adjacency entry. It is subsequently used for encapsulation during switching of packets.

A route might have several paths to a destination prefix, such as when a device is configured for simultaneous load balancing and redundancy. For each resolved path, a pointer is added for the adjacency corresponding to the next-hop interface for that path. This mechanism is used for load balancing across several paths.

IPv6 Anycast RP Solution

PIMv6 Anycast RP Solution Overview

The anycast RP solution in IPv6 PIM allows an IPv6 network to support anycast services for the PIM-SM RP. It allows anycast RP to be used inside a domain that runs PIM only. Anycast RP can be used in IPv4 as well as IPv6, but it does not depend on the Multicast Source Discovery Protocol (MSDP), which runs only on IPv4. This feature is useful when interdomain connection is not required.

Anycast RP is a mechanism that ISP-based backbones use to get fast convergence when a PIM RP device fails. To allow receivers and sources to rendezvous to the closest RP, the packets from a source need to get to all RPs to find joined receivers.

A unicast IP address is chosen as the RP address. This address is either statically configured or distributed using a dynamic protocol to all PIM devices throughout the domain. A set of devices in the domain is chosen to act as RPs for this RP address; these devices are called the anycast RP set. Each device in the anycast RP set is configured with a loopback interface using the RP address. Each device in the anycast RP set also needs a separate physical IP address to be used for communication between the RPs. Each device in the Anycast set must contain the list of all the devices in the Anycast set.

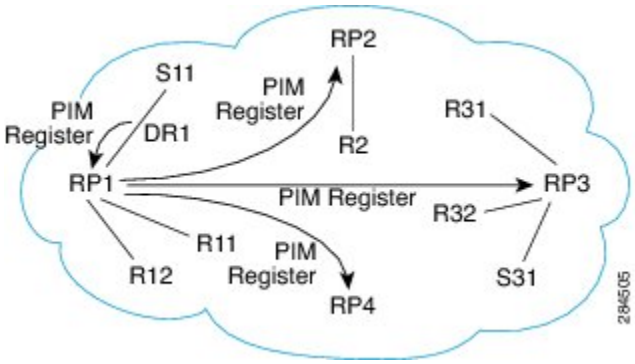
The RP address, or a prefix that covers the RP address, is injected into the unicast routing system inside of the domain. Each device in the anycast RP set is configured with the addresses of all other devices in the anycast RP set, and this configuration must be consistent in all RPs in the set. The IP address of the local device must be included in the set so that all devices in anycast set have the same IP addresses.

PIMv6 Anycast RP Normal Operation

The following illustration shows PIMv6 anycast RP normal operation and assumes the following:

- RP1, RP2, RP3, and RP4 are members in the same anycast RP group.
- S11 and S31 are sources that use RP1 and RP3, respectively, based on their unicast routing metric.

- R11, R12, R2, R31, and R32 are receivers. Based on their unicast routing metrics, R11 and R12 join to RP1, R2 joins to RP2 and R31, and R32 joins to RP3, respectively.

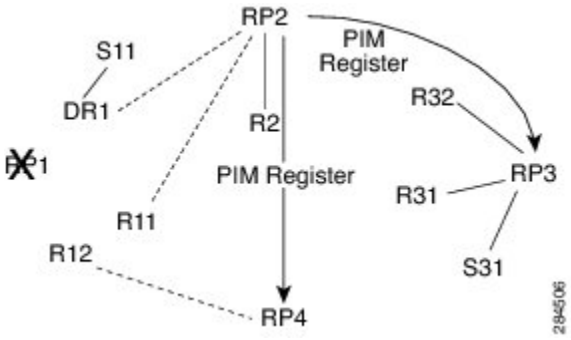


The following sequence of events occurs when S11 starts sending packets:

1. DR1 creates (S,G) states and sends a register to RP1. DR1 may also encapsulate the data packet in the register.
2. Upon receiving the register, RP1 performs normal PIM-SM RP functionality, and forwards the packets to R11 and R12.
3. RP1 also sends the register (which may encapsulate the data packets) to RP2, RP3, and RP4.
4. RP2, RP3, and RP4 do not further forward the register to each other.
5. RP2, RP3, and RP4 perform normal PIM-SM RP functionality, and if there is a data packet encapsulated, RP2 forwards the data packet to R2 and RP3 forwards the data packet to R31 and R32, respectively.
6. The previous five steps repeat for null registers sent by DR1.

PIMv6 Anycast RP Failover

The following illustration shows PIM anycast RP failover.



In failover, when RP1 is not reachable, the following occurs:

- Registers from DR1 will be routed transparently to RP2.
- R11 uses RP2 as the RP, and R12 uses RP4 as the RP.
- Registers from DR1 will be routed from RP2 to RP3 and RP4.

In this way, the loss of the RP (RP1 in this case) is transparent to DR1, R11, and R12, and the network can converge as soon as the IGP is converged.

IPv6 BSR

IPv6 BSR

PIM devices in a domain must be able to map each multicast group to the correct RP address. The BSR protocol for PIM-SM provides a dynamic, adaptive mechanism to distribute group-to-RP mapping information rapidly throughout a domain. With the IPv6 BSR feature, if an RP becomes unreachable, it will be detected and the mapping tables will be modified so that the unreachable RP is no longer used, and the new tables will be rapidly distributed throughout the domain.

Every PIM-SM multicast group needs to be associated with the IP or IPv6 address of an RP. When a new multicast sender starts sending, its local DR will encapsulate these data packets in a PIM register message and send them to the RP for that multicast group. When a new multicast receiver joins, its local DR will send a PIM join message to the RP for that multicast group. When any PIM device sends a (*, G) join message, the PIM device needs to know which is the next device toward the RP so that G (Group) can send a message to that device. Also, when a PIM device is forwarding data packets using (*, G) state, the PIM device needs to know which is the correct incoming interface for packets destined for G, because it needs to reject any packets that arrive on other interfaces.

A small set of devices from a domain are configured as candidate bootstrap routers (C-BSRs) and a single BSR is selected for that domain. A set of devices within a domain are also configured as candidate RPs (C-RPs); typically, these devices are the same devices that are configured as C-BSRs. Candidate RPs periodically unicast candidate-RP-advertisement (C-RP-Adv) messages to the BSR of that domain, advertising their willingness to be an RP. A C-RP-Adv message includes the address of the advertising C-RP, and an optional list of group addresses and mask length fields, indicating the group prefixes for which the candidacy is advertised. The BSR then includes a set of these C-RPs, along with their corresponding group prefixes, in bootstrap messages (BSMs) it periodically originates. BSMs are distributed hop-by-hop throughout the domain.

Bidirectional BSR support allows bidirectional RPs to be advertised in C-RP messages and bidirectional ranges in the BSM. All devices in a system must be able to use the bidirectional range in the BSM; otherwise, the bidirectional RP feature will not function.

IPv6 BSR: Configure RP Mapping

The IPv6 BSR ability to configure RP mapping allows IPv6 multicast devices to be statically configured to announce scope-to-RP mappings directly from the BSR instead of learning them from candidate-RP messages. Announcing RP mappings from the BSR is useful in several situations:

- When an RP address never changes because there is only a single RP or the group range uses an anycast RP, it may be less complex to configure the RP address announcement statically on the candidate BSRs.
- When an RP address is a virtual RP address (such as when using bidirectional PIM), it cannot be learned by the BSR from a candidate-RP. Instead, the virtual RP address must be configured as an announced RP on the candidate BSRs.

IPv6 BSR: Scoped Zone Support

BSR provides scoped zone support by distributing group-to-RP mappings in networks using administratively scoped multicast. The user can configure candidate BSRs and a set of candidate RPs for each administratively scoped region in the user's domain.

For BSR to function correctly with administrative scoping, a BSR and at least one C-RP must be within every administratively scoped region. Administratively scoped zone boundaries must be configured at the zone border devices, because they need to filter PIM join messages that might inadvertently cross the border due to error conditions. In addition, at least one C-BSR within the administratively scoped zone must be configured to be a C-BSR for the administratively scoped zone's address range.

A separate BSR election will then take place (using BSMs) for every administratively scoped range, plus one for the global range. Administratively scoped ranges are identified in the BSM because the group range is marked to indicate that this is an administrative scope range, not just a range that a particular set of RPs is configured to handle.

Unless the C-RP is configured with a scope, it discovers the existence of the administratively scoped zone and its group range through reception of a BSM from the scope zone's elected BSR containing the scope zone's group range. A C-RP stores each elected BSR's address and the administratively scoped range contained in its BSM. It separately unicasts C-RP-Adv messages to the appropriate BSR for every administratively scoped range within which it is willing to serve as an RP.

All PIM devices within a PIM bootstrap domain where administratively scoped ranges are in use must be able to receive BSMs and store the winning BSR and RP set for all administratively scoped zones that apply.

IPv6 Multicast: RPF Flooding of BSR Packets

Cisco IPv6 devices provide support for the RPF flooding of BSR packets so that the device will not disrupt the flow of BSMs. The device will recognize and parse enough of the BSM to identify the BSR address. The device performs an RPF check for this BSR address and forwards the packet only if it is received on the RPF interface. The device also creates a BSR entry containing RPF information to use for future BSMs from the same BSR. When BSMs from a given BSR are no longer received, the BSR entry is timed out.

IPv6 Multicast Groups

An IPv6 address must be configured on an interface before the interface can forward IPv6 traffic. Configuring a site-local or global IPv6 address on an interface automatically configures a link-local address and activates IPv6 for that interface. Additionally, the configured interface automatically joins the following required multicast groups for that link:

- Solicited-node multicast group FF02:0:0:0:0:1:FF00::/104 for each unicast and anycast address assigned to the interface

  Note The solicited-node multicast address is used in the neighbor discovery process.

- All-nodes link-local multicast group FF02::1
- All-routers link-local multicast group FF02::2

IPv6 Multicast Address Group Range Support

This feature provides an access control mechanism for IPv6 multicast edge routing. The ACL specifies the multicast groups or channels that are to be permitted or denied. For groups or channels that are denied, the device ignores protocol traffic and actions (for example, no MLD states are created, no mroute states are created, no PIM joins are forwarded), and drops data traffic on all interfaces in the system, disabling multicast for groups or channels denied by the ACL.

How to Configure Basic IP Multicast in IPv6 Networks

Enabling IPv6 Multicast Routing

IPv6 multicast uses MLD version 2. This version of MLD is fully backward-compatible with MLD version 1 (described in *RFC 2710*). Hosts that support only MLD version 1 will interoperate with a device running MLD version 2. Mixed LANs with both MLD version 1 and MLD version 2 hosts are likewise supported.

Before You Begin

You must first enable IPv6 unicast routing on all interfaces of the device on which you want to enable IPv6 multicast routing .

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 multicast-routing** [**vrf** *vrf-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 multicast-routing** [**vrf** *vrf-name*] **Example:** `Device(config)# ipv6 multicast-routing`	Enables multicast routing on all IPv6-enabled interfaces and enables multicast forwarding for PIM and MLD on all enabled interfaces of the device.

	Command or Action	Purpose
		• IPv6 multicast routing is disabled by default when IPv6 unicast routing is enabled. IPv6 multicast-routing needs to be enabled for IPv6 multicast routing to function.

Disabling the Device from Receiving Unauthenticated Multicast Traffic

In some situations, access control may be needed to prevent multicast traffic from being received unless the subscriber is authenticated and the channels are authorized as per access control profiles. That is, there should be no traffic at all unless specified otherwise by access control profiles.

Perform this task to disable the device from receiving multicast traffic to be received from unauthenticated groups or unauthorized channels.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 multicast** [**vrf** *vrf-name*] **group-range**[*access-list-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 multicast** [**vrf** *vrf-name*] **group-range**[*access-list-name*] **Example:** `Device(config)# ipv6 multicast group-range`	Disables multicast protocol actions and traffic forwarding for unauthorized groups or channels on all the interfaces in a device.

Troubleshooting IPv6 Multicast

SUMMARY STEPS

1. **enable**
2. **debug ipv6 mfib** *group-name* | *group-address*] [**adjacency** | **signal** | **db** | **init** | **mrib** | **pak** | **ps**
3. debug ipv6 mld [group-name | group-address | interface-type]
4. **debug ipv6 mld explicit** [*group-name* | *group-address*
5. **debug ipv6 pim** [*group-name* | *group-address* | *interface-type* | **neighbor** | **bsr**
6. **debug bgp ipv6** {**unicast** | **multicast**} **dampening** [**prefix-list** *prefix-list-name*
7. **debug bgp ipv6** {**unicast** | **multicast**} **updates** [*ipv6-address*] [**prefix-list** *prefix-list-name*] [**in** | **out**
8. **debug ipv6 mrib client**
9. **debug ipv6 mrib io**
10. **debug ipv6 mrib issu**
11. **debug ipv6 mrib proxy**
12. **debug ipv6 mrib route** [*group-name* | *group-address*
13. **debug ipv6 mrib table**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug ipv6 mfib** *group-name* | *group-address*] [**adjacency** | **signal** | **db** | **init** | **mrib** | **pak** | **ps** **Example:** `Device# debug ipv6 mfib pak FF04::10`	Enables debugging output on the IPv6 MFIB.
Step 3	debug ipv6 mld [group-name | group-address | interface-type] **Example:** `Device# debug ipv6 mld`	Enables debugging on MLD protocol activity.
Step 4	**debug ipv6 mld explicit** [*group-name* | *group-address* **Example:** `Device# debug ipv6 mld explicit`	Displays information related to the explicit tracking of hosts.

	Command or Action	Purpose
Step 5	**debug ipv6 pim** [*group-name* | *group-address* | *interface-type* | **neighbor** | **bsr** **Example:** `Device# debug ipv6 pim`	Enables debugging on PIM protocol activity.
Step 6	**debug bgp ipv6** {**unicast** | **multicast**} **dampening** [**prefix-list** *prefix-list-name* **Example:** `Device# debug bgp ipv6 multicast`	Displays debugging messages for IPv6 BGP dampening.
Step 7	**debug bgp ipv6** {**unicast** | **multicast**} **updates** [*ipv6-address*] [**prefix-list** *prefix-list-name*] [**in** | **out** **Example:** `Device# debug bgp ipv6 multicast updates`	Displays debugging messages for IPv6 BGP update packets.
Step 8	**debug ipv6 mrib client** **Example:** `Device# debug ipv6 mrib client`	Enables debugging on MRIB client management activity.
Step 9	**debug ipv6 mrib io** **Example:** `Device# debug ipv6 mrib io`	Enables debugging on MRIB I/O events.
Step 10	**debug ipv6 mrib issu** **Example:** `Device# debug ipv6 mrib issu`	Enables debugging on MRIB in service software update.
Step 11	**debug ipv6 mrib proxy** **Example:** `Device# debug ipv6 mrib proxy`	Enables debugging on MRIB proxy activity between the route processor and line cards on distributed devices.
Step 12	**debug ipv6 mrib route** [*group-name* | *group-address* **Example:** `Device# debug ipv6 mrib route`	Displays information about MRIB routing entry-related activity.

	Command or Action	Purpose
Step 13	**debug ipv6 mrib table** **Example:** `Device# debug ipv6 mrib table`	Enables debugging on MRIB table management activity.

Configuring PIMv6 Anycast RP

This task describes how to configure two PIMv6 anycast RP peers. Steps 3 through 11 show the configuration for RP1, and Steps 12 through 19 show the configuration for RP2.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 pim** [**vrf** *vrf-name*] **rp-address** *ipv6-address* [*group-address-list*] [**bidir**]
4. **interface** *type number*
5. **ipv6 address** {*ipv6-address*/*prefix-length* | *prefix-name sub-bits* /*prefix-length*}
6. **no shut**
7. **interface** *type number*
8. **ipv6 address** {*ipv6-address*/*prefix-length* | *prefix-name sub-bits* /*prefix-length*}
9. **no shut**
10. **exit**
11. **ipv6 pim anycast-RP** *rp-address peer-address*
12. **ipv6 pim** [**vrf** *vrf-name*] **rp-address** *ipv6-address* [*group-address-list*] [**bidir**]
13. **interface** *type number*
14. **ipv6 address** {*ipv6-address*/*prefix-length* | *prefix-name sub-bits* /*prefix-length*}
15. **no shut**
16. **interface** *type number*
17. **ipv6 address** {*ipv6-address*/*prefix-length* | *prefix-name sub-bits* /*prefix-length*}
18. **no shut**
19. **ipv6 pim anycast-RP** *rp-address peer-address*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Device> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 pim** [**vrf** *vrf-name*] **rp-address** *ipv6-address* [*group-address-list*] [**bidir**] **Example:** `Device(config)# ipv6 pim rp-address 2001:DB8::1:1 acl_sparse1`	Configures the address of a PIM RP for a particular group range.
Step 4	**interface** *type number* **Example:** `Device(config)# interface Loopback4`	Specifies an interface type and number, and places the device in interface configuration mode.
Step 5	**ipv6 address** {*ipv6-address/prefix-length* | *prefix-name sub-bits /prefix-length*} **Example:** `Device(config-if)# ipv6 address 2001:DB8::4:4/64`	Configures an IPv6 address based on an IPv6 general prefix and enable IPv6 processing on an interface.
Step 6	**no shut** **Example:** `Device(config-if)# no shut`	Enables an interface.
Step 7	**interface** *type number* **Example:** `Device(config-if)# interface Loopback5`	Specifies an interface type and number, and places the device in interface configuration mode.
Step 8	**ipv6 address** {*ipv6-address/prefix-length* | *prefix-name sub-bits /prefix-length*} **Example:** `Device(config-if)# ipv6 address 2001:DB8:0:ABCD::1/64`	Configures an IPv6 address based on an IPv6 general prefix and enable IPv6 processing on an interface.
Step 9	**no shut** **Example:** `Device(config-if)# no shut`	Enables an interface.

	Command or Action	Purpose
Step 10	**exit** **Example:** `Device(config-if)# exit`	Enter this command to exit interface configuration mode and enter global configuration mode.
Step 11	**ipv6 pim anycast-RP** *rp-address peer-address* **Example:** `Device(config)# ipv6 pim anycast-rp 2001:DB8:0:ABCD::1 2001:DB8::3:3`	Use this command to configure the address of the PIM RP for an anycast group range. • The IP address of the local device must be included in the set so that all devices in anycast set have the same IP addresses.
Step 12	**ipv6 pim** [**vrf** *vrf-name*] **rp-address** *ipv6-address* [*group-address-list*] [**bidir**] **Example:** `Device(config)# ipv6 pim rp-address 2001:DB8::1:1 acl_sparse1`	Configures the address of a PIM RP for a particular group range.
Step 13	**interface** *type number* **Example:** `Device(config)# interface Loopback4`	Specifies an interface type and number, and places the device in interface configuration mode.
Step 14	**ipv6 address** {*ipv6-address/prefix-length* | *prefix-name sub-bits /prefix-length*} **Example:** `Device(config-if)# ipv6 address 2001:DB8::3:3/64`	Configures an IPv6 address based on an IPv6 general prefix and enables IPv6 processing on an interface.
Step 15	**no shut** **Example:** `Device(config-if)# no shut`	Enables an interface.
Step 16	**interface** *type number* **Example:** `Device(config-if)# interface Loopback5`	Specifies an interface type and number, and places the device in interface configuration mode.
Step 17	**ipv6 address** {*ipv6-address/prefix-length* | *prefix-name sub-bits /prefix-length*} **Example:** `Device(config-if)# ipv6 address 2001:DB8:0:ABCD::1/64`	Configures an IPv6 address based on an IPv6 general prefix and enables IPv6 processing on an interface.

	Command or Action	Purpose
Step 18	**no shut** **Example:** `Device(config-if)# no shut`	Enables an interface
Step 19	**ipv6 pim anycast-RP** *rp-address peer-address* **Example:** `Device(config-if)# ipv6 pim anycast-rp 2001:DB8::1:1 2001:DB8::4:4`	Use this command to configure the address of the PIM RP for an anycast group range.

Configuring a BSR and Verifying BSR Information

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 pim** [**vrf** *vrf-name*] **bsr candidate bsr** *ipv6-address*[*hash-mask-length*] [**priority** *priority-value*]
4. **interface** *type number*
5. **ipv6 pim bsr border**
6. **end**
7. **show ipv6 pim** [**vrf** *vrf-name*] **bsr** {**election** | **rp-cache** | **candidate-rp**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 pim** [**vrf** *vrf-name*] **bsr candidate bsr** *ipv6-address*[*hash-mask-length*] [**priority** *priority-value*]	Configures a device to be a candidate BSR.

	Command or Action	Purpose
	Example: `Device(config)# ipv6 pim bsr candidate bsr 2001:DB8:3000:3000::42 124 priority 10`	
Step 4	**interface** *type number* **Example:** `Device(config)# interface FastEthernet 1/0`	Specifies an interface type and number, and places the device in interface configuration mode.
Step 5	**ipv6 pim bsr border** **Example:** `Device(config-if)# ipv6 pim bsr border`	Configures a border for all BSMs of any scope on a specified interface.
Step 6	**end** **Example:** `Device(config-if)# end`	Exits to privileged EXEC mode.
Step 7	**show ipv6 pim** [**vrf** *vrf-name*] **bsr** {**election** | **rp-cache** | **candidate-rp**} **Example:** `Device# show ipv6 pim bsr election`	Displays information related to PIM BSR protocol processing.

Sending PIM RP Advertisements to the BSR

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 pim** [**vrf** *vrf-name*] **bsr candidate rp** *ipv6-address* [**group-list** *access-list-name*] [**priority** *priority-value*] [**interval** *seconds*] [**scope** *scope-value*] [**bidir**]
4. **interface** *type number*
5. **ipv6 pim bsr border**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 pim** [**vrf** *vrf-name*] **bsr candidate rp** *ipv6-address* [**group-list** *access-list-name*] [**priority** *priority-value*] [**interval** *seconds*] [**scope** *scope-value*] [**bidir**] **Example:** `Device(config)# ipv6 pim bsr candidate rp 2001:DB8:3000:3000::42 priority 0`	Sends PIM RP advertisements to the BSR.
Step 4	**interface** *type number* **Example:** `Device(config)# interface FastEthernet 1/0`	Specifies an interface type and number, and places the device in interface configuration mode.
Step 5	**ipv6 pim bsr border** **Example:** `Device(config-if)# ipv6 pim bsr border`	Configures a border for all BSMs of any scope on a specified interface.

Configuring BSR for Use Within Scoped Zones

A user can configure candidate BSRs and a set of candidate RPs for each administratively scoped region in the domain.

If scope is specified on the candidate RP, then this device will advertise itself as C-RP only to the BSR for the specified scope. If the group list is specified along with the scope, then only prefixes in the access list with the same scope as that configured will be advertised.

If a scope is specified on the bootstrap device, the BSR will originate BSMs including the group range associated with the scope and accept C-RP announcements for groups that belong to the given scope.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 pim** [**vrf** *vrf-name*] **bsr candidate bsr** *ipv6-address* [*hash-mask-length*] [**priority** *priority-value*]
4. **ipv6 pim** [**vrf** *vrf-name*] **bsr candidate rp** *ipv6-address* [**group-list** *access-list-name*] [**priority** *priority-value*] [**interval** *seconds*] [**scope** *scope-value*] [**bidir**]
5. **interface** *type number*
6. **ipv6 multicast boundary scope** *scope-value*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 pim** [**vrf** *vrf-name*] **bsr candidate bsr** *ipv6-address* [*hash-mask-length*] [**priority** *priority-value*] **Example:** `Device(config)# ipv6 pim bsr candidate bsr 2001:DB8:1:1:4`	Configures a device to be a candidate BSR.
Step 4	**ipv6 pim** [**vrf** *vrf-name*] **bsr candidate rp** *ipv6-address* [**group-list** *access-list-name*] [**priority** *priority-value*] [**interval** *seconds*] [**scope** *scope-value*] [**bidir**] **Example:** `Device(config)# ipv6 pim bsr candidate rp 2001:DB8:1:1:1 group-list list scope 6`	Configures the candidate RP to send PIM RP advertisements to the BSR.
Step 5	**interface** *type number* **Example:** `Device(config)# interface FastEthernet 1/0`	Specifies an interface type and number, and places the device in interface configuration mode.

	Command or Action	Purpose
Step 6	**ipv6 multicast boundary scope** *scope-value* **Example:** `Device(config-if)# ipv6 multicast boundary scope 6`	Configures a multicast boundary on the interface for a specified scope.

Configuring BSR Devices to Announce Scope-to-RP Mappings

IPv6 BSR devices can be statically configured to announce scope-to-RP mappings directly instead of learning them from candidate-RP messages. A user might want to configure a BSR device to announce scope-to-RP mappings so that an RP that does not support BSR is imported into the BSR. Enabling this feature also allows an RP positioned outside the enterprise's BSR domain to be learned by the known remote RP on the local candidate BSR devices.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 pim** [**vrf** *vrf-name*] **bsr announced rp** *ipv6-address* [**group-list** *access-list-name*] [**priority** *priority-value*] [**bidir**] [**scope** *scope-value*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 pim** [**vrf** *vrf-name*] **bsr announced rp** *ipv6-address* [**group-list** *access-list-name*] [**priority** *priority-value*] [**bidir**] [**scope** *scope-value*] **Example:** `Device(config)# ipv6 pim bsr announced rp 2001:DB8:3000:3000::42 priority 0`	Announces scope-to-RP mappings directly from the BSR for the specified candidate RP.

Configuration Examples for Configuring IP Multicast Basic in IPv6 Networks

Example: Enabling IPv6 Multicast Routing

The following example enables multicast routing on all interfaces and also enables multicast forwarding for PIM and MLD on all enabled interfaces of the device.

```
Device> enable
Device# configure terminal
Device(config)# ipv6 multicast-routing
```

Examples: Disabling IPv6 Multicast Address Group Range Support

The following example ensures that the device disables multicast for groups or channels denied by an access list named list2:

```
        ipv6 multicast group-range list2
```

The following example shows that the command in the previous example is overridden on an interface specified by int2. On int2, MLD states are created for groups or channels permitted by int-list2 but are not created for groups or channels denied by int-list2. On all other interfaces, the access-list named list2 is used for access control.

In this example, list2 can be specified to deny all or most multicast groups or channels, and int-list2 can be specified to permit authorized groups or channels only for interface int2.

```
Device(config)# interface int2
Device(config-if)# ipv6 mld access-group int-list2
```

Example: Verifying IPv6 MRIB Information

The following example displays information about the IPv6 MRIB client:

```
Device# show ipv6 mrib client

IP MRIB client-connections
igmp:145        (connection id 0)
pim:146 (connection id 1)
mfib ipv6:3     (connection id 2)
slot 3  mfib ipv6 rp agent:16   (connection id 3)
slot 1  mfib ipv6 rp agent:16   (connection id 4)
slot 0  mfib ipv6 rp agent:16   (connection id 5)
slot 4  mfib ipv6 rp agent:16   (connection id 6)
slot 2  mfib ipv6 rp agent:16   (connection id 7)
```

The following example displays summary information about the IPv6 MRIB route:

```
Device# show ipv6 mrib route summary

MRIB Route-DB Summary
  No. of (*,G) routes = 52
```

```
  No. of (S,G) routes = 0
  No. of Route x Interfaces (RxI) = 10
```

Example: Configuring PIMv6 Anycast RP

```
RP1
Device1(config)# ipv6 pim rp-address 2001:DB8::1:1 acl_sparse1
Device1(config)# interface Loopback4
Device1(config-if)# ipv6 address 2001:DB8::4:4/64
Device1(config-if)# no shut

Device1(config)# interface Loopback5
Device1(config-if)# ipv6 address 2001:DB8:0:ABCD::1/64
Device1(config-if)# no shut
Device1(config-if)# exit
Device1(config)# ipv6 pim anycast-rp 2001:DB8:0:ABCD::1 2001:DB8::3:3

RP2 (Anycast RP Peer)
Device2(config)# ipv6 pim rp-address 2001:DB8::1:1 acl_sparse1
Device2(config)# interface Loopback4
Device2(config-if)# ipv6 address 2001:DB8::3:3/64
Device2(config-if)# no shut

Device2(config)# interface Loopback5
Device2(config-if)# ipv6 address 2001:DB8:0:ABCD::1/64
Device2(config-if)# no shut
Device2(config)# ipv6 pim anycast-rp 2001:DB8::1:1 2001:DB8::4:4
```

```
Device2 show ipv6 pim anycast-rp 2001:DB8::1:1

Anycast RP Peers For 2001:DB8::1:1   Last Register/Register-Stop received
  2001:DB8::3:3 00:00:00/00:00:00
  2001:DB8::4:4 00:00:00/00:00:00
```

Example: Configuring a BSR

```
Device# show ipv6 pim bsr election

PIMv2 BSR information
BSR Election Information
Scope Range List: ff00::/8
This system is the Bootstrap Router (BSR)
BSR Address: 60::1:1:4
Uptime: 00:11:55, BSR Priority: 0, Hash mask length: 126
RPF: FE80::A8BB:CCFF:FE03:C400,Ethernet0/0
BS Timer: 00:00:07
This system is candidate BSR
Candidate BSR address: 60::1:1:4, priority: 0, hash mask length: 126
```

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	*IPv6 Configuration Guide*
Cisco IOS commands	Cisco IOS Master Commands List, All Releases

Related Topic	Document Title
IP multicast commands	Cisco IOS IP Multicast Command Reference
IPv6 commands	Cisco IOS IPv6 Command Reference
Cisco IOS IPv6 features	Cisco IOS IPv6 Feature Mapping

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	*IPv6 RFCs*

MIBs

MIB	MIBs Link
	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Configuring Basic IP Multicast in IPv6 Networks

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 4: Feature Information for Configuring Basic IP Multicast in IPv6 Networks

Feature Name	Releases	Feature Information
IPv6 Multicast	12.0(26)S 12.2(25)SG 12.2(33)SRA 12.2(18)SXE 12.3(2)T 12.4 12.4(2)T 15.0(2)SE Cisco IOS XE Release 2.1	IPv6 multicast allows a host to send a single data stream to a subset of all hosts simultaneously. The following commands were introduced or modified: **clear ipv6 pim topology**, **debug ipv6 mld**, **debug ipv6 mrib**, **debug ipv6 pim**, **debug ipv6 pim neighbor**, **ipv6 mld join-group**, **ipv6 mld query-interval**, **ipv6 mld query-max-response-time**, **ipv6 mld query-timeout**, **ipv6 mld router**, **ipv6 mld static-group**, **ipv6 multicast-routing** , **ipv6 pim**, **ipv6 pim dr-priority**, **ipv6 pim hello-interval**, **ipv6 pim rp-address** , **ipv6 pim spt-threshold infinity** , **show ipv6 mld groups**, **show ipv6 mld groups summary**, **show ipv6 mld interface**, **show ipv6 mrib client**, **show ipv6 mrib route**, **show ipv6 mroute**, **show ipv6 pim group-map**, **show ipv6 pim interface**, **show ipv6 pim neighbor**, **show ipv6 pim range-list**, **show ipv6 pim topology**, **show ipv6 pim tunnel**.
IPv6 Multicast Address Group Range Support	15.0(1)M 12.2(40)SG 3.2.0SG 15.0(2)SG 12.2(33)SRE 12.2(33)SXI Cisco IOS XE Release 2.6	This feature is also known as Disable Group Ranges. This feature provides an access control mechanism for IPv6 multicast edge routing. The following commands were introduced or modified: **ipv6 mld access-group**, **ipv6 multicast boundary scope**, **ipv6 multicast group-range**.

Feature Name	Releases	Feature Information
IPv6 Multicast: Scope Boundaries	12.0(26)S 12.2(18)S 12.2(25)SG 12.2(33)SRA 12.3(2)T 12.4 12.4(2)T 15.0(1)S	IPv6 includes support for global and nonglobal addresses. This feature describes the usage of IPv6 addresses of different scopes.
IPv6 Multicast: Bootstrap Router	12.0(28)S 12.2(25)S 12.2(25)SG 12.2(33)SRA 12.2(33)SXH 12.3(11)T 12.4 12.4(2)T Cisco IOS XE Release 2.4 15.0(1)S	If an RP becomes unreachable, this feature allows the RP to be detected and the mapping tables modified so that the unreachable RP is no longer used, and the new tables will be rapidly distributed throughout the domain. The following commands were introduced or modified: **debug ipv6 pim bsr**, **ipv6 pim bsr border**, **ipv6 pim bsr candidate bsr**, **ipv6 pim bsr candidate rp**, **show ipv6 pim bsr**, **show ipv6 pim group-map**.
IPv6 BSR: Configure RP Mapping	12.2(33)SRE 12.2(50)SY 12.4(2)T Cisco IOS XE Release 2.4 15.0(1)S	This feature allows IPv6 multicast devices to be statically configured to announce scope-to-RP mappings directly from the BSR instead of learning them from candidate-RP messages. The following commands were introduced or modified: **ipv6 multicast-routing**, **ipv6 pim bsr announced rp**, **ipv6 pim bsr candidate bsr**.
IPv6 Multicast: RPF Flooding of BSR Packets	Cisco IOS XE Release 2.1	The RPF flooding of BSR packets feature enables a Cisco IPv6 device to not disrupt the flow of BSMs. The following command was introduced: **show ipv6 pim bsr**.

Feature Name	Releases	Feature Information
IPv6 Multicast VRF Lite	15.1(4)M Cisco IOS XE Release 3.4S 15.1(2)SY	This feature provides IPv6 multicast support for multiple virtual routing/forwarding contexts (VRFs), the scope of which is limited to the device in which the VRFs are defined.

CHAPTER 5

Using MSDP to Interconnect Multiple PIM-SM Domains

This module describes the tasks associated with using Multicast Source Discovery Protocol (MSDP) to interconnect multiple PIM-SM domains. The tasks explain how to configure MSDP peers, mesh groups, and default peers, how to use filters to control and scope MSDP activity, and how to monitor and maintain MSDP. Using MSDP with PIM-SM greatly reduces the complexity of connecting multiple PIM-SM domains.

- Finding Feature Information, page 97
- Prerequisites for MSDP, page 97
- Information About Using MSDP to Interconnect Multiple PIM-SM Domains, page 98
- How to Use MSDP to Interconnect Multiple PIM-SM Domains, page 112
- Configuration Examples for Using MSDP to Interconnect Multiple PIM-SM Domains, page 137
- Additional References, page 140
- Feature Information for Using MSDP to Interconnect Multiple PIM-SM Domains, page 141

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for MSDP

To use MSDP, the switch or stack master must be running the IP services feature set.

To use MSDP, you must enable IP services feature set on Catalyst 3560-CX switches.

Information About Using MSDP to Interconnect Multiple PIM-SM Domains

Benefits of Using MSDP to Interconnect Multiple PIM-SM Domains

- Allows a rendezvous point (RP) to dynamically discover active sources outside of its domain.
- Introduces a more manageable approach for building multicast distribution trees between multiple domains.

Use of MSDP to Interconnect Multiple PIM-SM Domains

MSDP is a mechanism to connect multiple PIM-SM domains. The purpose of MSDP is to discover multicast sources in other PIM domains. The main advantage of MSDP is that it reduces the complexity of interconnecting multiple PIM-SM domains by allowing PIM-SM domains to use an interdomain source tree (rather than a common shared tree). When MSDP is configured in a network, RPs exchange source information with RPs in other domains. An RP can join the interdomain source tree for sources that are sending to groups for which it has receivers. The RP can do that because it is the root of the shared tree within its domain, which has branches to all points in the domain where there are active receivers. When a last-hop router learns of a new source outside the PIM-SM domain (through the arrival of a multicast packet from the source down the shared tree), it then can send a join toward the source and join the interdomain source tree.

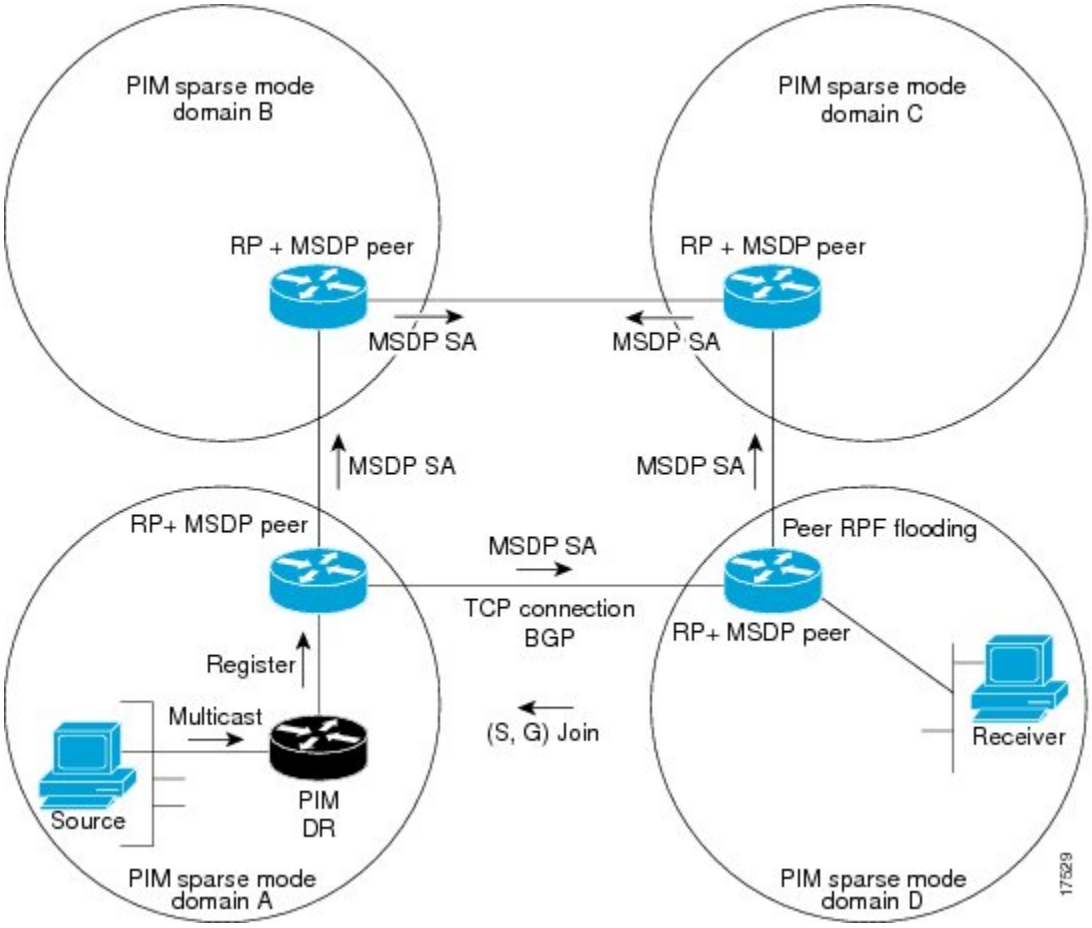
Note If the RP either has no shared tree for a particular group or a shared tree whose outgoing interface list is null, it does not send a join to the source in another domain.

When MSDP is enabled, an RP in a PIM-SM domain maintains MSDP peering relationships with MSDP-enabled routers in other domains. This peering relationship occurs over a TCP connection, where primarily a list of sources sending to multicast groups is exchanged. MSDP uses TCP (port 639) for its peering connections. As with BGP, using point-to-point TCP peering means that each peer must be explicitly configured. The TCP connections between RPs, moreover, are achieved by the underlying routing system. The receiving RP uses the source lists to establish a source path. If the multicast sources are of interest to a domain that has receivers, multicast data is delivered over the normal, source-tree building mechanism provided by PIM-SM. MSDP is also used to announce sources sending to a group. These announcements must originate at the RP of the domain.

Note MSDP depends on BGP or multiprotocol BGP (MBGP) for interdomain operation. We recommended that you run MSDP on RPs sending to global multicast groups.

The figure illustrates MSDP operating between two MSDP peers. PIM uses MSDP as the standard mechanism to register a source with the RP of a domain.

Figure 13: MSDP Running Between RP Peers



When MSDP is implemented, the following sequence of events occurs:

1 When a PIM designated router (DR) registers a source with its RP as illustrated in the figure, the RP sends a Source-Active (SA) message to all of its MSDP peers.

Note The DR sends the encapsulated data to the RP only once per source (when the source goes active). If the source times out, this process happens again when it goes active again. This situation is different from the periodic SA message that contains all sources that are registered to the originating RP. Those SA messages are MSDP control packets, and, thus, do not contain encapsulated data from active sources.

1 The SA message identifies the source address, the group that the source is sending to, and the address or the originator ID of the RP, if configured.

2 Each MSDP peer that receives the SA message floods the SA message to all of its peers downstream from the originator. In some cases (such as the case with the RPs in PIM-SM domains B and C in the figure),

an RP may receive a copy of an SA message from more than one MSDP peer. To prevent looping, the RP consults the BGP next-hop database to determine the next hop toward the originator of the SA message. If both MBGP and unicast BGP are configured, MBGP is checked first, and then unicast BGP. That next-hop neighbor is the RPF-peer for the originator. SA messages that are received from the originator on any interface other than the interface to the RPF peer are dropped. The SA message flooding process, therefore, is referred to as peer-RPF flooding. Because of the peer-RPF flooding mechanism, BGP or MBGP must be running in conjunction with MSDP.

Note (M)BGP is not required in MSDP mesh group scenarios. For more information about MSDP mesh groups, see the Configuring an MSDP Mesh Group, on page 122 section.

Note (M)BGP is not required in default MSDP peer scenarios or in scenarios where only one MSDP peer is configured. For more information, see the Configuring a Default MSDP Peer, on page 121 section.

1. When an RP receives an SA message, it checks to see whether there are any members of the advertised groups in its domain by checking to see whether there are interfaces on the group's (*, G) outgoing interface list. If there are no group members, the RP does nothing. If there are group members, the RP sends an (S, G) join toward the source. As a result, a branch of the interdomain source tree is constructed across autonomous system boundaries to the RP. As multicast packets arrive at the RP, they are then forwarded down its own shared tree to the group members in the RP's domain. The members' DRs then have the option of joining the rendezvous point tree (RPT) to the source using standard PIM-SM procedures.
2. The originating RP continues to send periodic SA messages for the (S, G) state every 60 seconds for as long as the source is sending packets to the group. When an RP receives an SA message, it caches the SA message. Suppose, for example, that an RP receives an SA message for (172.16.5.4, 228.1.2.3) from originating RP 10.5.4.3. The RP consults its mroute table and finds that there are no active members for group 228.1.2.3, so it passes the SA message to its peers downstream of 10.5.4.3. If a host in the domain then sends a join to the RP for group 228.1.2.3, the RP adds the interface toward the host to the outgoing interface list of its (*, 224.1.2.3) entry. Because the RP caches SA messages, the router will have an entry for (172.16.5.4, 228.1.2.3) and can join the source tree as soon as a host requests a join.

Note In all current and supported software releases, caching of MSDP SA messages is mandatory and cannot be manually enabled or disabled. By default, when an MSDP peer is configured, the **ip multicast cache-sa-state** command will automatically be added to the running configuration.

MSDP Message Types

There are four basic MSDP message types, each encoded in their own Type, Length, and Value (TLV) data format.

SA Messages

SA messages are used to advertise active sources in a domain. In addition, these SA messages may contain the initial multicast data packet that was sent by the source.

SA messages contain the IP address of the originating RP and one or more (S, G) pairs being advertised. In addition, the SA message may contain an encapsulated data packet.

Note For more information about SA messages, see the SA Message Origination Receipt and Processing, on page 101 section.

SA Request Messages

SA request messages are used to request a list of active sources for a specific group. These messages are sent to an MSDP SA cache that maintains a list of active (S, G) pairs in its SA cache. Join latency can be reduced by using SA request messages to request the list of active sources for a group instead of having to wait up to 60 seconds for all active sources in the group to be readvertised by originating RPs.

SA Response Messages

SA response messages are sent by the MSDP peer in response to an SA request message. SA response messages contain the IP address of the originating RP and one or more (S, G) pairs of the active sources in the originating RP's domain that are stored in the cache.

Keepalive Messages

Keepalive messages are sent every 60 seconds in order to keep the MSDP session active. If no keepalive messages or SA messages are received for 75 seconds, the MSDP session is reset.

SA Message Origination Receipt and Processing

The section describes SA message origination, receipt, and processing in detail.

SA Message Origination

SA messages are triggered by an RP (assuming MSDP is configured) when any new source goes active within a local PIM-SM domain. A local source is a source that is directly connected to the RP or is the first-hop DR that has registered with it. An RP originates SA messages only for local sources in its PIM-SM domain; that is, for local sources that register with it.

Note A local source is denoted by the A flag being set in the (S, G) mroute entry on the RP (which can be viewed in the output of the **show ip mroute** command). This flag indicates that the source is a candidate for advertisement by the RP to other MSDP peers.

When a source is in the local PIM-SM domain, it causes the creation of (S, G) state in the RP. New sources are detected by the RP either by the receipt of a register message or the arrival of the first (S, G) packet from a directly connected source. The initial multicast packet sent by the source (either encapsulated in the register message or received from a directly connected source) is encapsulated in the initial SA message.

SA Message Receipt

SA messages are only accepted from the MSDP RPF peer that is in the best path back toward the originator. The same SA message arriving from other MSDP peers must be ignored or SA loops can occur. Deterministically selecting the MSDP RPF peer for an arriving SA message requires knowledge of the MSDP topology. However, MSDP does not distribute topology information in the form of routing updates. MSDP infers this information by using (M)BGP routing data as the best approximation of the MSDP topology for the SA RPF check mechanism. An MSDP topology, therefore, must follow the same general topology as the BGP peer topology. Besides a few exceptions (such as default MSDP peers and MSDP peers in MSDP mesh groups), MSDP peers, in general should also be (M)BGP peers.

How RPF Check Rules Are Applied to SA Messages

The rules that apply to RPF checks for SA messages are dependent on the BGP peerings between the MSDP peers:

- Rule 1: Applied when the sending MSDP peer is also an interior (M)BGP peer.
- Rule 2: Applied when the sending MSDP peer is also an exterior (M)BGP peer.
- Rule 3: Applied when the sending MSDP peer is not an (M)BGP peer.

RPF checks are not performed in the following cases:

- If the sending MSDP peer is the only MSDP peer, which would be the case if only a single MSDP peer or a default MSDP peer is configured.
- If the sending MSDP peer is a member of a mesh group.
- If the sending MSDP peer address is the RP address contained in the SA message.

How the Software Determines the Rule to Apply to RPF Checks

The software uses the following logic to determine which RPF rule to apply to RPF checks:

- Find the (M)BGP neighbor that has the same IP address as the sending MSDP peer.
    - If the matching (M)BGP neighbor is an internal BGP (iBGP) peer, apply Rule 1.
    - If the matching (M)BGP neighbor is an external BGP (eBGP) peer, apply Rule 2.
    - If no match is found, apply Rule 3.

The implication of the RPF check rule selection is as follows: The IP address used to configure an MSDP peer on a device must match the IP address used to configure the (M)BGP peer on the same device.

Rule 1 of RPF Checking of SA Messages in MSDP

Rule 1 of RPF checking in MSDP is applied when the sending MSDP peer is also an i(M)BGP peer. When Rule 1 is applied, the RPF check proceeds as follows:

1. The peer searches the BGP Multicast Routing Information Base (MRIB) for the best path to the RP that originated the SA message. If a path is not found in the MRIB, the peer then searches the Unicast Routing Information Base (URIB). If a path is still not found, the RPF check fails.
2. If the previous search succeeds (that is, the best path is found), the peer then determines the address of the BGP neighbor for this best path, which will be the address of the BGP neighbor that sent the peer the path in BGP update messages.

Note The BGP neighbor address is not the same as the next-hop address in the path. Because i(M)BGP peers do not update the next-hop attribute of a path, the next-hop address usually is not the same as the address of the BGP peer that sent us the path.

Note The BGP neighbor address is not necessarily the same as the BGP ID of the peer that sent the peer the path.

1. If the IP address of the sending MSDP peer is the same as the BGP neighbor address (that is, the address of the BGP peer that sent the peer the path), then the RPF check succeeds; otherwise it fails.

Implications of Rule 1 of RPF Checking on MSDP

The MSDP topology must mirror the (M)BGP topology. In general, wherever there is an i(M)BGP peer connection between two devices, an MSDP peer connection should be configured. More specifically, the IP address of the far-end MSDP peer connection must be the same as the far-end i(M)BGP peer connection. The addresses must be the same because the BGP topology between i(M)BGP peers inside an autonomous system is not described by the AS path. If it were always the case that i(M)BGP peers updated the next-hop address in the path when sending an update to another i(M)BGP peer, then the peer could rely on the next-hop address to describe the i(M)BGP topology (and hence the MSDP topology). However, because the default behavior for i(M)BGP peers is to not update the next-hop address, the peer cannot rely on the next-hop address to describe the (M)BGP topology (MSDP topology). Instead, the i(M)BGP peer uses the address of the i(M)BGP peer that sent the path to describe the i(M)BGP topology (MSDP topology) inside the autonomous system.

Tip Care should be taken when configuring the MSDP peer addresses to make sure that the same address is used for both i(M)BGP and MSDP peer addresses.

Rule 2 of RPF Checking of SA Messages in MSDP

Rule 2 of RPF checking in MSDP is applied when the sending MSDP peer is also an e(M)BGP peer. When Rule 2 is applied, the RPF check proceeds as follows:

1. The peer searches the BGP MRIB for the best path to the RP that originated the SA message. If a path is not found in the MRIB, the peer then searches the URIB. If a path is still not found, the RPF check fails.
2. If the previous search succeeds (that is, the best path is found), the peer then examines the path. If the first autonomous system in the best path to the RP is the same as the autonomous system of the e(M)BGP peer (which is also the sending MSDP peer), then the RPF check succeeds; otherwise it fails.

Implications of Rule 2 of RPF Checking on MSDP

The MSDP topology must mirror the (M)BGP topology. In general, wherever there is an e(M)BGP peer connection between two devices, an MSDP peer connection should be configured. As opposed to Rule 1, the IP address of the far-end MSDP peer connection does not have to be the same as the far-end e(M)BGP peer connection.The reason that the addresses do not have to be identical is that BGP topology between two e(M)BGP peers is not described by the AS path.

Rule 3 of RPF Checking of SA Messages in MSDP

Rule 3 of RPF checking is applied when the sending MSDP peer is not a (M)BGP peer at all. When Rule 3 is applied, the RPF check proceeds as follows:

1. The peer searches the BGP MRIB for the best path to the RP that originated the SA message. If a path is not found in the MRIB, the peer then searches the URIB. If a path is still not found, the RPF check fails.
2. If the previous search succeeds (that is, the best path to the RP that originated the SA message is found), the peer then searches the BGP MRIB for the best path to the MSDP peer that sent the SA message. If a path is not found in the MRIB, the peer then searches the URIB. If a path is still not found, the RPF check fails.

Note The autonomous system of the MSDP peer that sent the SA is the origin autonomous system, which is the last autonomous system in the AS path to the MSDP peer.

1. If the first autonomous system in the best path to the RP is the same as the autonomous system of the sending MSDP peer, then the RPF check succeeds; otherwise it fails.

SA Message Processing

The following steps are taken by an MSDP peer whenever it processes an SA message:

1. Using the group address G of the (S, G) pair in the SA message, the peer locates the associated (*, G) entry in the mroute table. If the (*, G) entry is found and its outgoing interface list is not null, then there are active receivers in the PIM-SM domain for the source advertised in the SA message.
2. The MSDP peer then creates an (S, G) entry for the advertised source.
3. If the (S, G) entry did not already exist, the MSDP peer immediately triggers an (S, G) join toward the source in order to join the source tree.
4. The peer then floods the SA message to all other MSDP peers with the exception of:
   - The MSDP peer from which the SA message was received.

- Any MSDP peers that are in the same MSDP mesh group as this device (if the peer is a member of a mesh group).

Note SA messages are stored locally in the device's SA cache.

MSDP Peers

Like BGP, MSDP establishes neighbor relationships with other MSDP peers. MSDP peers connect using TCP port 639. The lower IP address peer takes the active role of opening the TCP connection. The higher IP address peer waits in LISTEN state for the other to make the connection. MSDP peers send keepalive messages every 60 seconds. The arrival of data performs the same function as the keepalive message and keeps the session from timing out. If no keepalive messages or data is received for 75 seconds, the TCP connection is reset.

MSDP MD5 Password Authentication

The MSDP MD5 password authentication feature is an enhancement to support Message Digest 5 (MD5) signature protection on a TCP connection between two MSDP peers. This feature provides added security by protecting MSDP against the threat of spoofed TCP segments being introduced into the TCP connection stream.

How MSDP MD5 Password Authentication Works

Developed in accordance with RFC 2385, the MSDP MD5 password authentication feature is used to verify each segment sent on the TCP connection between MSDP peers. The **ip msdp password peer** command is used to enable MD5 authentication for TCP connections between two MSDP peers. When MD5 authentication is enabled between two MSDP peers, each segment sent on the TCP connection between the peers is verified. MD5 authentication must be configured with the same password on both MSDP peers; otherwise, the connection between them will not be made. Configuring MD5 authentication causes the Cisco IOS software to generate and verify the MD5 digest of every segment sent on the TCP connection.

Benefits of MSDP MD5 Password Authentication

- Protects MSDP against the threat of spoofed TCP segments being introduced into the TCP connection stream.
- Uses the industry-standard MD5 algorithm for improved reliability and security.

SA Message Limits

The **ip msdp sa-limit** command is used to limit the overall number of SA messages that a device can accept from specified MSDP peers. When the **ip msdp sa-limit** command is configured, the device maintains a per-peer count of SA messages stored in the SA cache and will ignore new messages from a peer if the configured SA message limit for that peer has been reached.

The **ip msdp sa-limit** command was introduced as a means to protect an MSDP-enabled device from denial of service (DoS) attacks. We recommended that you configure SA message limits for all MSDP peerings on the device. An appropriately low SA limit should be configured on peerings with a stub MSDP region (for example, a peer that may have some further downstream peers but that will not act as a transit for SA messages across the rest of the Internet). A high SA limit should be configured for all MSDP peerings that act as transits for SA messages across the Internet.

MSDP Keepalive and Hold-Time Intervals

The **ip msdp keepalive** command is used to adjust the interval at which an MSDP peer will send keepalive messages and the interval at which the MSDP peer will wait for keepalive messages from other peers before declaring them down.

Once an MSDP peering session is established, each side of the connection sends a keepalive message and sets a keepalive timer. If the keepalive timer expires, the local MSDP peer sends a keepalive message and restarts its keepalive timer; this interval is referred to as the keepalive interval. The *keepalive-interval*argument is used to adjust the interval for which keepalive messages will be sent. The keepalive timer is set to the value specified for the *keepalive-interval*argument when the peer comes up. The keepalive timer is reset to the value of the *keepalive-interval* argument whenever an MSDP keepalive message is sent to the peer and reset when the timer expires. The keepalive timer is deleted when an MSDP peering session is closed. By default, the keepalive timer is set to 60 seconds.

Note The value specified for the *keepalive-interval* argument must be less than the value specified for the *holdtime-interval*argument and must be at least one second.

The hold-time timer is initialized to the value of the *hold-time-interval* argument whenever an MSDP peering connection is established, and is reset to the value of the *hold-time-interval*argument whenever an MSDP keepalive message is received. The hold-time timer is deleted whenever an MSDP peering connection is closed. By default, the hold-time interval is set to 75 seconds.

Use the *hold-time-interval* argument to adjust the interval at which the MSDP peer will wait for keepalive messages from other peers before declaring them down.

MSDP Connection-Retry Interval

You can adjust the interval at which all MSDP peers will wait after peering sessions are reset before attempting to reestablish the peering sessions. This interval is referred to as the connection-retry interval. By default, MSDP peers will wait 30 seconds after the session is reset before attempting to reestablish sessions with other peers. The modified configured connection-retry interval applies to all MSDP peering sessions on the device.

MSDP Compliance with IETF RFC 3618

When the MSDP Compliance with IETF RFC 3618 feature is configured, the peer-RPF forwarding rules defined in IETF RFC 3618 are applied to MSDP peers. IETF RFC 3618 provides peer-RPF forwarding rules that are used for forwarding SA messages throughout an MSDP-enabled internet. Unlike the RPF check used when forwarding data packets, which compares a packet's source address against the interface upon which the packet was received, the peer-RPF check compares the RP address carried in the SA message against the

MSDP peer from which the message was received. Except when MSDP mesh groups are being used, SA messages from an RP address are accepted from only one MSDP peer to avoid looping SA messages.

Note For more information about the MSDP peer-forwarding rules defined in RFC 3618, see RFC 3618, Multicast Source Discovery Protocol (MSDP) .

Benefits of MSDP Compliance with RFC 3618

- You can use BGP route reflectors (RRs) without running MSDP on them. This capability is useful to service providers that need to reduce the load on RRs.
- You can use an Interior Gateway Protocol (IGP) for the Reverse Path Forwarding (RPF) checks and thereby run peerings without (M)BGP. This capability is useful to enterprise customers that do not run (M)BGP and require larger topologies than mesh groups can provide.

Note IGP peerings must always be between directly connected MSDP peers or else the RPF checks will fail.

- You can have peerings between routers in nondirectly connected autonomous systems (that is, with one or more autonomous systems between them). This capability helps in confederation configurations and for redundancy.

Default MSDP Peers

In most scenarios, an MSDP peer is also a BGP peer. If an autonomous system is a stub or nontransit autonomous system, and particularly if the autonomous system is not multihomed, there is little or no reason to run BGP to its transit autonomous system. A static default route at the stub autonomous system, and a static route pointing to the stub prefixes at the transit autonomous system, is generally sufficient. But if the stub autonomous system is also a multicast domain and its RP must peer with an RP in the neighboring domain, MSDP depends on the BGP next-hop database for its peer-RPF checks. You can disable this dependency on BGP by defining a default peer from which to accept all SA messages without performing the peer-RPF check, using the **ip msdp default-peer** command. A default MSDP peer must be a previously configured MSDP peer.

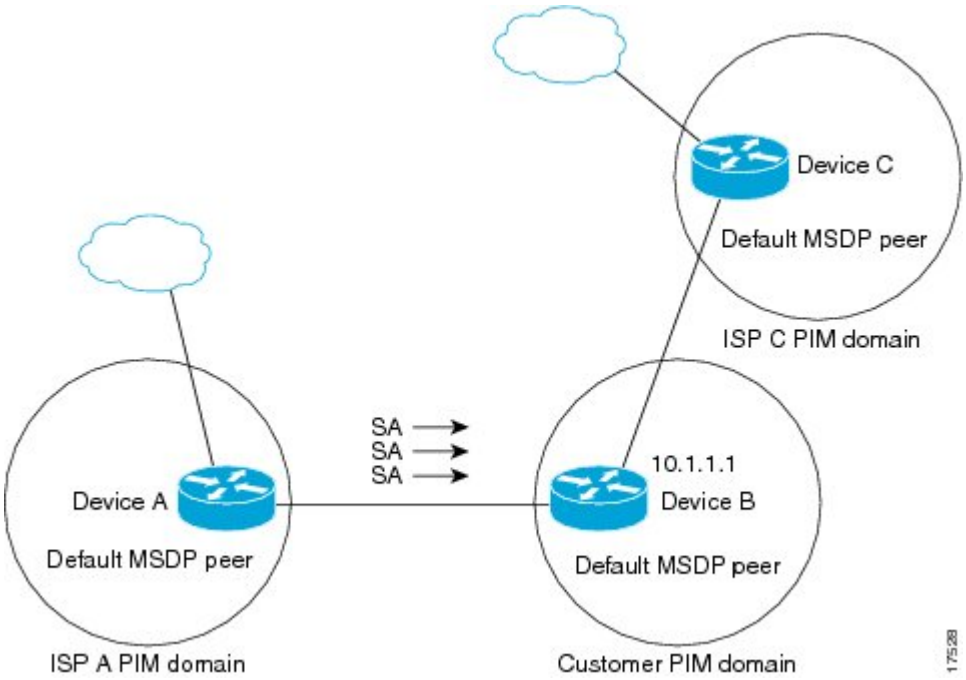
A stub autonomous system also might want to have MSDP peerings with more than one RP for the sake of redundancy. For example, SA messages cannot just be accepted from multiple default peers, because there is no RPF check mechanism. Instead, SA messages are accepted from only one peer. If that peer fails, SA messages are then accepted from the other peer. The underlying assumption here, of course, is that both default peers are sending the same SA messages.

The figure illustrates a scenario where default MSDP peers might be used. In the figure, a customer that owns Router B is connected to the Internet through two Internet service providers (ISPs), one that owns Router A and the other that owns Router C. They are not running BGP or MBGP between them. In order for the customer to learn about sources in the ISP domain or in other domains, Router B identifies Router A as its default MSDP peer. Router B advertises SA messages to both Router A and Router C, but accepts SA messages either from Router A only or Router C only. If Router A is the first default peer in the configuration, it will be used if it is up and running. Only if Router A is not running will Router B accept SA messages from Router C.

The ISP will also likely use a prefix list to define which prefixes it will accept from the customer router. The customer will define multiple default peers, each having one or more prefixes associated with it.

The customer has two ISPs to use. The customer defines both ISPs as default peers. As long as the first default peer identified in the configuration is up and running, it will be the default peer and the customer will accept all SA messages it receives from that peer.

Figure 14: Default MSDP Peer Scenario



Router B advertises SAs to Router A and Router C, but uses only Router A or Router C to accept SA messages. If Router A is first in the configuration, it will be used if it is up and running. Only when Router A is not running will Router B accept SAs from Router C. This is the behavior without a prefix list.

If you specify a prefix list, the peer will be a default peer only for the prefixes in the list. You can have multiple active default peers when you have a prefix list associated with each. When you do not have any prefix lists, you can configure multiple default peers, but only the first one is the active default peer as long as the router has connectivity to this peer and the peer is alive. If the first configured peer goes down or the connectivity to this peer goes down, the second configured peer becomes the active default, and so on.

MSDP Mesh Groups

An MSDP mesh group is a group of MSDP speakers that have fully meshed MSDP connectivity between one another. In other words, each of the MSDP peers in the group must have an MSDP peering relationship (MSDP connection) to every other MSDP peer in the group. When an MSDP mesh group is configured between a group of MSDP peers, SA message flooding is reduced. Because when an MSDP peer in the group receives an SA message from another MSDP peer in the group, it assumes that this SA message was sent to all the other MSDP peers in the group. As a result, it is not necessary for the receiving MSDP peer to flood the SA message to the other MSDP peers in the group.

Benefits of MSDP Mesh Groups

- Optimizes SA flooding--MSDP mesh groups are particularly useful for optimizing SA flooding when two or more peers are in a group.
- Reduces the amount of SA traffic across the Internet--When MSDP mesh groups are used, SA messages are not flooded to other mesh group peers.
- Eliminates RPF checks on arriving SA messages--When an MSDP mesh group is configured, SA messages are always accepted from mesh group peers.

SA Origination Filters

By default, an RP that is configured to run MSDP will originate SA messages for all local sources for which it is the RP. Local sources that register with an RP, therefore, will be advertised in SA messages, which in some cases is not desirable. For example, if sources inside a PIM-SM domain are using private addresses (for example, network 10.0.0.0/8), you should configure an SA origination filter to restrict those addresses from being advertised to other MSDP peers across the Internet.

To control what sources are advertised in SA messages, you can configure SA origination filters on an RP. By creating SA origination filters, you can control the sources advertised in SA messages as follows:

- You can configure an RP to prevent the device from advertising local sources in SA messages. The device will still forward SA messages from other MSDP peers in the normal fashion; it will just not originate any SA messages for local sources.
- You can configure the device to only originate SA messages for local sources sending to specific groups that match (S, G) pairs defined in the extended access list. All other local sources will not be advertised in SA messages.
- You can configure the device to only originate SA messages for local sources sending to specific groups that the match AS paths defined in an AS-path access list. All other local sources will not be advertised in SA messages.
- You can configure the device to only originate SA messages for local sources that match the criteria defined in the route map. All other local sources will not be advertised in SA messages.
- You configure an SA origination filter that includes an extended access list, an AS-path access list, and route map, or a combination thereof. In this case, all conditions must be true before any local sources are advertised in SA messages.

Use of Outgoing Filter Lists in MSDP

By default, an MSDP-enabled device forwards all SA messages it receives to all of its MSDP peers. However, you can prevent SA messages from being forwarded to MSDP peers by creating outgoing filter lists. Outgoing filter lists apply to all SA messages, whether locally originated or received from another MSDP peer, whereas SA origination filters apply only to locally originated SA messages. For more information about enabling a filter for MSDP SA messages originated by the local device, see the Controlling SA Messages Originated by an RP for Local Sources section.

By creating an outgoing filter list, you can control the SA messages that a device forwards to a peer as follows:

- You can filter all outgoing SA messages forwarded to a specified MSDP peer by configuring the device to stop forwarding its SA messages to the MSDP peer.
- You can filter a subset of outgoing SA messages forwarded to a specified MSDP peer based on (S, G) pairs defined in an extended access list by configuring the device to only forward SA messages to the MSDP peer that match the (S, G) pairs permitted in an extended access list. The forwarding of all other SA messages to the MSDP peer will be stopped.
- You can filter a subset of outgoing SA messages forwarded to a specified MSDP peer based on match criteria defined in a route map by configuring the device to only forward SA messages that match the criteria defined in the route map. The forwarding of all other SA messages to the MSDP peer will be stopped.
- You can filter a subset of outgoing SA messages from a specified peer based on the announcing RP address contained in the SA message by configuring the device to filter outgoing SA messages based on their origin, even after an SA message has been transmitted across one or more MSDP peers. The forwarding of all other SA messages to the MSDP peer will be stopped.
- You can configure an outgoing filter list that includes an extended access list, a route map, and either an RP access list or an RP route map. In this case, all conditions must be true for the MSDP peer to forward the outgoing SA message.

Caution Arbitrary filtering of SA messages can result in downstream MSDP peers being starved of SA messages for legitimate active sources. Care, therefore, should be taken when using these sorts of filters. Normally, outgoing filter lists are used only to reject undesirable sources, such as sources using private addresses.

Use of Incoming Filter Lists in MSDP

By default, an MSDP-enabled device receives all SA messages sent to it from its MSDP peers. However, you can control the source information that a device receives from its MSDP peers by creating incoming filter lists.

By creating incoming filter lists, you can control the incoming SA messages that a device receives from its peers as follows:

- You can filter all incoming SA messages from a specified MSDP peer by configuring the device to ignore all SA messages sent to it from the specified MSDP peer.
- You can filter a subset of incoming SA messages from a specified peer based on (S, G) pairs defined in an extended access list by configuring the device to only receive SA messages from the MSDP peer that match the (S, G) pairs defined in the extended access list. All other incoming SA messages from the MSDP peer will be ignored.
- You can filter a subset of incoming SA request messages from a specified peer based on match criteria defined in a route map by configuring the device to only receive SA messages that match the criteria defined in the route map. All other incoming SA messages from the MSDP peer will be ignored.
- You can filter a subset of incoming SA messages from a specified peer based on both (S, G) pairs defined in an extended access list and on match criteria defined in a route map by configuring the device to only receive incoming SA messages that both match the (S, G) pairs defined in the extended access list and match the criteria defined in the route map. All other incoming SA messages from the MSDP peer will be ignored.

- You can filter a subset of incoming SA messages from a specified peer based on the announcing RP address contained in the SA message by configuring the device to filter incoming SA messages based on their origin, even after the SA message may have already been transmitted across one or more MSDP peers.
- You can configure an incoming filter list that includes an extended access list, a route map, and either an RP access list or an RP route map. In this case, all conditions must be true for the MSDP peer to receive the incoming SA message.

Caution Arbitrary filtering of SA messages can result in downstream MSDP peers being starved of SA messages for legitimate active sources. Care, therefore, should be taken when using these sorts of filters. Normally, incoming filter lists are used only to reject undesirable sources, such as sources using private addresses.

TTL Thresholds in MSDP

The time-to-live (TTL) value provides a means to limit the number of hops a packet can take before being dropped. The **ip multicast ttl-threshold** command is used to specify a TTL for data-encapsulated SA messages sent to specified MSDP peers. By default, multicast data packets in SA messages are sent to an MSDP peer, provided the TTL value of the packet is greater than 0, which is standard TTL behavior.

In general, a TTL-threshold problem can be introduced by the encapsulation of a source's initial multicast packet in an SA message. Because the multicast packet is encapsulated inside of the unicast SA message (whose TTL is 255), its TTL is not decremented as the SA message travels to the MSDP peer. Furthermore, the total number of hops that the SA message traverses can be drastically different than a normal multicast packet because multicast and unicast traffic may follow completely different paths to the MSDP peer and hence the remote PIM-SM domain. As a result, encapsulated packets can end up violating TTL thresholds. The solution to this problem is to configure a TTL threshold that is associated with any multicast packet that is encapsulated in an SA message sent to a particular MSDP peer using the **ip multicast ttl-threshold** command. The **ip msdp ttl-threshold** command prevents any multicast packet whose TTL in the IP header is less than the TTL value specified for the *ttl-value*argument from being encapsulated in SA messages sent to that peer.

SA Request Messages

You can configure a noncaching device to send SA request messages to one or more specified MSDP peers.

If an noncaching RP has an MSDP peer that is caching SAs, you can reduce the join latency for a noncaching peer by enabling the noncaching peer to send SA request messages. When a host requests a join to a particular group, the noncaching RP sends an SA request message to its caching peers. If a peer has cached source information for the group in question, it sends the information to the requesting RP with an SA response message. The requesting RP uses the information in the SA response but does not forward the message to any other peers. If a noncaching RP receives an SA request, it sends an error message back to the requestor.

Note In all current and supported software releases, caching of MSDP SA messages is mandatory and cannot be manually enabled or disabled. By default, when an MSDP peer is configured, the configured commands are automatically added to the running configuration.

SA Request Filters

By default, a device honors all outgoing SA request messages from its MSDP peers; that is, it sends cached source information to requesting MSDP peers in SA response messages. You can control the outgoing SA request messages that a device will honor from specified peers by creating an SA request filter. An SA request filter controls the outgoing SA requests that the device will honor from MSDP peers as follows:

- You can filter all SA request messages from a specified peer by configuring the device to ignore all SA requests from the specified MSDP peer.
- You can filter a subset of SA request messages from a specified peer based on groups defined in a standard access list by configuring the device to honor only SA request messages from the MSDP peer that match the groups defined in a standard access list. SA request messages from the specified peer for other groups will be ignored.

MSDP MIB

The MSDP MIB describes managed objects that can be used to remotely monitor MSDP speakers using SNMP. The MSDP MIB module contains four scalar objects and three tables. The tables are the Requests table, the Peer table, and the Source-Active (SA) Cache table. The Cisco implementation supports the Peer table and SA Cache table only. The Requests table contains information used to determine which peer to send SA requests to. However, the MSDP implementation used in Cisco IOS software does not associate sending SA requests to peers with group addresses (or group address masks).

Note The MSDP-MIB.my file can be downloaded from the Cisco MIB website on Cisco.com at the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml .

How to Use MSDP to Interconnect Multiple PIM-SM Domains

The first task is required; all other tasks are optional.

Configuring an MSDP Peer

Note By enabling an MSDP peer, you implicitly enable MSDP.

Before You Begin

- IP multicast routing must be enabled and PIM-SM must be configured.
- With the exception of a single MSDP peer, default MSDP peer, and MSDP mesh group scenarios, all MSDP peers must be configured to run BGP prior to being configured for MSDP.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip msdp peer** {*peer-name*| *peer-address*} [*connect-source type number*] [**remote-as** *as-number*]
4. **ip msdp description** {*peer-name*| *peer-address*} *text*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip msdp peer** {*peer-name*| *peer-address*} [*connect-source type number*] [**remote-as** *as-number*] **Example:** `Device(config)# ip msdp peer 192.168.1.2 connect-source loopback0`	Enables MSDP and configures an MSDP peer as specified by the DNS name or IP address. **Note** The device that is selected to be configured as an MSDP peer is also usually a BGP neighbor. If it is not, see the Configuring a Default MSDP Peer, on page 121 section or the Configuring an MSDP Mesh Group, on page 122 section. • If you specify the **connect-source**keyword, the primary address of the specified local interface *type* and *number* values are used as the source IP address for the TCP connection. The **connect-source**keyword is recommended, especially for MSDP peers on a border that peer with a device inside of a remote domain.
Step 4	**ip msdp description** {*peer-name*| *peer-address*} *text* **Example:** `Device(config)# ip msdp description 192.168.1.2 router at customer a`	(Optional) Configures a description for a specified peer to make it easier to identify in a configuration or in **show** command output.
Step 5	**end** **Example:** `Device(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Shutting Down an MSDP Peer

Perform this optional task to shut down an MSDP peer.

If you are configuring several MSDP peers and you do not want any of the peers to go active until you have finished configuring all of them, you can shut down each peer, configure each peer, and later bring each peer up. You might also want to shut down an MSDP session without losing the configuration for that MSDP peer.

Note When an MSDP peer is shut down, the TCP connection is terminated and not restarted until the peer is brought back up using the **no ip msdp shutdown** command (for the specified peer).

Before You Begin

MSDP is running and the MSDP peers must be configured.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip msdp shutdown** {*peer-name* | *peer-address*}
4. Repeat Step 3 to shut down additional MSDP peers.
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `SwitchControllerDevice> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `SwitchControllerDevice# configure terminal`	Enters global configuration mode.
Step 3	**ip msdp shutdown** {*peer-name* | *peer-address*} **Example:** `SwitchControllerDevice(config)# ip msdp shutdown 192.168.1.3`	Administratively shuts down the specified MSDP peer.

	Command or Action	Purpose
Step 4	Repeat Step 3 to shut down additional MSDP peers.	--
Step 5	**end** **Example:** `SwitchControllerDevice(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring MSDP MD5 Password Authentication Between MSDP Peers

Perform this optional task to configure MSDP MD5 password authentication between MSDP peers.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip msdp password peer** {*peer-name* | *peer-address*} [*encryption-type*] *string*
4. **exit**
5. **show ip msdp peer** [peer-address | peer-name]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip msdp password peer** {*peer-name* | *peer-address*} [*encryption-type*] *string* **Example:** `Device(config)# ip msdp password peer 10.32.43.144 0 test`	Enables MD5 password encryption for a TCP connection between two MSDP peers. **Note** MD5 authentication must be configured with the same password on both MSDP peers; otherwise, the connection between them will not be made. • If you configure or change the password or key, which is used for MD5 authentication between two MSDP peers, the local device does not disconnect the existing session after you configure the

	Command or Action	Purpose
		password. You must manually disconnect the session to activate the new or changed password.
Step 4	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.
Step 5	**show ip msdp peer** [peer-address | peer-name] **Example:** `Device# show ip msdp peer`	(Optional) Displays detailed information about MSDP peers. **Note** Use this command to verify whether MD5 password authentication is enabled on an MSDP peer.

Troubleshooting Tips

If a device has a password configured for an MSDP peer but the MSDP peer does not, a message such as the following will appear on the console while the devices attempt to establish an MSDP session between them:

```
%TCP-6-BADAUTH: No MD5 digest from [peer's IP address]:11003 to [local router's
IP address]:179
```

Similarly, if the two devices have different passwords configured, a message such as the following will appear on the console:

```
%TCP-6-BADAUTH: Invalid MD5 digest from [peer's IP address]:11004 to [local router's
IP address]:179
```

The **debug ip tcp transactions** command is used to display information on significant TCP transactions such as state changes, retransmissions, and duplicate packets. In the context of monitoring or troubleshooting MSDP MD5 password authentication, use the **debug ip tcp transactions** command to verify that the MD5 password is enabled and that the keepalive message is received by the MSDP peer.

Preventing DoS Attacks by Limiting the Number of SA Messages Allowed in the SA Cache from Specified MSDP Peers

Perform this optional (but highly recommended) task to limit the overall number of SA messages that the device can accept from specified MSDP peers. Performing this task protects an MSDP-enabled device from distributed denial-of-service (DoS) attacks.

Note We recommend that you perform this task for all MSDP peerings on the device.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip msdp sa-limit** {*peer-address* | *peer-name*} *sa-limit*
4. Repeat Step 3 to configure SA limits for additional MSDP peers.
5. **exit**
6. **show ip msdp count** [*as-number*]
7. **show ip msdp peer** [*peer-address* | *peer-name*]
8. **show ip msdp summary**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip msdp sa-limit** {*peer-address* | *peer-name*} *sa-limit* **Example:** `Device(config)# ip msdp sa-limit 192.168.10.1 100`	Limits the number of SA messages allowed in the SA cache from the specified MSDP.
Step 4	Repeat Step 3 to configure SA limits for additional MSDP peers.	--
Step 5	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.
Step 6	**show ip msdp count** [*as-number*] **Example:** `Device# show ip msdp count`	(Optional) Displays the number of sources and groups originated in MSDP SA messages and the number of SA messages from an MSDP peer in the SA cache.
Step 7	**show ip msdp peer** [*peer-address* | *peer-name*]	(Optional) Displays detailed information about MSDP peers.

	Command or Action	Purpose
	Example: `Device# show ip msdp peer`	**Note** The output of this command displays the number of SA messages received from MSDP peers that are stored in the cache.
Step 8	**show ip msdp summary** **Example:** `Device# show ip msdp summary`	(Optional) Displays MSDP peer status. **Note** The output of this command displays a per-peer "SA Count" field that displays the number of SAs stored in the cache.

Adjusting the MSDP Keepalive and Hold-Time Intervals

Perform this optional task to adjust the interval at which an MSDP peer will send keepalive messages and the interval at which the MSDP peer will wait for keepalive messages from other peers before declaring them down. By default, it may take as long as 75 seconds for an MSDP peer to detect that a peering session with another MSDP peer has gone down. In network environments with redundant MSDP peers, decreasing the hold-time interval can expedite the reconvergence time of MSDP peers in the event that an MSDP peer fails.

Note We recommend that you do not change the command defaults for the **ip msdp keepalive** command, because the command defaults are in accordance with RFC 3618, *Multicast Source Discovery Protocol*. If your network environment requires that you modify the defaults, you must configure the same time values for the *keepalive-interval* and *hold-time-interval* arguments on both ends of the MSDP peering session.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip msdp keepalive** {*peer-address* | *peer-name*} *keepalive-interval hold-time-interval*
4. Repeat Step 3 to adjust the keepalive message interval for additional MSDP peers.
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip msdp keepalive** {*peer-address* | *peer-name*} *keepalive-interval hold-time-interval* **Example:** `Device(config)# ip msdp keepalive 10.1.1.3 40 55`	Configures the interval at which an MSDP peer will send keepalive messages and the interval at which the MSDP peer will wait for keepalive messages from other peers before declaring them down.
Step 4	Repeat Step 3 to adjust the keepalive message interval for additional MSDP peers.	--
Step 5	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Adjusting the MSDP Connection-Retry Interval

Perform this optional task to adjust the interval at which MSDP peers will wait after peering sessions are reset before attempting to reestablish the peering sessions. In network environments where fast recovery of SA messages is required, such as in trading floor network environments, you may want to decrease the connection-retry interval to a time value less than the default value of 30 seconds.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip msdp timer** *connection-retry-interval*
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip msdp timer** *connection-retry-interval* **Example:** `Device# ip msdp timer 45`	Configures the interval at which MSDP peers will wait after peering sessions are reset before attempting to reestablish the peering sessions.
Step 4	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring MSDP Compliance with IETF RFC 3618

Perform this optional task to configure MSDP peers to be compliant with Internet Engineering Task Force (IETF) RFC 3618 specifications for MSDP.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip msdp rpf rfc3618**
4. **end**
5. **show ip msdp rpf-peer** *rp-address*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip msdp rpf rfc3618** **Example:** `Router(config)# ip msdp rpf rfc3618`	Enables compliance with the peer-RPF forwarding rules specified in IETF RFC 3618.
Step 4	**end** **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.
Step 5	**show ip msdp rpf-peer** *rp-address* **Example:** `Router# show ip msdp rpf-peer 192.168.1.5`	(Optional) Displays the unique MSDP peer information from which a router will accept SA messages originating from the specified RP.

Configuring a Default MSDP Peer

Perform this optional task to configure a default MSDP peer.

Before You Begin

An MSDP default peer must be a previously configured MSDP peer. Before configuring a default MSDP peer, you must first configure an MSDP peer.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip msdp default-peer** {*peer-address* | *peer-name*} [**prefix-list** *list*]
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Device> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip msdp default-peer** {*peer-address* | *peer-name*} [**prefix-list** *list*] **Example:** `Device(config)# ip msdp default-peer 192.168.1.3`	Configures a default peer from which to accept all MSDP SA messages
Step 4	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring an MSDP Mesh Group

Perform this optional task to configure an MSDP mesh group.

Note You can configure multiple mesh groups per device.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip msdp mesh-group** *mesh-name* {*peer-address* | *peer-name*}
4. Repeat Step 3 to add MSDP peers as members of the mesh group.
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `SwitchControllerDevice> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `SwitchControllerDevice# configure terminal`	Enters global configuration mode.
Step 3	**ip msdp mesh-group** *mesh-name* {*peer-address* | *peer-name*} **Example:** `SwitchControllerDevice(config)# ip msdp mesh-group peermesh`	Configures an MSDP mesh group and indicates that an MSDP peer belongs to that mesh group. **Note** All MSDP peers on a device that participate in a mesh group must be fully meshed with all other MSDP peers in the group. Each MSDP peer on each device must be configured as a peer using the **ip msdp peer** command and also as a member of the mesh group using the **ip msdp mesh-group** command.
Step 4	Repeat Step 3 to add MSDP peers as members of the mesh group.	--
Step 5	**exit** **Example:** `SwitchControllerDevice(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Controlling SA Messages Originated by an RP for Local Sources

Perform this task to control SA messages originated by an RP by enabling a filter to restrict which registered sources are advertised in SA messages.

Note For best practice information related to configuring MSDP SA message filters, see the Multicast Source Discovery Protocol SA Filter Recommendations tech note.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip msdp redistribute** [**list** *access-list*] [**asn** *as-access-list*] [**route-map** *map-name*]
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip msdp redistribute** [**list** *access-list*] [**asn** *as-access-list*] [**route-map** *map-name*] **Example:** `Device(config)# ip msdp redistribute route-map customer-sources`	Enables a filter for MSDP SA messages originated by the local device. **Note** The **ip msdp redistribute** command can also be used to advertise sources that are known to the RP but not registered. However, it is strongly recommended that you not originate advertisements for sources that have not registered with the RP.
Step 4	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Controlling the Forwarding of SA Messages to MSDP Peers Using Outgoing Filter Lists

Perform this optional task to control the forwarding of SA messages to MSDP peers by configuring outgoing filter lists.

Note For best practice information related to configuring MSDP SA message filters, see the Multicast Source Discovery Protocol SA Filter Recommendations tech note.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip msdp sa-filter out** {*peer-address* | *peer-name*} [**list** *access-list*] [**route-map** *map-name*] [**rp-list** *access-list* | **rp-route-map** *map-name*]
4. Repeat Step 3 to configure outgoing filter lists for additional MSDP peers.
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip msdp sa-filter out** {*peer-address* | *peer-name*} [**list** *access-list*] [**route-map** *map-name*] [**rp-list** *access-list* | **rp-route-map** *map-name*] **Example:** `Device(config)# ip msdp sa-filter out 192.168.1.5 peerone`	Enables a filter for outgoing MSDP messages.
Step 4	Repeat Step 3 to configure outgoing filter lists for additional MSDP peers.	--
Step 5	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Controlling the Receipt of SA Messages from MSDP Peers Using Incoming Filter Lists

Perform this optional task to control the receipt of incoming SA messages from MSDP peers.

Note For best practice information related to configuring MSDP SA message filters, see the Multicast Source Discovery Protocol SA Filter Recommendations tech note.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip msdp sa-filter in** {*peer-address* | *peer-name*} [**list** *access-list*] [**route-map** *map-name*] [**rp-list** *access-list* | **rp-route-map** *map-name*]
4. Repeat Step 3 to configure incoming filter lists for additional MSDP peers.
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip msdp sa-filter in** {*peer-address* | *peer-name*} [**list** *access-list*] [**route-map** *map-name*] [**rp-list** *access-list* | **rp-route-map** *map-name*] **Example:** `Device(config)# ip msdp sa-filter in 192.168.1.3`	Enables a filter for incoming MSDP SA messages.
Step 4	Repeat Step 3 to configure incoming filter lists for additional MSDP peers.	--
Step 5	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Using TTL Thresholds to Limit the Multicast Data Sent in SA Messages

Perform this optional task to establish a time to live (TTL) threshold to limit the multicast data sent in SA messages.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip msdp ttl-threshold** {*peer-address* | *peer-name*} *ttl-value*
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip msdp ttl-threshold** {*peer-address* | *peer-name*} *ttl-value* **Example:** **Example:** `Device(config)# ip msdp ttl-threshold 192.168.1.5 8`	Sets a TTL value for MSDP messages originated by the local device. • By default, multicast data packets in SA messages are sent to an MSDP peer, provided the TTL value of the packet is greater than 0, which is standard TTL behavior.
Step 4	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Requesting Source Information from MSDP Peers

Perform this optional task to enable a device to request source information from MSDP peers.

Note Because SA caching is enabled by default and cannot be explicitly enabled or disabled in earlier Cisco software releases, performing this task is seldom needed.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip msdp sa-request** {*peer-address* | *peer-name*}
4. Repeat Step 3 to specify that the device send SA request messages to additional MSDP caching peers.
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip msdp sa-request** {*peer-address* | *peer-name*} **Example:** `Device(config)# ip msdp sa-request 192.168.10.1`	Specifies that the device send SA request messages to the specified MSDP peer.
Step 4	Repeat Step 3 to specify that the device send SA request messages to additional MSDP caching peers.	--
Step 5	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Controlling the Response to Outgoing SA Request Messages from MSDP Peers Using SA Request Filters

Perform this optional task to control the outgoing SA request messages that the device will honor from MSDP peers.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip msdp filter-sa-request** {*peer-address* | *peer-name*} [**list** *access-list*]
4. Repeat Step 3 to configure SA request filters for additional MSDP peers.
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip msdp filter-sa-request** {*peer-address* | *peer-name*} [**list** *access-list*] **Example:** `Device(config)# ip msdp filter sa-request 172.31.2.2 list 1`	Enables a filter for outgoing SA request messages. **Note** Only one SA request filter can be configured per MSDP peer.
Step 4	Repeat Step 3 to configure SA request filters for additional MSDP peers.	--
Step 5	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Including a Bordering PIM Dense Mode Region in MSDP

Perform this optional task to configure a border device to send SA messages for sources active in a PIM dense mode (PIM-DM) region.

You can have a device that borders a PIM-SM region and a PIM-DM region. By default, sources in the PIM-DM domain are not included in MSDP. You can configure this border device to send SA messages for sources active in the PIM-DM domain. If you do so, it is very important to also configure the **ip msdp redistribute** command to control what local sources from the PIM-DM domain are advertised. Not configuring this command can result in the (S, G) state remaining long after a source in the PIM-DM domain has stopped sending. For configuration information, see the Controlling SA Messages Originated by an RP for Local Sources, on page 123 section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip msdp border sa-address** *type number*
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip msdp border sa-address** *type number* **Example:** `Device(config)# ip msdp border sa-address gigabitethernet0/0/0`	Configures the device on the border between a PIM-SM and PIM-DM domain to originate SA messages for active sources in the PIM-DM domain. • The IP address of the interface is used as the originator ID, which is the RP field in the SA message.
Step 4	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring an Originating Address Other Than the RP Address

Perform this optional task to allow an MSDP speaker that originates an SA message to use the IP address of its interface as the RP address in the SA message.

You can also change the originator ID for any one of the following reasons:

- If you configure multiple devices in an MSDP mesh group for Anycast RP.
- If you have a device that borders a PIM-SM domain and a PIM-DM domain. If a device borders a PIM-SM domain and a PIM-DM domain and you want to advertise active sources within the PIM-DM domain, configure the RP address in SA messages to be the address of the originating device's interface.

Before You Begin

MSDP is enabled and the MSDP peers are configured. For more information about configuring MSDP peers, see the Configuring an MSDP Peer, on page 112 section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip msdp originator-id** *type number*
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip msdp originator-id** *type number* **Example:** `Device(config)# ip msdp originator-id ethernet 1`	Configures the RP address in SA messages to be the address of the originating device's interface.

	Command or Action	Purpose
Step 4	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Monitoring MSDP

Perform this optional task to monitor MSDP SA messages, peers, state, and peer status.

SUMMARY STEPS

1. **enable**
2. **debug ip msdp** [*peer-address* | *peer-name*] [**detail**] [**routes**]
3. **debug ip msdp resets**
4. **show ip msdp count** [*as-number*]
5. **show ip msdp peer** [*peer-address* | *peer-name*]
6. **show ip msdp sa-cache** [*group-address* | *source-address* | *group-name* | *source-name*] [*as-number*]
7. **show ip msdp summary**

DETAILED STEPS

Step 1 **enable**

Example:

```
Device# enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **debug ip msdp** [*peer-address* | *peer-name*] [**detail**] [**routes**]
Use this command to debug MSDP activity.

Use the optional *peer-address* or *peer-name* argument to specify for which peer debug events are logged.

The following is sample output from the **debug ip msdp** command:

Example:

```
Device# debug ip msdp
MSDP debugging is on
Device#
MSDP: 224.150.44.254: Received 1388-byte message from peer
```

```
MSDP: 224.150.44.254: SA TLV, len: 1388, ec: 115, RP: 172.31.3.92
MSDP: 224.150.44.254: Peer RPF check passed for 172.31.3.92, used EMBGP peer
MSDP: 224.150.44.250: Forward 1388-byte SA to peer
MSDP: 224.150.44.254: Received 1028-byte message from peer
MSDP: 224.150.44.254: SA TLV, len: 1028, ec: 85, RP: 172.31.3.92
MSDP: 224.150.44.254: Peer RPF check passed for 172.31.3.92, used EMBGP peer
MSDP: 224.150.44.250: Forward 1028-byte SA to peer
MSDP: 224.150.44.254: Received 1388-byte message from peer
MSDP: 224.150.44.254: SA TLV, len: 1388, ec: 115, RP: 172.31.3.111
MSDP: 224.150.44.254: Peer RPF check passed for 172.31.3.111, used EMBGP peer
MSDP: 224.150.44.250: Forward 1388-byte SA to peer
MSDP: 224.150.44.250: Received 56-byte message from peer
MSDP: 224.150.44.250: SA TLV, len: 56, ec: 4, RP: 192.168.76.241
MSDP: 224.150.44.250: Peer RPF check passed for 192.168.76.241, used EMBGP peer
MSDP: 224.150.44.254: Forward 56-byte SA to peer
MSDP: 224.150.44.254: Received 116-byte message from peer
MSDP: 224.150.44.254: SA TLV, len: 116, ec: 9, RP: 172.31.3.111
MSDP: 224.150.44.254: Peer RPF check passed for 172.31.3.111, used EMBGP peer
MSDP: 224.150.44.250: Forward 116-byte SA to peer
MSDP: 224.150.44.254: Received 32-byte message from peer
MSDP: 224.150.44.254: SA TLV, len: 32, ec: 2, RP: 172.31.3.78
MSDP: 224.150.44.254: Peer RPF check passed for 172.31.3.78, used EMBGP peer
MSDP: 224.150.44.250: Forward 32-byte SA to peer
```

Step 3 **debug ip msdp resets**

Use this command to debug MSDP peer reset reasons.

Example:

```
Device# debug ip msdp resets
```

Step 4 **show ip msdp count** [*as-number*]

Use this command to display the number of sources and groups originated in MSDP SA messages and the number of SA messages from an MSDP peer in the SA cache. The **ip msdp cache-sa-state** command must be configured for this command to produce any output.

The following is sample output from the **show ip msdp count**command:

Example:

```
Device# show ip msdp count
SA State per Peer Counters, <Peer>: <# SA learned>
    192.168.4.4: 8
SA State per ASN Counters, <asn>: <# sources>/<# groups>
    Total entries: 8
    ?: 8/8
```

Step 5 **show ip msdp peer** [*peer-address* | *peer-name*]

Use this command to display detailed information about MSDP peers.

Use the optional *peer-address* or *peer-name* argument to display information about a particular peer.

The following is sample output from the **show ip msdp peer**command:

Example:

```
Device# show ip msdp peer 192.168.4.4
MSDP Peer 192.168.4.4 (?), AS 64512 (configured AS)
  Connection status:
    State: Up, Resets: 0, Connection source: Loopback0 (2.2.2.2)
    Uptime(Downtime): 00:07:55, Messages sent/received: 8/18
    Output messages discarded: 0
    Connection and counters cleared 00:08:55 ago
```

```
  SA Filtering:
    Input (S,G) filter: none, route-map: none
    Input RP filter: none, route-map: none
    Output (S,G) filter: none, route-map: none
    Output RP filter: none, route-map: none
  SA-Requests:
    Input filter: none
  Peer ttl threshold: 0
  SAs learned from this peer: 8
  Input queue size: 0, Output queue size: 0
  MD5 signature protection on MSDP TCP connection: not enabled
```

Step 6 **show ip msdp sa-cache** [*group-address* | *source-address* | *group-name* | *source-name*] [*as-number*]
Use this command to display the (S, G) state learned from MSDP peers.

The following is sample output from the **show ip msdp sa-cache**command:

Example:

```
Device# show ip msdp sa-cache
MSDP Source-Active Cache - 8 entries
(10.44.44.5, 239.232.1.0), RP 192.168.4.4, BGP/AS 64512, 00:01:20/00:05:32, Peer 192.168.4.4
(10.44.44.5, 239.232.1.1), RP 192.168.4.4, BGP/AS 64512, 00:01:20/00:05:32, Peer 192.168.4.4
(10.44.44.5, 239.232.1.2), RP 192.168.4.4, BGP/AS 64512, 00:01:19/00:05:32, Peer 192.168.4.4
(10.44.44.5, 239.232.1.3), RP 192.168.4.4, BGP/AS 64512, 00:01:19/00:05:32, Peer 192.168.4.4
(10.44.44.5, 239.232.1.4), RP 192.168.4.4, BGP/AS 64512, 00:01:19/00:05:32, Peer 192.168.4.4
(10.44.44.5, 239.232.1.5), RP 192.168.4.4, BGP/AS 64512, 00:01:19/00:05:32, Peer 192.168.4.4
(10.44.44.5, 239.232.1.6), RP 192.168.4.4, BGP/AS 64512, 00:01:19/00:05:32, Peer 192.168.4.4
(10.44.44.5, 239.232.1.7), RP 192.168.4.4, BGP/AS 64512, 00:01:19/00:05:32, Peer 192.168.4.4
```

Step 7 **show ip msdp summary**
Use this command to display MSDP peer status.

The following is sample output from the **show ip msdp summary** command:

Example:

```
Device# show ip msdp summary
MSDP Peer Status Summary
Peer Address     AS    State    Uptime/  Reset SA    Peer Name
                                Downtime Count Count
192.168.4.4      4     Up       00:08:05 0     8     ?
```

Clearing MSDP Connections Statistics and SA Cache Entries

Perform this optional task to clear MSDP connections, statistics, and SA cache entries.

SUMMARY STEPS

1. **enable**
2. **clear ip msdp peer** [*peer-address* | *peer-name*]
3. **clear ip msdp statistics** [*peer-address* | peer-name]
4. **clear ip msdp sa-cache** [*group-address*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**clear ip msdp peer** [*peer-address* | *peer-name*] **Example:** `Device#` **clear ip msdp peer**	Clears the TCP connection to the specified MSDP peer and resets all MSDP message counters.
Step 3	**clear ip msdp statistics** [*peer-address* | peer-name] **Example:** `Device# clear ip msdp statistics`	Clears the statistics counters for the specified MSDP peer and resets all MSDP message counters.
Step 4	**clear ip msdp sa-cache** [*group-address*] **Example:** `Device# clear ip msdp sa-cache`	Clears SA cache entries. • If the **clear ip msdp sa-cache** is specified with the optional *group-address* argument or *source-address*argument, all SA cache entries are cleared. • Use the optional *group-address* argument to clear all SA cache entries associated with a specific group.

Enabling SNMP Monitoring of MSDP

Perform this optional task to enable Simple Network Management Protocol (SNMP) monitoring of MSDP.

Before You Begin

- SNMP and MSDP is configured on your devices.
- In each PIM-SM domain there should be a device that is configured as the MSDP speaker. This device must have SNMP and the MSDP MIB enabled.

Note

- All MSDP-MIB objects are implemented as read-only.
- The Requests table is not supported in Cisco's implementation of the MSDP MIB.
- The msdpEstablished notification is not supported in Cisco's implementation of the MSDP MIB.

SUMMARY STEPS

1. **enable**
2. **snmp-server enable traps msdp**
3. **snmp-server host** *host* [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth**| **priv** | **noauth**]}] *community-string* [**udp-port** *port-number*] **msdp**
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**snmp-server enable traps msdp** **Example:** `Device# snmp-server enable traps msdp`	Enables the sending of MSDP notifications for use with SNMP. **Note** The **snmp-server enable traps msdp** command enables both traps and informs.
Step 3	**snmp-server host** *host* [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth**| **priv** | **noauth**]}] *community-string* [**udp-port** *port-number*] **msdp** **Example:** `Device# snmp-server host examplehost msdp`	Specifies the recipient (host) for MSDP traps or informs.
Step 4	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Troubleshooting Tips

You can compare the results of MSDP MIB notifications to the output from the software by using the **show ip msdp summary** and **show ip msdp peer** commands on the appropriate device. You can also compare the results of these commands to the results from SNMP Get operations. You can verify SA cache table entries using the **show ip msdp sa-cache** command. Additional troubleshooting information, such as the local address of the connection, the local port, and the remote port, can be obtained using the output from the **debug ip msdp** command.

Configuration Examples for Using MSDP to Interconnect Multiple PIM-SM Domains

Example: Configuring an MSDP Peer

The following example shows how to establish MSDP peering connections between three MSDP peers:

Device A

```
!
interface Loopback 0
 ip address 10.220.8.1 255.255.255.255
!
ip msdp peer 10.220.16.1 connect-source Loopback0
ip msdp peer 10.220.32.1 connect-source Loopback0
!
```

Device B

```
!
interface Loopback 0
 ip address 10.220.16.1 255.255.255.255
!
ip msdp peer 10.220.8.1 connect connect-source Loopback0
ip msdp peer 10.220.32.1 connect connect-source Loopback0
!
```

Device C

```
!
interface Loopback 0
 ip address 10.220.32.1 255.255.255.255
!
ip msdp peer 10.220.8.1 connect 10.220.8.1 connect-source Loopback0
ip msdp peer 10.220.16.1 connect 10.220.16.1 connect-source Loopback0
!
```

Example: Configuring MSDP MD5 Password Authentication

The following example shows how to enable MD5 password authentication for TCP connections between two MSDP peers:

Device A

```
!
ip msdp peer 10.3.32.154
ip msdp password peer 10.3.32.154 0 test
!
```

Device B

```
!
ip msdp peer 10.3.32.153
ip msdp password peer 10.3.32.153 0 test
!
```

Configuring MSDP Compliance with IETF RFC 3618 Example

The following example shows how to configure the MSDP peers at 10.10.2.4 and 10.20.1.2 to be compliant with peer-RPF forwarding rules specified in IETF RFC 3618:

```
ip msdp peer 10.10.2.4
ip msdp peer 10.20.1.2
ip msdp rpf rfc3618
```

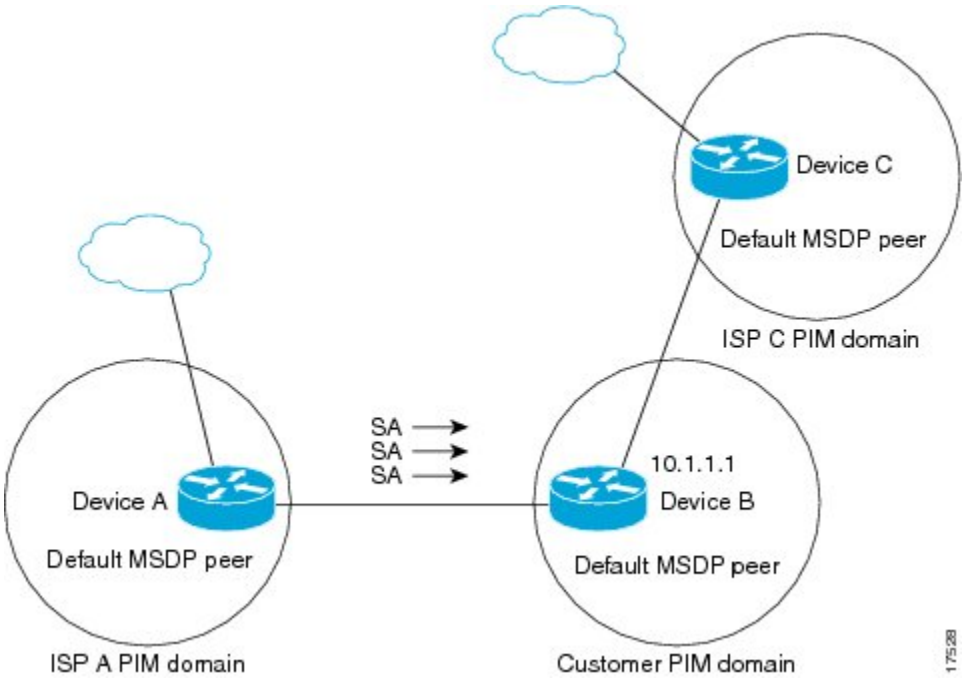
Configuring a Default MSDP Peer Example

The figure illustrates a scenario where default MSDP peers might be used. In the figure, a customer that owns Router B is connected to the internet through two ISPs, one that owns Router A and the other that owns Router C. They are not running (M)BGP between them. In order for the customer to learn about sources in the ISP domain or in other domains, Router B identifies Router A as its default MSDP peer. Router B advertises SA messages to both Router A and Router C, but accepts SA messages either from Router A only or Router C only. If Router A is the first default peer in the configuration, it will be used if it is up and running. Only if Router A is not running will Router B accept SA messages from Router C.

The ISP will also likely use a prefix list to define which prefixes it will accept from the customer router. The customer will define multiple default peers, each having one or more prefixes associated with it.

The customer has two ISPs to use. The customer defines both ISPs as default peers. As long as the first default peer identified in the configuration is up and running, it will be the default peer and the customer will accept all SA messages it receives from that peer.

Figure 15: Default MSDP Peer Scenario



Router B advertises SAs to Router A and Router C, but uses only Router A or Router C to accept SA messages. If Router A is first in the configuration file, it will be used if it is up and running. Only when Router A is not running will Router B accept SAs from Router C. This is the behavior without a prefix list.

If you specify a prefix list, the peer will be a default peer only for the prefixes in the list. You can have multiple active default peers when you have a prefix list associated with each. When you do not have any prefix lists, you can configure multiple default peers, but only the first one is the active default peer as long as the router has connectivity to this peer and the peer is alive. If the first configured peer goes down or the connectivity to this peer goes down, the second configured peer becomes the active default, and so on.

The following example shows a partial configuration of Router A and Router C in the figure. Each of these ISPs may have more than one customer using default peering, like the customer in the figure. In that case, they may have similar configurations. That is, they will only accept SAs from a default peer if the SA is permitted by the corresponding prefix list.

Router A Configuration

```
ip msdp default-peer 10.1.1.1
ip msdp default-peer 10.1.1.1 prefix-list site-b ge 32
ip prefix-list site-b permit 10.0.0.0/8
```

Router C Configuration

```
ip msdp default-peer 10.1.1.1 prefix-list site-b ge 32
ip prefix-list site-b permit 10.0.0.0/8
```

Example: Configuring MSDP Mesh Groups

The following example shows how to configure three devices to be fully meshed members of an MSDP mesh group:

Device A Configuration

```
ip msdp peer 10.2.2.2
ip msdp peer 10.3.3.3
ip msdp mesh-group test-mesh-group 10.2.2.2
ip msdp mesh-group test-mesh-group 10.3.3.3
```

Device B Configuration

```
ip msdp peer 10.1.1.1
ip msdp peer 10.3.3.3
ip msdp mesh-group test-mesh-group 10.1.1.1
ip msdp mesh-group test-mesh-group 10.3.3.3
```

Device C Configuration

```
ip msdp peer 10.1.1.1
ip msdp peer 10.2.2.2
ip msdp mesh-group test-mesh-group 10.1.1.1
ip msdp mesh-group test-mesh-group 10.2.2.2
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IP multicast commands	Cisco IOS IP Multicast Command Reference

Standards and RFC

Standard/RFC	Title
RFC 2385	Protection of BGP Sessions via the TCP MD5 Signature Option
RFC 2858	Multiprotocol Extensions for BGP-4
RFC 3618	Multicast Source Discovery Protocol

MIBs

MIB	MIBs Link
MSDP-MIB.my	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Using MSDP to Interconnect Multiple PIM-SM Domains

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 5: Feature Information for Using MSDP to Interconnect Multiple PIM-SM Domains

Feature Name	Releases	Feature Information
Multicast Source Discovery Protocol (MSDP)	Cisco IOS XE Release 2.1 Cisco IOS Xe Release 3.5S Cisco IOS XE 3.14 S	Multicast Source Discovery Protocol (MSDP) is a mechanism to connect multiple PIM sparse-mode (SM) domains. MSDP allows multicast sources for a group to be known to all rendezvous points (RPs) in different domains. Each PIM-SM domain uses its own RPs and need not depend on RPs in other domains. An RP runs MSDP over TCP to discover multicast sources in other domains. In Cisco IOS XE Release 3.5S, support was added for the Cisco ASR 903 Router. In Cisco IOS XE 3.14S, support was added for the Cisco ASR 920 Series Aggregation Services Router (ASR-920-12CZ-A, ASR-920-12CZ-D, ASR-920-4SZ-A, ASR-920-4SZ-D, ASR-920-10SZ-PD, ASR-920-24SZ-IM, ASR-920-24SZ-M, and ASR-920-24TZ-M).

Feature Name	Releases	Feature Information
MSDP Compliance with IETF RFC 3618	Cisco IOS XE Release 2.1	The MSDP Compliance with IETF RFC 3618 feature enables you to configure MSDP to comply with the peer-RPF forwarding rules defined in the IETF RFC 3618 specifications. Enabling the MSDP Compliance with IETF RFC 3618 feature prevents SA message loops. Additionally, enabling the MSDP Compliance with IETF RFC 3618 feature eliminates the requirement that BGP RRs run MSDP, enables the use of an IGP for the RPF check, and allows MSDP peerings between routers in nondirectly connected autonomous systems. The following commands were introduced or modified by this feature: **ip msdp rpf rfc3618**, **show ip msdp rpf-peer**.
MSDP MD5 Password Authentication	Cisco IOS XE Release 2.5 Cisco IOS XE Release 3.8S Cisco IOS XE Release 3.9S	The MSDP MD5 password authentication feature is an enhancement to support MD5 signature protection on a TCP connection between two MSDP peers. This feature provides added security by protecting MSDP against the threat of spoofed TCP segments being introduced into the TCP connection stream. In Cisco IOS XE Release 3.8S, support was added for the Cisco ISR 4400 Series router. In Cisco IOS XE Release 3.9S, support was aded for the Cisco CSR 1000V. The following commands were introduced or modified by this feature: **ip msdp password peer**, **show ip msdp peer**.

CHAPTER 6

PIM Allow RP

This module describes how to configure the PIM Allow RP feature in IPv4 or IPv6 networks for inter-connecting Protocol Independent Multicast (PIM) Sparse Mode (SM) domains with different rendezvous points (RPs). PIM Allow RP enables the receiving device to use its own RP to create state and build shared trees when an incoming (*, G) Join is processed and a different RP is identified. This allows the receiving device to accept the (*, G) Join from the different RP.

- Finding Feature Information, page 145
- Restrictions for PIM Allow RP, page 145
- Information About PIM Allow RP, page 146
- How to Configure PIM Allow RP, page 147
- Configuration Examples for PIM Allow RP, page 152
- Additional References for PIM Allow RP, page 154
- Feature Information for PIM Allow RP, page 155

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for PIM Allow RP

- PIM Allow RP only supports connecting PIM SM domains.
- PIM Allow RP is applicable for downstream traffic only, that is, it is only applicable for building the shared tree.

- PIM Allow RP does not work with Auto-RP or Boot Strap Router (BSR). Only static configuration is supported. However, it does allow the embedded RP in the consumer network to be different than the one configured statically in the service provider network.

Information About PIM Allow RP

Rendezvous Points

A rendezvous point (RP) is a role that a device performs when operating in Protocol Independent Multicast (PIM) Sparse Mode (SM). An RP is required only in networks running PIM SM. In the PIM-SM model, only network segments with active receivers that have explicitly requested multicast data will be forwarded the traffic. This method of delivering multicast data is in contrast to PIM Dense Mode (PIM DM). In PIM DM, multicast traffic is initially flooded to all segments of the network. Routers that have no downstream neighbors or directly connected receivers prune back the unwanted traffic.

An RP acts as the meeting place for sources and receivers of multicast data. In a PIM-SM network, sources must send their traffic to the RP. This traffic is then forwarded to receivers down a shared distribution tree. By default, when the first hop device of the receiver learns about the source, it will send a Join message directly to the source, creating a source-based distribution tree from the source to the receiver. This source tree does not include the RP unless the RP is located within the shortest path between the source and receiver.

In most cases, the placement of the RP in the network is not a complex decision. By default, the RP is needed only to start new sessions with sources and receivers. Consequently, the RP experiences little overhead from traffic flow or processing. In PIM version 2, the RP performs less processing than in PIM version 1 because sources must only periodically register with the RP to create state.

PIM Allow RP

There are three types of networks: publisher, consumer, and transport. Many publisher networks can originate content and many consumer networks can be interested in the content. The transport network, owned and operated by a service provider, connects the publisher and the consumer networks.

The consumer and the transport networks are connected as follows:

For a specific group range, or all-groups range (similar to a default route), the service provider defines a particular rendezvous point (RP), such as RP-A. Reverse path forwarding of RP-A from a consumer device will cause a (*,G) Join to be sent towards the transport network.

For the same group, the service provider may define a different RP, such as RP-B, that is used to build the shared tree within the transport network for G. RP-A and RP-B are typically different RPs and each RP is defined for different group ranges.

RFC 4601 dictates that if a device receives a (*, G) Join and the RP that is specified in the (*, G) Join is different than what the receiving device expects (unknown RPs), the incoming (*, G) Join must be ignored. The PIM Allow RP feature enables the receiving device to use its own RP to create state and build shared trees when an incoming (*, G) Join is processed and a different RP is identified. This allows the receiving device to accept the (*, G) Join from the different RP.

PIM Allow RP is only applicable for downstream traffic, for building the shared tree. It does not work with Auto-RP or BSR. Only static configuration is supported. However, PIM Allow RP does compensate for the

embedded RP in the consumer network to be different than the one configured statically in the transport network.

How to Configure PIM Allow RP

Configuring RPs for PIM-SM

Before You Begin

All access lists should be configured prior to beginning the configuration task. For information about how to configure an access list, see the "Creating an IP Access List and Applying It to an Interface" module of the *Security Configuration Guide: Access Control Lists* guide.

For IPv6 network devices, you must first enable IPv6 unicast routing on all interfaces of the device on which you want to enable IPv6 multicast routing.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. • **ip multicast-routing** [**vrf** *vrf-name*] **distributed**
   • **ipv6 multicast-routing** [**vrf** *vrf-name*]
4. **interface** *type number*
5. • **ip pim sparse-mode**
   • **ipv6 pim enable**
6. **ipv6 address** {*ipv6-address* | *prefix-length* | *prefix-name* *sub-bits* | *prefix-length*}
7. **no shut**
8. **exit**
9. Repeat Steps 4 through 8 on every interface that uses IP multicast.
10. • **ip pim** [**vrf** *vrf-name*] **rp-address** *rp-address* [*access-list*] [**override**]
    • **ipv6 pim** [**vrf** *vrf-name*] **rp-address** *ipv6-address* [*group-address-list*]
11. **exit**
12. **show ip pim rp** [**mapping**] [*rp-address*]
13. **show ip mroute**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Device> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

Step 3	• **ip multicast-routing** [**vrf** *vrf-name*] **distributed**
	• **ipv6 multicast-routing** [**vrf** *vrf-name*]
	
	Example:
	`Device(config)# ip multicast-routing`
	`Device(config)# ipv6 multicast-routing`
		• For IPv4: Enables multicast routing on all interfaces of the device. In Cisco IOS XE Release 3.2S and earlier releases, the **distributed** keyword is optional.
		• For IPv6: Enables multicast routing on all interfaces of the device and also enables multicast forwarding for PIM and MLD on all multicast-enabled interfaces of the device.
		Note IPv6 multicast routing is disabled by default when IPv6 unicast routing is enabled. On certain devices, the IPv6 multicast routing must also be enabled in order to use IPv6 unicast routing.

Step 4	**interface** *type number* **Example:** `Device(config)# interface gigabitethernet 1/0/0`	Selects an interface that is connected to hosts on which PIM can be enabled.

Step 5	• **ip pim sparse-mode**
	• **ipv6 pim enable**
	
	Example:
	`Device(config-if)# ip pim sparse-mode`
	`Device(config-if)# ipv6 pim enable`
		• For IPv4: Enables PIM. You must use sparse mode.
		• For IPv6: Enables IPv6 and by default, IPv6 PIM.

Step 6	**ipv6 address** {*ipv6-address* | *prefix-length* | *prefix-name sub-bits* | *prefix-length*} **Example:** `Device(config-if)# ipv6 address 2001:DB8::4:4/64`	For IPv6 only: Configures an IPv6 address based on an IPv6 general prefix and enables IPv6 processing on an interface.
Step 7	**no shut** **Example:** `Device(config-if)# no shut`	Enables an interface.

	Command or Action	Purpose
Step 8	**exit** **Example:** `Device(config-if)# exit`	— Returns to global configuration mode.
Step 9	Repeat Steps 4 through 8 on every interface that uses IP multicast.	

Step 10	• **ip pim** [**vrf** *vrf-name*] **rp-address** *rp-address* [*access-list*] [**override**]
	• **ipv6 pim** [**vrf** *vrf-name*] **rp-address** *ipv6-address* [*group-address-list*]
	
	Example:
	`Device(config)# ip pim rp-address 192.0.2.1 acl-sparse`
	
	`Device(config)# ipv6 pim rp-address 2001:DB8::1:1 acl_sparse1`
		• For IPv4: Configures the address of a PIM RP. If no access list is specified, the RP address is applied to all multicast groups, 224/4.
		• For IPv6: Configures the address of a PIM RP. If no group-address list is specified, the RP address is applied to the entire routable IPv6 multicast group range, excluding SSM, which ranges from FFX[3-f]::/8 to FF3X::/96.

Step 11	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode.
Step 12	**show ip pim rp** [**mapping**] [*rp-address*] **Example:** `Device# show ip pim rp mapping`	(Optional) Displays RPs known in the network and shows how the router learned about each RP.
Step 13	**show ip mroute** **Example:** `Device# show ip mroute`	(Optional) Displays the contents of the IP mroute table.

Enabling PIM Allow RP

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. • **ip pim allow-rp** [**group-list** *access-list* | **rp-list** *access-list* [**group-list** *access-list*]]
   • **ipv6 pim allow-rp** [**group-list** *access-list* | **rp-list** *access-list* [**group-list** *access-list*]]
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

Step 3	• **ip pim allow-rp** [**group-list** *access-list* | **rp-list** *access-list* [**group-list** *access-list*]]
	• **ipv6 pim allow-rp** [**group-list** *access-list* | **rp-list** *access-list* [**group-list** *access-list*]]
	
	Example:
	`Device(config)# ip pim allow-rp`
	`Device(config)# ipv6 pim allow-rp`
		Enables PIM Allow RP.

Step 4	**exit** **Example:** `Device(config)# exit`	Returns to privileged EXEC mode.

Displaying Information About PIM-SM and RPs

SUMMARY STEPS

1. **enable**
2. • **show ip pim** [**vrf** *vrf-name*] **rp** [**metric**] [*rp-address*]
   • **show ipv6 pim** [**vrf** *vrf-name*] **interface** [**state-on**] [**state-off**] [*type number*]
3. • **show ip pim** [**vrf** *vrf-name*] **rp mapping** [*rp-address*]
   • **show ipv6 pim** [**vrf** *vrf-name*] **group-map** [*group-name* | *group-address*] | [*group-range* | *group-mask*] [**info-source** {**bsr** | **default** | **embedded-rp** | **static**}]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

Step 2	• **show ip pim** [**vrf** *vrf-name*] **rp** [**metric**] [*rp-address*]
	• **show ipv6 pim** [**vrf** *vrf-name*] **interface** [**state-on**] [**state-off**] [*type number*]
	
	Example:
	`Device# show ip pim interface`
	`Device# show ipv6 pim interface`
		Displays information about interfaces configured for PIM.

Step 3	• **show ip pim** [**vrf** *vrf-name*] **rp mapping** [*rp-address*]
	• **show ipv6 pim** [**vrf** *vrf-name*] **group-map** [*group-name* | *group-address*] | [*group-range* | *group-mask*] [**info-source** {**bsr** | **default** | **embedded-rp** | **static**}]
	
	Example:
	`Device# show ipv6 pim rp mapping`
	`Device# show ipv6 pim group-map static`
		Displays the mappings for the PIM group to the active rendezvous points.

Configuration Examples for PIM Allow RP

Example: IPv4 PIM Allow RP

In the following example:

1. The downstream device loopback (Loopback100) creates a static (*,239.1.2.3) Join to a nonexistent RP (11.30.3.3).
2. The static route makes the device think that this RP can be reached through the upstream device via 11.10.2.1, causing the downstream device to send a (*,239.1.2.3) PIM Join with an RP address (11.30.3.3) to the upstream router.
3. When the upstream device receives the (*,239.1.2.3) PIM Join, it realizes that the RP address in the Join (11.30.3.3) is different from the known (configured) interface-to-RP address (11.10.3.3).
4. The PIM allow RP configuration on the upstream device permits the (*,239.1.2.3) to be processed and creates a (*,239.1.2.3) join to the RP (11.10.3.3).

Note If the **pim allow-rp** command is not configured on the upstream device, the upstream device must ignore Joins with different RPs.

```
###################
#   Downstream
###################
!
hostname downstream-router
!
!
ip multicast-routing distributed
!
!
interface Loopback100
ip address 101.10.1.2 255.255.255.0
ip igmp static-group 239.1.2.3
ip pim sparse-dense-mode
no shut
!
interface Ethernet1/2
ip address 11.10.2.2 255.255.255.0
ip pim sparse-dense-mode
no shut
!
router ospf 200
network 11.0.0.0 0.255.255.255 area 1
network 101.0.0.0 0.255.255.255 area 1
!
ip pim rp-address 11.30.3.3
ip mroute 11.30.3.3 255.255.255.255 11.10.2.1
!
end


###################
#   Upstream
###################
!
hostname Upstream-router
!
!
```

```
ip multicast-routing distributed
!
!
interface FastEthernet0/0/2
ip address 11.10.2.1 255.255.255.0
ip pim sparse-dense-mode
no shut
!
interface FastEthernet0/0/4
! interface to RP (11.10.3.3)
ip address 10.10.4.1 255.255.255.0
ip pim sparse-dense-mode
no shut
!
router ospf 200
network 10.0.0.0 0.255.255.255 area 1
network 11.0.0.0 0.255.255.255 area 1
!
ip pim rp-address 11.10.3.3
ip pim allow-rp
!
end
```

Example: IPv6 PIM Allow RP

In the following example:

1. The downstream device loopback creates an static (*,FF03::1) Join to a non-existent RP (80::1:1:3).
2. The static route makes the device think that this RP can be reach via the upstream device via 10::1:1:1 and causes the downstream device to send a (*,FF03::1) PIM Join with an RP address (80::1:1:3) to the upstream device.
3. When the upstream device receives the (*,FF03::1) PIM Join, it realizes that the RP address in the Join (80::1:1:3) is different from the (known) configured address (20::1:1:3).
4. The PIM allow RP configuration on the upstream device permits the (*,FF03::1) to be processed, and creates a (*,FF03::1) Join to the RP (20::1:1:3).

Note If the **pim allow-rp** command is not configured on the upstream device, the upstream device must ignore Joins with different RPs .

```
##################
# Downstream
##################

!
hostname downstream-router
!
!
ipv6 unicast-routing
ipv6 multicast-routing
!
!
interface Loopback100
ipv6 address FE80::50:1:2 link-local
ipv6 address 50::1:1:2/64
ipv6 enable
ipv6 ospf 1 area 0
ipv6 mld join-group FF03::1
!
```

```
interface Ethernet1/2
ipv6 address FE80::10:1:2 link-local
ipv6 address 10::1:1:2/64
ipv6 enable
ipv6 ospf 1 area 0
no keepalive
!
!
ipv6 pim rp-address 80::1:1:3
ipv6 route 80::1:1:3/128 10::1:1:1 multicast
!
ipv6 router ospf 1
router-id 205.2.0.2
!
!
end


####################
#  Upstream
####################
!
hostname Upstream-router
!
!
ipv6 unicast-routing
ipv6 multicast-routing
!
!
interface FastEthernet0/0/2
ipv6 address FE80::10:1:1 link-local
ipv6 address 10::1:1:1/64
ipv6 enable
ipv6 ospf 1 area 0
!
interface FastEthernet0/0/3
! interface to the RP (20::1:1:3)
ipv6 address FE80::20:1:1 link-local
ipv6 address 20::1:1:1/64
ipv6 enable
ipv6 ospf 1 area 0
!
!
ipv6 pim rp-address 20::1:1:3
ipv6 pim allow-rp
!
ipv6 router ospf 1
router-id 205.1.0.1
!
!
end
```

Additional References for PIM Allow RP

Standards and RFCs

Standard/RFC	Title
RFC 4601	*Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for PIM Allow RP

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 6: Feature Information for PIM Allow RP

Feature Name	Releases	Feature Information
PIM Allow RP	15.2(4)T Cisco IOS XE Release 3.7S 15.3(1)T	The PIM Allow RP feature enables the receiving device to use its own RP to create state and build shared trees when an incoming (*, G) Join is processed and a different RP is identified. This process permits the receiving device to accept the (*, G) Join from a different RP. The following commands were introduced or modified: **ip pim allow-rp**, **ipv6 pim allow-rp**.

CHAPTER 7

Configuring Source Specific Multicast

This module describes how to configure Source Specific Multicast (SSM). The Source Specific Multicast feature is an extension of IP multicast where datagram traffic is forwarded to receivers from only those multicast sources to which the receivers have explicitly joined. For multicast groups configured for SSM, only source-specific multicast distribution trees (no shared trees) are created.

- Finding Feature Information, page 157
- Restrictions for Source Specific Multicast, page 157
- Information About Source Specific Multicast, page 159
- How to Configure Source Specific Multicast, page 165
- Configuration Examples of Source Specific Multicast, page 166
- Additional References, page 167
- Feature Information for Source Specific Multicast, page 169

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Source Specific Multicast

Legacy Applications Within the SSM Range Restrictions

Existing applications in a network predating SSM will not work within the SSM range unless they are modified to support (S, G) channel subscriptions or are enabled through URL Rendezvous Directory (URD). Therefore,

enabling SSM in a network may cause problems for existing applications if they use addresses within the designated SSM range.

IGMP v3lite and URD Require a Cisco Last Hop Router

SSM and IGMPv3 are solutions that are being standardized in the IETF. However, IGMP v3lite and URD are Cisco-developed solutions. For IGMP v3lite and URD to operate properly for a host, the last hop router toward that host must be a Cisco router with IGMP v3lite or URD enabled.

Note This limitation does not apply to an application using the Host Side IGMP Library (HSIL) if the host has kernel support for IGMPv3, because then the HSIL will use the kernel IGMPv3 instead of IGMP v3lite.

Address Management Restrictions

Address management is still necessary to some degree when SSM is used with Layer 2 switching mechanisms. Cisco Group Management Protocol (CGMP), IGMP snooping, or Router-Port Group Management Protocol (RGMP) currently support only group-specific filtering, not (S, G) channel-specific filtering. If different receivers in a switched network request different (S, G) channels sharing the same group, then they will not benefit from these existing mechanisms. Instead, both receivers will receive all (S, G) channel traffic (and filter out the unwanted traffic on input). Because of the ability of SSM to reuse the group addresses in the SSM range for many independent applications, this situation can lead to less than expected traffic filtering in a switched network. For this reason it is important to follow the recommendations set forth in the IETF drafts for SSM to use random IP addresses out of the SSM range for an application to minimize the chance for reuse of a single address within the SSM range between different applications. For example, an application service providing a set of television channels should, even with SSM, use a different group for each television (S, G) channel. This setup will guarantee that multiple receivers to different channels within the same application service will never experience traffic aliasing in networks that include Layer 2 switches.

IGMP Snooping and CGMP Limitations

IGMPv3 uses new membership report messages that may not be recognized correctly by older IGMP Snooping switches, in which case hosts will not properly receive traffic. This situation is not an issue if URD or IGMP v3lite is used with hosts where the operating system is not upgraded for IGMPv3, because IGMP v3lite and URD rely only on IGMPv1 or IGMPv2 membership reports.

URD Intercept URL Limitations

A URD intercept URL string must be fewer than 256 bytes in length, starting from the */path* argument. In the HTTP/TCP connection, this string must also be contained within a single TCP/IP packet. For example, for a 256-byte string, a link maximum transmission unit (MTU) of 128 bytes between the host and intercepting router would cause incorrect operation of URD.

State Maintenance Limitations

In PIM-SSM, the last hop router will continue to periodically send (S, G) join messages if appropriate (S, G) subscriptions are on the interfaces. Therefore, as long as receivers send (S, G) subscriptions, the shortest path tree (SPT) state from the receivers to the source will be maintained, even if the source is not sending traffic for longer periods of time (or even never).

This case is opposite to PIM-SM, where (S, G) state is maintained only if the source is sending traffic and receivers are joining the group. If a source stops sending traffic for more than 3 minutes in PIM-SM, the (S,

G) state will be deleted and only reestablished after packets from the source arrive again through the RPT. Because no mechanism in PIM-SSM notifies a receiver that a source is active, the network must maintain the (S, G) state in PIM-SSM as long as receivers are requesting receipt of that channel.

HSIL Limitations

As explained in the IGMP v3lite Host Signalling, on page 162 concept, the HSIL tries to determine if the host operating system supports IGMPv3. This check is made so that a single application can be used both on hosts where the operating system has been upgraded to IGMPv3 and on hosts where the operating system only supports IGMPv1 or IGMPv2.

Checking for the availability of IGMPv3 in the host operating system can only be made by the HSIL if IGMPv3 kernel support exists for at least one version of this operating system at the time when the HSIL was provided. If such an IGMPv3 kernel implementation has become available only recently, then users may need to also upgrade the HSIL on their hosts so that applications compiled with the HSIL will then dynamically bind to the newest version of the HSIL, which should support the check for IGMPv3 in the operating system kernel. Upgrading the HSIL can be done independently of upgrading the application itself.

Information About Source Specific Multicast

SSM Overview

Source Specific Multicast (SSM). SSM is an extension of IP multicast where datagram traffic is forwarded to receivers from only those multicast sources that the receivers have explicitly joined. For multicast groups configured for SSM, only source-specific multicast distribution trees (not shared trees) are created.

SSM Components Overview

SSM is a datagram delivery model that best supports one-to-many applications, also known as broadcast applications. It is an extension of IP multicast in which datagram traffic is forwarded to receivers from only those multicast sources that the receivers have explicitly joined. For multicast groups configured for SSM, only SSM distribution trees (no shared trees) are created.

SSM is a core networking technology for Cisco's implementation of IP multicast solutions targeted for audio and video broadcast application environments and is described in RFC 3569. The following components together support the implementation of SSM:

- Protocol Independent Multicast source-specific mode (PIM-SSM)
- Internet Group Management Protocol Version 3 (IGMPv3)

Protocol Independent Multicast (PIM) SSM, or PIM-SSM, is the routing protocol that supports the implementation of SSM and is derived from PIM sparse mode (PIM-SM). IGMP is the Internet Engineering Task Force (IETF) standards track protocol used for hosts to signal multicast group membership to routers. IGMP Version 3 supports source filtering, which is required for SSM. IGMP For SSM to run with IGMPv3, SSM must be supported in the router, the host where the application is running, and the application itself.

How SSM Differs from Internet Standard Multicast

The standard IP multicast infrastructure in the Internet and many enterprise intranets is based on the PIM-SM protocol and Multicast Source Discovery Protocol (MSDP). These protocols have proved to be reliable, extensive, and efficient. However, they are bound to the complexity and functionality limitations of the Internet Standard Multicast (ISM) service model. For example, with ISM, the network must maintain knowledge about which hosts in the network are actively sending multicast traffic. With SSM, this information is provided by receivers through the source addresses relayed to the last-hop devices by IGMPv3. SSM is an incremental response to the issues associated with ISM and is intended to coexist in the network with the protocols developed for ISM. In general, SSM provides IP multicast service for applications that utilize SSM.

ISM service is described in RFC 1112. This service consists of the delivery of IP datagrams from any source to a group of receivers called the multicast host group. The datagram traffic for the multicast host group consists of datagrams with an arbitrary IP unicast source address S and the multicast group address G as the IP destination address. Systems will receive this traffic by becoming members of the host group. Membership in a host group simply requires signaling the host group through IGMP Version 1, 2, or 3.

In SSM, delivery of datagrams is based on (S, G) channels. Traffic for one (S, G) channel consists of datagrams with an IP unicast source address S and the multicast group address G as the IP destination address. Systems will receive this traffic by becoming members of the (S, G) channel. In both SSM and ISM, no signaling is required to become a source. However, in SSM, receivers must subscribe or unsubscribe to (S, G) channels to receive or not receive traffic from specific sources. In other words, receivers can receive traffic only from (S, G) channels to which they are subscribed, whereas in ISM, receivers need not know the IP addresses of sources from which they receive their traffic. The proposed standard approach for channel subscription signaling utilizes IGMP INCLUDE mode membership reports, which are supported only in IGMP Version 3.

SSM can coexist with the ISM service by applying the SSM delivery model to a configured subset of the IP multicast group address range. The Internet Assigned Numbers Authority (IANA) has reserved the address range from 232.0.0.0 through 232.255.255.255 for SSM applications and protocols. The software allows SSM configuration for an arbitrary subset of the IP multicast address range from 224.0.0.0 through 239.255.255.255. When an SSM range is defined, an existing IP multicast receiver application will not receive any traffic when it tries to use addresses in the SSM range unless the application is modified to use explicit (S, G) channel subscription or is SSM-enabled through a URL Rendezvous Directory (URD).

SSM Operations

An established network in which IP multicast service is based on PIM-SM can support SSM services. SSM can also be deployed alone in a network without the full range of protocols that are required for interdomain PIM-SM. That is, SSM does not require an RP, so there is no need for an RP mechanism such as Auto-RP, MSDP, or bootstrap router (BSR).

If SSM is deployed in a network that is already configured for PIM-SM, then only the last-hop routers must be upgraded to a software image that supports SSM. Routers that are not directly connected to receivers do not have to upgrade to a software image that supports SSM. In general, these non-last-hop routers must only run PIM-SM in the SSM range. They may need additional access control configuration to suppress MSDP signaling, registering, or PIM-SM shared-tree operations from occurring within the SSM range.

The SSM mode of operation is enabled by configuring the SSM range using the **ip pim ssm** global configuration command. This configuration has the following effects:

- For groups within the SSM range, (S, G) channel subscriptions are accepted through IGMPv3 INCLUDE mode membership reports.

- PIM operations within the SSM range of addresses change to PIM-SSM, a mode derived from PIM-SM. In this mode, only PIM (S, G) Join and Prune messages are generated by the router. Incoming messages related to rendezvous point tree (RPT) operations are ignored or rejected, and incoming PIM register messages are immediately answered with Register-Stop messages. PIM-SSM is backward-compatible with PIM-SM unless a router is a last-hop router. Therefore, routers that are not last-hop routers can run PIM-SM for SSM groups (for example, if they do not yet support SSM).
- For groups within the SSM range, no MSDP Source-Active (SA) messages within the SSM range will be accepted, generated, or forwarded.

IGMPv3 Host Signaling

IGMPv3 is the third version of the IETF standards track protocol in which hosts signal membership to last-hop routers of multicast groups. IGMPv3 introduces the ability for hosts to signal group membership that allows filtering capabilities with respect to sources. A host can signal either that it wants to receive traffic from all sources sending to a group except for some specific sources (a mode called EXCLUDE) or that it wants to receive traffic only from some specific sources sending to the group (a mode called INCLUDE).

IGMPv3 can operate with both ISM and SSM. In ISM, both EXCLUDE and INCLUDE mode reports are accepted by the last-hop router. In SSM, only INCLUDE mode reports are accepted by the last-hop router.

Benefits of SSM

IP Multicast Address Management Not Required

In the ISM service, applications must acquire a unique IP multicast group address because traffic distribution is based only on the IP multicast group address used. If two applications with different sources and receivers use the same IP multicast group address, then receivers of both applications will receive traffic from the senders of both applications. Even though the receivers, if programmed appropriately, can filter out the unwanted traffic, this situation would cause generally unacceptable levels of unwanted traffic.

Allocating a unique IP multicast group address for an application is still a problem. Most short-lived applications use mechanisms like Session Description Protocol (SDP) and Session Announcement Protocol (SAP) to get a random address, a solution that does not work well with a rising number of applications in the Internet. The best current solution for long-lived applications is described in RFC 2770, but this solution suffers from the restriction that each autonomous system is limited to only 255 usable IP multicast addresses.

In SSM, traffic from each source is forwarded between routers in the network independent of traffic from other sources. Thus different sources can reuse multicast group addresses in the SSM range.

Denial of Service Attacks from Unwanted Sources Inhibited

In SSM, multicast traffic from each individual source will be transported across the network only if it was requested (through IGMPv3, IGMP v3lite, or URD memberships) from a receiver. In contrast, ISM forwards traffic from any active source sending to a multicast group to all receivers requesting that multicast group. In Internet broadcast applications, this ISM behavior is highly undesirable because it allows unwanted sources to easily disturb the actual Internet broadcast source by simply sending traffic to the same multicast group. This situation depletes bandwidth at the receiver side with unwanted traffic and thus disrupts the undisturbed reception of the Internet broadcast. In SSM, this type of denial of service (DoS) attack cannot be made by simply sending traffic to a multicast group.

Easy to Install and Manage

SSM is easy to install and provision in a network because it does not require the network to maintain which active sources are sending to multicast groups. This requirement exists in ISM (with IGMPv1, IGMPv2, or IGMPv3).

The current standard solutions for ISM service are PIM-SM and MSDP. Rendezvous point (RP) management in PIM-SM (including the necessity for Auto-RP or BSR) and MSDP is required only for the network to learn about active sources. This management is not necessary in SSM, which makes SSM easier than ISM to install and manage, and therefore easier than ISM to operationally scale in deployment. Another factor that contributes to the ease of installation of SSM is the fact that it can leverage preexisting PIM-SM networks and requires only the upgrade of last hop routers to support IGMPv3, IGMP v3lite, or URD.

Ideal for Internet Broadcast Applications

The three benefits previously described make SSM ideal for Internet broadcast-style applications for the following reasons:

- The ability to provide Internet broadcast services through SSM without the need for unique IP multicast addresses allows content providers to easily offer their service (IP multicast address allocation has been a serious problem for content providers in the past).
- The prevention against DoS attacks is an important factor for Internet broadcast services because, with their exposure to a large number of receivers, they are the most common targets for such attacks.
- The ease of installation and operation of SSM makes it ideal for network operators, especially in those cases where content needs to be forwarded between multiple independent PIM domains (because there is no need to manage MSDP for SSM between PIM domains).

IGMP v3lite Host Signalling

IGMP v3lite is a Cisco-developed transitional solution for application developers to immediately start programming SSM applications. It allows you to write and run SSM applications on hosts that do not yet support IGMPv3 in their operating system kernel.

Applications must be compiled with the Host Side IGMP Library (HSIL) for IGMP v3lite. This software provides applications with a subset of the IGMPv3 applications programming interface (API) that is required to write SSM applications. HSIL was developed for Cisco by Talarian and is available from the following web page:

http://www.talarianmulticast.com/cgi-bin/igmpdownld

One part of the HSIL is a client library linked to the SSM application. It provides the SSM subset of the IGMPv3 API to the SSM application. If possible, the library checks whether the operating system kernel supports IGMPv3. If it does, then the API calls simply are passed through to the kernel. If the kernel does not support IGMPv3, then the library uses the IGMP v3lite mechanism.

When using the IGMP v3lite mechanism, the library tells the operating system kernel to join to the whole multicast group, because joining to the whole group is the only method for the application to receive traffic for that multicast group (if the operating system kernel only supports IGMPv1 or IGMPv2). In addition, the library signals the (S, G) channel subscriptions to an IGMP v3lite server process, which is also part of the HSIL. A server process is needed because multiple SSM applications may be on the same host. This server process will then send IGMP v3lite-specific (S, G) channel subscriptions to the last hop Cisco IOS router, which needs to be enabled for IGMP v3lite. This router will then “see” both the IGMPv1 or IGMPv2 group membership report from the operating system kernel and the (S, G) channel subscription from the HSIL

daemon. If the router sees both of these messages, it will interpret them as an SSM (S, G) channel subscription and join to the channel through PIM-SSM. We recommend referring to the documentation accompanying the HSIL software for further information on how to utilize IGMP v3lite with your application.

IGMP v3lite is supported by Cisco only through the API provided by the HSIL, not as a function of the router independent of the HSIL. By default, IGMP v3lite is disabled. When IGMP v3lite is configured through the **ip igmp v3lite** interface configuration command on an interface, it will be active only for IP multicast addresses in the SSM range.

URD Host Signalling

URD is a Cisco-developed transitional solution that allows existing IP multicast receiver applications to be used with SSM without the need to modify the application and change or add any software on the receiver host running the application. URD is a content provider solution in which the receiver applications can be started or controlled through a web browser.

URD operates by passing a special URL from the web browser to the last hop router. This URL is called a URD intercept URL. A URD intercept URL is encoded with the (S, G) channel subscription and has a format that allows the last hop router to easily intercept it.

As soon as the last hop router intercepts both an (S, G) channel subscription encoded in a URD intercept URL and sees an IGMP group membership report for the same multicast group from the receiver application, the last hop router will use PIM-SSM to join toward the (S, G) channel as long as the application maintains the membership for the multicast group G. The URD intercept URL is thus only needed initially to provide the last hop router with the address of the sources to join to.

A URD intercept URL has the following syntax:

```
http://
webserver
:465/
path
?group=
group
&source=
source1
&...source=
sourceN
&
```

The *webserver* string is the name or IP address to which the URL is targeted. This target need not be the IP address of an existing web server, except for situations where the web server wants to recognize that the last hop router failed to support the URD mechanism. The number 465 indicates the URD port. Port 465 is reserved for Cisco by the IANA for the URD mechanism so that no other applications can use this port.

When the browser of a host encounters a URD intercept URL, it will try to open a TCP connection to the web server on port 465. If the last hop router is enabled for URD on the interface where the router receives the TCP packets from the host, it will intercept all packets for TCP connections destined to port 465 independent of the actual destination address of the TCP connection (independent of the address of the web server). Once intercepted, the last hop router will “speak” a very simple subset of HTTP on this TCP connection, emulating a web server. The only HTTP request that the last hop router will understand and reply to is the following GET request:

```
GET
argument
 HTTP/1.0
argument
 = /
path
```

```
?group=
group
&source=
source1
&...source=
sourceN
&
```

When it receives a GET command, the router tries to parse the argument according to this syntax to derive one or more (S, G) channel memberships. The *path* string of the argument is anything up to, but not including, the first question mark, and is ignored. The *group* and *source1* through *sourceN* strings are the IP addresses or fully qualified domain names of the channels for which this argument is a subscription request. If the argument matches the syntax shown, the router interprets the argument to be subscriptions for the channels (*source1* , *group*) through (*sourceN* , *group*).

The router will accept the channel subscriptions if the following conditions are met:

- The IP address of the multicast group is within the SSM range.
- The IP address of the host that originated the TCP connection is directly connected to the router.

If the channel subscription is accepted, the router will respond to the TCP connection with the following HTML page format:

```
HTTP/1.1 200 OK
Server:cisco IOS
Content-Type:text/html
<html>
<body>
Retrieved URL string successfully
</body>
</html>
```

If an error condition occurs, the <body> part of the returned HTML page will carry an appropriate error message. The HTML page is a by-product of the URD mechanism. This returned text may, depending on how the web pages carrying a URD intercept URL are designed, be displayed to the user or be sized so that the actual returned HTML page is invisible.

The primary effect of the URD mechanism is that the router will remember received channel subscriptions and will match them against IGMP group membership reports received by the host. The router will “remember” a URD (S, G) channel subscription for up to 3 minutes without a matching IGMP group membership report. As soon as the router sees that it has received both an IGMP group membership report for a multicast group G and a URD (S, G) channel subscription for the same group G, it will join the (S, G) channel through PIM-SSM. The router will then continue to join to the (S, G) channel based only on the presence of a continuing IGMP membership from the host. Thus, one initial URD channel subscription is all that is needed to be added through a web page to enable SSM with URD.

If the last hop router from the receiver host is not enabled for URD, then it will not intercept the HTTP connection toward the web server on port 465. This situation will result in a TCP connection to port 465 on the web server. If no further provisions on the web server are taken, then the user may see a notice (for example, “Connection refused”) in the area of the web page reserved for displaying the URD intercept URL (if the web page was designed to show this output). It is also possible to let the web server “listen” to requests on port 465 and install a Common Gateway Interface (CGI) script that would allow the web server to know if a channel subscription failed (for example, to subsequently return more complex error descriptions to the user).

Because the router returns a Content-Type of text and HTML, the best way to include the URD intercept URL into a web page is to use a frame. By defining the size of the frame, you can also hide the URD intercept URL on the displayed page.

By default, URD is disabled on all interfaces. When URD is configured through the **ip urd** interface configuration command on an interface, it will be active only for IP multicast addresses in the SSM range.

How to Configure Source Specific Multicast

Configuring SSM

To configure SSM, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. Router(config)# **ip pim ssm** [**default** | **range***access-list*]
2. Router(config)# **interface** type number
3. Router(config-if)# **ip pim** {**sparse-mode** | **sparse-dense-mode**}
4. Do one of the following:
   - Router(config-if)# **ip igmp version 3**
   -
   -
   -
   - Router(config-if)# **ip igmp v3lite**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **ip pim ssm** [**default** | **range***access-list*]	Defines the SSM range of IP multicast addresses.
Step 2	Router(config)# **interface** type number	Selects an interface that is connected to hosts on which IGMPv3, IGMP v3lite, and URD can be enabled.
Step 3	Router(config-if)# **ip pim** {**sparse-mode** | **sparse-dense-mode**}	Enables PIM on an interface. You must use either sparse mode or sparse-dense mode.
Step 4	Do one of the following: • Router(config-if)# **ip igmp version 3** • • • • Router(config-if)# **ip igmp v3lite** **Example:**	Enables IGMPv3 on this interface. The default version of IGMP is set to Version 2. or Enables the acceptance and processing of IGMP v3lite membership reports on an interface. or Enables interception of TCP packets sent to the reserved URD port 465 on an interface and processing of URD channel subscription reports.

	Command or Action	Purpose
	Example: **Example:** **Example:** `Router(config-if)#` **ip urd**	

Monitoring SSM

To monitor SSM, use the following commands in privileged EXEC mode, as needed:

Command	Purpose
`SwitchControllerDevice#` **show ip igmp groups detail**	Displays the (S, G) channel subscription through IGMPv3.
`SwitchControllerDevice#` **show ip mroute**	Displays whether a multicast group supports SSM service or whether a source-specific host report was received.

Configuration Examples of Source Specific Multicast

tbd

SSM with IGMPv3 Example

The following example shows how to configure a router (running IGMPv3) for SSM:

```
ip multicast-routing
!
interface GigabitEthernet3/1/0
 ip address 172.21.200.203 255.255.255.0
 description backbone interface
 ip pim sparse-mode
!
interface GigabitEthernet3/2/0
 ip address 131.108.1.2 255.255.255.0
 ip pim sparse-mode
```

```
 description ethernet connected to hosts
 ip igmp version 3
!
ip pim ssm default
```

SSM with IGMP v3lite and URD Example

The following example shows how to configure IGMP v3lite and URD on interfaces connected to hosts for SSM. Configuring IGMP v3lite and URD is not required or recommended on backbone interfaces.

```
interface gigabitethernet 3/1/1
 ip address 172.21.200.203 255.255.255.0
 ip pim sparse-dense-mode
 description gigabitethernet connected to hosts
!
interface gigabitethernet 1/1/1
description gigabitethernet connected to hosts
 ip address 131.108.1.2 255.255.255.0
 ip pim sparse-dense-mode
 ip urd
 ip igmp v3lite
```

SSM Filtering Example

The following example shows how to configure filtering on legacy RP routers running software releases that do not support SSM routing. This filtering will suppress all unwanted PIM-SM and MSDP traffic in the SSM range. Without this filtering, SSM will still operate, but there may be additional RPT traffic if legacy first hop and last hop routers exist in the network.

```
ip access-list extended  no-ssm-range
  deny   ip any 232.0.0.0 0.255.255.255 ! SSM range
  permit ip any any
! Deny registering in SSM range
ip pim accept-register list no-ssm-range
ip access-list extended msdp-nono-list
  deny   ip any 232.0.0.0 0.255.255.255 ! SSM Range
  ! .
  ! .
  ! .
  ! See ftp://ftpeng.cisco.com/ipmulticast/config-notes/msdp-sa-filter.txt for other SA
  ! messages that typically need to be filtered.
  permit ip any any
! Filter generated SA messages in SSM range. This configuration is only needed if there
! are directly connected sources to this router. The “ip pim accept-register” command
! filters remote sources.
ip msdp redistribute list msdp-nono-list
! Filter received SA messages in SSM range. “Filtered on receipt” means messages are
! neither processed or forwarded. Needs to be configured for each MSDP peer.
ip msdp sa-filter in msdp-peer1 list msdp-nono-list
! .
! .
! .
ip msdp sa-filter in msdp-peerN list msdp-nono-list
```

Additional References

The following sections provide references related to Source Specific Multicast.

Related Documents

Related Topic	Document Title
PIM-SM and SSM concepts and configuration examples	“Configuring Basic IP Multicast ” module
IP multicast commands: complete command syntax, command mode, defaults, command history, usage guidelines, and examples	

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing standards has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS XE releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing standards has not been modified by this feature.	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for Source Specific Multicast

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 7: Feature Information for Source Specific Multicast

Feature Name	Release	Feature Information
Source Specific Multicast (SSM)	12.3(4)T 12.2(25)S 12.0(28)S 12.2(33)SXH 12.2(33)SRA 15.0(1)S Cisco IOS XE Release 2.1 Cisco IOS XE Release 3.1.0SG Cisco IOS XE Release 3.5S	SSM is an extension of IP multicast where datagram traffic is forwarded to receivers from only those multicast sources that the receivers have explicitly joined. For multicast groups configured for SSM, only source-specific multicast distribution trees (not shared trees) are created. In Cisco IOS XE Release 3.5S, support was added for the Cisco ASR 903 Router.

CHAPTER 8

Tunneling to Connect Non-IP Multicast Areas

This module describes how to configure a Generic Route Encapsulation (GRE) tunnel to tunnel IP multicast packets between non-IP multicast areas. The benefit is that IP multicast traffic can be sent from a source to a multicast group, over an area where IP multicast is not supported.

- Finding Feature Information, page 171
- Prerequisites for Tunneling to Connect Non-IP Multicast Areas, page 171
- Information About Tunneling to Connect Non-IP Multicast Areas, page 172
- How to Connect Non-IP Multicast Areas, page 173
- Configuration Examples for Tunneling to Connect Non-IP Multicast Areas, page 175
- Additional References, page 178
- Feature Information for Tunneling to Connect Non-IP Multicast Areas, page 179

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Tunneling to Connect Non-IP Multicast Areas

This module assumes you understand the concepts in the “IP Multicast Technology Overview” module.

Information About Tunneling to Connect Non-IP Multicast Areas

Benefits of Tunneling to Connect Non-IP Multicast Areas

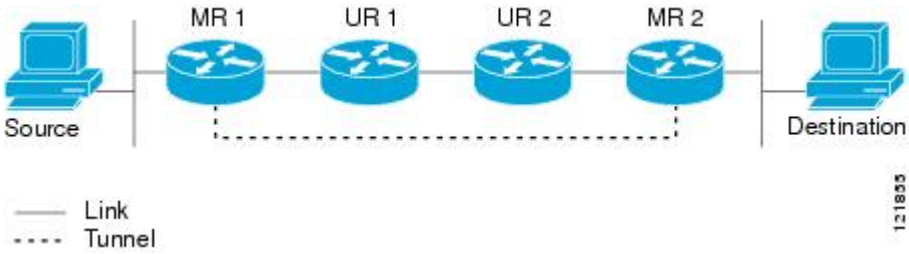
- If the path between a source and a group member (destination) does not support IP multicast, a tunnel between them can transport IP multicast packets.
- Per packet load balancing can be used. Load balancing in IP multicast is normally per (S,G). Therefore, (S1, G) can go over Link X and (S2, G) can go over Link Y, where X and Y are parallel links. If you create a tunnel between the routers, you can get per packet load balancing because the load balancing is done on the tunnel unicast packets.

IP Multicast Static Route

IP multicast static routes (mroutes) allow you to have multicast paths diverge from the unicast paths. When using Protocol Independent Multicast (PIM), the router expects to receive packets on the same interface where it sends unicast packets back to the source. This expectation is beneficial if your multicast and unicast topologies are congruent. However, you might want unicast packets to take one path and multicast packets to take another.

The most common reason for using separate unicast and multicast paths is tunneling. When a path between a source and a destination does not support multicast routing, a solution is to configure two routers with a GRE tunnel between them. In the figure, each unicast router (UR) supports unicast packets only; each multicast router (MR) supports multicast packets.

Figure 16: Tunnel for Multicast Packets



In the figure, Source delivers multicast packets to Destination by using MR 1 and MR 2. MR 2 accepts the multicast packet only if it believes it can reach Source over the tunnel. If this situation is true, when Destination sends unicast packets to Source, MR 2 sends them over the tunnel. The check that MR2 can reach Source over the tunnel is a Reverse Path Forwarding (RPF) check, and the static mroute allows the check to be successful when the interface that the multicast packet arrives on is not the unicast path back to the source. Sending the packet over the tunnel could be slower than natively sending it through UR 2, UR 1, and MR 1.

A multicast static route allows you to use the configuration in the figure by configuring a static multicast source. The system uses the configuration information instead of the unicast routing table to route the traffic. Therefore, multicast packets can use the tunnel without having unicast packets use the tunnel. Static mroutes are local to the router they are configured on and not advertised or redistributed in any way to any other router.

How to Connect Non-IP Multicast Areas

Configuring a Tunnel to Connect Non-IP Multicast Areas

Configure a multicast static route if you want your multicast paths to differ from your unicast paths. For example, you might have a tunnel between two routers because the unicast path between a source and destination does not support multicast routing.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel** *number*
4. **ip unnumbered** *type number*
5. **ip pim sparse-mode**
6. **tunnel source** {*ip-address* | *type number*}
7. **tunnel destination** {*hostname* | *ip-address*}
8. Repeat Steps 1 through 7 on the router at the opposite end of the tunnel, reversing the tunnel source and destination addresses.
9. **end**
10. **ip mroute** *source-address mask* **tunnel** *number* [*distance*]
11. **ip mroute** *source-address mask* **tunnel** *number* [*distance*]
12. **end**
13. **show ip mroute** [*group-address* | *group-name*] [*source-address* | *source-name*] [*interface-type interface-number*] [**summary**] [**count**] [**active** *kbps*]
14. **show ip rpf** {*source-address* | *source-name*} [**metric**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**interface tunnel** *number* **Example:** `Router(config)# interface tunnel 0`	Configures a tunnel interface.
Step 4	**ip unnumbered** *type number* **Example:** `Router(config-if)# ip unnumbered gigabitethernet 0/0/0`	Enables IP processing without assigning an IP address to the interface.
Step 5	**ip pim sparse-mode** **Example:** `Router(config-if)# ip pim sparse-mode`	Enables PIM sparse mode on the tunnel interface.
Step 6	**tunnel source** {*ip-address* | *type number*} **Example:** `Router(config-if)# tunnel source 100.1.1.1`	Configures the tunnel source.
Step 7	**tunnel destination** {*hostname* | *ip-address*} **Example:** `Router(config-if)# tunnel destination 100.1.5.3`	Configures the tunnel destination.
Step 8	Repeat Steps 1 through 7 on the router at the opposite end of the tunnel, reversing the tunnel source and destination addresses.	Router A's tunnel source address will match Router B's tunnel destination address. Router A's tunnel destination address will match Router B's tunnel source address.
Step 9	**end** **Example:** `Router(config-if)# end`	Ends the current configuration session and returns to privileged EXEC mode.
Step 10	**ip mroute** *source-address mask* **tunnel** *number* [*distance*] **Example:** `Router(config)# ip mroute 0.0.0.0 0.0.0.0 tunnel 0`	Configures a static multicast route over which to reverse path forward to the other end of the tunnel. • Because the use of the tunnel makes the multicast topology incongruent with the unicast topology, and only multicast traffic traverses the tunnel, you must configure the routers to reverse path forward correctly over the tunnel. • When a source range is specified, the mroute applies only to those sources.

	Command or Action	Purpose
		• In the example, the *source-address* and *mask* of 0.0.0.0 0.0.0.0 indicate any address. • The shorter distance is preferred. • The default distance is 0.
Step 11	**ip mroute** *source-address mask* **tunnel** *number* [*distance*] **Example:** `Router(config)# ip mroute 0.0.0.0 0.0.0.0 tunnel 0`	Configures a static route over which to reverse path forward from the access router to the other end of the tunnel.
Step 12	**end** **Example:** `Router(config)# end`	(Optional) Ends the current configuration session and returns to privileged EXEC mode.
Step 13	**show ip mroute** [*group-address* | *group-name*] [*source-address* | *source-name*] [*interface-type interface-number*] [**summary**] [**count**] [**active** *kbps*] **Example:** `Router# show ip mroute`	(Optional) Displays the contents of the IP multicast routing (mroute) table.
Step 14	**show ip rpf** {*source-address* | *source-name*} [**metric**] **Example:** `Router# show ip rpf 10.2.3.4`	(Optional) Displays how IP multicast routing does RPF.

Configuration Examples for Tunneling to Connect Non-IP Multicast Areas

Tunneling to Connect Non-IP Multicast Areas Example

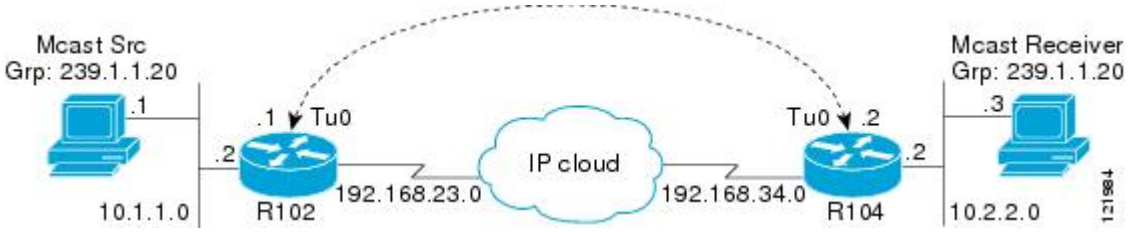
The following example also appears online at:

http://www.cisco.com/en/US/tech/tk828/tk363/technologies_configuration_example09186a00801a5aa2.shtml

In the figure below, the multicast source (10.1.1.1) is connected to R102 and is configured for multicast group 239.1.1.20. The multicast receiver (10.2.2.3) is connected to R104 and is configured to receive multicast

packets for group 239.1.1.20. Separating R102 and R104 is an IP cloud, which is not configured for multicast routing.

Figure 17: Tunnel Connecting Non-IP Multicast Areas



A tunnel is configured between R102 to R104 sourced with their loopback interfaces. The **ip pim sparse-dense-mode** command is configured on tunnel interfaces and multicast-routing is enabled on R102 and R104. Sparse-dense mode configuration on the tunnel interfaces allows sparse-mode or dense-mode packets to be forwarded over the tunnel depending on rendezvous point (RP) configuration for the group.

Note For dense mode--With PIM dense mode configured over the tunnel, an **ip mroute 10.1.1.0 255.255.255.0 tunnel 0** command is configured on R104 to ensure a successful RPF for multicast source address 10.1.1.1. Incoming (10.1.1.1, 239.1.1.20) multicast packets over Tunnel0 (Tu0) are checked for Reverse Path Forwarding (RPF) using this mroute statement. After a successful check, the multicast packets are forwarded to outgoing interface list (OIL) interfaces.

Note For sparse mode--With PIM sparse mode configured over the tunnel, ensure that the following points are addressed:

- For a successful RPF verification of multicast traffic flowing over the shared tree (*,G) from RP, an **ip mroute rp-address nexthop** command needs to be configured for the RP address, pointing to the tunnel interface.

Assuming R102 to be the RP (RP address 2.2.2.2) in this case, the mroute would be the **ip mroute 2.2.2.2 255.255.255.255 tunnel 0**command, which ensures a successful RPF check for traffic flowing over the shared tree.

- For a successful RPF verification of multicast (S,G) traffic flowing over the Shortest Path Tree (SPT), an **ip mroute source-address nexthop** command needs to be configured for the multicast source, pointing to the tunnel interface.

In this case, when SPT traffic is flowing over tunnel interface an **ip mroute 10.1.1.0 255.255.255.0 tunnel 0** command is configured on R104 to ensure a successful RPF verification for incoming (10.1.1.1, 239.1.1.20) multicast packets over the Tunnel 0 interface.

R102#

```
version 12.2
hostname r102
ip subnet-zero
```

```
no ip domain-lookup
!--- It stops IP domain lookup, which improves the show command response time.
!
ip multicast-routing
!--- Enables IP multicast routing.
!
interface Loopback0
 ip address 2.2.2.2 255.255.255.255
!--- Tunnel Source interface.
!
interface Tunnel0
!--- Tunnel interface configured for PIM and carrying multicast packets to R104.
 ip address 192.168.24.1 255.255.255.252
 ip pim sparse-dense-mode
 tunnel source Loopback0
 tunnel destination 4.4.4.4
!
interface Ethernet0/0
!--- Interface connected to Source.
ip address 10.1.1.2 255.255.255.0
 ip pim sparse-dense-mode
!
interface Serial8/0
 ip address 192.168.23.1 255.255.255.252
!--- Note IP PIM sparse-dense mode is not configured on Serial interface.
!
router ospf 1
 log-adjacency-changes
 network 2.2.2.2 0.0.0.0 area 0
 network 10.1.1.0 0.0.0.255 area 0
 network 192.168.23.0 0.0.0.255 area 0
!
ip classless
ip pim bidir-enable
!
line con 0
line aux 0
line vty 0 4
 login
!
end
```

R104#

```
version 12.2
!
hostname r104
!
ip subnet-zero
no ip domain-lookup
!--- It stops IP domain lookup, which improves the show command response time.
!
ip multicast-routing
!--- Enables IP multicast routing.
!
interface Loopback0
 ip address 4.4.4.4 255.255.255.255
!--- Tunnel Source interface.
!
interface Tunnel0
 ip address 192.168.24.2 255.255.255.252
!--- Tunnel interface configured for PIM and carrying multicast packets.
ip pim sparse-dense-mode
 tunnel source Loopback0
 tunnel destination 2.2.2.2
!
interface Ethernet0/0
 ip address 10.2.2.2 255.255.255.0
 ip pim sparse-dense-mode
!
interface Serial9/0
```

```
 ip address 192.168.34.1 255.255.255.252
!--- Note IP PIM sparse-dense mode is not configured on Serial interface.
!
!
router ospf 1
 log-adjacency-changes
 network 4.4.4.4 0.0.0.0 area 0
 network 10.2.2.0 0.0.0.255 area 0
 network 192.168.34.0 0.0.0.255 area 0
!
ip classless
no ip http server
ip pim bidir-enable
ip mroute 10.1.1.0 255.255.255.0 Tunnel0
!--- This Mroute ensures a successful RPF check for packets flowing from the source.
!--- 10.1.1.1 over Shared tree in case of Dense more and SPT in case of Sparse mode.
!
ip mroute 2.2.2.2 255.255.255.255 tunnel 0
!--- This Mroute is required for RPF check when Sparse mode multicast traffic is
!--- flowing from RP (assuming R102 with 2.2.2.2 as RP)  towards receiver via tunnel
!--- before the SPT switchover.
line con 0
line aux 0
line vty 0 4
 login
!
end
```

Additional References

Related Documents

Related Topic	Document Title
IP multicast commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS IP Multicast Command Reference*

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing standards has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS XE releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for Tunneling to Connect Non-IP Multicast Areas

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 8: Feature Information for Tunneling to Connect Non-IP Multicast Areas

Feature Name	Releases	Feature Configuration Information
This table is intentionally left blank because no features were introduced or modified in Cisco IOS XE Release 2.1 or later. This table will be updated when feature information is added to this module.	--	--

CHAPTER 9

Automatic Multicast Tunneling

Automatic Multicast Tunneling (AMT) provides a method to tunnel multicast data over a unicast network. The tunneling is performed between AMT relays and AMT gateways, using User Datagram Protocol (UDP) encapsulation. AMT enables service providers and their customers to participate in delivering multicast traffic even in the absence of end-to-end multicast connectivity.

- Finding Feature Information, page 181
- Restrictions for Automatic Multicast Tunneling, page 181
- Information About Automatic Multicast Tunneling, page 182
- How to Configure Automatic Multicast Tunneling, page 184
- Configuration Examples for Automatic Multicast Tunneling, page 197
- Additional References for Automatic Multicast Tunneling, page 198
- Feature Information for Automatic Multicast Tunneling, page 198

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Automatic Multicast Tunneling

- AMT tunnel only support PIM passive mode on AMT Gateway side.
- AMT only support SSM modes for PIM signaling.
- AMT only support ipv4 transport for tunnel.
- For AMT, auto-rp is invalid between relay and gateway.

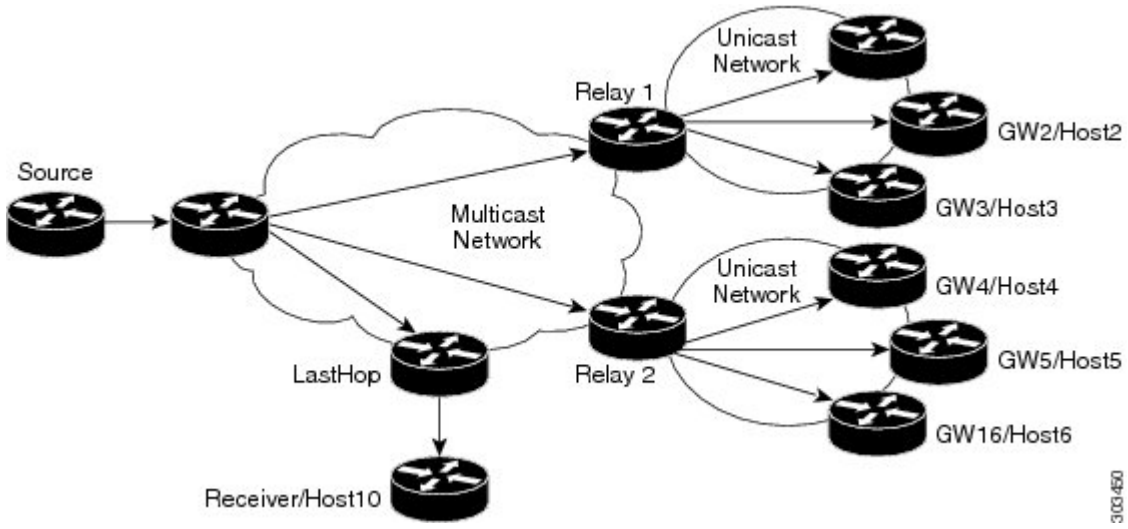
Information About Automatic Multicast Tunneling

Overview

The multicast source sends traffic to the first-hop. Multicast traffic flows through the network until it reaches the last-hop (receivers) or AMT relays. AMT Relay is a multicast router configured to support transit routing between nonmulticast capable internetwork and the native multicast infrastructure.

The following diagram provides a sample AMT network where Relay1 and Relay2 are two AMT relays, which encapsulate the traffic into AMT tunnels, and send one copy to each of the AMT gateways.

Figure 18: Automatic Multicast Tunneling (AMT)



Automatic Multicast Tunneling Message Exchanges

The AMT protocol defines seven message types for control and encapsulation. The message exchanges happen in the following sequence:

1. Relay Discovery—Gateway sends an AMT discovery message to an anycast address that represents the AMT relay.
2. Relay Advertisement—Relay responds with an advertisement message, which includes the relay's unique IP address.
3. Relay Request—Gateway sends an AMT Request message to the relay using the unique IP address as the destination, along with a nonce to be used for security.
4. Membership Query—Relay responds with an AMT query that includes the nonce from the AMT request and an opaque security code.
5. Membership Update—Gateway responds with a membership update that includes an encapsulated IGMPv3/MLDv2 packet.

6 Teardown—Gateway sends a message to stop the delivery of multicast data messages requested in an earlier membership update message.

7 After validation the Relay establishes the AMT Tunnel and starts sending multicast traffic [Type 6]. Any further (S,G) uses the same Request/Query/Update - three-way handshake because the tunnel is already established.

AMT Tunnel and Traffic Types

The multicast traffic carried in the AMT tunnel may be IPv4 or IPv6. The AMT tunnel may be setup with IPv4 or IPv6 endpoints, thereby providing the following possibilities.

- IPv4-in-IPv4—IPv4 multicast traffic carried over an IPv4 tunnel
- IPv6-in-IPv4—IPv6 multicast traffic carried over an IPv4 tunnel
- IPv6-in-IPv6—IPv6 multicast traffic carried over an IPv6 tunnel
- IPv4-in-IPv6—IPv4 multicast traffic carried over an IPv6 tunnel

Note In Cisco IOS XE Release 3.15S, AMT supports IPv4-in-IPv4 and IPv6-in-IPv4 only.

Advantages of Automatic Multicast Tunneling

- Simplicity—Instead of incurring the overhead of manually provisioning, establishing and maintaining GRE tunnels between two locations, the receiving network simply sends AMT advertisements to a well-known any-cast prefix. The rest of the tunnel establishment process is done automatically without the need for additional configuration.
- Resiliency—Because the relay discovery uses an any-cast address, gateways automatically find the closest relay. If that relay becomes unavailable or unreachable, the routing table reconverges on the next closest relay.
- Efficiency—AMT allows transit routers to perform flow-based load balancing for more efficient link utilization.

Automatic Multicast Tunneling supports IPv4 transport for tunnel and also support for IPv4 multicast traffic & IPv6 multicast traffic. You can also configure AMT relay-only, gateway-only and relay-gateway coexisting modes.

Prerequisites for AMT

- AMT relay and gateway tunnel requires an interface IP address. However the interface IP addresses do not need to be unique. You can configure the same addresses for the tunnel source address using the **ip unnumbered** command.
- You must configure IGMP version 3 on the tunnel interfaces for the SSM to work across tunnels.

- The tunnel source port and tunnel destination port must be configured to achieve a valid AMT configuration.

Configuration Recommendations for AMT

The tunnel source interface address should be an interface that is set up to be reachable from receivers under all instances. You can use a physical interface address, but it can cause the tunnel to go down if that physical interface is down. A loopback interface is recommended to sustain availability. You do not need a separate loopback address, you can reuse the loopback interface that you usually would have to carry router and router-ID IP address (usually Loopback 0).

IP PIM passive is the recommended and supported mode on AMT interfaces to enable IP multicast routing for AMT tunnel interfaces. This is recommended since no PIM messages (only AMT/IGMP messages) will be sent or received via the AMT tunnel.

On an AMT relay, you need only one tunnel interface to which all gateways can connect. Therefore the interface is a multipoint interface. Every gateway interface can only connect to one relay, but you can configure multiple tunnel interfaces.

Even though AMT tunnels (relay and gateway) only support IPv4 tunnels, the IPv4 tunnels can carry both IPv4 and IPv6 simultaneously. You can configure the AMT for the version(s) of IP that you need.

If you want to set up a redundant AMT relay, your AMT relay address configured on the gateway should be any IP address that you set up as an anycast address on your relays. If you do not plan to use redundant (Anycast) Relay, you can use the relays tunnel source address on the gateways.

If you shut down the anycast Loopback interface, the AMT relay would not accept new AMT gateway tunnel requests. IP routing for the anycast address would only point to any other relays active with the same address and new requests would therefore go to those relays. Any AMT gateways already connected to this relay would stay on this relay, because they already are using the relays interface address.

How to Configure Automatic Multicast Tunneling

Enabling and Configuring Automatic Multicast Tunneling on a Relay

Note Switch-over from active relay to backup relay can take more than 5 minutes.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel** *number*
4. **ip address** *ip-address mask*
5. **no ip redirects**
6. **ip pim sparse-mode**
7. **ip igmp version** *version number*
8. **ipv6 enable**
9. **tunnel source** *interface-type interface-number*
10. **tunnel mode udp multipoint**
11. **tunnel dst-port dynamic**
12. **tunnel src-port dynamic**
13. **amt relay traffic** {**ip** | **ipv6**}
14. **exit**
15. **ip multicast-routing distributed**
16. **ipv6 multicast-routing**
17. **ip pim ssm** {*default* | *range access-list*}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface tunnel** *number* **Example:** `Device(config)# interface tunnel 11`	Specifies the interface tunnel number and enters interface configuration mode.
Step 4	**ip address** *ip-address mask* **Example:** `Device(config-if)# 11.1.1.1 255.255.255.0`	Configures the IP address on the interface.
Step 5	**no ip redirects** **Example:** `Device(config-if)# no ip redirects`	Disables sending ICMP Redirect messages.

	Command or Action	Purpose
Step 6	**ip pim sparse-mode** **Example:** `Device(config-if)# ip pim sparse-mode`	Enable PIM sparse-mode operation.
Step 7	**ip igmp version** *version number* **Example:** `Device(config-if)# ip igmp version 3`	Specifies IGMP version.
Step 8	**ipv6 enable** **Example:** `Device(config-if)# ipv6 enable`	Enables IPv6 on interface.
Step 9	**tunnel source** *interface-type interface-number* **Example:** `Device(config-if)# tunnel source loopback 0`	Configures tunnel source as a loopback interface.
Step 10	**tunnel mode udp multipoint** **Example:** `Device(config-if)# tunnel mode udp multipoint`	Specifies the UDP encapsulation protocol.
Step 11	**tunnel dst-port dynamic** **Example:** `Device(config-if)# tunnel dst-port dynamic`	Specifies the tunnel destination port.
Step 12	**tunnel src-port dynamic** **Example:** `Device(config-if)# tunnel src-port dynamic`	Specifies the tunnel source port.
Step 13	**amt relay traffic** {**ip** | **ipv6**} **Example:** `Device(config-if)# amt relay traffic ipv6`	Enables IPv4 or IPv6 traffic on AMT relay interface.
Step 14	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.
Step 15	**ip multicast-routing distributed** **Example:** `Device(config)# ip multicast-routing distributed`	Enables Multicast Distributed Switching (MDS).
Step 16	**ipv6 multicast-routing** **Example:** `Device(config)# ipv6 multicast-routing`	Enables multicast routing using Protocol Independent Multicast (PIM) and Multicast Listener Discovery (MLD).

	Command or Action	Purpose
Step 17	**ip pim ssm** {*default* | *range access-list*} **Example:** `Device(config)# ip pim ssm default`	Specifies the Source Specific Multicast (SSM) range of IP multicast addresses.

Enabling and Configuring Automatic Multicast Tunneling on Gateway

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel** *number*
4. **ip address** *ip-address mask*
5. **ip pim passive**
6. **ip igmp version** *version number*
7. **ipv6 enable**
8. **ipv6 pim passive**
9. **tunnel source** *interface-type interface-number*
10. **tunnel mode udp ip**
11. **tunnel destination dynamic**
12. **tunnel dst-port dynamic**
13. **tunnel src-port dynamic**
14. **amt gateway traffic** {**ip** | **ipv6**}
15. **amt gateway relay-address** *IP address*
16. **exit**
17. **ip multicast-routing distributed**
18. **ipv6 multicast-routing**
19. **ip pim ssm** {*default* | *range access-list*}
20. **ipv6 multicast pim-passive-enable**
21. **ip route** *ip-address interface-type interface-number* [**multicast**]
22. **ipv6 route** *ipv6-prefix/prefix-length interface-type interface-number* [**multicast**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Device> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface tunnel** *number* **Example:** `Device(config)# interface tunnel 11`	Specifies the interface tunnel number and enters interface configuration mode.
Step 4	**ip address** *ip-address mask* **Example:** `Device(config-if)# 11.1.1.1 255.255.255.0`	Configures the IP address on the interface.
Step 5	**ip pim passive** **Example:** `Device(config-if)# ip pim passive`	Enables IP PIM passive mode operation.
Step 6	**ip igmp version** *version number* **Example:** `Device(config-if)# ip igmp version 3`	Specifies IGMP version.
Step 7	**ipv6 enable** **Example:** `Device(config-if)# ipv6 enable`	Enables IPv6 on interface.
Step 8	**ipv6 pim passive** **Example:** `Device(config-if)# ipv6 pim passive`	Enables IPv6 PIM passive mode operation.
Step 9	**tunnel source** *interface-type interface-number* **Example:** `Device(config-if)# tunnel source loopback 0`	Configures tunnel source as a loopback interface.
Step 10	**tunnel mode udp ip** **Example:** `Device(config-if)# tunnel mode udp ip`	Specifies the UDP encapsulation protocol.
Step 11	**tunnel destination dynamic** **Example:** `Device(config-if)# tunnel destination dynamic`	Applies the tunnel destination address dynamically to the tunnel interface.

	Command or Action	Purpose
Step 12	**tunnel dst-port dynamic** **Example:** `Device(config-if)# tunnel dst-port dynamic`	Applies the tunnel destination port dynamically.
Step 13	**tunnel src-port dynamic** **Example:** `Device(config-if)# tunnel src-port dynamic`	Applies the tunnel source port dynamically.
Step 14	**amt gateway traffic** {**ip** | **ipv6**} **Example:** `Device(config-if)# amt gateway traffic ipv6`	Enables IPv4 or IPv6 traffic on AMT gateway interface.
Step 15	**amt gateway relay-address** *IP address* **Example:** `Device(config-if)# amt gateway relay-address 172.16.0.0`	Specifies the destination IP address of AMT discovery.
Step 16	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.
Step 17	**ip multicast-routing distributed** **Example:** `Device(config)# ip multicast-routing distributed`	Enables Multicast Distributed Switching (MDS).
Step 18	**ipv6 multicast-routing** **Example:** `Device(config)# ipv6 multicast-routing`	Enables multicast routing using Protocol Independent Multicast (PIM) and Multicast Listener Discovery (MLD).
Step 19	**ip pim ssm** {*default* | *range access-list*} **Example:** `Device(config)# ip pim ssm default`	Specifies the Source Specific Multicast (SSM) range of IP multicast addresses.
Step 20	**ipv6 multicast pim-passive-enable** **Example:** `Device(config)# ipv6 multicast pim-passive-enable`	Enables passive PIM operation.
Step 21	**ip route** *ip-address interface-type interface-number* [**multicast**] **Example:** `Device(config)# ip route 101.0.0.2 255.255.255.255 tunnel10 multicast`	Specifies the IP address along with interface type, interface number, and multicast route.

	Command or Action	Purpose
Step 22	**ipv6 route** *ipv6-prefix/prefix-length interface-type interface-number* [**multicast**] **Example:** `Device(config)# ipv6 route 2011::101:0:0:2/128 Tunnel10 multicast`	Specifies the IPv6 prefix and length along with interface type, interface number, and multicast route (route only usable by multicast).

Displaying and Verifying AMT Configuration

Before You Begin

SUMMARY STEPS

1. **ping** *3.3.3.3* **source** *5.5.5.5*
2. **show ip igmp membership**
3. **show ip mroute**
4. **show ip rpf***10.3.3.1*

DETAILED STEPS

Step 1 **ping** *3.3.3.3* **source** *5.5.5.5*

Example:
```
Device# ping 3.3.3.3 source 5.5.5.5
   Type escape sequence to abort.
   Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:
   Packet sent with a source address of 5.5.5.5
   !!!!!
   Success rate is 100 percent (5/5), round-trip min/avg/max = 6/6/8 ms
```
Ping the relay tunnel source address from the gateway, using the gateways tunnel source address and the gateway address (if both are different as the example).

Step 2 **show ip igmp membership**

Example:
```
Device# show ip igmp membership
  ...
   Channel/Group                  Reporter        Uptime   Exp.  Flags  Interface
  /*,232.2.3.4                    0.0.0.0         00:03:02 stop  2MA    Lo0
   10.3.3.1,232.2.3.4                             00:03:02 stop  A      Lo0
```
Note The command is executed at destination gateway.

You can use the **ip igmp static-group** command, you create an IGMP membership request on the interface. You can do this on any physical interface configured for IP multicast, but if there are multiple routers attached to the interface, then the AMT gateway router may not become the PIM-DR and therefore not join to the multicast traffic. It can therefore be easier to put the join on an existing loopback interface and also enable it for IP multicast (IP PIM passive).

Step 3 **show ip mroute**

Example:

```
Device# show ip mroute
  ...
  (10.3.3.1, 232.2.3.4), 00:01:53/00:01:08, flags: sTI
    Incoming interface: Tunnel1, RPF nbr 0.0.0.0, Mroute
    Outgoing interface list:
      Loopback0, Forward/Sparse-Dense, 00:01:51/00:01:08
```

Note The command is executed at destination gateway.

The AMT gateway will join the multicast traffic towards the AMT relay if the mroute shows the incoming interface as the Tunnel interface and when it is joined for example, when there are one or more outgoing interfaces.
When the command is executed on the source gateway, the mroute state on the relay will show the relay interface as an adjacency in the outgoing interface list. Because there is one interface for all joining relays, each outgoing copy across the AMT relay interface is identified by the AMT relay interface, the IP address of the gateway and the UDP port number of the relay as seen by the relay. If there are multiple gateways in a home behind a NAT/PAT (single IP address to the internet), there would be multiple adjacencies shown with the same gateway IP address, but different UDP ports. If state is not built as expected, you can use **debug ip igmp** to troubleshoot it. There are no additional AMT debugs for the AMT/IGMP joins, instead those are all part of IGMP debugs.

Step 4 **show ip rpf***10.3.3.1*

Example:

```
Device#
RPF information for ? (10.3.3.1)
  RPF interface: Tunnel1
  RPF neighbor: ? (0.0.0.0)
  RPF route/mask: 10.3.3.0/24
  RPF type: multicast (static)
  Doing distance-preferred lookups across tables
  RPF topology: ipv4 multicast base
```

Note The command is executed at destination gateway.

Verifies Multicast RPF.

If the output is not showing the desired AMT gateway tunnel interface as the RPF interface, then your routing configuration for IP multicast into the AMT tunnel is not set up correctly. If you have only one AMT gateway interface, you can use a static mroute. If you have multiple AMT tunnel for different relays, you need to configure the source prefixes (and RP-addresses when you use PIM-SM) towards their respective AMT tunnel.

For IP multicast tree to flow correctly via the AMT tunnels, you must first check if the IP multicast state is correctly built from gateway to relay. This primarily means that the (S,G) join for a source in PIM-SSM/PIM-SM or the (*,G) join to the RP address in PIM-SM need to RPF towards the desired AMT gateway tunnel.

Displaying and Verifying AMT Relay Configuration

SUMMARY STEPS

1. **enable**
2. **show ip amt tunnel**
3. **show ip mroute section** [**group-address**]
4. **show ipv6 mroute section** [**group-address**]
5. **show ip mfib section** [**group-address**]
6. **show ipv6 mfib section** [**group-address**]
7. **show platform software ip rp active mfib section** [**group-address**]
8. **show platform software ipv6 rp active mfib section** [**group-address**]
9. **show platform software mlist rp active index** *multicast-index-number*
10. **show platform software adjacency rp active index** *platform-allocated-index-value*
11. **show ip interface brief**

DETAILED STEPS

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **show ip amt tunnel**

Example:

```
Device# show ip amt tunnel

AMT Relay tunnel:
    Local address       UDP port
      11.11.11.11       2268 (0x8DC )
    Remote address                      Expire time
      33.33.33.33       59464(0xE848)   00:03:07
    Connected to 1 Gateway

  Total active Gateways: 1
```

Displays AMT relay configuration.

Step 3 **show ip mroute section** [**group-address**]

Example:

```
Device# show ip mroute section 232.1.1.1

(101.0.0.2, 232.1.1.1), 2d00h/00:02:18, flags: sTI
  Incoming interface: GigabitEthernet0/0/4, RPF nbr 0.0.0.0
  Outgoing interface list:
    Tunnel10, 33.33.33.33, UDP port 59464, Forward/Sparse, 2d00h/00:02:18
```

Displays information about sparse mode routes in the IP multicast routing (mroute) table for the specified multicast group.

Step 4 **show ipv6 mroute section** [**group-address**]

Example:

```
Device# show ipv6 mroute section 232.1.1.1

(2011::101:0:0:2, FF3F::232:1:1:1), 2d00h/never, flags: sTI
  Incoming interface: GigabitEthernet0/0/4
  RPF nbr: 2011::101:0:0:2
  Immediate Outgoing interface list:
    Tunnel10, AMT NH 33.33.33.33, UDP Port 59464, Forward, 2d00h/never
```

Displays information about sparse mode routes in the IPv6 mroute table for the specified multicast group.

Step 5 **show ip mfib section** [**group-address**]

Example:

```
Device# show ip mfib section 232.1.1.1

(101.0.0.2,232.1.1.1) Flags: HW
   SW Forwarding: 0/0/0/0, Other: 0/0/0
   HW Forwarding:   NA/NA/NA/NA, Other: NA/NA/NA
   GigabitEthernet0/0/4 Flags: A
   Tunnel10, AMT Encap 33.33.33.33, UDP Port:59464 Flags: F NS
     Pkts: 0/0
```

Displays the status of entries and interfaces in the IPv4 Multicast Forwarding Information Base (MFIB) for the specified multicast group.

Step 6 **show ipv6 mfib section** [**group-address**]

Example:

```
Device# show ipv6 mfib section 232.1.1.1

(2011::101:0:0:2,FF3F::232:1:1:1) Flags: HW
   SW Forwarding: 0/0/0/0, Other: 0/0/0
   HW Forwarding:   NA/NA/NA/NA, Other: NA/NA/NA
   GigabitEthernet0/0/4 Flags: A
   Tunnel10, AMT Encap 33.33.33.33, UDP Port:59464 Flags: F NS
     Pkts: 0/0
```

Displays the status of entries and interfaces in the IPv6 Multicast Forwarding Information Base (MFIB) for the specified multicast group.

Step 7 **show platform software ip rp active mfib section** [**group-address**]

Example:

```
Device# show platform software ip rp active mfib section 232.1.1.1

232.1.1.1, 101.0.0.2/64 --> OBJ_INTF_LIST (0x5a)
                Obj id: 0x5a, Flags:
                OM handle: 0x421712c4
```

Displays platform software IPv4 MFIB route processor information for the specified multicast group.

Step 8 **show platform software ipv6 rp active mfib section** [**group-address**]

Example:

```
Device# show platform software ipv6 rp active mfib section 232.1.1.1

ff3f::232:1:1:1, 2011::101:0:0:2/256 --> OBJ_INTF_LIST (0x5b)
                Obj id: 0x5b, Flags:
                OM handle: 0x42171d24
```

Displays platform software IPv6 MFIB route processor information for the specified multicast group.

Step 9 **show platform software mlist rp active index** *multicast-index-number*

Example:

```
Device# show platform software mlist rp active index 0x5a

OCE              Type             OCE Flags        Interface
--------------------------------------------------------------------------------
0x57             OBJ_ADJACENCY    NS, F            Tunnel10
0xf80000c1       OBJ_ADJACENCY    A                GigabitEthernet0/0/4
```

Displays platform software route processor information for the specified multicast list index.

Step 10 **show platform software adjacency rp active index** *platform-allocated-index-value*

Example:

```
Device# show platform software adjacency rp active index 0x57

Number of adjacency objects: 22

Adjacency id: 0x57 (87)
  Interface: Tunnel10, IF index: 20, Link Type: MCP_LINK_IP
  Encap: 45:0:0:0:0:0:0:0:ff:11:63:95:b:b:b:b:21:21:21:21:8:dc:e8:48:0:0:0:0:6:0
  Encap Length: 30, Encap Type: MCP_ET_TUNNEL, MTU: 1470
  Flags: no-l3-inject
  Incomplete behavior type: None
  Fixup: gre
  Fixup_Flags_2: pmip-udp
  Nexthop addr: 33.33.33.33
  IP FRR MCP_ADJ_IPFRR_NONE 0
  OM handle: 0x4217013c
```

Displays platform software adjacency route processor information for the specified platform allocated index.

Step 11 **show ip interface brief**

Example:

```
Device(source gateway)# show ip interface brief

  Interface              IP-Address      OK? Method Status                Protocol
    Tunnel1                3.3.3.3         YES TFTP   up                    up
    ....
```

The above output indicates that the relay has no connection from a gateway. The AMT relay interface will be up after it is correctly configured. If the output displays Protocol "down", you must check your configuration. If the interface command shows **administratively down**, you have not configured the "no shut" in the interface.

Displays errors in AMT gateway configuration.

Displaying and Verifying AMT Gateway Configuration

SUMMARY STEPS

1. **enable**
2. **show ip amt tunnel**
3. **show ip mroute section** [**group-address**]
4. **show ipv6 mroute section** [**group-address**]
5. **show ip mfib section** [**group-address**]
6. **show ipv6 mfib section** [**group-address**]
7. **show platform software adjacency rp active index** *platform-allocated-index-value*
8. **show ip interface brief**

DETAILED STEPS

Step 1 **enable**

Example:
```
Device> enable
```
Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **show ip amt tunnel**

Example:
```
Device(destination gateway)# show ip amt tunnel

AMT Gateway tunnel Tunnel1:
       Local address       UDP port
            5.5.5.5           54358(0xD456)
       Remote address
            3.3.3.3           2268 (0x8DC )

  Total active Relays: 1
Device(source gateway)# show ip amt tunnel
AMT Relay tunnel:
      Local address       UDP port
        3.3.3.3           2268 (0x8DC )
      Remote address                      Expire time
        5.5.5.5           54358(0xD456)   00:03:53
      Connected to 1 Gateway
```
The above output is displayed if both relay and gateway is working correctly.

Displays AMT gateway configuration.

Step 3 **show ip mroute section** [**group-address**]

Example:
```
Device# show ip mroute section 232.1.1.1

(101.0.0.2, 232.1.1.1), 2d00h/00:02:54, flags: sTI
  Incoming interface: Tunnel10, RPF nbr 0.0.0.0, Mroute
```

```
  Outgoing interface list:
    GigabitEthernet0/0/4, Forward/Sparse, 2d00h/00:02:54
```

Displays information about the IP multicast routing (mroute) table for the specified multicast group.

Step 4 **show ipv6 mroute section** [**group-address**]

Example:

```
Device# show ipv6 mroute section 232.1.1.1

(2011::101:0:0:2, FF3F::232:1:1:1), 2d00h/never, flags: sTI
  Incoming interface: Tunnel10
  RPF nbr: ::
  Immediate Outgoing interface list:
    GigabitEthernet0/0/4, Forward, 2d00h/never
```

Displays information about the IPv6 mroute table for the specified multicast group.

Step 5 **show ip mfib section** [**group-address**]

Example:

```
Device# show ip mfib section 232.1.1.1

(101.0.0.2,232.1.1.1) Flags: HW
   SW Forwarding: 0/0/0/0, Other: 0/0/0
   HW Forwarding:   NA/NA/NA/NA, Other: NA/NA/NA
   Tunnel10 Flags: A
   GigabitEthernet0/0/4 Flags: F NS
     Pkts: 0/0
```

Displays the entries and interfaces in the IPv4 Multicast Forwarding Information Base (MFIB) for the specified multicast group.

Step 6 **show ipv6 mfib section** [**group-address**]

Example:

```
Device# show ipv6 mfib section 232.1.1.1

(2011::101:0:0:2,FF3F::232:1:1:1) Flags: HW
   SW Forwarding: 0/0/0/0, Other: 0/0/0
   HW Forwarding:   NA/NA/NA/NA, Other: NA/NA/NA
   Tunnel10 Flags: A
   GigabitEthernet0/0/4 Flags: F NS
     Pkts: 0/0
```

Displays the entries and interfaces in the IPv6 Multicast Forwarding Information Base (MFIB) for the specified multicast group.

Step 7 **show platform software adjacency rp active index** *platform-allocated-index-value*

Example:

```
Device# show platform software adjacency rp active index 0x57

Number of adjacency objects: 19
Adjacency id: 0xf8000126 (4160749862)
  Interface: Tunnel10, IF index: 18, Link Type: MCP_LINK_IP
  Encap: 45:0:0:0:0:0:0:0:ff:11:63:95:21:21:21:21:b:b:b:b:e8:48:8:dc:0:0:0:0:6:0
  Encap Length: 30, Encap Type: MCP_ET_TUNNEL, MTU: 1470
  Incomplete behavior type: None
  Fixup: gre
  Fixup_Flags_2: pmip-udp
  IP FRR MCP_ADJ_IPFRR_NONE 0
  OM handle: 0x4216aaf4
```

Displays platform software adjacency route processor information for the specified platform allocated index.

Step 8 **show ip interface brief**

Example:

```
Device(destination gateway)# show ip interface brief

  Interface              IP-Address      OK? Method Status                Protocol
  Tunnel1                5.5.5.5         YES TFTP   up                    down
```

The Protocol: down displayed in the above output indicates that the gateway has no connection to the relay. If the interface command shows **administratively down**, you have not configured the "no shut" in the interface. If the command displays UNKNOWN but Protocol shows "up", then the gateway did have a connection to the relay hat was terminated.

Note It takes a few minutes before a gateway will consider a relay to be unreachable after not receiving packets from it. The gateway will then revert trying to reach the anycast address to find a new relay (in case the existing relay is down).

Displays errors in AMT gateway configuration.

Configuration Examples for Automatic Multicast Tunneling

Example: AMT Relay Configuration

The following example shows how to configure AMT relay:

```
enable
configure terminal
interface Tunnel10
 ip address 11.1.1.1 255.255.255.0
 no ip redirects
 ip pim sparse-mode
 ip igmp version 3
 ipv6 enable
 tunnel source Loopback0
 tunnel mode udp multipoint
 tunnel dst-port dynamic
 tunnel src-port dynamic
 amt relay traffic ip
 amt relay traffic ipv6
exit

ip multicast-routing distributed
ipv6 multicast-routing
ip pim ssm default
end
```

Example: AMT Gateway Configuration

The following example shows how to configure AMT gateway:

```
enable
configure terminal
interface Tunnel10
 ip address 33.1.1.1 255.255.255.0
 ip pim passive
 ip igmp version 3
 ipv6 enable
 ipv6 pim passive
 tunnel source Loopback0
 tunnel mode udp ip
```

```
 tunnel destination dynamic
 tunnel dst-port dynamic
 tunnel src-port dynamic
 amt gateway traffic ip
 amt gateway traffic ipv6
 amt gateway relay-address 167.3.0.1
exit

ip multicast-routing distributed
ipv6 multicast-routing
ip pim ssm default
ipv6 multicast pim-passive-enable
ip route 101.0.0.2 255.255.255.255 Tunnel10 multicast
ipv6 route 2011::101:0:0:2/128 Tunnel10 multicast
end
```

Additional References for Automatic Multicast Tunneling

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IP Multicast commands	Cisco IOS IP Multicast Command Reference

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Automatic Multicast Tunneling

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 9: Feature Information for Automatic Multicast Tunneling

Feature Name	Releases	Feature Information
Automatic Multicast Tunneling	Cisco IOS XE Release 3.15S	Automatic Multicast Tunneling (AMT) provides a method to tunnel multicast data over a unicast network. The tunneling is performed between AMT relays and AMT gateways, using User Datagram Protocol (UDP) encapsulation. In Cisco IOS XE Release 3.15S, this feature was introduced on Cisco ASR 1000 Series Aggregation Services Routers. The following commands were introduced or modified by this feature: **amt gateway traffic ip**, **amt gateway traffic ipv6**, **amt gateway relay-address**, **amt relay traffic ip**, **amt relay traffic ipv6**, **show ip amt tunnel**, **show ip amt vrf**, **show ipv mfib detail**, **show ipv6 mfib detail**, **show ip mroute detail**, **show ipv6 mroute detail**, **show platform software adjacency fp active**, **show platform software adjacency rp active**, **show platform software ip rp active mfib**, **show platform software ip fp active mfib**, **show platform software ipv6 rp active mfib**, **show platform software ipv6 fp active mfib**, **show platform software mlist**.

CHAPTER 10

BFD Support for Multicast (PIM)

This module contains information for enabling the Bidirectional Forwarding Detection (BFD) detection protocol on Protocol Independent Multicast (PIM) interfaces in your IP v4 and IPv6 network. Enabling PIM BFD enables PIM to use BFD's quicker adjacent system failure detection and avoid the slower query-interval in its own detection mechanisms.

- Restrictions for BFD Support for Multicast (PIM), page 201
- Information About BFD Support for Multicast (PIM), page 201
- How to Configure BFD Support for Multicast (PIM), page 202
- Configuration Examples for BFD Support for Multicast (PIM), page 204
- Additional References for BFD Support for Multicast (PIM), page 204
- Feature Information for BFD Support for Multicast (PIM), page 204

Restrictions for BFD Support for Multicast (PIM)

- This feature is not supported for Multicast VPN (MVPN).
- This feature is supported only on interfaces on which both PIM and BFD are supported.

Information About BFD Support for Multicast (PIM)

PIM BFD

Bidirectional Forwarding Detection (BFD) is a detection protocol designed to provide fast forwarding path failure detection times for all media types, encapsulations, topologies, and routing protocols and independent of the higher layer protocols. In addition to fast forwarding path failure detection, BFD provides a consistent failure detection method for network administrators. Because the network administrator can use BFD to detect forwarding path failures at a uniform rate, rather than the variable rates for different routing protocol hello mechanisms, network profiling and planning is easier and reconvergence time is consistent and predictable.

Protocol Independent Multicast (PIM) uses a hello mechanism for discovering new neighbors and for detecting failures between adjacent nodes. The minimum failure detection time in PIM is 3 times the PIM Query-Interval. To enable faster failure detection, the rate at which a PIM Hello message is transmitted on an interface is configurable. However, lower intervals increase the load on the protocol and can increase CPU and memory utilization and cause a system-wide negative impact on performance. Lower intervals can also cause PIM neighbors to expire frequently as the neighbor expiry can occur before the hello messages received from those neighbors are processed.

The BFD Support for Multicast (PIM) feature, also known as PIM BFD, registers PIM as a client of BFD. PIM can then utilize BFD to initiate a session with an adjacent PIM node to support BFD's fast adjacency failure detection in the protocol layer. PIM registers just once for both PIM and IPv6 PIM.

At PIMs request (as a BFD client), BFD establishes and maintains a session with an adjacent node for maintaining liveness and detecting forwarding path failure to the adjacent node. PIM hellos will continue to be exchanged between the neighbors even after BFD establishes and maintains a BFD session with the neighbor. The behavior of the PIM hello mechanism is not altered due to the introduction of this feature.

Although PIM depends on the Interior Gateway Protocol (IGP) and BFD is supported in IGP, PIM BFD is independent of IGP's BFD.

How to Configure BFD Support for Multicast (PIM)

Enabling BFD PIM on an Interface

Before You Begin

- For IPv4 networks, IP multicast must be enabled and Protocol Independent Multicast (PIM)must be configured on the interface. For information, see the “Configuring Basic IP Multicast in IPv4 Networks” module of the *IP Multicast: PIM Configuration Guide*.
- For IPv6 networks, IPv6 multicast must be enabled and Protocol Independent Multicast (PIM) must be configured on the interface. For information, see the *IP Multicast: PIM Configuration Guide*.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface***type number*
4. **bfd interval** *milliseconds* **min_rx** *milliseconds* **multiplier** *interval-multiplier*
5. Use one of the following:
   - **ip pim bfd**
   - **ipv6 pim bfd**
6. Repeat the preceding steps for each interface to be enabled for BFD PIM.
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface***type number* **Example:** `Device(config)# interface fastethernet 1/6`	Enters interface configuration mode for the specified interface.
Step 4	**bfd interval** *milliseconds* **min_rx** *milliseconds* **multiplier** *interval-multiplier* **Example:** `Device(config-if)# bfd interval 500 min_rx 500 multiplier 5`	Enables BFD on the interface.

Step 5	Use one of the following:
	• **ip pim bfd**
	• **ipv6 pim bfd**
	
	Example:
	`Device(config-if)# ip pim bfd`
	`Device(config-if)# ipv6 pim bfd`
		Enables PIM BFD on the interface.

Step 6	Repeat the preceding steps for each interface to be enabled for BFD PIM.	
Step 7	**end** **Example:** `Device(config-if)# end`	Exits to privileged EXEC mode .

Configuration Examples for BFD Support for Multicast (PIM)

Additional References for BFD Support for Multicast (PIM)

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
IP multicast commands	Cisco IOS IP Multicast Command Reference
Bidirectional Forwarding Detection (BFD) detection protocol	*IP Routing BFD Configuration Guide*
Protocol Independent Multicast (PIM) in an IPv4 network	"Configuring Basic IP Multicast in IPv4 Networks" module of the *IP Multicast: PIM Configuration Guide*
PIM in an IPv6 network	*IP Multicast: PIM Configuration Guide*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for BFD Support for Multicast (PIM)

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 10: Feature Information for BFD Support for Multicast (PIM)

Feature Name	Releases	Feature Information
BFD Support for Multicast (PIM)	Cisco IOS Release 15.4(1)T	This feature enables multicast PIM to use BFD's quicker adjacent system failure detection and avoid the slower query-interval in its own detection mechanisms. The following commands were introduced or modified: **ip pim bfd**, **ipv6 pim bfd**, **show ip pim**, **show ipv6 pim interface**.

CHAPTER 11

HSRP Aware PIM

This module describes how to configure the HSRP Aware PIM feature for enabling multicast traffic to be forwarded through the Hot Standby Router Protocol (HSRP) active router (AR), allowing Protocol Independent Multicast (PIM) to leverage HSRP redundancy, avoid potential duplicate traffic, and enable failover.

- Finding Feature Information, page 207
- Restrictions for HSRP Aware PIM, page 207
- Information About HSRP Aware PIM, page 208
- How to Configure HSRP Aware PIM, page 209
- Configuration Examples for HSRP Aware PIM, page 212
- Additional References for HSRP Aware PIM, page 213
- Feature Information for HSRP Aware PIM, page 214

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for HSRP Aware PIM

- HSRP IPv6 is not supported.
- Stateful failover is not supported. During PIM stateless failover, the HSRP group's virtual IP address transfers to the standby router but no mrouting sate information is transferred. PIM listens and responds to state change events and creates mroute states upon failover.
- The maximum number of HSRP groups that can be tracked by PIM on each interface is 16.

- The redundancy priority for a PIM DR must be greater than the configured or default value (1) of the PIM DR priority on any device for which the same HSRP group is enabled or the HSRP Active will fail to win the DR election.
- Dense mode is not supported.

Information About HSRP Aware PIM

HSRP

Hot Standby Router Protocol (HSRP) is a Cisco proprietary redundancy protocol for establishing a fault-tolerant default gateway.

The protocol establishes a framework between network devices in order to achieve default gateway failover if the primary gateway becomes inaccessible. By sharing an IP address and a MAC (Layer 2) address, two or more devices can act as a single virtual router. The members of a virtual router group continually exchange status messages and one device can assume the routing responsibility of another, should it go out of commission for either planned or unplanned reasons. Hosts continue to forward IP packets to a consistent IP and MAC addres,s and the changeover of devices doing the routing is transparent.

HSRP is useful for hosts that do not support a router discovery protocol and cannot switch to a new device when their selected device reloads or loses power. Because existing TCP sessions can survive the failover, this protocol also provides a more transparent recovery for hosts that dynamically choose a next hop for routing IP traffic.

When HSRP is configured on a network segment, it provides a virtual MAC address and an IP address that is shared among a group of devices running HSRP. The address of this HSRP group is referred to as the virtual IP address. One of these devices is selected by the protocol to be the active router (AR). The AR receives and routes packets destined for the MAC address of the group.

HSRP uses a priority mechanism to determine which HSRP configured device is to be the default AR. To configure a device as the AR, you assign it a priority that is higher than the priority of all the other HSRP-configured devices. The default priority is 100, so if you configure just one device to have a higher priority, that device will be the default AR.

Devices that are running HSRP send and receive multicast User Datagram Protocol (UDP)-based hello messages to detect device failure and to designate active and standby devices. When the AR fails to send a hello message within a configurable period of time, the standby device with the highest priority becomes the AR. The transition of packet forwarding functions between devices is completely transparent to all hosts on the network.

You can configure multiple Hot Standby groups on an interface, thereby making fuller use of redundant devices and load sharing.

HSRP is not a routing protocol as it does not advertise IP routes or affect the routing table in any way.

HSRP has the ability to trigger a failover if one or more interfaces on the device fail. This can be useful for dual branch devices each with a single serial link back to the head end. If the serial link of the primary device goes down, the backup device takes over the primary functionality and thus retains connectivity to the head end.

HSRP Aware PIM

Protocol Independent Multicast (PIM) has no inherent redundancy capabilities and its operation is completely independent of Hot Standby Router Protocol (HSRP) group states. As a result, IP multicast traffic is forwarded not necessarily by the same device as is elected by HSRP. The HSRP Aware PIM feature provides consistent IP multicast forwarding in a redundant network with virtual routing groups enabled.

HSRP Aware PIM enables multicast traffic to be forwarded through the HSRP active router (AR), allowing PIM to leverage HSRP redundancy, avoid potential duplicate traffic, and enable failover, depending on the HSRP states in the device. The PIM designated router (DR) runs on the same gateway as the HSRP AR and maintains mroute states.

In a multiaccess segment (such as LAN), PIM DR election is unaware of the redundancy configuration, and the elected DR and HSRP AR may not be the same router. In order to ensure that the PIM DR is always able to forward PIM Join/Prune message towards RP or FHR, the HSRP AR becomes the PIM DR (if there is only one HSRP group). PIM is responsible for adjusting DR priority based on the group state. When a failover occurs, multicast states are created on the new AR elected by the HSRP group and the AR assumes responsibility for the routing and forwarding of all the traffic addressed to the HSRP virtual IP address.

With HSRP Aware PIM enabled, PIM sends an additional PIM Hello message using the HSRP virtual IP addresses as the source address for each active HSRP group when a device becomes HSRP Active. The PIM Hello will carry a new GenID in order to trigger other routers to respond to the failover. When a downstream device receives this PIM Hello, it will add the virtual address to its PIM neighbor list. The new GenID carried in the PIM Hello will trigger downstream routers to resend PIM Join messages towards the virtual address. Upstream routers will process PIM Join/Prunes (J/P) based on HSRP group state.

If the J/P destination matches the HSRP group virtual address and if the destination device is in HSRP active state, the new AR processes the PIM Join because it is now the acting PIM DR. This allows all PIM Join/Prunes to reach the HSRP group virtual address and minimizes changes and configurations at the downstream routers side.

The IP routing service utilizes the existing virtual routing protocol to provide basic stateless failover services to client applications, such as PIM. Changes in the local HSRP group state and standby router responsibility are communicated to interested client applications. Client applications may build on top of IRS to provide stateful or stateless failover. PIM, as an HSRP client, listens to the state change notifications from HSRP and automatically adjusts the priority of the PIM DR based on the HSRP state. The PIM client also triggers communication between upstream and downstream devices upon failover in order to create an mroute state on the new AR.

How to Configure HSRP Aware PIM

Configuring an HSRP Group on an Interface

Before You Begin

- IP multicast must already be configured on the device.
- PIM must already be configured on the interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number* [*name-tag*]
4. **ip address** *ip-address mask*
5. **standby** [*group-number*] **ip** [*ip-address* [*secondary*]]
6. **standby** [*group-number*] **timers** [**msec**] *hellotime* [**msec**] *holdtime*
7. **standby** [*group-number*] **priority** *priority*
8. **standby** [*group-number*] **name** *group-name*
9. **end**
10. **show standby** [*type number* [*group*]] [**all** | **brief**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* [*name-tag*] **Example:** `Device(config)# interface ethernet 0/0`	Specifies an interface to be configured and enters interface configuration mode.
Step 4	**ip address** *ip-address mask* **Example:** `Device(config-if)# ip address 10.0.0.2 255.255.255.0`	Sets a primary or secondary IP address for an interface.
Step 5	**standby** [*group-number*] **ip** [*ip-address* [*secondary*]] **Example:** `Device(config-if)# standby 1 ip 192.0.2.99`	Activates HSRP and defines an HRSP group.
Step 6	**standby** [*group-number*] **timers** [**msec**] *hellotime* [**msec**] *holdtime* **Example:** `Device(config-if)# standby 1 timers 5 15`	(Optional) Configures the time between hello packets and the time before other devices declare an HSRP active or standby router to be down.

	Command or Action	Purpose
Step 7	**standby** [*group-number*] **priority** *priority* **Example:** `Device(config-if)# standby 1 priority 120`	(Optional) Assigns the HSRP priority to be used to help select the HSRP active and standby routers.
Step 8	**standby** [*group-number*] **name** *group-name* **Example:** `Device(config-if)# standby 1 name HSRP1`	(Optional) Defines a name for the HSRP group. **Note** We recommend that you always configure the **standby ip name** command when configuring an HSRP group to be used for HSRP Aware PIM.
Step 9	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.
Step 10	**show standby** [*type number* [*group*]] [**all** | **brief**] **Example:** `Device# show standby`	Displays HSRP group information for verifying the configuration.

Configuring PIM Redundancy

Before You Begin

The HSRP group must already be configured on the interface. See the “Configuring an HSRP Group on an Interface” section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number* [*name-tag*]
4. **ip address** *ip-address mask*
5. **ip pim redundancy** *group* **dr-priority** *priority*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Device> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* [*name-tag*] **Example:** `Device(config)# interface ethernet 0/0`	Specifies an interface to be configured and enters interface configuration mode.
Step 4	**ip address** *ip-address mask* **Example:** `Device(config-if)# ip address 10.0.0.2 255.255.255.0`	Sets a primary or secondary IP address for an interface.
Step 5	**ip pim redundancy** *group* **dr-priority** *priority* **Example:** `Device(config-if)# ip pim redundancy HSRP1 dr-priority 60`	Enables PIM redundancy and assigns a redundancy priority value to the active PIM designated router (DR). • Because HSRP group names are case sensitive, the value of the *group* argument must match the group name configured by using the **standby ip name** command. • The redundancy priority for a PIM DR must be greater than the configured or default value (1) of the PIM DR priority on any device for which the same HSRP group is enabled.
Step 6	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.

Configuration Examples for HSRP Aware PIM

Example: Configuring an HSRP Group on an Interface

```
interface ethernet 0/0
 ip address 10.0.0.2 255.255.255.0
 standby 1 ip 192.0.2.99
 standby 1 timers 5 15
 standby 1 priority 120
 standby 1 name HSRP1
```

```
 !
!
```

Example: Configuring PIM Redundancy

```
interface ethernet 0/0
 ip address 10.0.0.2 255.255.255.0
 ip pim redundancy HSRP1 dr-priority 60
 !
!
```

Additional References for HSRP Aware PIM

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IP multicast commands	Cisco IOS IP Multicast Command Reference
HSRP commands	First Hop Redundancy Protocol Command Reference

Standards and RFCs

Standard/RFC	Title
RFC 2281	*Cisco Hot Standby Router Protocol (HSRP)*

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for HSRP Aware PIM

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 11: Feature Information for HSRP Aware PIM

Feature Name	Releases	Feature Information
HSRP Aware PIM	15.2(4)S 15.3(1)T 15.3(1)SY1 15.2(1)E	The HSRP Aware PIM feature provides consistent IP multicast forwarding in a redundant network with virtual routing groups by enabling multicast traffic to be forwarded through a Hot Standby Router Protocol (HSRP) active router, allowing PIM to leverage HSRP redundancy, avoid potential duplicate traffic, and enable failover, depending on the HSRP states in the device.

CHAPTER 12

VRRP Aware PIM

The Virtual Router Redundancy Protocol (VRRP) eliminates the single point of failure inherent in the static default routed environment. VRRP is an election protocol that dynamically assigns responsibility for one or more virtual routers to the VRRP routers on a LAN, allowing several routers on a multi access link to utilize the same virtual IP address.

VRRP Aware PIM is a redundancy mechanism for the Protocol Independent Multicast (PIM) to interoperate with VRRP. It allows PIM to track VRRP state and to preserve multicast traffic upon fail over in a redundant network with virtual routing groups enabled.

This module explains how to configure VRRP Aware PIM in a network.

- Finding Feature Information, page 215
- Restrictions for VRRP Aware PIM, page 216
- Information About VRRP Aware PIM, page 216
- How to Configure VRRP Aware PIM, page 217
- Configuration Examples for VRRP Aware PIM, page 219
- Additional References for VRRP Aware PIM, page 219
- Feature Information for VRRP Aware PIM, page 220

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for VRRP Aware PIM

- Only PIM sparse mode (SM) and source specific multicast (SSM) modes are supported. Bidirectional (BiDir) PIM is not supported.
- PIM interoperability with Hot Standby Router Protocol (HSRP) IPv6 is not supported.
- PIM tracks only one virtual group, either Virtual Router Redundancy Protocol (VRRP) or HSRP, per interface.
- VRRP Aware PIM is not supported on a Transit network. PIM redundancy enabled interface does not support the PIM joining the network from down stream.

Information About VRRP Aware PIM

Overview of VRRP Aware PIM

Virtual Router Redundancy Protocol (VRRP) is a redundancy protocol for establishing a fault-tolerant default gateway. The protocol establishes a framework between network devices in order to achieve default gateway failover if the primary gateway becomes inaccessible.

Protocol Independent Multicast (PIM) has no inherent redundancy capabilities and its operation is completely independent of VRRP group states. As a result, IP multicast traffic is forwarded not necessarily by the same device as is elected by VRRP. The VRRP Aware PIM feature provides consistent IP multicast forwarding in a redundant network with virtual routing groups enabled.

In a multi-access segment (such as LAN), PIM designated router (DR) election is unaware of the redundancy configuration, and the elected DR and VRRP master router (MR) may not be the same router. In order to ensure that the PIM DR is always able to forward PIM Join/Prune message towards RP or FHR, the VRRP MR becomes the PIM DR (if there is only one VRRP group). PIM is responsible for adjusting DR priority based on the group state. When a fail over occurs, multicast states are created on the new MR elected by the VRRP group and the MR assumes responsibility for the routing and forwarding of all the traffic addressed to the VRRP virtual IP address. This ensures the PIM DR runs on the same gateway as the VRRP MR and maintains mroute states. It enables multicast traffic to be forwarded through the VRRP MR, allowing PIM to leverage VRRP redundancy, avoid potential duplicate traffic, and enable fail over, depending on the VRRP states in the device.

Virtual Router Redundancy Service (VRRS) provides public APIs for a client to communicate with VRRP. VRRP Aware PIM is a feature of VRRS that supports VRRPv3 (unified VRRP) in both IPv4 and IPv6.

PIM, as a VRRS client, uses the VRRS client API to obtain generic First Hop Redundancy Protocol (FHRP) state and configuration information in order to provide multicast redundancy functionalities.

PIM performs the following as a VRRS client:

- Listens to state change and update notification from VRRS server (i.e., VRRP).
- Automatically adjust PIM DR priority based on VRRP state.
- Upon VRRP fail over, PIM receives state change notification from VRRS for the tracked VRRP group and ensures traffic is forwarded through VRRP MR.

How to Configure VRRP Aware PIM

Configuring VRRP Aware PIM

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **fhrp version vrrp** *version*
4. **interface** *type number*
5. **ip address** *address*
6. **vrrp** *group id* **address-family ipv4**
7. **vrrs leader** *group name*
8. **vrrp** *group id* **ip** *ip address*
9. **exit**
10. **interface** *type number*
11. **ip pim redundancy** *group name* **vrrp dr-priority** *priority-value*
12. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**fhrp version vrrp** *version* **Example:** `Device(config)# fhrp version vrrp v3`	Enables the ability to configure VRRPv3 and VRRS.
Step 4	**interface** *type number* **Example:** `Device(config)# interface Ethernet0/0`	Specifies an interface to be configured and enters interface configuration mode.

	Command or Action	Purpose
Step 5	**ip address** *address* **Example:** `Device(config-if)# ip address 192.0.2.2`	Specifies a primary or secondary address for the VRRP group.
Step 6	**vrrp** *group id* **address-family ipv4** **Example:** `Device(config-if)# vrrp 1 address-family ipv4`	Creates a VRRP group and enters VRRP configuration mode.
Step 7	**vrrs leader** *group name* **Example:** `Device(config-if-vrrp)# vrrs leader VRRP1`	Enables community and (or) extended community exchange with the specified neighbor.
Step 8	**vrrp** *group id* **ip** *ip address* **Example:** `Device(config-if-vrrp)# vrrp 1 ip 10.1.6.1`	Exits address family configuration mode and returns to router configuration mode.
Step 9	**exit** **Example:** `Device(config-if-vrrp)# exit`	Exits VRRP configuration mode and returns to global configuration mode.
Step 10	**interface** *type number* **Example:** `Device(config)# interface Ethernet0/0`	Specifies an interface to be configured and enters interface configuration mode.
Step 11	**ip pim redundancy** *group name* **vrrp dr-priority** *priority-value* **Example:** `Device(config-if)# ip pim redundancy VRRP1 vrrp dr-priority 90`	sets the priority for which a router is elected as the designated router (DR). • The redundancy dr-priority value should be same on all routers that are enabled with VRRP Aware PIM feature.
Step 12	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Configuration Examples for VRRP Aware PIM

Example: VRRP Aware PIM

```
conf terminal
 fhrp version vrrp v3
interface Ethernet0/0
 ip  address 192.0.2.2
 vrrp 1 address-family ipv4

 vrrp 1 ip 10.1.6.1

 vrrs leader VRRP1
interface Ethernet0/0
 ip pim redundancy VRRP1 vrrp  dr-priority 90
 !
```

Additional References for VRRP Aware PIM

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IP multicast commands	Cisco IOS IP Multicast Command Reference
Configuring VRRP	First Hop Redundancy Protocols Configuration Guide
IP multicast PIM	IP Multicast: PIM Configuration Guide

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for VRRP Aware PIM

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 12: Feature Information for VRRP Aware PIM

Feature Name	Releases	Feature Information
VRRP Aware PIM	Cisco IOS XE Release 3.10S	VRRP Aware PIM is a redundancy mechanism for the Protocol Independent Multicast (PIM) to interoperate with VRRP. It allows PIM to track VRRP state and to preserve multicast traffic upon failover in a redundant network with virtual routing groups enabled. No commands were introduced or modified.

CHAPTER 13

Verifying IP Multicast Operation

This module describes how to verify IP multicast operation in a network after Protocol Independent Multicast (PIM) sparse mode (PIM-SM) or Source Specific Multicast (PIM-SSM) has been implemented. The tasks in this module can be used to test IP multicast reachability and to confirm that receivers and sources are operating as expected in an IP multicast network.

- Finding Feature Information, page 221
- Prerequisites for Verifying IP Multicast Operation, page 221
- Restrictions for Verifying IP Multicast Operation, page 222
- Information About Verifying IP Multicast Operation, page 222
- How to Verify IP Multicast Operation, page 225
- Configuration Examples for Verifying IP Multicast Operation, page 233
- Additional References, page 238
- Feature Information for Verifying IP Multicast Operation, page 239

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Verifying IP Multicast Operation

- Before performing the tasks in this module, you should be familiar with the concepts described in the " IP Multicast Technology Overview " module.

- The tasks in this module assume that IP multicast has been enabled and that PIM-SM or SSM has been configured using the relevant tasks described in the " Configuring Basic IP Multicast " module.

Restrictions for Verifying IP Multicast Operation

- For PIM-SM, this module assumes that the shortest path tree (SPT) threshold for PIM-enabled routers is set to the value of zero (the default) and not infinity. For more information about setting the SPT threshold, see the **ip pim spt-threshold** command page in the *Cisco IOS IP Multicast Command Reference*.
- Verifying IP multicast operation in a bidirectional PIM (bidir-PIM) network or a PIM-SM network with a finite or infinite SPT threshold is outside the scope of this module.

Information About Verifying IP Multicast Operation

Guidelines for Verifying IP Multicast Operation in a PIM-SM and PIM-SSM Network Environment

When you verify the operation of IP multicast in a PIM-SM network environment or in an PIM-SSM network environment, a useful approach is to begin the verification process on the last hop router, and then continue the verification process on the routers along the SPT until the first hop router has been reached. The goal of the verification is to ensure that IP multicast traffic is being routed properly through an IP multicast network.

Common Commands Used to Verify IP Multicast Operation on the Last Hop Router for PIM-SM and PIM-SSM

The table describes the common commands used to verify IP multicast operation on the last hop router in PIM-SM and PIM-SSM network environments.

Table 13: Common IP Multicast Verification Commands (Last Hop Router)

Command	Description and Purpose
show ip igmp groups	Displays the multicast groups with receivers that are directly connected to the router and that were learned through the Internet Group Management Protocol (IGMP). • Use this command to confirm that the IGMP cache is being properly populated on the last hop router for the groups that receivers on the LAN have joined.

Command	Description and Purpose
show ip pim rp mapping	Displays all group-to-RP mappings of which the router is aware (either configured or learned from Auto-RP or BSR). • Use this command to confirm that the group-to-RP mappings are being populated correctly on the last hop router. **Note** The **show ip pim rp mapping**command does not work with routers in a PIM-SSM network because PIM-SSM does not use rendezvous points (RPs).
show ip mroute	Displays the contents of the multicast routing (mroute) table. • Use this command to verify that the mroute table is being populated properly on the last hop router.
show ip interface	Displays information and statistics about configured interfaces. • Use this command to verify that IP multicast fast switching is enabled on the outgoing interface on the last hop router.
show ip mfib	Displays the forwarding entries and interfaces in the IP Multicast Forwarding Information Base (MFIB).
show ip pim interface count	Displays statistics related to the number of multicast packets received by and sent out a PIM-enabled interface. • Use this command on the last hop router to confirm that multicast traffic is being forwarded on the last hop router.
show ip mroute active	Displays the rate that active sources are sending to multicast groups, in kilobits per second (kb/s). • Use this command to display information about the multicast packet rate for active sources sending to groups on the last hop router.

Command	Description and Purpose
show ip mroute count	Displays statistics related to mroutes in the mroute table. • Use this command on the last hop router to confirm that multicast traffic is flowing on the last hop router.

Common Commands Used to Verify IP Multicast Operation on Routers Along the SPT for PIM-SM and PIM-SSM

The table describes the common commands used to verify IP multicast operation on routers along the SPT in PIM-SM and PIM-SSM network environments.

Table 14: Common IP Multicast Verification Commands (Routers Along SPT)

Command	Description and Purpose
show ip mroute	Displays the contents of the mroute table. • Use this command to confirm that the Reverse Path Forwarding (RPF) neighbor toward the source is the expected RPF neighbor for each router along the SPT.
show ip mroute active	Displays the rate that active sources are sending to multicast groups, in kb/s. • Use this command to display information about the multicast packet rate for active sources sending to groups on routers along the SPT.

Common Commands Used to Verify IP Multicast Operation on the First Hop Router for PIM-SM and PIM-SSM

The table describes the common commands used to verify IP multicast operation on the first hop router in PIM-SM and PIM-SSM network environments.

Table 15: Common IP Multicast Verification Commands (First Hop Router)

Command	Description and Purpose
show ip mroute	Displays the contents of the mroute table. • Use this command to confirm that the F flag is set for the mroutes on the first hop router.

Command	Description and Purpose
show ip mroute active	Displays the rate that active sources are sending to multicast groups, in kb/s. • Use this command to display information about the multicast packet rate for active sources sending to groups on the first hop router.

How to Verify IP Multicast Operation

Using PIM-Enabled Routers to Test IP Multicast Reachability

If all the PIM-enabled routers and access servers that you administer are members of a multicast group, pinging that group causes all routers to respond, which can be a useful administrative and debugging tool.

To use PIM-enabled routers to test IP multicast reachability, perform the following tasks:

Configuring Routers to Respond to Multicast Pings

Follow these steps to configure a router to respond to multicast pings. Perform the task on all the interfaces of a router and on all the routers participating in the multicast network:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip igmp join-group** *group-address*
5. Repeat Step 3 and Step 4 for each interface on the router participating in the multicast network.
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `SwitchControllerDevice> enable`	Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `SwitchControllerDevice# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `SwitchControllerDevice(config)# interface gigabitethernet 1/0/0`	Enters interface configuration mode. For the *type* and *number* arguments, specify an interface that is directly connected to hosts or is facing hosts.
Step 4	**ip igmp join-group** *group-address* **Example:** `SwitchControllerDevice(config-if)# ip igmp join-group 225.2.2.2`	(Optional) Configures an interface on the router to join the specified group. For the purpose of this task, configure the same group address for the *group-address* argument on all interfaces on the router participating in the multicast network. **Note** With this method, the router accepts the multicast packets in addition to forwarding them. Accepting the multicast packets prevents the router from fast switching.
Step 5	Repeat Step 3 and Step 4 for each interface on the router participating in the multicast network.	--
Step 6	**end** **Example:** `SwitchControllerDevice(config-if)# end`	Ends the current configuration session and returns to privileged EXEC mode.

Pinging Routers Configured to Respond to Multicast Pings

Follow these steps on a router to initiate a ping test to the routers configured to respond to multicast pings. This task is used to test IP multicast reachability in a network.

SUMMARY STEPS

1. **enable**
2. **ping** *group-address*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `SwitchControllerDevice> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**ping** *group-address* **Example:** `SwitchControllerDevice# ping 225.2.2.2`	Pings an IP multicast group address. A successful response indicates that the group address is functioning.

Verifying IP Multicast Operation in a PIM-SM or a PIM-SSM Network

When you verify the operation of IP multicast in a PIM-SM network environment or in an PIM-SSM network environment, a useful approach is to begin the verification process on the last hop router, and then continue the verification process on the routers along the SPT until the first hop router has been reached. The goal of the verification is to ensure that IP multicast traffic is being routed properly through an IP multicast network.

Perform the following optional tasks to verify IP multicast operation in a PIM-SM or a PIM-SSM network. The steps in these tasks help to locate a faulty hop when sources and receivers are not operating as expected.

Note If packets are not reaching their expected destinations, you might want consider disabling IP multicast fast switching, which would place the router in process switching mode. If packets begin reaching their proper destinations after IP multicast fast switching has been disabled, then the issue most likely was related to IP multicast fast switching.

Verifying IP Multicast Operation on the Last Hop Router

Perform the following task to verify the operation of IP multicast on the last hop router.

Note If you are verifying a last hop router in a PIM-SSM network, ignore Step 3.

SUMMARY STEPS

1. **enable**
2. **show ip igmp groups**
3. **show ip pim rp mapping**
4. **show ip mroute**
5. **show ip interface** [*type number*]
6. **show ip mfib**
7. **show ip pim interface count**
8. **show ip mroute count**
9. **show ip mroute active** [*kb/s*]

DETAILED STEPS

Step 1 **enable**

Enables privileged EXEC mode. Enter your password if prompted.

```
SwitchControllerDevice> enable
```

Step 2 **show ip igmp groups**

Use this command to verify IGMP memberships on the last hop router. This information will confirm the multicast groups with receivers that are directly connected to the last hop router and that are learned through IGMP.

The following is sample output from the **show ip igmp groups** command:

Example:

```
Router# show ip igmp groups
IGMP Connected Group Membership
Group Address    Interface                Uptime    Expires   Last Reporter
239.1.2.3        GigabitEthernet1/0/0     00:05:14  00:02:14  10.1.0.6
224.0.1.39       GigabitEthernet0/0/0     00:09:11  00:02:08  172.31.100.1
```

Step 3 **show ip pim rp mapping**

Use this command to confirm that the group-to-RP mappings are being populated correctly on the last hop router.

Note Ignore this step if you are verifying a last hop router in a PIM-SSM network. The **show ip pim rp mapping**command does not work with routers in a PIM-SSM network because PIM-SSM does not use RPs. In addition, if configured correctly, PIM-SSM groups should not appear in the output of the **show ip pim rp mapping**command.

The following is sample output from the **show ip pim rp mapping**command:

Example:

```
Router# show ip pim rp mapping
PIM Group-to-RP Mappings

Group(s) 224.0.0.0/4
  RP 172.16.0.1 (?), v2v1
```

```
    Info source: 172.16.0.1 (?), elected via Auto-RP
         Uptime: 00:09:11, expires: 00:02:47
```

Step 4 **show ip mroute**

Use this command to verify that the mroute table is being populated properly on the last hop router.

The following is sample output from the **show ip mroute** command:

Example:

```
Router# show ip mroute
(*, 239.1.2.3), 00:05:14/00:03:04, RP 172.16.0.1, flags: SJC
  Incoming interface: GigabitEthernet0/0/0, RPF nbr 172.31.100.1
  Outgoing interface list:
  GigabitEthernet1/0, Forward/Sparse-Dense, 00:05:10/00:03:04

(10.0.0.1, 239.1.2.3), 00:02:49/00:03:29, flags: T
  Incoming interface: GigabitEthernet0/0/0, RPF nbr 172.31.100.1
  Outgoing interface list:
  GigabitEthernet1/0, Forward/Sparse-Dense, 00:02:49/00:03:04

(*, 224.0.1.39), 00:10:05/stopped, RP 0.0.0.0, flags: DC
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    GigabitEthernet1/0, Forward/Sparse-Dense, 00:05:15/00:00:00
    GigabitEthernet0/0, Forward/Sparse-Dense, 00:10:05/00:00:00

(172.16.0.1, 224.0.1.39), 00:02:00/00:01:33, flags: PTX
  Incoming interface: GigabitEthernet0/0/0, RPF nbr 172.31.100.1
```

Step 5 **show ip interface** [*type number*]

Use this command to verify that multicast fast switching is enabled for optimal performance on the outgoing interface on the last hop router.

Note Using the **no ip mroute-cache** interface command disables IP multicast fast-switching. When IP multicast fast switching is disabled, packets are forwarded through the process-switched path.

The following is sample output from the **show ip interface**command for a particular interface:

Example:

```
Router# show ip interface GigabitEthernet 0/0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 172.31.100.2/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.1 224.0.0.22 224.0.0.13
      224.0.0.5 224.0.0.6
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is disabled
  IP Fast switching turbo vector
  IP multicast fast switching is enabled
```

```
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Policy routing is disabled
  Network address translation is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
  BGP Policy Mapping is disabled
```

Step 6 **show ip mfib**

Use this command to display the forwarding entries and interfaces in the IP Multicast Forwarding Information Base (MFIB).

Example:

Step 7 **show ip pim interface count**

Use this command to confirm that multicast traffic is being forwarded on the last hop router.

The following is sample output from the **show ip pim interface** command with the **count** keyword:

Example:

```
Router# show ip pim interface count

State: * - Fast Switched, D - Distributed Fast Switched
       H - Hardware Switching Enabled
Address          Interface                FS Mpackets In/Out
172.31.100.2     GigabitEthernet0/0/0     *   4122/0
10.1.0.1         GigabitEthernet1/0/0     *   0/3193
```

Step 8 **show ip mroute count**

Use this command to confirm that multicast traffic is being forwarded on the last hop router.

The following is sample output from the **show ip mroute**command with the **count** keyword:

Example:

```
Router# show ip mroute count
IP Multicast Statistics
6 routes using 4008 bytes of memory
3 groups, 1.00 average sources per group
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
Other counts: Total/RPF failed/Other drops(OIF-null, rate-limit etc)

Group: 239.1.2.3, Source count: 1, Packets forwarded: 3165, Packets received: 3165
  RP-tree: Forwarding: 0/0/0/0, Other: 0/0/0
  Source: 10.0.0.1/32, Forwarding: 3165/20/28/4, Other: 0/0/0

Group: 224.0.1.39, Source count: 1, Packets forwarded: 21, Packets received: 120
  Source: 172.16.0.1/32, Forwarding: 21/1/48/0, Other: 120/0/99

Group: 224.0.1.40, Source count: 1, Packets forwarded: 10, Packets received: 10
  Source: 172.16.0.1/32, Forwarding: 10/1/48/0, Other: 10/0/0
```

Step 9 **show ip mroute active** [*kb/s*]

Use this command on the last hop router to display information about active multicast sources sending traffic to groups on the last hop router. The output of this command provides information about the multicast packet rate for active sources.

Note By default, the output of the **show ip mroute** command with the **active** keyword displays information about active sources sending traffic to groups at a rate greater than or equal to 4 kb/s. To display information about active sources sending low-rate traffic to groups (that is, traffic less than 4 kb/s), specify a value of 1 for the *kb/s* argument. Specifying a value of 1 for this argument displays information about active sources sending traffic to groups at a rate equal to or greater than 1 kb/s, which effectively displays information about all possible active source traffic.

The following is sample output from the **show ip mroute**command with the **active** keyword:

Example:

```
Router# show ip mroute active
Active IP Multicast Sources - sending >= 4 kbps

Group: 239.1.2.3, (?)
   Source: 10.0.0.1 (?)
     Rate: 20 pps/4 kbps(1sec), 4 kbps(last 50 secs), 4 kbps(life avg)
```

Verifying IP Multicast on Routers Along the SPT

Perform the following task to verify the operation of IP multicast on routers along the SPT in a PIM-SM or PIM-SSM network.

SUMMARY STEPS

1. **enable**
2. **show ip mroute** [*group-address*]
3. **show ip mroute active**

DETAILED STEPS

Step 1 **enable**

Enables privileged EXEC mode. Enter your password if prompted.

```
Router> enable
```

Step 2 **show ip mroute** [*group-address*]

Use this command on routers along the SPT to confirm the RPF neighbor toward the source for a particular group or groups.

The following is sample output from the **show ip mroute**command for a particular group:

Example:

```
Router# show ip mroute 239.1.2.3
(*, 239.1.2.3), 00:17:56/00:03:02, RP 172.16.0.1, flags: S
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    GigabitEthernet0/0/0, Forward/Sparse-Dense, 00:17:56/00:03:02

(10.0.0.1, 239.1.2.3), 00:15:34/00:03:28, flags: T
  Incoming interface: Serial1/0, RPF nbr 172.31.200.1
  Outgoing interface list:
    GigabitEthernet0/0/0, Forward/Sparse-Dense, 00:15:34/00:03:02
```

Step 3 **show ip mroute active**

Use this command on routers along the SPT to display information about active multicast sources sending to groups. The output of this command provides information about the multicast packet rate for active sources.

Note By default, the output of the **show ip mroute** command with the **active** keyword displays information about active sources sending traffic to groups at a rate greater than or equal to 4 kb/s. To display information about active sources sending low-rate traffic to groups (that is, traffic less than 4 kb/s), specify a value of 1 for the *kb/s* argument. Specifying a value of 1 for this argument displays information about active sources sending traffic to groups at a rate equal to or greater than 1 kb/s, which effectively displays information about all possible active source traffic.

The following is sample output from the **show ip mroute** command with the **active** keyword:

Example:

```
Router# show ip mroute active
Active IP Multicast Sources - sending >= 4 kbps

Group: 239.1.2.3, (?)
   Source: 10.0.0.1 (?)
     Rate: 20 pps/4 kbps(1sec), 4 kbps(last 30 secs), 4 kbps(life avg)
```

Verifying IP Multicast on the First Hop Router

Perform the following task to verify the operation of IP multicast on the first hop router.

SUMMARY STEPS

1. **enable**
2. **show ip mroute** [*group-address*]
3. **show ip mroute active** [*kb/s*]

DETAILED STEPS

Step 1 **enable**

Enables privileged EXEC mode.

- Enter your password if prompted.

```
Router> enable
```

Step 2 **show ip mroute** [*group-address*]

Use this command on the first hop router to confirm the F flag has been set for mroutes on the first hop router.

The following is sample output from the **show ip mroute**for a particular group:

Example:

```
Router# show ip mroute 239.1.2.3
(*, 239.1.2.3), 00:18:10/stopped, RP 172.16.0.1, flags: SPF
  Incoming interface: Serial1/0, RPF nbr 172.31.200.2
  Outgoing interface list: Null

(10.0.0.1, 239.1.2.3), 00:18:10/00:03:22, flags: FT
  Incoming interface: GigabitEthernet0/0/0, RPF nbr 0.0.0.0
  Outgoing interface list:
    Serial1/0, Forward/Sparse-Dense, 00:18:10/00:03:19
```

Step 3 **show ip mroute active** [*kb/s*]

Use this command on the first hop router to display information about active multicast sources sending to groups. The output of this command provides information about the multicast packet rate for active sources.

Note By default, the output of the **show ip mroute** command with the **active** keyword displays information about active sources sending traffic to groups at a rate greater than or equal to 4 kb/s. To display information about active sources sending low-rate traffic to groups (that is, traffic less than 4 kb/s), specify a value of 1 for the *kb/s* argument. Specifying a value of 1 for this argument displays information about active sources sending traffic to groups at a rate equal to or greater than 1 kb/s, which effectively displays information about all possible active source traffic.

The following is sample output from the **show ip mroute** command with the **active** keyword:

Example:

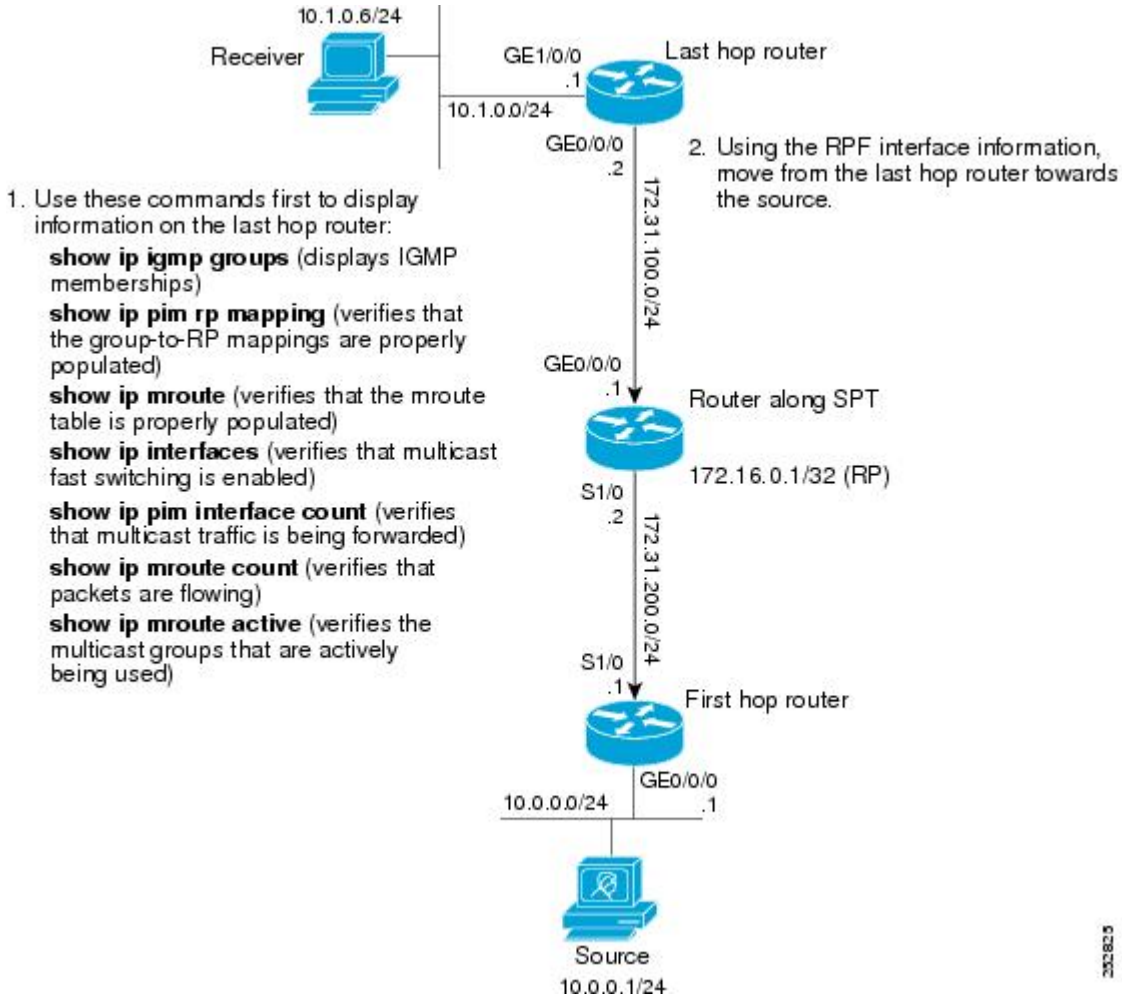
```
Router# show ip mroute active
Active IP Multicast Sources - sending >= 4 kbps

Group: 239.1.2.3, (?)
   Source: 10.0.0.1 (?)
     Rate: 20 pps/4 kbps(1sec), 4 kbps(last 30 secs), 4 kbps(life avg)
```

Configuration Examples for Verifying IP Multicast Operation

Verifying IP Multicast Operation in a PIM-SM or PIM-SSM Network Example

The following example shows how to verify IP multicast operation after PIM-SM has been deployed in a network. The example is based on the PIM-SM topology illustrated in the figure.

From the last hop router to the first hop router shown in the figure, this example shows how to verify IP multicast operation for this particular PIM-SM network topology.



Verifying IP Multicast on the Last Hop Router Example

The following is sample output from the **show ip igmp groups** command. The sample output displays the IGMP memberships on the last hop router shown in the figure. This command is used in this example to confirm that the IGMP cache is being properly populated for the groups that receivers on the LAN have joined.

```
Router# show ip igmp groups
IGMP Connected Group Membership
Group Address    Interface                Uptime    Expires   Last Reporter
239.1.2.3        GigabitEthernet1/0/0     00:05:14  00:02:14  10.1.0.6
224.0.1.39       GigabitEthernet0/0/0     00:09:11  00:02:08  172.31.100.1
```

The following is sample output from the **show ip pim rp mapping**command. In the sample output, notice the RP address displayed for the RP field. Use the RP address and group information to verify that the group-to-RP mappings have been properly populated on the last hop router shown in the figure.

Note In the output, the "(?)" indicates that the router is unable to resolve an IP address to a hostname.

```
Router# show ip pim rp mapping
PIM Group-to-RP Mappings

Group(s) 224.0.0.0/4
  RP 172.16.0.1 (?), v2v1
    Info source: 172.16.0.1 (?), elected via Auto-RP
         Uptime: 00:09:11, expires: 00:02:47
```

The following is sample output from the **show ip mroute** command. This command is used to verify that the mroute table is being properly populated on the last hop router shown in the figure. In the sample output, notice the T flag for the (10.0.0.1, 239.1.2.3) mroute. The T flag indicates that the SPT-bit has been set, which means a multicast packet was received on the SPT tree for this particular mroute. In addition, the RPF nbr field should point toward the RPF neighbor with the highest IP address determined by unicast routing toward the multicast source.

```
Router# show ip mroute
(*, 239.1.2.3), 00:05:14/00:03:04, RP 172.16.0.1, flags: SJC
  Incoming interface: GigabitEthernet0/0/0, RPF nbr 172.31.100.1
  Outgoing interface list:
    Ethernet1/0, Forward/Sparse-Dense, 00:05:10/00:03:04

(10.0.0.1, 239.1.2.3), 00:02:49/00:03:29, flags: T
  Incoming interface: GigabitEthernet0/0/0, RPF nbr 172.31.100.1
  Outgoing interface list:
    Ethernet1/0, Forward/Sparse-Dense, 00:02:49/00:03:04

(*, 224.0.1.39), 00:10:05/stopped, RP 0.0.0.0, flags: DC
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    Ethernet1/0, Forward/Sparse-Dense, 00:05:15/00:00:00
    Ethernet0/0, Forward/Sparse-Dense, 00:10:05/00:00:00
```

The following is sample output from the **show ip interface** command for the incoming interface. This command is used in this example to confirm that IP multicast fast switching is enabled on the last hop router shown in the figure. When IP multicast fast switching is enabled, the line "IP multicast fast switching is enabled" displays in the output.

```
Router# show ip interface GigabitEthernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Internet address is 172.31.100.2/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.1 224.0.0.22 224.0.0.13
      224.0.0.5 224.0.0.6
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is disabled
  IP Fast switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
```

```
  IP route-cache flags are Fast
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Policy routing is disabled
  Network address translation is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
  BGP Policy Mapping is disabled
```

The following is sample output from the **show ip pim interface count** command. This command is used in this example to confirm that multicast traffic is being forwarded to the last hop router shown in the figure. In the sample output, notice the Mpackets In/Out field. This field displays the number of multicast packets received by and sent on each interface listed in the output.

```
Router# show ip pim interface count

State: * - Fast Switched, D - Distributed Fast Switched
       H - Hardware Switching Enabled
Address          Interface                FS Mpackets In/Out
172.31.100.2     GigabitEthernet0/0/0     *   4122/0
10.1.0.1         GigabitEthernet1/0/0     *   0/3193
```

The following is sample output from the **show ip mroute**command with the **count** keyword. This command is used on the last hop router shown in the figure to verify the packets being sent to groups from active sources. In the sample output, notice the packet count displayed for the Forwarding field. This field displays the packet forwarding count for sources sending to groups.

```
Router# show ip mroute count
IP Multicast Statistics
6 routes using 4008 bytes of memory
3 groups, 1.00 average sources per group
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
Other counts: Total/RPF failed/Other drops(OIF-null, rate-limit etc)

Group: 239.1.2.3, Source count: 1, Packets forwarded: 3165, Packets received: 3165
  RP-tree: Forwarding: 0/0/0/0, Other: 0/0/0
  Source: 10.0.0.1/32, Forwarding: 3165/20/28/4, Other: 0/0/0

Group: 224.0.1.39, Source count: 1, Packets forwarded: 21, Packets received: 120
  Source: 172.16.0.1/32, Forwarding: 21/1/48/0, Other: 120/0/99

Group: 224.0.1.40, Source count: 1, Packets forwarded: 10, Packets received: 10
  Source: 172.16.0.1/32, Forwarding: 10/1/48/0, Other: 10/0/0
```

The following is sample output from the **show ip mroute**command with the **active** keyword. This command is used on the last hop router shown in the figure to confirm the multicast groups with active sources on the last hop router.

Note In the output, the “(?)” indicates that the router is unable to resolve an IP address to a hostname.

```
Router# show ip mroute active
Active IP Multicast Sources - sending >= 4 kbps

Group: 239.1.2.3, (?)
   Source: 10.0.0.1 (?)
     Rate: 20 pps/4 kbps(1sec), 4 kbps(last 50 secs), 4 kbps(life avg)
```

Verifying IP Multicast on Routers Along the SPT Example

The following is sample output from the **show ip mroute**for a particular group. This command is used in this example to verify that the RPF neighbor toward the source is the expected RPF neighbor for the router along the SPT shown in the figure.

```
Router# show ip mroute 239.1.2.3
(*, 239.1.2.3), 00:17:56/00:03:02, RP 172.16.0.1, flags: S
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    Ethernet0/0, Forward/Sparse-Dense, 00:17:56/00:03:02

(10.0.0.1, 239.1.2.3), 00:15:34/00:03:28, flags: T
  Incoming interface: Serial1/0, RPF nbr 172.31.200.1
  Outgoing interface list:
```

Ethernet0/0, Forward/Sparse-Dense, 00:15:34/00:03:02

The following is sample output from the **show ip mroute** command with the **active** keyword from the router along the SPT shown in the figure. This command is used to confirm the multicast groups with active sources on this router.

Note In the output, the "(?)" indicates that the router is unable to resolve an IP address to a hostname.

```
Router# show ip mroute active
Active IP Multicast Sources - sending >= 4 kbps

Group: 239.1.2.3, (?)
   Source: 10.0.0.1 (?)
     Rate: 20 pps/4 kbps(1sec), 4 kbps(last 30 secs), 4 kbps(life avg)
```

Verifying IP Multicast on the First Hop Router Example

The following is sample output from the **show ip mroute**for a particular group. This command is used in this example to verify the packets being sent to groups from active sources on the first hop router shown in the figure. In the sample output, notice the packet count displayed for the Forwarding field. This field displays the packet forwarding count for sources sending to groups on the first hop router.

Note The RPF nbr 0.0.0.0 field indicates that the source of an mroute has been reached.

```
Router# show ip mroute 239.1.2.3
(*, 239.1.2.3), 00:18:10/stopped, RP 172.16.0.1, flags: SPF
  Incoming interface: Serial1/0, RPF nbr 172.31.200.2
  Outgoing interface list: Null

(10.0.0.1, 239.1.2.3), 00:18:10/00:03:22, flags: FT
  Incoming interface: GigabitEthernet0/0/0, RPF nbr 0.0.0.0
  Outgoing interface list:
    Serial1/0/0, Forward/Sparse-Dense, 00:18:10/00:03:19
```

The following is sample output from the **show ip mroute** command with the **active** keyword from the first hop router shown in the figure:

Note In the output, the "(?)" indicates that the router is unable to resolve an IP address to a host name.

```
Router# show ip mroute active
Active IP Multicast Sources - sending >= 4 kbps

Group: 239.1.2.3, (?)
   Source: 10.0.0.1 (?)
     Rate: 20 pps/4 kbps(1sec), 4 kbps(last 30 secs), 4 kbps(life avg)
```

Additional References

Related Documents

Related Topic	Document Title
Overview of the IP multicast technology area	" IP Multicast Technology Overview " module
PIM-SM and SSM concepts and configuration examples	" Configuring Basic IP Multicast " module
IP multicast commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS IP Multicast Command Reference*

Standards

Standard	Title
No new or modified standards are supported, and support for existing standards has not been modified.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported, and support for existing MIBs has not been modified.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported, and support for existing RFCs has not been modified.	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for Verifying IP Multicast Operation

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 16: Feature Information for Verifying IP Multicast Operation

Feature Name	Releases	Feature Information
This table is intentionally left blank because no features were introduced or modified in this module since Cisco IOS XE Release 2(1). This table will be updated when feature information is added to this module.	--	--

CHAPTER 14

Monitoring and Maintaining IP Multicast

This module describes many ways to monitor and maintain an IP multicast network, such as

- displaying which neighboring multicast routers are peering with the local router
- displaying multicast packet rates and loss information
- tracing the path from a source to a destination branch for a multicast distribution tree
- displaying the contents of the IP multicast routing table, information about interfaces configured for PIM, the PIM neighbors discovered by the router, and contents of the IP fast-switching cache
- clearing caches, tables, and databases
- monitoring the delivery of IP multicast packets and being alerted if the delivery fails to meet certain parameters (IP multicast heartbeat)
- using session description and announcement protocols and applications to assist the advertisement of multicast multimedia conferences and other multicast sessions and communicating the relevant session setup information to prospective participants (SAP listener support)
- storing IP multicast packet headers in a cache and displaying them to find out information such as who is sending IP multicast packets to what groups and any multicast forwarding loops in your network
- using managed objects to remotely monitor and configure PIM using Simple Network Management Protocol (SNMP)
- disabling fast switching of IP multicast in order to log debug messages

- Finding Feature Information, page 242
- Prerequisites for Monitoring and Maintaining IP Multicast, page 242
- Information About Monitoring and Maintaining IP Multicast, page 242
- How to Monitor and Maintain IP Multicast, page 244
- Configuration Examples for Monitoring and Maintaining IP Multicast, page 253
- Additional References, page 256
- Feature Information for Monitoring and Maintaining IP Multicast, page 257

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Monitoring and Maintaining IP Multicast

- Before performing the tasks in this module, you should be familiar with the concepts described in the "IP Multicast Technology Overview" module.
- You must also have enabled IP multicast and have Protocol Independent Multicast (PIM) configured and running on your network. Refer to the "Configuring Basic IP Multicast" module.

Information About Monitoring and Maintaining IP Multicast

IP Multicast Heartbeat

The IP Multicast Heartbeat feature enables you to monitor the delivery of IP multicast packets and to be alerted if the delivery fails to meet certain parameters.

Although you could alternatively use MRM to monitor IP multicast, you can perform the following tasks with IP multicast heartbeat that you cannot perform with MRM:

- Generate an SNMP trap
- Monitor a production multicast stream

When IP multicast heartbeat is enabled, the router monitors IP multicast packets destined for a particular multicast group at a particular interval. If the number of packets observed is less than a configured minimum amount, the router sends an SNMP trap to a specified network management station to indicate a loss of heartbeat exception.

The **ip multicast heartbeat** command does not create a heartbeat if there is no existing multicast forwarding state for *group* in the router. This command will not create a multicast forwarding state in the router. Use the **ip igmp static-group**commandon the router or on a downstream router to force forwarding of IP multicast traffic. Use the **snmp-server host ipmulticast** command to enable the sending of IP multicast traps to specific receiver hosts. Use the **debug ip mhbeat**command to debug the Multicast Heartbeat feature.

Session Announcement Protocol (SAP)

Session Announcement Protocol (SAP) listener support is needed to use session description and announcement protocols and applications to assist the advertisement of multicast multimedia conferences and other multicast sessions and to communicate the relevant session setup information to prospective participants.

Sessions are described by the Session Description Protocol (SDP), which is defined in RFC 2327. SDP provides a formatted, textual description of session properties (for example, contact information, session lifetime, and the media) being used in the session (for example, audio, video, and whiteboard) with their specific attributes such as time-to-live (TTL) scope, group address, and User Datagram Protocol (UDP) port number.

Many multimedia applications rely on SDP for session descriptions. However, they may use different methods to disseminate these session descriptions. For example, IP/TV relies on the web to disseminate session descriptions to participants. In this example, participants must know of a web server that provides the session information.

MBONE applications (for example, vic, vat, and wb) and other applications rely on multicast session information sent throughout the network. In these cases, SAP is used to transport the SDP session announcements. SAP Version 2 uses the well-known session directory multicast group 224.2.127.254 to disseminate SDP session descriptions for global scope sessions and group 239.255.255.255 for administrative scope sessions.

Note The Session Directory (SDR) application is commonly used to send and receive SDP/SAP session announcements.

PIM MIB Extensions for SNMP Traps for IP Multicast

Protocol Independent Multicast (PIM) is an IP multicast routing protocol used for routing multicast data packets to multicast groups. RFC 2934 defines the PIM MIB for IPv4, which describes managed objects that enable users to remotely monitor and configure PIM using Simple Network Management Protocol (SNMP).

PIM MIB extensions introduce the following new classes of PIM notifications:

- neighbor-change--This notification results from the following conditions:
  - A router's PIM interface is disabled or enabled (using the **ip pim** command in interface configuration mode)
  - A router's PIM neighbor adjacency expires (defined in RFC 2934)
- rp-mapping-change--This notification results from a change in the rendezvous point (RP) mapping information due to either Auto-RP messages or bootstrap router (BSR) messages.
- invalid-pim-message--This notification results from the following conditions:
  - An invalid (*, G) Join or Prune message is received by the device (for example, when a router receives a Join or Prune message for which the RP specified in the packet is not the RP for the multicast group)
  - An invalid PIM register message is received by the device (for example, when a router receives a register message from a multicast group for which it is not the RP)

Benefits of PIM MIB Extensions

PIM MIB extensions:

- Allow users to identify changes in the multicast topology of their network by detecting changes in the RP mapping.
- Provide traps to monitor the PIM protocol on PIM-enabled interfaces.
- Help users identify routing issues when multicast neighbor adjacencies expire on a multicast interface.
- Enable users to monitor RP configuration errors (for example, errors due to flapping in dynamic RP allocation protocols like Auto-RP).

How to Monitor and Maintain IP Multicast

Displaying Multicast Peers Packet Rates and Loss Information and Tracing a Path

Monitor IP multicast routing when you want to know which neighboring multicast routers are peering with the local router, what the multicast packet rates and loss information are, or when you want to trace the path from a source to a destination branch for a multicast distribution tree.

SUMMARY STEPS

1. **enable**
2. **mrinfo** [*host-name* | *host-address*] [*source-address* | *interface*]
3. **mstat** {*source-name* | *source-address*} [*destination-name* | *destination-address*] [*group-name* | *group-address*]
4. **mtrace** {*source-name* | *source-address*} [*destination-name* | *destination-address*] [*group-name* | *group-address*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**mrinfo** [*host-name* | *host-address*] [*source-address* | *interface*] **Example:** `Router# mrinfo`	(Optional) Queries which neighboring multicast routers are “peering” with the local router.

	Command or Action	Purpose
Step 3	**mstat** {*source-name* | *source-address*} [*destination-name* | *destination-address*] [*group-name* | *group-address*] **Example:** `Router# mstat allsource`	(Optional) Displays IP multicast packet rate and loss information.
Step 4	**mtrace** {*source-name* | *source-address*} [*destination-name* | *destination-address*] [*group-name* | *group-address*] **Example:** `Router# mtrace allsource`	(Optional) Traces the path from a source to a destination branch for a multicast distribution tree.

Displaying IP Multicast System and Network Statistics

Display IP multicast system statistics to show the contents of the IP multicast routing table, information about interfaces configured for PIM, the PIM neighbors discovered by the router, contents of the IP fast-switching cache, and the contents of the circular cache header buffer.

SUMMARY STEPS

1. **enable**
2. **ping** [*group-name* | *group-address*]
3. **show ip mroute** [*group-address* | *group-name*] [*source-address* | *source-name*] [*type number*] [**summary**] [**count**] [**active** *kbps*]
4. **show ip pim interface** [*type number*] [**df** | **count**] [*rp-address*] [**detail**]
5. **show ip pim neighbor** [*type number*]
6. **show ip pim rp** [**mapping** | **metric**] [*rp-address*]
7. **show ip rpf** {*source-address* | *source-name*} [**metric**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**ping** [*group-name* | *group-address*] **Example:** `Router# ping cbone-audio`	(Optional) Sends an ICMP echo request message to a multicast group address or group name.
Step 3	**show ip mroute** [*group-address* | *group-name*] [*source-address* | *source-name*] [*type number*] [**summary**] [**count**] [**active** *kbps*] **Example:** `Router# show ip mroute cbone-audio`	(Optional) Displays the contents of the IP multicast routing table.
Step 4	**show ip pim interface** [*type number*] [**df** | **count**] [*rp-address*] [**detail**] **Example:** `Router# show ip pim interface gigabitethernet1/0/0 detail`	(Optional) Displays information about interfaces configured for PIM.
Step 5	**show ip pim neighbor** [*type number*] **Example:** `Router# show ip pim neighbor`	(Optional) Lists the PIM neighbors discovered by the router.
Step 6	**show ip pim rp** [**mapping** | **metric**] [*rp-address*] **Example:** `Router# show ip pim rp metric`	(Optional) Displays the RP routers associated with a sparse mode multicast group.
Step 7	**show ip rpf** {*source-address* | *source-name*} [**metric**] **Example:** `Router# show ip rpf 172.16.10.13`	(Optional) Displays how the router is doing RPF (that is, from the unicast routing table, DVMRP routing table, or static mroutes). Also displays the unicast routing metric.

Clearing IP Multicast Routing Table or Caches

Clear IP multicast caches and tables to delete entries from the IP multicast routing table, the Auto-RP cache, the IGMP cache, and the caches of Catalyst switches. When these entries are cleared, the information is refreshed by being relearned, thus eliminating any incorrect entries.

SUMMARY STEPS

1. **enable**
2. **clear ip mroute** {* | *group-name* [*source-name* | *source-address*] | *group-address* [*source-name* | *source-address*]}
3. **clear ip pim auto-rp** *rp-address*
4. **clear ip igmp group** [*group-name* | *group-address* | *interface-type interface-number*]
5. **clear ip cgmp** [*interface-type interface-number*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**clear ip mroute** {* | *group-name* [*source-name* | *source-address*] | *group-address* [*source-name* | *source-address*]} **Example:** `Router# clear ip mroute 224.2.205.42 228.3.0.0`	(Optional) Deletes entries from the IP multicast routing table.
Step 3	**clear ip pim auto-rp** *rp-address* **Example:** `Router# clear ip pim auto-rp 224.5.6.7`	(Optional) Clears the Auto-RP cache.
Step 4	**clear ip igmp group** [*group-name* | *group-address* | *interface-type interface-number*] **Example:** `Router# clear ip igmp group 224.0.255.1`	(Optional) Deletes entries from the IGMP cache.
Step 5	**clear ip cgmp** [*interface-type interface-number*] **Example:** `Router# clear ip cgmp`	(Optional) Clears all group entries from the caches of Catalyst switches.

Monitoring IP Multicast Delivery Using IP Multicast Heartbeat

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip multicast-routing distributed**
4. **snmp-server host** {*hostname* | *ip-address*} [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string*[**udp-port** *port*] [*notification-type*]
5. **snmp-server enable traps ipmulticast**
6. **ip multicast heartbeat** *group-address minimum-number window-size interval*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip multicast-routing distributed** **Example:** `Router(config)# ip multicast-routing distributed`	Enables IP multicast routing.
Step 4	**snmp-server host** {*hostname* | *ip-address*} [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string*[**udp-port** *port*] [*notification-type*] **Example:** `Router(config)# snmp-server host 224.1.0.1 traps public`	Specifies the recipient of an SNMP notification operation.
Step 5	**snmp-server enable traps ipmulticast** **Example:** `Router(config)# snmp-server enable traps ipmulticast`	Enables the router to send IP multicast traps.

	Command or Action	Purpose
Step 6	**ip multicast heartbeat** *group-address minimum-number window-size interval* **Example:** `Router(config)# ip multicast heartbeat 224.1.1.1 1 1 10`	Enables the monitoring of the IP multicast packet delivery. • The *interval* should be set to a multiple of 10 seconds on platforms that use Multicast Distributed Fast Switching (MDFS) because on those platforms, the packet counters are only updated once every 10 seconds. Other platforms may have other increments.

Advertising Multicast Multimedia Sessions Using SAP Listener

Enable SAP listener support when you want to use session description and announcement protocols and applications to assist the advertisement of multicast multimedia conferences and other multicast sessions and to communicate the relevant session setup information to prospective participants.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip sap cache-timeout** *minutes*
4. **interface** *type number*
5. **ip sap listen**
6. **end**
7. **clear ip sap** [*group-address* | " *session-name* "]
8. **show ip sap** [*group-address* | " *session-name* "| **detail**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**ip sap cache-timeout** *minutes* **Example:** `Router(config)# ip sap cache-timeout 600`	(Optional) Limits how long a SAP cache entry stays active in the cache. • By default, SAP cache entries are deleted 24 hours after they are received from the network.
Step 4	**interface** *type number* **Example:** `Router(config)# interface gigabitethernet 1/0/0`	Selects an interface that is connected to hosts on which IGMPv3 can be enabled.
Step 5	**ip sap listen** **Example:** `Router(config-if)# ip sap listen`	Enables the Cisco IOS XE software to listen to session directory announcements.
Step 6	**end** **Example:** `Router(config-if)# end`	Ends the session and returns to EXEC mode.
Step 7	**clear ip sap** [*group-address* | " *session-name* "] **Example:** `Router# clear ip sap "Sample Session"`	Deletes a SAP cache entry or the entire SAP cache.
Step 8	**show ip sap** [*group-address* | " *session-name* "| **detail**] **Example:** `Router# show ip sap 224.2.197.250 detail`	(Optional) Displays the SAP cache.

Disabling Fast Switching of IP Multicast

Disable fast switching if you want to log debug messages, because when fast switching is enabled, debug messages are not logged.

You might also want to disable fast switching, which places the router in process switching, if packets are not reaching their destinations. If fast switching is disabled and packets are reaching their destinations, then switching may be the cause.

Fast switching of IP multicast packets is enabled by default on all interfaces (including generic routing encapsulation [GRE] and DVMRP tunnels), with one exception: It is disabled and not supported over X.25 encapsulated interfaces. The following are properties of fast switching:

- If fast switching is disabled on an *incoming* interface for a multicast routing table entry, the packet is sent at process level for all interfaces in the outgoing interface list.
- If fast switching is disabled on an *outgoing* interface for a multicast routing table entry, the packet is process-level switched for that interface, but may be fast switched for other interfaces in the outgoing interface list.
- When fast switching is enabled, debug messages are not logged.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **no ip mroute-cache**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface gigabitethernet 1/0/0`	Specifies an interface.
Step 4	**no ip mroute-cache** **Example:** `Router(config-if)# no ip mroute-cache`	Disables fast switching of IP multicast.

Enabling PIM MIB Extensions for IP Multicast

Perform this task to enable PIM MIB extensions for IP multicast.

Note

- The pimInterfaceVersion object was removed from RFC 2934 and, therefore, is no longer supported in software.
- The following MIB tables are not supported in Cisco software:
  - pimIpMRouteTable
  - pimIpMRouteNextHopTable

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps pim** [**neighbor-change** | **rp-mapping-change** | **invalid-pim-message**]
4. **snmp-server host** *host-address* [**traps** | **informs**] *community-string* **pim**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server enable traps pim** [**neighbor-change** | **rp-mapping-change** | **invalid-pim-message**] **Example:** `Device(config)# snmp-server enable traps pim neighbor-change`	Enables a device to send PIM notifications. • **neighbor-change** --This keyword enables notifications indicating when a device's PIM interface is disabled or enabled, or when a device's PIM neighbor adjacency expires. • **rp-mapping-change** --This keyword enables notifications indicating a change in RP mapping information due to either Auto-RP messages or BSR messages. • **invalid-pim-message** --This keyword enables notifications for monitoring invalid PIM protocol operations (for example, when a device receives a join or prune message for which the RP specified in the packet is not the RP for the multicast group or when a device receives a register message from a multicast group for which it is not the RP).

	Command or Action	Purpose
Step 4	**snmp-server host** *host-address* [**traps** | **informs**] *community-string* **pim** **Example:** `Device(config)# snmp-server host 10.10.10.10 traps public pim`	Specifies the recipient of a PIM SNMP notification operation.

Configuration Examples for Monitoring and Maintaining IP Multicast

Displaying IP Multicast System and Network Statistics Example

The following is sample output from the **mrinfo** command:

```
Router# mrinfo

192.31.7.37 (labs-allcompany) [version cisco 12.3] [flags: PMSA]:
192.31.7.37 -> 192.31.7.34 (lab-southwest) [1/0/pim]
192.31.7.37 -> 192.31.7.47 (lab-northwest) [1/0/pim]
192.31.7.37 -> 192.31.7.44 (lab-southeast) [1/0/pim]
131.119.26.10 -> 131.119.26.9 (lab-northeast) [1/32/pim]
```

The following is sample output from the **mstat** command in user EXEC mode:

```
Router> mstat labs-in-china 172.16.0.1 224.0.255.255

Type escape sequence to abort.
Mtrace from 172.16.0.0 to 172.16.0.10 via group 224.0.255.255
>From source (labs-in-china) to destination (labs-in-africa)
Waiting to accumulate statistics......
Results after 10 seconds:
Source Response Dest Packet Statistics For Only For Traffic
172.16.0.0      172.16.0.10 All Multicast Traffic From 172.16.0.0
| __/ rtt 48 ms Lost/Sent = Pct Rate To 224.0.255.255
v / hop 48 ms --------------------- --------------------
172.16.0.1      labs-in-england
| ^ ttl 1
v | hop 31 ms 0/12 = 0% 1 pps 0/1 = --% 0 pps
172.16.0.2
172.16.0.3   infolabs.com
| ^ ttl 2
v | hop -17 ms -735/12 = --% 1 pps 0/1 = --% 0 pps
172.16.0.4
172.16.0.5      infolabs2.com
| ^ ttl 3
v | hop -21 ms -678/23 = --% 2 pps 0/1 = --% 0 pps
172.16.0.6
172.16.0.7      infolabs3.com
| ^ ttl 4
v | hop 5 ms 605/639 = 95% 63 pps 1/1 = --% 0 pps
172.16.0.8
172.16.0.9      infolabs.cisco.com
```

```
| \__ ttl 5
v \ hop 0 ms 4 0 pps 0 0 pps
172.16.0.0      172.16.0.10
Receiver Query Source
```

The following is sample output from the **mtrace** command in user EXEC mode:

```
Router> mtrace 172.16.0.0 172.16.0.10 239.254.254.254
Type escape sequence to abort.
Mtrace from 172.16.0.0 to 172.16.0.10 via group 239.254.254.254
From source (?) to destination (?)
Querying full reverse path...
0 172.16.0.10
-1 172.16.0.8 PIM thresh^ 0 0 ms
-2 172.16.0.6 PIM thresh^ 0 2 ms
-3 172.16.0.5 PIM thresh^ 0 894 ms
-4 172.16.0.3 PIM thresh^ 0 893 ms
-5 172.16.0.2 PIM thresh^ 0 894 ms
-6 172.16.0.1 PIM thresh^ 0 893 ms
```

Monitoring IP Multicast Delivery Using IP Multicast Heartbeat Example

The following example shows how to monitor IP multicast packets forwarded through this router to group address 244.1.1.1. If no packet for this group is received in a 10-second interval, an SNMP trap will be sent to the SNMP management station with the IP address of 224.1.0.1.

```
!
ip multicast-routing
!
snmp-server host 224.1.0.1 traps public
snmp-server enable traps ipmulticast
ip multicast heartbeat 224.1.1.1 1 1 10
```

Advertising Multicast Multimedia Sessions Using SAP Listener Example

The following example enables a router to listen to session directory announcements and changes the SAP cache timeout to 30 minutes.

```
ip multicast routing
ip sap cache-timeout 30
interface loopback 0
 ip address 10.0.0.51 255.255.255.0
 ip pim sparse-dense mode
 ip sap listen
```

The following is sample output from the **show ip sap** command for a session using multicast group 224.2.197.250:

```
Router# show ip sap 224.2.197.250
SAP Cache - 198 entries
Session Name: Session1
   Description: This broadcast is brought to you courtesy of Name1.
   Group: 0.0.0.0, ttl: 0, Contiguous allocation: 1
   Lifetime: from 10:00:00 PDT Jul 4 1999 until 10:00:00 PDT Aug 1 1999
   Uptime: 4d05h, Last Heard: 00:01:40
   Announcement source: 128.102.84.134
   Created by: sample 3136541828 3139561476 IN IP4 128.102.84.134
   Phone number: Sample Digital Video Lab (555) 555-5555
   Email: email1 <name@email.com>
   URL: http://url.com/
   Media: audio 20890 RTP/AVP 0
     Media group: 224.2.197.250, ttl: 127
     Attribute: ptime:40
```

```
   Media: video 62806 RTP/AVP 31
     Media group: 224.2.190.243, ttl: 127
```

Displaying IP Multicast System and Network Statistics Example

show ip mroute

The following is sample output from the **show ip mroute** command for a router operating in sparse mode:

```
Router# show ip mroute

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report, Z - Multicast Tunnel,
       Y - Joined MDT-data group, y - Sending to MDT-data group
Timers: Uptime/Expires
Interface state: Interface, Next-Hop, State/Mode
(*, 224.0.255.3), uptime 5:29:15, RP is 192.168.37.2, flags: SC
  Incoming interface: Tunnel0, RPF neighbor 10.3.35.1, Dvmrp
  Outgoing interface list:
    GigabitEthernet0, Forward/Sparse, 5:29:15/0:02:57
(192.168.46.0/24, 224.0.255.3), uptime 5:29:15, expires 0:02:59, flags: C
  Incoming interface: Tunnel0, RPF neighbor 10.3.35.1
  Outgoing interface list:
 GigabitEthernet0, Forward/Sparse, 5:29:15/0:02:57
```

show ip pim interface

The following is sample output from the **show ip pim interface** command when an interface is specified:

```
Router# show ip pim interface GigabitEthernet1/0/0

Address          Interface                Ver/   Nbr    Query  DR     DR
                                          Mode   Count  Intvl  Prior
172.16.1.4       GigabitEthernet1/0/0     v2/S   1      100 ms 1      172.16.1.4
```

The following is sample output from the **show ip pim rp** command:

```
Router# show ip pim rp

Group:227.7.7.7, RP:10.10.0.2, v2, v1, next RP-reachable in 00:00:48
```

show ip pim rp

The following is sample output from the **show ip pim rp** command when the **mapping** keyword is specified:

```
Router# show ip pim rp mapping
PIM Group-to-RP Mappings
This system is an RP (Auto-RP)
This system is an RP-mapping agent
Group(s) 227.0.0.0/8
  RP 10.10.0.2 (?), v2v1, bidir
    Info source:10.10.0.2 (?), via Auto-RP
         Uptime:00:01:42, expires:00:00:32
Group(s) 228.0.0.0/8
  RP 10.10.0.3 (?), v2v1, bidir
    Info source:10.10.0.3 (?), via Auto-RP
         Uptime:00:01:26, expires:00:00:34
Group(s) 229.0.0.0/8
  RP 10.10.0.5 (mcast1.cisco.com), v2v1, bidir
    Info source:10.10.0.5 (mcast1.cisco.com), via Auto-RP
```

```
         Uptime:00:00:52, expires:00:00:37
Group(s) (-)230.0.0.0/8
  RP 10.10.0.5 (mcast1.cisco.com), v2v1, bidir
    Info source:10.10.0.5 (mcast1.cisco.com), via Auto-RP
         Uptime:00:00:52, expires:00:00:37
```

The following is sample output from the **show ip pim rp** command when the **metric** keyword is specified:

```
Router# show ip pim rp metric

RP Address      Metric Pref    Metric       Flags   RPF Type   Interface
10.10.0.2       0              0              L     unicast    Loopback0
10.10.0.3       90             409600         L     unicast    GigabitEthernet3/3/0
10.10.0.5       90             435200         L     unicast    GigabitEthernet3/3/0
```

show ip rpf

The following is sample output from the **show ip rpf** command:

```
Router# show ip rpf 172.16.10.13

RPF information for host1 (172.16.10.13)
  RPF interface: BRI0
  RPF neighbor: sj1.cisco.com (172.16.121.10)
  RPF route/mask: 172.16.0.0/255.255.0.0
  RPF type: unicast
  RPF recursion count: 0
  Doing distance-preferred lookups across tables
```

The following is sample output from the **show ip rpf**command when the **metric**keyword is specified:

```
Router# show ip rpf 172.16.10.13 metric
RPF information for host1.cisco.com (172.16.10.13)
  RPF interface: BRI0
  RPF neighbor: neighbor.cisco.com (172.16.121.10)
  RPF route/mask: 172.16.0.0/255.255.0.0
  RPF type: unicast
  RPF recursion count: 0
  Doing distance-preferred lookups across tables
  Metric preference: 110
```

Enabling PIM MIB Extensions for IP Multicast Example

The following example shows how to configure a router to generate notifications indicating that a PIM interface of the router has been enabled. The first line configures PIM traps to be sent as SNMP v2c traps to the host with IP address 10.0.0.1. The second line configures the router to send the neighbor-change class of trap notification to the host.

```
snmp-server host 10.0.0.1 traps version 2c public pim
snmp-server enable traps pim neighbor-change
interface ethernet0/0
 ip pim sparse-dense-mode
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases

Related Topic	Document Title
Cisco IOS IP SLAs commands	Cisco IOS IP Multicast Command Reference

Standards and RFCs

Standard/RFC	Title
RFC 2934	*Protocol Independent Multicast for IPv4 MIB*

MIBs

MIB	MIBs Link
• CISCO-IPMROUTE-MIB • MSDP-MIB • IGMP-STD-MIB	To locate and download MIBs for selected platforms, Cisco IOS XE releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Monitoring and Maintaining IP Multicast

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 17: Feature Information for Monitoring and Maintaining IP Multicast

Feature Names	Releases	Feature Configuration Information
PIM MIB Extensions	Cisco IOS XE Release 2.1	Protocol Independent Multicast (PIM) is an IP multicast routing protocol used for routing multicast data packets to multicast groups. RFC 2934 defines the PIM for IPv4 MIB, which describes managed objects that enable users to remotely monitor and configure PIM using Simple Network Management Protocol (SNMP).
Multicast Heartbeat	Cisco IOS XE Release 2.1	The IP multicast heartbeat feature provides a way to monitor the status of IP multicast delivery and be informed when the delivery fails (via Simple Network Management Protocol [SNMP] traps).

CHAPTER 15

Multicast User Authentication and Profile Support

- Finding Feature Information, page 259
- Restrictions for Multicast User Authentication and Profile Support, page 259
- Information About Multicast User Authentication and Profile Support, page 260
- How to Configure Multicast User Authentication and Profile Support, page 260
- Configuration Examples for Multicast User Authentication and Profile Support, page 263
- Additional References for IPv6 Services: AAAA DNS Lookups, page 263
- Feature Information for Multicast User Authentication and Profile Support, page 265

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Multicast User Authentication and Profile Support

The port, interface, VC, or VLAN ID is the user or subscriber identity. User identity by hostname, user ID, or password is not supported.

Information About Multicast User Authentication and Profile Support

IPv6 Multicast User Authentication and Profile Support

IPv6 multicast by design allows any host in the network to become a receiver or a source for a multicast group. Therefore, multicast access control is needed to control multicast traffic in the network. Access control functionality consists mainly of source access control and accounting, receiver access control and accounting, and provisioning of this access control mechanism.

Multicast access control provides an interface between multicast and authentication, authorization, and accounting (AAA) for provisioning, authorizing, and accounting at the last-hop device, receiver access control functions in multicast, and group or channel disabling capability in multicast.

When you deploy a new multicast service environment, it is necessary to add user authentication and provide a user profile download on a per-interface basis. The use of AAA and IPv6 multicast supports user authentication and downloading of the user profile in a multicast environment.

The event that triggers the download of a multicast access-control profile from the RADIUS server to the access device is arrival of an MLD join on the access device. When this event occurs, a user can cause the authorization cache to time out and request download periodically or use an appropriate multicast clear command to trigger a new download in case of profile changes.

Accounting occurs via RADIUS accounting. Start and stop accounting records are sent to the RADIUS server from the access device. In order for you to track resource consumption on a per-stream basis, these accounting records provide information about the multicast source and group. The start record is sent when the last-hop device receives a new MLD report, and the stop record is sent upon MLD leave or if the group or channel is deleted for any reason.

How to Configure Multicast User Authentication and Profile Support

Enabling AAA Access Control for IPv6 Multicast

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Enables the AAA access control system.

Specifying Method Lists and Enabling Multicast Accounting

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa authorization multicast default** [*method3* | *method4*
4. **aaa accounting multicast default** [**start-stop** | **stop-only**] [**broadcast**] [*method1*] [*method2*] [*method3*] [*method4*
5. **interface** *type number*
6. **ipv6 multicast aaa account receive** *access-list-name* [**throttle** *throttle-number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa authorization multicast default** [*method3* | *method4* **Example:** `Device(config)# aaa authorization multicast default`	Enables AAA authorization and sets parameters that restrict user access to an IPv6 multicast network.
Step 4	**aaa accounting multicast default** [**start-stop** | **stop-only**] [**broadcast**] [*method1*] [*method2*] [*method3*] [*method4* **Example:** `Device(config)# aaa accounting multicast default`	Enables AAA accounting of IPv6 multicast services for billing or security purposes when you use RADIUS.
Step 5	**interface** *type number* **Example:** `Device(config)# interface FastEthernet 1/0`	Specifies an interface type and number, and places the device in interface configuration mode.
Step 6	**ipv6 multicast aaa account receive** *access-list-name* [**throttle** *throttle-number* **Example:** `Device(config-if)# ipv6 multicast aaa account receive list1`	Enables AAA accounting on specified groups or channels.

Disabling the Device from Receiving Unauthenticated Multicast Traffic

In some situations, access control may be needed to prevent multicast traffic from being received unless the subscriber is authenticated and the channels are authorized as per access control profiles. That is, there should be no traffic at all unless specified otherwise by access control profiles.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 multicast group-range** [*access-list-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 multicast group-range** [*access-list-name*] **Example:** `Device(config)# ipv6 multicast group-range`	Disables multicast protocol actions and traffic forwarding for unauthorized groups or channels on all the interfaces in a device.

Configuration Examples for Multicast User Authentication and Profile Support

Example: Enabling AAA Access Control, Specifying Method Lists, and Enabling Multicast Accounting for IPv6

```
Device(config)# aaa new-model
Device(config)# aaa authorization multicast default
Device(config)# aaa accounting multicast default
Device(config)# interface FastEthernet 1/0
Device(config-if)# ipv6 multicast aaa account receive list1
```

Additional References for IPv6 Services: AAAA DNS Lookups

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	*IPv6 Configuration Guide*
IPv4 services configuration	*IP Application Services Configuration Guide*

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IPv6 commands	*Cisco IOS IPv6 Command Reference*
Cisco IOS IPv6 features	Cisco IOS IPv6 Feature Mapping

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	*IPv6 RFCs*

MIBs

MIB	MIBs Link
None.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Multicast User Authentication and Profile Support

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 18: Feature Information for User Authentication and Profile Support

Feature Name	Releases	Feature Information
Multicast User Authentication and Profile Support	12.4(4)T Cisco IOS XE Release 3.8S	Multicast access control provides an interface between multicast and AAA for provisioning, authorizing, and accounting at the last-hop router, receiver access control functions in multicast, and group or channel disabling capability in multicast. The following commands were introduced or modified: **aaa accounting multicast default**, **aaa authorization multicast default**, **clear ipv6 multicast aaa authorization**, **ipv6 multicast aaa account receive**.

CHAPTER 16

IPv6 Multicast: Bootstrap Router

- Finding Feature Information, page 267
- Information About IPv6 Multicast: Bootstrap Router, page 267
- How to Configure IPv6 Multicast: Bootstrap Router, page 269
- Configuration Examples for IPv6 Multicast: Bootstrap Router, page 274
- Additional References, page 274
- Feature Information for IPv6 Multicast: Bootstrap Router, page 275

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About IPv6 Multicast: Bootstrap Router

IPv6 BSR

PIM devices in a domain must be able to map each multicast group to the correct RP address. The BSR protocol for PIM-SM provides a dynamic, adaptive mechanism to distribute group-to-RP mapping information rapidly throughout a domain. With the IPv6 BSR feature, if an RP becomes unreachable, it will be detected and the mapping tables will be modified so that the unreachable RP is no longer used, and the new tables will be rapidly distributed throughout the domain.

Every PIM-SM multicast group needs to be associated with the IP or IPv6 address of an RP. When a new multicast sender starts sending, its local DR will encapsulate these data packets in a PIM register message and send them to the RP for that multicast group. When a new multicast receiver joins, its local DR will send

a PIM join message to the RP for that multicast group. When any PIM device sends a (*, G) join message, the PIM device needs to know which is the next device toward the RP so that G (Group) can send a message to that device. Also, when a PIM device is forwarding data packets using (*, G) state, the PIM device needs to know which is the correct incoming interface for packets destined for G, because it needs to reject any packets that arrive on other interfaces.

A small set of devices from a domain are configured as candidate bootstrap routers (C-BSRs) and a single BSR is selected for that domain. A set of devices within a domain are also configured as candidate RPs (C-RPs); typically, these devices are the same devices that are configured as C-BSRs. Candidate RPs periodically unicast candidate-RP-advertisement (C-RP-Adv) messages to the BSR of that domain, advertising their willingness to be an RP. A C-RP-Adv message includes the address of the advertising C-RP, and an optional list of group addresses and mask length fields, indicating the group prefixes for which the candidacy is advertised. The BSR then includes a set of these C-RPs, along with their corresponding group prefixes, in bootstrap messages (BSMs) it periodically originates. BSMs are distributed hop-by-hop throughout the domain.

Bidirectional BSR support allows bidirectional RPs to be advertised in C-RP messages and bidirectional ranges in the BSM. All devices in a system must be able to use the bidirectional range in the BSM; otherwise, the bidirectional RP feature will not function.

IPv6 BSR: Configure RP Mapping

The IPv6 BSR ability to configure RP mapping allows IPv6 multicast devices to be statically configured to announce scope-to-RP mappings directly from the BSR instead of learning them from candidate-RP messages. Announcing RP mappings from the BSR is useful in several situations:

- When an RP address never changes because there is only a single RP or the group range uses an anycast RP, it may be less complex to configure the RP address announcement statically on the candidate BSRs.
- When an RP address is a virtual RP address (such as when using bidirectional PIM), it cannot be learned by the BSR from a candidate-RP. Instead, the virtual RP address must be configured as an announced RP on the candidate BSRs.

IPv6 BSR: Scoped Zone Support

BSR provides scoped zone support by distributing group-to-RP mappings in networks using administratively scoped multicast. The user can configure candidate BSRs and a set of candidate RPs for each administratively scoped region in the user’s domain.

For BSR to function correctly with administrative scoping, a BSR and at least one C-RP must be within every administratively scoped region. Administratively scoped zone boundaries must be configured at the zone border devices, because they need to filter PIM join messages that might inadvertently cross the border due to error conditions. In addition, at least one C-BSR within the administratively scoped zone must be configured to be a C-BSR for the administratively scoped zone’s address range.

A separate BSR election will then take place (using BSMs) for every administratively scoped range, plus one for the global range. Administratively scoped ranges are identified in the BSM because the group range is marked to indicate that this is an administrative scope range, not just a range that a particular set of RPs is configured to handle.

Unless the C-RP is configured with a scope, it discovers the existence of the administratively scoped zone and its group range through reception of a BSM from the scope zone’s elected BSR containing the scope zone’s group range. A C-RP stores each elected BSR's address and the administratively scoped range contained

in its BSM. It separately unicasts C-RP-Adv messages to the appropriate BSR for every administratively scoped range within which it is willing to serve as an RP.

All PIM devices within a PIM bootstrap domain where administratively scoped ranges are in use must be able to receive BSMs and store the winning BSR and RP set for all administratively scoped zones that apply.

IPv6 Multicast: RPF Flooding of BSR Packets

Cisco IPv6 devices provide support for the RPF flooding of BSR packets so that the device will not disrupt the flow of BSMs. The device will recognize and parse enough of the BSM to identify the BSR address. The device performs an RPF check for this BSR address and forwards the packet only if it is received on the RPF interface. The device also creates a BSR entry containing RPF information to use for future BSMs from the same BSR. When BSMs from a given BSR are no longer received, the BSR entry is timed out.

How to Configure IPv6 Multicast: Bootstrap Router

Configuring a BSR and Verifying BSR Information

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 pim** [**vrf** *vrf-name*] **bsr candidate bsr** *ipv6-address*[*hash-mask-length*] [**priority** *priority-value*]
4. **interface** *type number*
5. **ipv6 pim bsr border**
6. **end**
7. **show ipv6 pim** [**vrf** *vrf-name*] **bsr** {**election** | **rp-cache** | **candidate-rp**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**ipv6 pim** [**vrf** *vrf-name*] **bsr candidate bsr** *ipv6-address*[*hash-mask-length*] [**priority** *priority-value*] **Example:** `Device(config)# ipv6 pim bsr candidate bsr 2001:DB8:3000:3000::42 124 priority 10`	Configures a device to be a candidate BSR.
Step 4	**interface** *type number* **Example:** `Device(config)# interface FastEthernet 1/0`	Specifies an interface type and number, and places the device in interface configuration mode.
Step 5	**ipv6 pim bsr border** **Example:** `Device(config-if)# ipv6 pim bsr border`	Configures a border for all BSMs of any scope on a specified interface.
Step 6	**end** **Example:** `Device(config-if)# end`	Exits to privileged EXEC mode.
Step 7	**show ipv6 pim** [**vrf** *vrf-name*] **bsr** {**election** | **rp-cache** | **candidate-rp**} **Example:** `Device# show ipv6 pim bsr election`	Displays information related to PIM BSR protocol processing.

Sending PIM RP Advertisements to the BSR

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 pim** [**vrf** *vrf-name*] **bsr candidate rp** *ipv6-address* [**group-list** *access-list-name*] [**priority** *priority-value*] [**interval** *seconds*] [**scope** *scope-value*] [**bidir**]
4. **interface** *type number*
5. **ipv6 pim bsr border**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 pim** [**vrf** *vrf-name*] **bsr candidate rp** *ipv6-address* [**group-list** *access-list-name*] [**priority** *priority-value*] [**interval** *seconds*] [**scope** *scope-value*] [**bidir**] **Example:** `Device(config)# ipv6 pim bsr candidate rp 2001:DB8:3000:3000::42 priority 0`	Sends PIM RP advertisements to the BSR.
Step 4	**interface** *type number* **Example:** `Device(config)# interface FastEthernet 1/0`	Specifies an interface type and number, and places the device in interface configuration mode.
Step 5	**ipv6 pim bsr border** **Example:** `Device(config-if)# ipv6 pim bsr border`	Configures a border for all BSMs of any scope on a specified interface.

Configuring BSR for Use Within Scoped Zones

A user can configure candidate BSRs and a set of candidate RPs for each administratively scoped region in the domain.

If scope is specified on the candidate RP, then this device will advertise itself as C-RP only to the BSR for the specified scope. If the group list is specified along with the scope, then only prefixes in the access list with the same scope as that configured will be advertised.

If a scope is specified on the bootstrap device, the BSR will originate BSMs including the group range associated with the scope and accept C-RP announcements for groups that belong to the given scope.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 pim** [**vrf** *vrf-name*] **bsr candidate bsr** *ipv6-address* [*hash-mask-length*] [**priority** *priority-value*]
4. **ipv6 pim** [**vrf** *vrf-name*] **bsr candidate rp** *ipv6-address* [**group-list** *access-list-name*] [**priority** *priority-value*] [**interval** *seconds*] [**scope** *scope-value*] [**bidir**]
5. **interface** *type number*
6. **ipv6 multicast boundary scope** *scope-value*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 pim** [**vrf** *vrf-name*] **bsr candidate bsr** *ipv6-address* [*hash-mask-length*] [**priority** *priority-value*] **Example:** `Device(config)# ipv6 pim bsr candidate bsr 2001:DB8:1:1:4`	Configures a device to be a candidate BSR.
Step 4	**ipv6 pim** [**vrf** *vrf-name*] **bsr candidate rp** *ipv6-address* [**group-list** *access-list-name*] [**priority** *priority-value*] [**interval** *seconds*] [**scope** *scope-value*] [**bidir**] **Example:** `Device(config)# ipv6 pim bsr candidate rp 2001:DB8:1:1:1 group-list list scope 6`	Configures the candidate RP to send PIM RP advertisements to the BSR.
Step 5	**interface** *type number* **Example:** `Device(config)# interface FastEthernet 1/0`	Specifies an interface type and number, and places the device in interface configuration mode.

	Command or Action	Purpose
Step 6	**ipv6 multicast boundary scope** *scope-value* **Example:** `Device(config-if)# ipv6 multicast boundary scope 6`	Configures a multicast boundary on the interface for a specified scope.

Configuring BSR Devices to Announce Scope-to-RP Mappings

IPv6 BSR devices can be statically configured to announce scope-to-RP mappings directly instead of learning them from candidate-RP messages. A user might want to configure a BSR device to announce scope-to-RP mappings so that an RP that does not support BSR is imported into the BSR. Enabling this feature also allows an RP positioned outside the enterprise's BSR domain to be learned by the known remote RP on the local candidate BSR devices.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 pim** [**vrf** *vrf-name*] **bsr announced rp** *ipv6-address* [**group-list** *access-list-name*] [**priority** *priority-value*] [**bidir**] [**scope** *scope-value*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 pim** [**vrf** *vrf-name*] **bsr announced rp** *ipv6-address* [**group-list** *access-list-name*] [**priority** *priority-value*] [**bidir**] [**scope** *scope-value*] **Example:** `Device(config)# ipv6 pim bsr announced rp 2001:DB8:3000:3000::42 priority 0`	Announces scope-to-RP mappings directly from the BSR for the specified candidate RP.

Configuration Examples for IPv6 Multicast: Bootstrap Router

Example: Configuring a BSR

```
Device# show ipv6 pim bsr election

PIMv2 BSR information
BSR Election Information
Scope Range List: ff00::/8
This system is the Bootstrap Router (BSR)
BSR Address: 60::1:1:4
Uptime: 00:11:55, BSR Priority: 0, Hash mask length: 126
RPF: FE80::A8BB:CCFF:FE03:C400,Ethernet0/0
BS Timer: 00:00:07
This system is candidate BSR
Candidate BSR address: 60::1:1:4, priority: 0, hash mask length: 126
```

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	*IPv6 Configuration Guide*
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IPv6 commands	Cisco IOS IPv6 Command Reference
Cisco IOS IPv6 features	Cisco IOS IPv6 Feature Mapping

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	*IPv6 RFCs*

MIBs

MIB	MIBs Link
	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for IPv6 Multicast: Bootstrap Router

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 19: Feature Information for IPv6 Multicast: Bootstrap Router

Feature Name	Releases	Feature Information
IPv6 Multicast: Bootstrap Router	12.0(28)S 12.2(25)S 12.2(25)SG 12.2(33)SRA 12.2(33)SXH 12.3(11)T 12.4 12.4(2)T Cisco IOS XE Release 2.4 15.0(1)S	If an RP becomes unreachable, this feature allows the RP to be detected and the mapping tables modified so that the unreachable RP is no longer used, and the new tables will be rapidly distributed throughout the domain. The following commands were introduced or modified: **debug ipv6 pim bsr**, **ipv6 pim bsr border**, **ipv6 pim bsr candidate bsr**, **ipv6 pim bsr candidate rp**, **show ipv6 pim bsr**, **show ipv6 pim group-map**.
IPv6 BSR Bi-Dir Support	12.2(33)SRE 12.3(14)T 15.0(1)S Cisco IOS XE Release 3.8S Cisco IOS XE Release 3.9S	Bidirectional BSR support allows bidirectional RPs to be advertised in C-RP messages and bidirectional ranges in the BSM. In Cisco IOS XE Release 3.8S, support was added for the Cisco ISR 4400 Series router. In Cisco IOS XE Release 3.9S, support was added for the Cisco CSR 1000V.
IPv6 BSR: Configure RP Mapping	12.2(33)SRE 12.2(50)SY 12.4(2)T Cisco IOS XE Release 2.4 15.0(1)S 15.1(1)SY	This feature allows IPv6 multicast devices to be statically configured to announce scope-to-RP mappings directly from the BSR instead of learning them from candidate-RP messages. The following commands were introduced or modified: **ipv6 multicast-routing**, **ipv6 pim bsr announced rp**, **ipv6 pim bsr candidate bsr**.

Feature Name	Releases	Feature Information
IPv6 Multicast: RPF Flooding of BSR Packets	12.0(26)S 12.3(4)T 12.2(25)S 12.2(25)SG 12.2(33)SRA 12.2(33)SXH 12.4 12.4(2)T 15.0(1)S	The RPF flooding of BSR packets feature enables a Cisco IPv6 device to not disrupt the flow of BSMs. The following command was introduced: **show ipv6 pim bsr**.
IPv6 BSR Scoped Zone Support	12.2(18)SXE Cisco IOS XE Release 3.8S Cisco IOS XE Release 3.9S	BSR provides scoped zone support by distributing group-to-RP mappings in networks using administratively scoped multicast. The user can configure candidate BSRs and a set of candidate RPs for each administratively scoped region in the user's domain. In Cisco IOS XE Release 3.8S, support was added for the Cisco ISR 4400 Series router. In Cisco IOS XE Release 3.9S, support was added for the Cisco CSR 1000V. The following commands were introduced or modified: **ipv6 multicast boundary scope**, **ipv6 pim bsr candidate bsr**, **ipv6 pim bsr candidate rp**.

CHAPTER 17

IPv6 Multicast: PIM Sparse Mode

IPv6 multicast provides support for intradomain multicast routing using PIM sparse mode (PIM-SM). PIM-SM uses unicast routing to provide reverse-path information for multicast tree building, but it is not dependent on any particular unicast routing protocol.

- Finding Feature Information, page 279
- Information About IPv6 Multicast PIM Sparse Mode, page 279
- How to Configure IPv6 Multicast PIM Sparse Mode, page 284
- Configuration Examples for IPv6 Multicast PIM Sparse Mode, page 291
- Additional References, page 293
- Feature Information for IPv6 Multicast PIM Sparse Mode, page 294

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About IPv6 Multicast PIM Sparse Mode

Protocol Independent Multicast

Protocol Independent Multicast (PIM) is used between devices so that they can track which multicast packets to forward to each other and to their directly connected LANs. PIM works independently of the unicast routing protocol to perform send or receive multicast route updates like other protocols. Regardless of which unicast routing protocols are being used in the LAN to populate the unicast routing table, Cisco IOS PIM uses the

existing unicast table content to perform the Reverse Path Forwarding (RPF) check instead of building and maintaining its own separate routing table.

You can configure IPv6 multicast to use either a PIM- Sparse Mode (SM) or PIM-Source Specific Multicast (SSM) operation, or you can use both PIM-SM and PIM-SSM together in your network.

PIM-Sparse Mode

IPv6 multicast provides support for intradomain multicast routing using PIM-SM. PIM-SM uses unicast routing to provide reverse-path information for multicast tree building, but it is not dependent on any particular unicast routing protocol.

PIM-SM is used in a multicast network when relatively few devices are involved in each multicast and these devices do not forward multicast packets for a group, unless there is an explicit request for the traffic. PIM-SM distributes information about active sources by forwarding data packets on the shared tree. PIM-SM initially uses shared trees, which requires the use of an RP.

Requests are accomplished via PIM joins, which are sent hop by hop toward the root node of the tree. The root node of a tree in PIM-SM is the RP in the case of a shared tree or the first-hop device that is directly connected to the multicast source in the case of a shortest path tree (SPT). The RP keeps track of multicast groups and the hosts that send multicast packets are registered with the RP by that host's first-hop device.

As a PIM join travels up the tree, devices along the path set up multicast forwarding state so that the requested multicast traffic will be forwarded back down the tree. When multicast traffic is no longer needed, a device sends a PIM prune up the tree toward the root node to prune (or remove) the unnecessary traffic. As this PIM prune travels hop by hop up the tree, each device updates its forwarding state appropriately. Ultimately, the forwarding state associated with a multicast group or source is removed.

A multicast data sender sends data destined for a multicast group. The designated router (DR) of the sender takes those data packets, unicast-encapsulates them, and sends them directly to the RP. The RP receives these encapsulated data packets, de-encapsulates them, and forwards them onto the shared tree. The packets then follow the (*, G) multicast tree state in the devices on the RP tree, being replicated wherever the RP tree branches, and eventually reaching all the receivers for that multicast group. The process of encapsulating data packets to the RP is called registering, and the encapsulation packets are called PIM register packets.

Designated Router

Cisco devices use PIM-SM to forward multicast traffic and follow an election process to select a designated device when there is more than one device on a LAN segment.

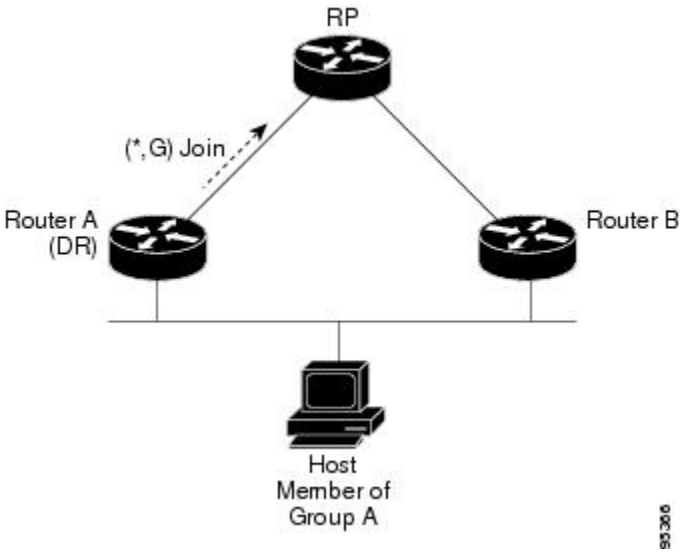
The designated router (DR) is responsible for sending PIM register and PIM join and prune messages toward the RP to inform it about active sources and host group membership.

If there are multiple PIM-SM devices on a LAN, a DR must be elected to avoid duplicating multicast traffic for connected hosts. The PIM device with the highest IPv6 address becomes the DR for the LAN unless you choose to force the DR election by use of the **ipv6 pim dr-priority** command. This command allows you to specify the DR priority of each device on the LAN segment (default priority = 1) so that the device with the highest priority will be elected as the DR. If all devices on the LAN segment have the same priority, then the highest IPv6 address is again used as the tiebreaker.

The figure below illustrates what happens on a multiaccess segment. Device A and Device B are connected to a common multiaccess Ethernet segment with Host A as an active receiver for Group A. Only Device A, operating as the DR, sends joins to the RP to construct the shared tree for Group A. If Device B was also permitted to send (*, G) joins to the RP, parallel paths would be created and Host A would receive duplicate multicast traffic. Once Host A begins to source multicast traffic to the group, the DR's responsibility is to

send register messages to the RP. If both devices were assigned the responsibility, the RP would receive duplicate multicast packets and result in wastage of bandwidth.

Figure 19: Designated Router Election on a Multiaccess Segment



If the DR should fail, the PIM-SM provides a way to detect the failure of Device A and elect a failover DR. If the DR (Device A) became inoperable, Device B would detect this situation when its neighbor adjacency with Device A timed out. Because Device B has been hearing MLD membership reports from Host A, it already has MLD state for Group A on this interface and would immediately send a join to the RP when it became the new DR. This step reestablishes traffic flow down a new branch of the shared tree via Device B. Additionally, if Host A were sourcing traffic, Device B would initiate a new register process immediately after receiving the next multicast packet from Host A. This action would trigger the RP to join the SPT to Host A via a new branch through Device B.

Tip Two PIM devices are neighbors if there is a direct connection between them. To display your PIM neighbors, use the **show ipv6 pim neighbor** command in privileged EXEC mode.

Note The DR election process is required only on multiaccess LANs.

Rendezvous Point

Note Embedded RP is not supported on Cisco RSP3 Module.

IPv6 PIM provides embedded RP support. Embedded RP support allows the device to learn RP information using the multicast group destination address instead of the statically configured RP. For devices that are the RP, the device must be statically configured as the RP.

The device searches for embedded RP group addresses in MLD reports or PIM messages and data packets. On finding such an address, the device learns the RP for the group from the address itself. It then uses this learned RP for all protocol activity for the group. For devices that are the RP, the device is advertised as an embedded RP must be configured as the RP.

To select a static RP over an embedded RP, the specific embedded RP group range or mask must be configured in the access list of the static RP. When PIM is configured in sparse mode, you must also choose one or more devices to operate as an RP. An RP is a single common root placed at a chosen point of a shared distribution tree and is configured statically in each box.

PIM DRs forward data from directly connected multicast sources to the RP for distribution down the shared tree. Data is forwarded to the RP in one of two ways:

- Data is encapsulated in register packets and unicast directly to the RP by the first-hop device operating as the DR.
- If the RP has itself joined the source tree, it is multicast-forwarded per the RPF forwarding algorithm described in the PIM-Sparse Mode section.

The RP address is used by first-hop devices to send PIM register messages on behalf of a host sending a packet to the group. The RP address is also used by last-hop devices to send PIM join and prune messages to the RP to inform it about group membership. You must configure the RP address on all devices (including the RP device).

A PIM device can be an RP for more than one group. Only one RP address can be used at a time within a PIM domain for a certain group. The conditions specified by the access list determine for which groups the device is an RP.

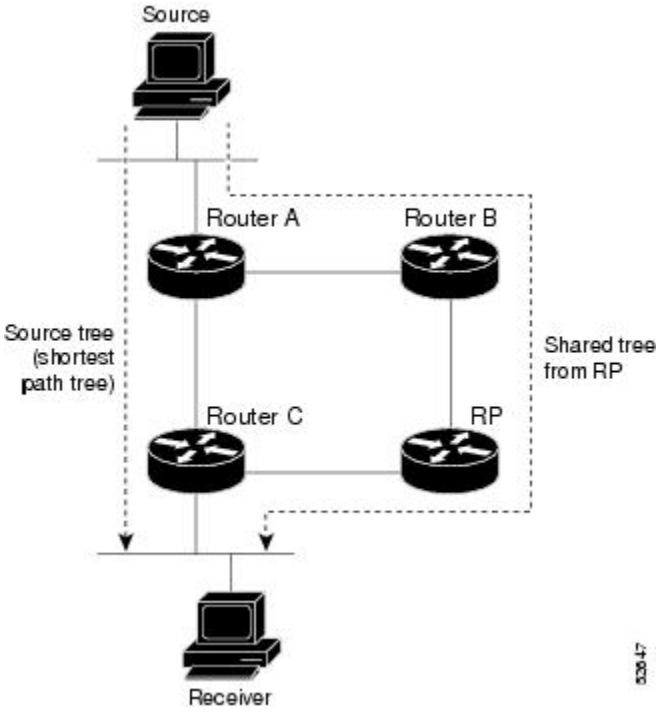
IPv6 multicast supports the PIM accept register feature, which is the ability to perform PIM-SM register message filtering at the RP. The user can match an access list or compare the AS path for the registered source with the AS path specified in a route map.

PIM Shared Tree and Source Tree (Shortest-Path Tree)

By default, members of a group receive data from senders to the group across a single data distribution tree rooted at the RP. This type of distribution tree is called shared tree or rendezvous point tree (RPT), as illustrated

in the figure below. Data from senders is delivered to the RP for distribution to group members joined to the shared tree.

Figure 20: Shared Tree and Source Tree (Shortest Path Tree)



If the data threshold warrants, leaf devices on the shared tree may initiate a switch to the data distribution tree rooted at the source. This type of distribution tree is called a shortest path tree or source tree. By default, the software switches to a source tree upon receiving the first data packet from a source.

The following process details the move from shared tree to source tree:

1. Receiver joins a group; leaf Device C sends a join message toward the RP.
2. RP puts the link to Device C in its outgoing interface list.
3. Source sends the data; Device A encapsulates the data in the register and sends it to the RP.
4. RP forwards the data down the shared tree to Device C and sends a join message toward the source. At this point, data may arrive twice at Device C, once encapsulated and once natively.
5. When data arrives natively (unencapsulated) at the RP, the RP sends a register-stop message to Device A.
6. By default, receipt of the first data packet prompts Device C to send a join message toward the source.
7. When Device C receives data on (S, G), it sends a prune message for the source up the shared tree.
8. RP deletes the link to Device C from the outgoing interface of (S, G).
9. RP triggers a prune message toward the source.

Join and prune messages are sent for sources and RPs. They are sent hop-by-hop and are processed by each PIM device along the path to the source or RP. Register and register-stop messages are not sent hop-by-hop.

They are sent by the designated router (DR) that is directly connected to a source and are received by the RP for the group.

Reverse Path Forwarding

Reverse-path forwarding is used for forwarding multicast datagrams. It functions as follows:

- If a device receives a datagram on an interface it uses to send unicast packets to the source, the packet has arrived on the RPF interface.
- If the packet arrives on the RPF interface, a device forwards the packet out the interfaces present in the outgoing interface list of a multicast routing table entry.
- If the packet does not arrive on the RPF interface, the packet is silently discarded to prevent loops.

PIM uses both source trees and RP-rooted shared trees to forward datagrams; the RPF check is performed differently for each, as follows:

- If a PIM device has source-tree state (that is, an (S, G) entry is present in the multicast routing table), the device performs the RPF check against the IPv6 address of the source of the multicast packet.
- If a PIM device has shared-tree state (and no explicit source-tree state), it performs the RPF check on the RP's address (which is known when members join the group).

Sparse-mode PIM uses the RPF lookup function to determine where it needs to send joins and prunes. (S, G) joins (which are source-tree states) are sent toward the source. (*, G) joins (which are shared-tree states) are sent toward the RP.

Note To do a RPF check, use the **show ipv6 rpf hostname** or **show ipv6 rpf vrf vrf_name hostname** command.

How to Configure IPv6 Multicast PIM Sparse Mode

Enabling IPv6 Multicast Routing

IPv6 multicast uses MLD version 2. This version of MLD is fully backward-compatible with MLD version 1 (described in *RFC 2710*). Hosts that support only MLD version 1 will interoperate with a device running MLD version 2. Mixed LANs with both MLD version 1 and MLD version 2 hosts are likewise supported.

Before You Begin

You must first enable IPv6 unicast routing on all interfaces of the device on which you want to enable IPv6 multicast routing .

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 multicast-routing** [**vrf** *vrf-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 multicast-routing** [**vrf** *vrf-name*] **Example:** `Device(config)# ipv6 multicast-routing`	Enables multicast routing on all IPv6-enabled interfaces and enables multicast forwarding for PIM and MLD on all enabled interfaces of the device. • IPv6 multicast routing is disabled by default when IPv6 unicast routing is enabled. IPv6 multicast-routing needs to be enabled for IPv6 multicast routing to function.

Configuring PIM-SM and Displaying PIM-SM Information for a Group Range

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 pim** [**vrf** *vrf-name*] **rp-address** *ipv6-address* [*group-access-list*] [**bidir**]
4. **end**
5. **show ipv6 pim** [**vrf** *vrf-name*] **interface** [**state-on**] [**state-off**] [*type number*]
6. **show ipv6 pim** [**vrf** *vrf-name*] **group-map** [*group-name* | *group-address*] | [*group-range* | *group-mask*] [**info-source** {**bsr** | **default** | **embedded-rp** | **static**}]
7. **show ipv6 pim** [**vrf** *vrf-name*] **neighbor** [**detail**] [*interface-type interface-number* | **count**]
8. **show ipv6 pim** [**vrf** *vrf-name*] **range-list**[**config**] [*rp-address* | *rp-name*]
9. **show ipv6 pim** [**vrf** *vrf-name*] **tunnel** [*interface-type interface-number*]
10. **debug ipv6 pim** [*group-name* | *group-address* | **interface** *interface-type* | **bsr** | **group** | **mvpn** | **neighbor**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 pim** [**vrf** *vrf-name*] **rp-address** *ipv6-address* [*group-access-list*] [**bidir**] **Example:** `Device(config)# ipv6 pim rp-address 2001:DB8::01:800:200E:8C6C acc-grp-1`	Configures the address of a PIM RP for a particular group range.
Step 4	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.
Step 5	**show ipv6 pim** [**vrf** *vrf-name*] **interface** [**state-on**] [**state-off**] [*type number*] **Example:** `Device# show ipv6 pim interface`	Displays information about interfaces configured for PIM.
Step 6	**show ipv6 pim** [**vrf** *vrf-name*] **group-map** [*group-name* | *group-address*] | [*group-range* | *group-mask*] [**info-source** {**bsr** | **default** | **embedded-rp** | **static**}] **Example:** `Device# show ipv6 pim group-map`	Displays an IPv6 multicast group mapping table.
Step 7	**show ipv6 pim** [**vrf** *vrf-name*] **neighbor** [**detail**] [*interface-type interface-number* | **count**] **Example:** `Device# show ipv6 pim neighbor`	Displays the PIM neighbors discovered by the Cisco IOS software.

	Command or Action	Purpose
Step 8	**show ipv6 pim** [**vrf** *vrf-name*] **range-list**[**config**] [*rp-address* | *rp-name*] **Example:** `Device# show ipv6 pim range-list`	Displays information about IPv6 multicast range lists.
Step 9	**show ipv6 pim** [**vrf** *vrf-name*] **tunnel** [*interface-type interface-number*] **Example:** `Device# show ipv6 pim tunnel`	Displays information about the PIM register encapsulation and de-encapsulation tunnels on an interface.
Step 10	**debug ipv6 pim** [*group-name* | *group-address* | **interface** *interface-type* | **bsr** | **group** | **mvpn** | **neighbor**] **Example:** `Device# debug ipv6 pim`	Enables debugging on PIM protocol activity.

Configuring PIM Options

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 pim** [**vrf** *vrf-name*] **spt-threshold infinity** [**group-list** *access-list-name*]
4. **ipv6 pim** [**vrf** *vrf-name*] **accept-register** {**list** *access-list* | **route-map** *map-name*}
5. **interface** *type number*
6. **ipv6 pim dr-priority** *value*
7. **ipv6 pim hello-interval** *seconds*
8. **ipv6 pim join-prune-interval** *seconds*
9. **exit**
10. **show ipv6 pim** [**vrf** *vrf-name*] **join-prune statistic** [*interface-type*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Device> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 pim** [**vrf** *vrf-name*] **spt-threshold infinity** [**group-list** *access-list-name*] **Example:** `Device(config)# ipv6 pim spt-threshold infinity group-list acc-grp-1`	Configures when a PIM leaf device joins the SPT for the specified groups.
Step 4	**ipv6 pim** [**vrf** *vrf-name*] **accept-register** {**list** *access-list* | **route-map** *map-name*} **Example:** `Device(config)# ipv6 pim accept-register route-map reg-filter`	Accepts or rejects registers at the RP.
Step 5	**interface** *type number* **Example:** `Device(config)# interface FastEthernet 1/0`	Specifies an interface type and number, and places the device in interface configuration mode.
Step 6	**ipv6 pim dr-priority** *value* **Example:** `Device(config-if)# ipv6 pim dr-priority 3`	Configures the DR priority on a PIM device.
Step 7	**ipv6 pim hello-interval** *seconds* **Example:** `Device(config-if)# ipv6 pim hello-interval 45`	Configures the frequency of PIM hello messages on an interface.
Step 8	**ipv6 pim join-prune-interval** *seconds* **Example:** `Device(config-if)# ipv6 pim join-prune-interval 75`	Configures periodic join and prune announcement intervals for a specified interface.

	Command or Action	Purpose
Step 9	**exit** **Example:** `Device(config-if)# exit`	Enter this command twice to exit interface configuration mode and enter privileged EXEC mode.
Step 10	**show ipv6 pim** [**vrf** *vrf-name*] **join-prune statistic** [*interface-type*] **Example:** `Device# show ipv6 pim join-prune statistic`	Displays the average join-prune aggregation for the most recently aggregated packets for each interface.

Resetting the PIM Traffic Counters

If PIM malfunctions, or in order to verify that the expected number of PIM packets are received and sent, clear PIM traffic counters. Once the traffic counters are cleared, you can verify that PIM is functioning correctly and that PIM packets are being received and sent correctly.

SUMMARY STEPS

1. **enable**
2. **clear ipv6 pim** [**vrf** *vrf-name*] **traffic**
3. **show ipv6 pim** [**vrf** *vrf-name*] **traffic**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**clear ipv6 pim** [**vrf** *vrf-name*] **traffic** **Example:** `Device# clear ipv6 pim traffic`	Resets the PIM traffic counters.

	Command or Action	Purpose
Step 3	**show ipv6 pim** [**vrf** *vrf-name*] **traffic** **Example:** `Device# show ipv6 pim traffic`	Displays the PIM traffic counters.

Turning Off IPv6 PIM on a Specified Interface

A user might want only specified interfaces to perform IPv6 multicast and will therefore want to turn off PIM on a specified interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **no ipv6 pim**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface FastEthernet 1/0`	Specifies an interface type and number, and places the device in interface configuration mode.
Step 4	**no ipv6 pim** **Example:** `Device(config-if)# no ipv6 pim`	Turns off IPv6 PIM on a specified interface.

Configuration Examples for IPv6 Multicast PIM Sparse Mode

Example: Enabling IPv6 Multicast Routing

The following example enables multicast routing on all interfaces and also enables multicast forwarding for PIM and MLD on all enabled interfaces of the device.

```
Device> enable
Device# configure terminal
Device(config)# ipv6 multicast-routing
```

Example: Configuring PIM

The following example shows how to configure a device to use PIM-SM using 2001:DB8::1 as the RP. It sets the SPT threshold to infinity to prevent switchover to the source tree when a source starts sending traffic and sets a filter on all sources that do not have a local multicast BGP prefix.

```
Device(config)# ipv6 multicast-routing
Device(config)# ipv6 pim rp-address 2001:DB8::1
Device(config)# ipv6 pim spt-threshold infinity
Device(config)# ipv6 pim accept-register route-map reg-filter
```

Example: Displaying IPv6 PIM Topology Information

```
Device# show ipv6 pim topology

IP PIM Multicast Topology Table
Entry state:(*/S,G)[RPT/SPT] Protocol Uptime Info
Entry flags:KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive,
    RA - Really Alive, LH - Last Hop, DSS - Don't Signal Sources,
    RR - Register Received, SR - Sending Registers, E - MSDP External,
    DCC - Don't Check Connected
Interface state:Name, Uptime, Fwd, Info
Interface flags:LI - Local Interest, LD - Local Dissinterest,
II - Internal Interest, ID - Internal Dissinterest,
LH - Last Hop, AS - Assert, AB - Admin Boundary

(*,FF05::1)
SM UP:02:26:56 JP:Join(now) Flags:LH
RP:2001:DB8:1:1:2
RPF:Ethernet1/1,FE81::1
  Ethernet0/1          02:26:56  fwd LI LH

(2001:DB8:1:1:200,FF05::1)
SM UP:00:00:07 JP:Null(never) Flags:
RPF:Ethernet1/1,FE80::30:1:4
  Ethernet1/1          00:00:07  off LI
```

Example: Displaying PIM-SM Information for a Group Range

This example displays information about interfaces configured for PIM:

```
Device# show ipv6 pim interface state-on

Interface          PIM  Nbr   Hello  DR
                        Count Intvl  Prior

Ethernet0          on   0     30     1
    Address:FE80::208:20FF:FE08:D7FF
    DR     :this system
POS1/0             on   0     30     1
    Address:FE80::208:20FF:FE08:D554
    DR     :this system
POS4/0             on   1     30   1
    Address:FE80::208:20FF:FE08:D554
    DR     :FE80::250:E2FF:FE8B:4C80
POS4/1             on   0     30   1
    Address:FE80::208:20FF:FE08:D554
    DR     :this system
Loopback0          on   0     30     1
    Address:FE80::208:20FF:FE08:D554
    DR     :this system
```

This example displays an IPv6 multicast group mapping table:

```
Device# show ipv6 pim group-map

FF33::/32*
      SSM
      Info source:Static
      Uptime:00:08:32, Groups:0
  FF34::/32*
      SSM
      Info source:Static
      Uptime:00:09:42, Groups:0
```

This example displays information about IPv6 multicast range lists:

```
Device# show ipv6 pim range-list

config SSM Exp:never Learnt from :::
 FF33::/32 Up:00:26:33
 FF34::/32 Up:00:26:33
 FF35::/32 Up:00:26:33
 FF36::/32 Up:00:26:33
 FF37::/32 Up:00:26:33
 FF38::/32 Up:00:26:33
 FF39::/32 Up:00:26:33
 FF3A::/32 Up:00:26:33
 FF3B::/32 Up:00:26:33
 FF3C::/32 Up:00:26:33
 FF3D::/32 Up:00:26:33
 FF3E::/32 Up:00:26:33
 FF3F::/32 Up:00:26:33
config SM RP:40::1:1:1 Exp:never Learnt from :::
 FF13::/64 Up:00:03:50
config SM RP:40::1:1:3 Exp:never Learnt from :::
 FF09::/64 Up:00:03:50
```

Example: Configuring PIM Options

The following example sets the DR priority, the PIM hello interval, and the periodic join and prune announcement interval on Ethernet interface 0/0.

```
Device(config)# interface Ethernet0/0
```

```
Device(config)# ipv6 pim hello-interval 60
Device(config)# ipv6 pim dr-priority 3
```

Example: Displaying Information About PIM Traffic

```
Device# show ipv6 pim traffic

PIM Traffic Counters
Elapsed time since counters cleared:00:05:29

                              Received     Sent
Valid PIM Packets               22          22
Hello                           22          22
Join-Prune                      0           0
Register                        0           0
Register Stop                   0           0
Assert                          0           0
Bidir DF Election               0           0

Errors:
Malformed Packets                           0
Bad Checksums                               0
Send Errors                                 0
Packet Sent on Loopback Errors              0
Packets Received on PIM-disabled Interface  0
Packets Received with Unknown PIM Version   0
```

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	*IPv6 Configuration Guide*
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IP multicast commands	Cisco IOS IP Multicast Command Reference
IPv6 commands	Cisco IOS IPv6 Command Reference
Cisco IOS IPv6 features	Cisco IOS IPv6 Feature Mapping

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	*IPv6 RFCs*

MIBs

MIB	MIBs Link
	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for IPv6 Multicast PIM Sparse Mode

Table 20: Feature Information for IPv6 Multicast: PIM Sparse Mode

Feature Name	Releases	Feature Information
IPv6 Multicast: PIM Accept Register	12.0(26)S 12.3(4)T 12.2(25)S 12.2(25)SG 12.2(33)SRA 12.2(33)SXH 12.4 12.4(2)T Cisco IOS XE Release 2.1 15.0(1)S	The PIM accept register feature is the ability to perform PIM-SM register message filtering at the RP. The following commands were introduced or modified: **ipv6 pim accept-register**.

Feature Name	Releases	Feature Information
IPv6 Multicast: PIM Embedded RP Support	12.3(4)T 12.4 12.2(40)SG 15.0(2)SG 12.2(33)SRA 12.2(33)SXH	Embedded RP support allows the router to learn RP information using the multicast group destination address instead of the statically configured RP. The following commands were introduced or modified: **ipv6 pim**, **ipv6 pim rp embedded**.
IPv6 Multicast: PIM Sparse Mode	12.0(26)S 12.2(18)S 12.2(25)SG 12.2(33)SRA 12.3(2)T 12.4 12.4(2)T Cisco IOS XE Release 2.4 15.0(1)S	PIM-SM uses unicast routing to provide reverse-path information for multicast tree building. PIM-SM is used in a multicast network when relatively few routers are involved in each multicast and these routers do not forward multicast packets for a group, unless there is an explicit request for the traffic. The following commands were introduced or modified: **clear ipv6 pim topology**, **debug ipv6 pim**, **debug ipv6 pim neighbor**, **ipv6 pim**, **ipv6 pim dr-priority**, **ipv6 pim hello-interval**, **ipv6 pim rp-address** , **ipv6 pim spt-threshold infinity**, **show ipv6 mroute**, **show ipv6 pim group-map**, **show ipv6 pim interface**, **show ipv6 pim neighbor**, **show ipv6 pim range-list**, **show ipv6 pim topology**, **show ipv6 pim tunnel**.

CHAPTER 18

IPv6 Multicast: Static Multicast Routing for IPv6

IPv6 static multicast routes, or mroutes, share the same database as IPv6 static routes and are implemented by extending static route support for reverse path forwarding (RPF) checks.

- Finding Feature Information, page 297
- Information About IPv6 Static Mroutes, page 297
- How to Configure IPv6 Static Multicast Routes, page 298
- Configuration Examples for IPv6 Static Multicast Routes, page 299
- Additional References, page 300
- Feature Information for IPv6 Multicast: Static Multicast Routing for IPv6, page 301

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About IPv6 Static Mroutes

IPv6 static mroutes behave much in the same way as IPv4 static mroutes used to influence the RPF check. IPv6 static mroutes share the same database as IPv6 static routes and are implemented by extending static route support for RPF checks. Static mroutes support equal-cost multipath mroutes, and they also support unicast-only static routes.

How to Configure IPv6 Static Multicast Routes

Configuring Static Mroutes

Static multicast routes (mroutes) in IPv6 can be implemented as an extension of IPv6 static routes. You can configure your device to use a static route for unicast routing only, to use a static multicast route for multicast RPF selection only, or to use a static route for both unicast routing and multicast RPF selection.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 route** *ipv6-prefix* / *prefix-length* *ipv6-address* | *interface-type interface-number ipv6-address*]} [*administrative-distance*] [*administrative-multicast-distance* | **unicast**| **multicast**] [**tag** *tag*
4. **end**
5. **show ipv6 mroute** [**vrf** *vrf-name*] [**link-local** | [*group-name* | *group-address* [*source-address* | *source-name*]] [**summary**] [**count**]
6. **show ipv6 mroute** [**vrf** *vrf-name*] [**link-local** | *group-name* | *group-address*] **active**[*kbps*]
7. **show ipv6 rpf** [**vrf** *vrf-name*] *ipv6-prefix*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 route** *ipv6-prefix* / *prefix-length* *ipv6-address* | *interface-type interface-number ipv6-address*]} [*administrative-distance*] [*administrative-multicast-distance* | **unicast**| **multicast**] [**tag** *tag* **Example:** `Device(config)# ipv6 route 2001:DB8::/64 6::6 100`	Establishes static IPv6 routes. The example shows a static route used for both unicast routing and multicast RPF selection.

	Command or Action	Purpose
Step 4	**end** **Example:** `Device(config-if)# end`	Exits to privileged EXEC mode.
Step 5	**show ipv6 mroute** [**vrf** *vrf-name*] [**link-local** | [*group-name* | *group-address* [*source-address* | *source-name*]] [**summary**] [**count**] **Example:** `Device# show ipv6 mroute ff07::1`	Displays the contents of the IPv6 multicast routing table.
Step 6	**show ipv6 mroute** [**vrf** *vrf-name*] [**link-local** | *group-name* | *group-address*] **active**[*kbps*] **Example:** `Device# show ipv6 mroute active`	Displays the active multicast streams on the device.
Step 7	**show ipv6 rpf** [**vrf** *vrf-name*] *ipv6-prefix* **Example:** `Device# show ipv6 rpf 2001:DB8::1:1:2`	Checks RPF information for a given unicast host address and prefix.

Configuration Examples for IPv6 Static Multicast Routes

Example: Configuring Static Mroutes

Using the **show ipv6 mroute** command allows you to verify that multicast IPv6 data is flowing:

```
Device# show ipv6 mroute ff07::1

Multicast Routing Table
Flags:D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers:Uptime/Expires
Interface state:Interface, State

(*, FF07::1), 00:04:45/00:02:47, RP 2001:DB8:6::6, flags:S
  Incoming interface:Tunnel5
  RPF nbr:6:6:6::6
  Outgoing interface list:
    POS4/0, Forward, 00:04:45/00:02:47

(2001:DB8:999::99, FF07::1), 00:02:06/00:01:23, flags:SFT
```

```
  Incoming interface:POS1/0
  RPF nbr:2001:DB8:999::99
  Outgoing interface list:
    POS4/0, Forward, 00:02:06/00:03:27
```

The following sample output displays information from the **show ipv6 mroute active** command:

```
Device# show ipv6 mroute active

Active IPv6 Multicast Sources - sending >= 4 kbps
Group:FF05::1
 Source:2001:DB8:1:1:1
   Rate:11 pps/8 kbps(1sec), 8 kbps(last 8 sec)
```

The following example displays RPF information for the unicast host with the IPv6 address of 2001:DB8:1:1:2:

```
Device# show ipv6 rpf 2001:DB8:1:1:2

RPF information for 2001:DB8:1:1:2
  RPF interface:Ethernet3/2
  RPF neighbor:FE80::40:1:3
  RPF route/mask:20::/64
  RPF type:Unicast
  RPF recursion count:0
  Metric preference:110
  Metric:30
```

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	*IPv6 Configuration Guide*
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IP multicast commands	Cisco IOS IP Multicast Command Reference
IPv6 commands	Cisco IOS IPv6 Command Reference
Cisco IOS IPv6 features	Cisco IOS IPv6 Feature Mapping

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	*IPv6 RFCs*

MIBs

MIB	MIBs Link
	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for IPv6 Multicast: Static Multicast Routing for IPv6

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 21: Feature Information for IPv6 Multicast: Static Multicast Routing for IPv6

Feature Name	Releases	Feature Information
IPv6 Multicast: Static Multicast Routing (mroute) for IPv6	12.0(26)S 12.3(4)T 12.2(25)S 12.2(33)SRA 12.2(33)SXH 12.4 12.4(2)T Cisco IOS XE Release 2.4 15.0(1)S	IPv6 static mroutes share the same database as IPv6 static routes and are implemented by extending static route support. The following commands were introduced or modified: **ipv6 route**, **show ipv6 mroute**, **show ipv6 mroute active**, **show ipv6 rpf**.

CHAPTER 19

IPv6 Multicast: PIM Source-Specific Multicast

The PIM source-specific multicast (SSM) routing protocol supports SSM implementation and is derived from PIM-SM. However, unlike PIM-SM data from all multicast sources are sent when there is a PIM join, the SSM feature forwards datagram traffic to receivers from only those multicast sources that the receivers have explicitly joined, thus optimizing bandwidth utilization and denying unwanted Internet broadcast traffic.

- Finding Feature Information, page 303
- Prerequisites for IPv6 Multicast: PIM Source-Specific Multicast , page 303
- Information About IPv6 Multicast: PIM Source-Specific Multicast, page 304
- How to Configure IPv6 Multicast: PIM Source-Specific Multicast, page 308
- Configuration Examples for IPv6 Multicast: PIM Source-Specific Multicast, page 312
- Additional References, page 314
- Feature Information for IPv6 Multicast: PIM Source-Specific Multicast, page 315

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for IPv6 Multicast: PIM Source-Specific Multicast

- Multicast Listener Discovery (MLD) version 2 is required for source-specific multicast (SSM) to operate.
- Before SSM will run with MLD, SSM must be supported by the Cisco IPv6 device, the host where the application is running, and the application itself.

Information About IPv6 Multicast: PIM Source-Specific Multicast

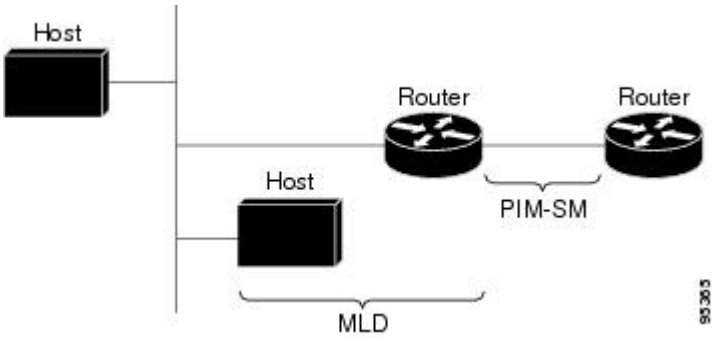
IPv6 Multicast Routing Implementation

Cisco software supports the following protocols to implement IPv6 multicast routing:

- MLD is used by IPv6 devices to discover multicast listeners (nodes that want to receive multicast packets destined for specific multicast addresses) on directly attached links. There are two versions of MLD:
  - MLD version 1 is based on version 2 of the Internet Group Management Protocol (IGMP) for IPv4.
  - MLD version 2 is based on version 3 of the IGMP for IPv4.
- IPv6 multicast for Cisco software uses both MLD version 2 and MLD version 1. MLD version 2 is fully backward-compatible with MLD version 1 (described in RFC 2710). Hosts that support only MLD version 1 will interoperate with a device running MLD version 2. Mixed LANs with both MLD version 1 and MLD version 2 hosts are likewise supported.
- PIM-SM is used between devices so that they can track which multicast packets to forward to each other and to their directly connected LANs.
- PIM in Source Specific Multicast (PIM-SSM) is similar to PIM-SM with the additional ability to report interest in receiving packets from specific source addresses (or from all but the specific source addresses) to an IP multicast address.

The figure below shows where MLD and PIM-SM operate within the IPv6 multicast environment.

Figure 21: IPv6 Multicast Routing Protocols Supported for IPv6



Protocol Independent Multicast

Protocol Independent Multicast (PIM) is used between devices so that they can track which multicast packets to forward to each other and to their directly connected LANs. PIM works independently of the unicast routing protocol to perform send or receive multicast route updates like other protocols. Regardless of which unicast routing protocols are being used in the LAN to populate the unicast routing table, Cisco IOS PIM uses the

existing unicast table content to perform the Reverse Path Forwarding (RPF) check instead of building and maintaining its own separate routing table.

You can configure IPv6 multicast to use either a PIM- Sparse Mode (SM) or PIM-Source Specific Multicast (SSM) operation, or you can use both PIM-SM and PIM-SSM together in your network.

PIM-Source Specific Multicast

PIM-SSM is the routing protocol that supports the implementation of SSM and is derived from PIM-SM. However, unlike PIM-SM where data from all multicast sources are sent when there is a PIM join, the SSM feature forwards datagram traffic to receivers from only those multicast sources that the receivers have explicitly joined, thus optimizing bandwidth utilization and denying unwanted Internet broadcast traffic. Further, instead of the use of RP and shared trees, SSM uses information found on source addresses for a multicast group. This information is provided by receivers through the source addresses relayed to the last-hop devices by MLD membership reports, resulting in shortest-path trees directly to the sources.

In SSM, delivery of datagrams is based on (S, G) channels. Traffic for one (S, G) channel consists of datagrams with an IPv6 unicast source address S and the multicast group address G as the IPv6 destination address. Systems will receive this traffic by becoming members of the (S, G) channel. Signaling is not required, but receivers must subscribe or unsubscribe to (S, G) channels to receive or not receive traffic from specific sources.

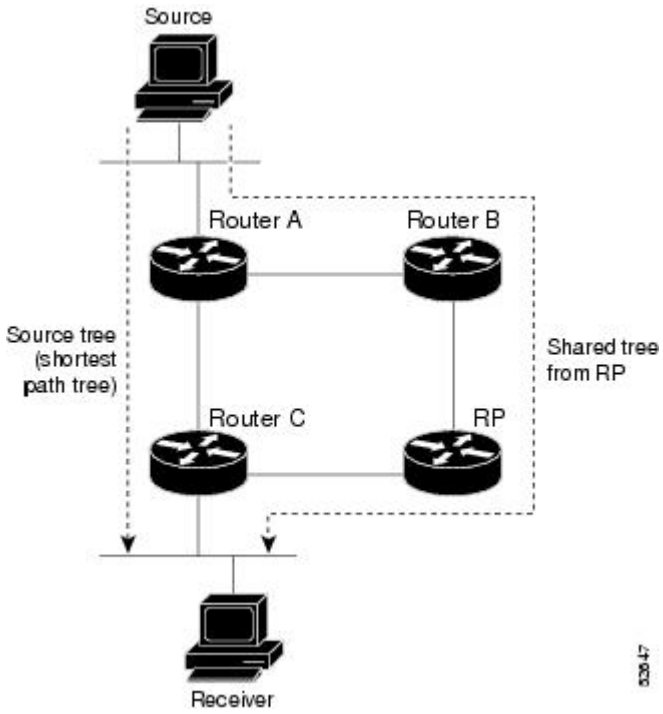
MLD version 2 is required for SSM to operate. MLD allows the host to provide source information. Before SSM will run with MLD, SSM must be supported in the Cisco IPv6 device, the host where the application is running, and the application itself.

PIM Shared Tree and Source Tree (Shortest-Path Tree)

By default, members of a group receive data from senders to the group across a single data distribution tree rooted at the RP. This type of distribution tree is called shared tree or rendezvous point tree (RPT), as illustrated

in the figure below. Data from senders is delivered to the RP for distribution to group members joined to the shared tree.

Figure 22: Shared Tree and Source Tree (Shortest Path Tree)



If the data threshold warrants, leaf devices on the shared tree may initiate a switch to the data distribution tree rooted at the source. This type of distribution tree is called a shortest path tree or source tree. By default, the software switches to a source tree upon receiving the first data packet from a source.

The following process details the move from shared tree to source tree:

1. Receiver joins a group; leaf Device C sends a join message toward the RP.
2. RP puts the link to Device C in its outgoing interface list.
3. Source sends the data; Device A encapsulates the data in the register and sends it to the RP.
4. RP forwards the data down the shared tree to Device C and sends a join message toward the source. At this point, data may arrive twice at Device C, once encapsulated and once natively.
5. When data arrives natively (unencapsulated) at the RP, the RP sends a register-stop message to Device A.
6. By default, receipt of the first data packet prompts Device C to send a join message toward the source.
7. When Device C receives data on (S, G), it sends a prune message for the source up the shared tree.
8. RP deletes the link to Device C from the outgoing interface of (S, G).
9. RP triggers a prune message toward the source.

Join and prune messages are sent for sources and RPs. They are sent hop-by-hop and are processed by each PIM device along the path to the source or RP. Register and register-stop messages are not sent hop-by-hop.

They are sent by the designated router (DR) that is directly connected to a source and are received by the RP for the group.

Reverse Path Forwarding

Reverse-path forwarding is used for forwarding multicast datagrams. It functions as follows:

- If a device receives a datagram on an interface it uses to send unicast packets to the source, the packet has arrived on the RPF interface.
- If the packet arrives on the RPF interface, a device forwards the packet out the interfaces present in the outgoing interface list of a multicast routing table entry.
- If the packet does not arrive on the RPF interface, the packet is silently discarded to prevent loops.

PIM uses both source trees and RP-rooted shared trees to forward datagrams; the RPF check is performed differently for each, as follows:

- If a PIM device has source-tree state (that is, an (S, G) entry is present in the multicast routing table), the device performs the RPF check against the IPv6 address of the source of the multicast packet.
- If a PIM device has shared-tree state (and no explicit source-tree state), it performs the RPF check on the RP's address (which is known when members join the group).

Sparse-mode PIM uses the RPF lookup function to determine where it needs to send joins and prunes. (S, G) joins (which are source-tree states) are sent toward the source. (*, G) joins (which are shared-tree states) are sent toward the RP.

Note To do a RPF check, use the **show ipv6 rpf hostname** or **show ipv6 rpf vrf vrf_name hostname** command.

How to Configure IPv6 Multicast: PIM Source-Specific Multicast

Configuring PIM Options

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 pim** [**vrf** *vrf-name*] **spt-threshold infinity** [**group-list** *access-list-name*]
4. **ipv6 pim** [**vrf** *vrf-name*] **accept-register** {**list** *access-list* | **route-map** *map-name*}
5. **interface** *type number*
6. **ipv6 pim dr-priority** *value*
7. **ipv6 pim hello-interval** *seconds*
8. **ipv6 pim join-prune-interval** *seconds*
9. **exit**
10. **show ipv6 pim** [**vrf** *vrf-name*] **join-prune statistic** [*interface-type*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 pim** [**vrf** *vrf-name*] **spt-threshold infinity** [**group-list** *access-list-name*] **Example:** `Device(config)# ipv6 pim spt-threshold infinity group-list acc-grp-1`	Configures when a PIM leaf device joins the SPT for the specified groups.
Step 4	**ipv6 pim** [**vrf** *vrf-name*] **accept-register** {**list** *access-list* | **route-map** *map-name*}	Accepts or rejects registers at the RP.

	Command or Action	Purpose
	Example: `Device(config)# ipv6 pim accept-register route-map reg-filter`	
Step 5	**interface** *type number* **Example:** `Device(config)# interface FastEthernet 1/0`	Specifies an interface type and number, and places the device in interface configuration mode.
Step 6	**ipv6 pim dr-priority** *value* **Example:** `Device(config-if)# ipv6 pim dr-priority 3`	Configures the DR priority on a PIM device.
Step 7	**ipv6 pim hello-interval** *seconds* **Example:** `Device(config-if)# ipv6 pim hello-interval 45`	Configures the frequency of PIM hello messages on an interface.
Step 8	**ipv6 pim join-prune-interval** *seconds* **Example:** `Device(config-if)# ipv6 pim join-prune-interval 75`	Configures periodic join and prune announcement intervals for a specified interface.
Step 9	**exit** **Example:** `Device(config-if)# exit`	Enter this command twice to exit interface configuration mode and enter privileged EXEC mode.
Step 10	**show ipv6 pim** [**vrf** *vrf-name*] **join-prune statistic** [*interface-type*] **Example:** `Device# show ipv6 pim join-prune statistic`	Displays the average join-prune aggregation for the most recently aggregated packets for each interface.

Resetting the PIM Traffic Counters

If PIM malfunctions, or in order to verify that the expected number of PIM packets are received and sent, clear PIM traffic counters. Once the traffic counters are cleared, you can verify that PIM is functioning correctly and that PIM packets are being received and sent correctly.

SUMMARY STEPS

1. **enable**
2. **clear ipv6 pim** [**vrf** *vrf-name*] **traffic**
3. **show ipv6 pim** [**vrf** *vrf-name*] **traffic**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**clear ipv6 pim** [**vrf** *vrf-name*] **traffic** **Example:** `Device# clear ipv6 pim traffic`	Resets the PIM traffic counters.
Step 3	**show ipv6 pim** [**vrf** *vrf-name*] **traffic** **Example:** `Device# show ipv6 pim traffic`	Displays the PIM traffic counters.

Clearing the PIM Topology Table to Reset the MRIB Connection

No configuration is necessary to use the MRIB. However, users may in certain situations want to clear the PIM topology table in order to reset the MRIB connection and verify MRIB information.

SUMMARY STEPS

1. **enable**
2. **clear ipv6 pim** [**vrf** *vrf-name*] **topology** [*group-name* | *group-address*]
3. **show ipv6 mrib** [**vrf** *vrf-name*] **client** [**filter**] [**name** {*client-name* | *client-name* **:** *client-id*}]
4. **show ipv6 mrib** [**vrf** *vrf-name*] **route** [**link-local**| **summary** | [*sourceaddress-or-name* | *****] [*groupname-or-address* [*prefix-length*]]]
5. **show ipv6 pim** [**vrf** *vrf-name*] **topology** [*groupname-or-address* [*sourcename-or-address*] | **link-local** | **route-count** [**detail**]]
6. **debug ipv6 mrib** [**vrf** *vrf-name*] **client**
7. **debug ipv6 mrib** [**vrf** *vrf-name*] **io**
8. **debug ipv6 mrib proxy**
9. **debug ipv6 mrib** [**vrf** *vrf-name*] **route** [*group-name* | *group-address*]
10. **debug ipv6 mrib** [**vrf** *vrf-name*] **table**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**clear ipv6 pim** [**vrf** *vrf-name*] **topology** [*group-name* | *group-address*] **Example:** `Device# clear ipv6 pim topology FF04::10`	Clears the PIM topology table.
Step 3	**show ipv6 mrib** [**vrf** *vrf-name*] **client** [**filter**] [**name** {*client-name* | *client-name* **:** *client-id*}] **Example:** `Device# show ipv6 mrib client`	Displays multicast-related information about an interface.
Step 4	**show ipv6 mrib** [**vrf** *vrf-name*] **route** [**link-local**| **summary** | [*sourceaddress-or-name* | *****] [*groupname-or-address* [*prefix-length*]]] **Example:** `Device# show ipv6 mrib route`	Displays the MRIB route information.

	Command or Action	Purpose
Step 5	**show ipv6 pim** [**vrf** *vrf-name*] **topology** [*groupname-or-address* [*sourcename-or-address*] | **link-local** | **route-count** [**detail**]] **Example:** `Device# show ipv6 pim topology`	Displays PIM topology table information for a specific group or all groups.
Step 6	**debug ipv6 mrib** [**vrf** *vrf-name*] **client** **Example:** `Device# debug ipv6 mrib client`	Enables debugging on MRIB client management activity.
Step 7	**debug ipv6 mrib** [**vrf** *vrf-name*] **io** **Example:** `Device# debug ipv6 mrib io`	Enables debugging on MRIB I/O events.
Step 8	**debug ipv6 mrib proxy** **Example:** `Device# debug ipv6 mrib proxy`	Enables debugging on MRIB proxy activity between the route processor and line cards on distributed router platforms.
Step 9	**debug ipv6 mrib** [**vrf** *vrf-name*] **route** [*group-name* | *group-address*] **Example:** `Device# debug ipv6 mrib route`	Displays information about MRIB routing entry-related activity.
Step 10	**debug ipv6 mrib** [**vrf** *vrf-name*] **table** **Example:** `Device# debug ipv6 mrib table`	Enables debugging on MRIB table management activity.

Configuration Examples for IPv6 Multicast: PIM Source-Specific Multicast

Example: Displaying IPv6 PIM Topology Information

```
Device# show ipv6 pim topology
```

```
IP PIM Multicast Topology Table
Entry state:(*/S,G)[RPT/SPT] Protocol Uptime Info
Entry flags:KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive,
    RA - Really Alive, LH - Last Hop, DSS - Don't Signal Sources,
    RR - Register Received, SR - Sending Registers, E - MSDP External,
    DCC - Don't Check Connected
Interface state:Name, Uptime, Fwd, Info
Interface flags:LI - Local Interest, LD - Local Dissinterest,
II - Internal Interest, ID - Internal Dissinterest,
LH - Last Hop, AS - Assert, AB - Admin Boundary

(*,FF05::1)
SM UP:02:26:56 JP:Join(now) Flags:LH
RP:2001:DB8:1:1:2
RPF:Ethernet1/1,FE81::1
  Ethernet0/1          02:26:56  fwd LI LH

(2001:DB8:1:1:200,FF05::1)
SM UP:00:00:07 JP:Null(never) Flags:
RPF:Ethernet1/1,FE80::30:1:4
  Ethernet1/1          00:00:07  off LI
```

Example: Configuring Join/Prune Aggregation

The following example shows how to provide the join/prune aggregation on Ethernet interface 0/0:

```
Device# show ipv6 pim join-prune statistic Ethernet0/0

PIM Average Join/Prune Aggregation for last (1K/10K/50K) packets
Interface             Transmitted             Received
Ethernet0/0      0    / 0             1    / 0
```

Example: Displaying Information About PIM Traffic

```
Device# show ipv6 pim traffic

PIM Traffic Counters
Elapsed time since counters cleared:00:05:29

                              Received     Sent
Valid PIM Packets               22          22
Hello                           22          22
Join-Prune                      0           0
Register                        0           0
Register Stop                   0           0
Assert                          0           0
Bidir DF Election               0           0

Errors:
Malformed Packets                           0
Bad Checksums                               0
Send Errors                                 0
Packet Sent on Loopback Errors              0
Packets Received on PIM-disabled Interface  0
Packets Received with Unknown PIM Version   0
```

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	*IPv6 Configuration Guide*
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IP multicast commands	Cisco IOS IP Multicast Command Reference
IPv6 commands	Cisco IOS IPv6 Command Reference
Cisco IOS IPv6 features	Cisco IOS IPv6 Feature Mapping

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	*IPv6 RFCs*

MIBs

MIB	MIBs Link
	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for IPv6 Multicast: PIM Source-Specific Multicast

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 22: Feature Information for IPv6 Multicast: PIM Source-Specific Multicast

Feature Name	Releases	Feature Information
IPv6 Multicast: PIM Source-Specific Multicast	12.0(26)S 12.2(18)S 12.2(25)SG 12.2(33)SRA 12.3(2)T 12.4 12.4(2)T Cisco IOS XE Release 2.1 15.0(1)S	PIM-SSM supports the implementation of SSM and is derived from PIM-SM. The SSM feature forwards datagram traffic to receivers from only those multicast sources that the receivers have explicitly joined, optimizing bandwidth utilization and denying unwanted Internet broadcast traffic. The following commands were introduced or modified: **clear ipv6 pim topology**, **debug ipv6 pim**, **debug ipv6 pim neighbor**, **ipv6 pim**, **ipv6 pim dr-priority**, **ipv6 pim hello-interval**, **ipv6 pim rp-address** , **ipv6 pim spt-threshold infinity**, **show ipv6 mroute**, **show ipv6 pim group-map**, **show ipv6 pim interface**, **show ipv6 pim neighbor**, **show ipv6 pim range-list**, **show ipv6 pim topology**, **show ipv6 pim tunnel**.

CHAPTER 20

IPv6 Source Specific Multicast Mapping

Source-specific multicast (SSM) SSM mapping for IPv6 supports both static and dynamic Domain Name System (DNS) mapping for MLD version 1 receivers. This feature allows deployment of IPv6 SSM with hosts that are incapable of providing MLD version 2 support in their TCP/IP host stack and their IP multicast receiving application.

- Finding Feature Information, page 317
- Information About IPv6 Source Specific Multicast Mapping, page 317
- How to Configure IPv6 Source Specific Multicast Mapping, page 318
- Configuration Examples for IPv6 Source Specific Multicast Mapping, page 319
- Additional References, page 320
- Feature Information for IPv6 Source Specific Multicast Mapping, page 321

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About IPv6 Source Specific Multicast Mapping

SSM mapping for IPv6 supports both static and dynamic Domain Name System (DNS) mapping for MLD version 1 receivers. This feature allows deployment of IPv6 SSM with hosts that are incapable of providing MLD version 2 support in their TCP/IP host stack and their IP multicast receiving application.

SSM mapping allows the device to look up the source of a multicast MLD version 1 report either in the running configuration of the device or from a DNS server. The device can then initiate an (S, G) join toward the source.

How to Configure IPv6 Source Specific Multicast Mapping

Configuring IPv6 SSM

When the SSM mapping feature is enabled, DNS-based SSM mapping is automatically enabled, which means that the device will look up the source of a multicast MLD version 1 report from a DNS server.

You can configure either DNS-based or static SSM mapping, depending on your device configuration. If you choose to use static SSM mapping, you can configure multiple static SSM mappings. If multiple static SSM mappings are configured, the source addresses of all matching access lists will be used.

Before You Begin

Note To use DNS-based SSM mapping, the device needs to find at least one correctly configured DNS server to which the device can be directly attached.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 mld** [**vrf** *vrf-name*] **ssm-map enable**
4. **no ipv6 mld** [**vrf** *vrf-name*] **ssm-map query dns**
5. **ipv6 mld** [**vrf** *vrf-name*] **ssm-map static** *access-list source-address*
6. **end**
7. **show ipv6 mld** [**vrf** *vrf-name*] **ssm-map** [*source-address*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**ipv6 mld** [**vrf** *vrf-name*] **ssm-map enable** **Example:** `Device(config)# ipv6 mld ssm-map enable`	Enables the SSM mapping feature for groups in the configured SSM range.
Step 4	**no ipv6 mld** [**vrf** *vrf-name*] **ssm-map query dns** **Example:** `Device(config)# no ipv6 mld ssm-map query dns`	Disables DNS-based SSM mapping.
Step 5	**ipv6 mld** [**vrf** *vrf-name*] **ssm-map static** *access-list source-address* **Example:** `Device(config)# ipv6 mld ssm-map static SSM_MAP_ACL_2 2001:DB8:1::1`	Configures static SSM mappings.
Step 6	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.
Step 7	**show ipv6 mld** [**vrf** *vrf-name*] **ssm-map** [*source-address*] **Example:** `Device# show ipv6 mld ssm-map`	Displays SSM mapping information.

Configuration Examples for IPv6 Source Specific Multicast Mapping

Example: IPv6 SSM Mapping

```
Device# show ipv6 mld ssm-map 2001:DB8::1

 Group address  : 2001:DB8::1
 Group mode ssm : TRUE
 Database       : STATIC
 Source list    : 2001:DB8::2
                  2001:DB8::3

Device# show ipv6 mld ssm-map 2001:DB8::2
```

```
Group address  : 2001:DB8::2
Group mode ssm : TRUE
Database       : DNS
Source list    : 2001:DB8::3
                 2001:DB8::1
```

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	*IPv6 Configuration Guide*
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IP multicast commands	Cisco IOS IP Multicast Command Reference
IPv6 commands	Cisco IOS IPv6 Command Reference
Cisco IOS IPv6 features	Cisco IOS IPv6 Feature Mapping

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	*IPv6 RFCs*

MIBs

MIB	MIBs Link
	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for IPv6 Source Specific Multicast Mapping

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 23: Feature Information for IPv6 Source Specific Multicast Mapping

Feature Name	Releases	Feature Information
IPv6 Source Specific Multicast Mapping	12.2(33)SRA 12.2(18)SXE 12.4(2)T Cisco IOS XE Release 2.1 15.0(1)S	This feature allows deployment of IPv6 SSM with hosts that are incapable of providing MLD version 2 support in their TCP/IP host stack and their IP multicast receiving application. The following commands were introduced or modified: **ipv6 mld ssm-map enable**, **ipv6 mld ssm-map query dns**, **ipv6 mld ssm-map static**, **show ipv6 mld ssm-map**.

CHAPTER 21

IPv6 Multicast: Explicit Tracking of Receivers

- Finding Feature Information, page 323
- Information About IPv6 Multicast Explicit Tracking of Receivers, page 323
- How to Configure IPv6 Multicast Explicit Tracking of Receivers, page 324
- Configuration Examples for IPv6 Multicast Explicit Tracking of Receivers, page 325
- Additional References, page 325
- Feature Information for IPv6 Multicast: Explicit Tracking of Receivers, page 326

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About IPv6 Multicast Explicit Tracking of Receivers

Explicit Tracking of Receivers

The explicit tracking feature allows a device to track the behavior of the hosts within its IPv6 network. This feature also enables the fast leave mechanism to be used with MLD version 2 host reports.

How to Configure IPv6 Multicast Explicit Tracking of Receivers

Configuring Explicit Tracking of Receivers to Track Host Behavior

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 mld explicit-tracking** *access-list-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface FastEthernet 1/0`	Specifies an interface type and number, and places the device in interface configuration mode.
Step 4	**ipv6 mld explicit-tracking** *access-list-name* **Example:** `Device(config-if)# ipv6 mld explicit-tracking list1`	Enables explicit tracking of hosts.

Configuration Examples for IPv6 Multicast Explicit Tracking of Receivers

Example: Configuring Explicit Tracking of Receivers

```
Device> enable
Device# configure terminal
Device(config)# interface FastEthernet 1/0
Device(config-if)# ipv6 mld explicit-tracking list1
```

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	*IPv6 Configuration Guide*
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IP multicast commands	Cisco IOS IP Multicast Command Reference
IPv6 commands	Cisco IOS IPv6 Command Reference
Cisco IOS IPv6 features	Cisco IOS IPv6 Feature Mapping

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	*IPv6 RFCs*

MIBs

MIB	MIBs Link
	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for IPv6 Multicast: Explicit Tracking of Receivers

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 24: Feature Information for IPv6 Multicast: Explicit Tracking of Receivers

Feature Name	Releases	Feature Information
IPv6 Multicast: Explicit Tracking of Receivers	12.2(25)S 12.2(25)SG 12.2(33)SRA 12.2(33)SXH 12.3(7)T 12.4 12.4(2)T Cisco IOS XE Release 2.1 15.0(1)S	This feature allows a devicer to track the behavior of the hosts within its IPv6 network. The following command was introduced: **ipv6 mld explicit-tracking**.

CHAPTER 22

IPv6 Bidirectional PIM

- Finding Feature Information, page 327
- Restrictions for IPv6 Bidirectional PIM, page 327
- Information About IPv6 Bidirectional PIM, page 328
- How to Configure IPv6 Bidirectional PIM, page 328
- Configuration Examples for IPv6 Bidirectional PIM, page 330
- Additional References, page 330
- Feature Information for IPv6 Bidirectional PIM, page 331

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for IPv6 Bidirectional PIM

When the bidirectional (bidir) range is used in a network, all devices in that network must be able to understand the bidirectional range in the bootstrap message (BSM).

Information About IPv6 Bidirectional PIM

Bidirectional PIM

Bidirectional PIM allows multicast devices to keep reduced state information, as compared with unidirectional shared trees in PIM-SM. Bidirectional shared trees convey data from sources to the RPA and distribute them from the RPA to the receivers. Unlike PIM-SM, bidirectional PIM does not switch over to the source tree, and there is no register encapsulation of data from the source to the RP.

A single designated forwarder (DF) exists for each RPA on every link within a bidirectional PIM domain (including multiaccess and point-to-point links). The only exception is the RPL on which no DF exists. The DF is the device on the link with the best route to the RPA, which is determined by comparing MRIB-provided metrics. A DF for a given RPA forwards downstream traffic onto its link and forwards upstream traffic from its link toward the rendezvous point link (RPL). The DF performs this function for all bidirectional groups that map to the RPA. The DF on a link is also responsible for processing Join messages from downstream devices on the link as well as ensuring that packets are forwarded to local receivers discovered through a local membership mechanism such as MLD.

Bidirectional PIM offers advantages when there are many moderate or low-rate sources. However, the bidirectional shared trees may have worse delay characteristics than do the source trees built in PIM-SM (depending on the topology).

Only static configuration of bidirectional RPs is supported in IPv6.

How to Configure IPv6 Bidirectional PIM

Configuring Bidirectional PIM and Displaying Bidirectional PIM Information

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 pim** [**vrf** *vrf-name*] **rp-address** *ipv6-address* [*group-access-list*] [**bidir**]
4. **exit**
5. **show ipv6 pim** [**vrf** *vrf-name*] **df** [*interface-type interface-number*] [*rp-address*]
6. **show ipv6 pim** [**vrf** *vrf-name*] **df winner**[*interface-type interface-number*] [*rp-address*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Device> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 pim** [**vrf** *vrf-name*] **rp-address** *ipv6-address* [*group-access-list*] [**bidir**] **Example:** `Device(config)# ipv6 pim rp-address 2001:DB8::01:800:200E:8C6C bidir`	Configures the address of a PIM RP for a particular group range. Use of the **bidir** keyword means that the group range will be used for bidirectional shared-tree forwarding.
Step 4	**exit** **Example:** `Device(config-if)# exit`	Exits global configuration mode, and returns the device to privileged EXEC mode.
Step 5	**show ipv6 pim** [**vrf** *vrf-name*] **df** [*interface-type interface-number*] [*rp-address*] **Example:** `Device# show ipv6 pim df`	Displays the designated forwarder (DF)-election state of each interface for RP.
Step 6	**show ipv6 pim** [**vrf** *vrf-name*] **df winner**[*interface-type interface-number*] [*rp-address*] **Example:** `Device# show ipv6 pim df winner ethernet 1/0 200::1`	Displays the DF-election winner on each interface for each RP.

Configuration Examples for IPv6 Bidirectional PIM

Example: Configuring Bidirectional PIM and Displaying Bidirectional PIM Information

The following example displays the DF-election states:

```
Device# show ipv6 pim df

Interface          DF State     Timer         Metrics
Ethernet0/0        Winner       4s 8ms        [120/2]
    RP :200::1
Ethernet1/0        Lose         0s 0ms        [inf/inf]
    RP :200::1
```

The following example displays information on the RP:

```
Device# show ipv6 pim df

Interface          DF State     Timer         Metrics
Ethernet0/0        None:RP LAN 0s 0ms        [inf/inf]
    RP :200::1
Ethernet1/0        Winner       7s 600ms      [0/0]
    RP :200::1
Ethernet2/0        Winner       9s 8ms        [0/0]
    RP :200::1
```

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	*IPv6 Configuration Guide*
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IP multicast commands	Cisco IOS IP Multicast Command Reference
IPv6 commands	Cisco IOS IPv6 Command Reference
Cisco IOS IPv6 features	Cisco IOS IPv6 Feature Mapping

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	*IPv6 RFCs*

MIBs

MIB	MIBs Link
	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for IPv6 Bidirectional PIM

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 25: Feature Information for IPv6 Bidirectional PIM

Feature Name	Releases	Feature Information
IPv6 Bidirectional PIM	12.2(25)SG 12.2(33)SRA 12.2(25)S 12.3(7)T 12.4 12.4(2)T Cisco IOS XE release 2.3 15.0(1)S	Bidirectional PIM allows multicast routers to keep reduced state information. Bidirectional shared trees convey data from sources to the RP and distribute them from the RP to the receivers. The following commands were introduced or modified: **debug ipv6 pim df-election**, **ipv6 pim rp-address**, **show ipv6 pim df**, **show ipv6 pim df winner**.

CHAPTER 23

IPv6 PIM Passive Mode

This feature allows PIM passive mode to be enabled on an interface so that a PIM passive interface cannot send and receive PIM control messages, but it can act as a reverse path forwarding (RPF) interface for multicast route entries, and it can accept and forward multicast data packets.

- Finding Feature Information, page 333
- Information About IPv6 PIM Passive Mode, page 333
- How to Configure IPv6 PIM Passive Mode, page 334
- Additional References, page 335
- Feature Information for IPv6 PIM Passive, page 336

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About IPv6 PIM Passive Mode

A device configured with PIM will always send out PIM hello messages to all interfaces enabled for IPv6 multicast routing, even if the device is configured not to accept PIM messages from any neighbor on the LAN. The IPv6 PIM passive mode feature allows PIM passive mode to be enabled on an interface so that a PIM passive interface cannot send and receive PIM control messages, but it can act as RPF interface for multicast route entries, and it can accept and forward multicast data packets.

How to Configure IPv6 PIM Passive Mode

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 multicast pim-passive-enable**
4. **interface** *type number*
5. **ipv6 pim passive**

DETAILED STEPS

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **ipv6 multicast pim-passive-enable**

Example:

```
Device(config)# ipv6 multicast pim-passive-enable
```

Enables the PIM passive feature on an IPv6 device.

Step 4 **interface** *type number*

Example:

```
Device(config)# interface GigabitEthernet 1/0/0
```

Specifies an interface type and number, and places the device in interface configuration mode.

Step 5 **ipv6 pim passive**

Example:

```
Device(config-if)# ipv6 pim passive
```

Enables the PIM passive feature on a specific interface.

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	*IPv6 Configuration Guide*
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IPv6 commands	Cisco IOS IPv6 Command Reference
Cisco IOS IPv6 features	Cisco IOS IPv6 Feature Mapping

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	*IPv6 RFCs*

MIBs

MIB	MIBs Link
	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for IPv6 PIM Passive

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 26: Feature Information for IPv6 PIM Passive

Feature Name	Releases	Feature Information
IPv6 PIM Passive	Cisco IOS XE Release 2.6	This feature allows PIM passive mode to be enabled on an interface so that a PIM passive interface cannot send and receive PIM control messages, but it can act as RPF interface for multicast route entries, and it can accept and forward multicast data packets. The following commands were introduced or modified: **ipv6 multicast pim-passive-enable**, **ipv6 pim passive**, **show ipv6 pim interface**.

CHAPTER 24

IPv6 Multicast: Routable Address Hello Option

The routable address hello option adds a PIM hello message option that includes all the addresses on the interface on which the PIM hello message is advertised.

- Finding Feature Information, page 337
- Information About the Routable Address Hello Option, page 337
- How to Configure IPv6 Multicast: Routable Address Hello Option, page 338
- Configuration Example for the Routable Address Hello Option, page 339
- Additional References, page 339
- Feature Information for IPv6 Multicast: Routable Address Hello Option, page 340

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About the Routable Address Hello Option

When an IPv6 interior gateway protocol is used to build the unicast routing table, the procedure to detect the upstream device address assumes the address of a PIM neighbor is always same as the address of the next-hop device, as long as they refer to the same device. However, it may not be the case when a device has multiple addresses on a link.

Two typical situations can lead to this situation for IPv6. The first situation can occur when the unicast routing table is not built by an IPv6 interior gateway protocol such as multicast BGP. The second situation occurs when the address of an RP shares a subnet prefix with downstream devices (note that the RP address has to be domain-wide and therefore cannot be a link-local address).

The routable address hello option allows the PIM protocol to avoid such situations by adding a PIM hello message option that includes all the addresses on the interface on which the PIM hello message is advertised. When a PIM device finds an upstream device for some address, the result of RPF calculation is compared with the addresses in this option, in addition to the PIM neighbor's address itself. Because this option includes all the possible addresses of a PIM device on that link, it always includes the RPF calculation result if it refers to the PIM device supporting this option.

Because of size restrictions on PIM messages and the requirement that a routable address hello option fits within a single PIM hello message, a limit of 16 addresses can be configured on the interface.

How to Configure IPv6 Multicast: Routable Address Hello Option

Configuring the Routable Address Hello Option

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 pim hello-interval** *seconds*

DETAILED STEPS

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **interface** *type number*

Example:

```
Device(config)# interface FastEthernet 1/0
```

Specifies an interface type and number, and places the device in interface configuration mode.

Step 4 **ipv6 pim hello-interval** *seconds*

Example:

```
Device(config-if)# ipv6 pim hello-interval 45
```

Configures the frequency of PIM hello messages on an interface.

Configuration Example for the Routable Address Hello Option

The following example shows output from the **show ipv6 pim neighbor** command using the **detail** keyword to identify the additional addresses of the neighbors learned through the routable address hello option:

```
Device# show ipv6 pim neighbor detail

Neighbor Address(es)        Interface     Uptime    Expires DR pri Bidir

FE80::A8BB:CCFF:FE00:401    Ethernet0/0   01:34:16  00:01:16 1      B
60::1:1:3

FE80::A8BB:CCFF:FE00:501    Ethernet0/0   01:34:15  00:01:18 1      B
60::1:1:4
```

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	*IPv6 Configuration Guide*
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IP multicast commands	Cisco IOS IP Multicast Command Reference
IPv6 commands	Cisco IOS IPv6 Command Reference
Cisco IOS IPv6 features	Cisco IOS IPv6 Feature Mapping

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	*IPv6 RFCs*

MIBs

MIB	MIBs Link
	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for IPv6 Multicast: Routable Address Hello Option

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 27: Feature Information for IPv6 Multicast: Routable Address Hello Option

Feature Name	Releases	Feature Information
IPv6 Multicast: Routable Address Hello Option	12.0(26)S 12.3(4)T 12.2(25)S 12.2(25)SG 12.2(33)SRA 12.2(33)SXH 12.4 12.4(2)T Cisco IOS XE Release 2.4 15.0(1)S	The routable address hello option adds a PIM hello message option that includes all the addresses on the interface on which the PIM hello message is advertised. The following commands were introduced or modified: **ipv6 pim hello-interval**, **show ipv6 pim neighbor**.

CHAPTER 25

PIMv6 Anycast RP Solution

- Finding Feature Information, page 343
- Information About the PIMv6 Anycast RP Solution, page 343
- How to Configure the PIMv6 Anycast RP Solution, page 345
- Configuration Examples for the PIMv6 Anycast RP Solution, page 349
- Additional References, page 349
- Feature Information for PIMv6 Anycast RP Solution, page 350

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About the PIMv6 Anycast RP Solution

PIMv6 Anycast RP Solution Overview

The anycast RP solution in IPv6 PIM allows an IPv6 network to support anycast services for the PIM-SM RP. It allows anycast RP to be used inside a domain that runs PIM only. Anycast RP can be used in IPv4 as well as IPv6, but it does not depend on the Multicast Source Discovery Protocol (MSDP), which runs only on IPv4. This feature is useful when interdomain connection is not required.

Anycast RP is a mechanism that ISP-based backbones use to get fast convergence when a PIM RP device fails. To allow receivers and sources to rendezvous to the closest RP, the packets from a source need to get to all RPs to find joined receivers.

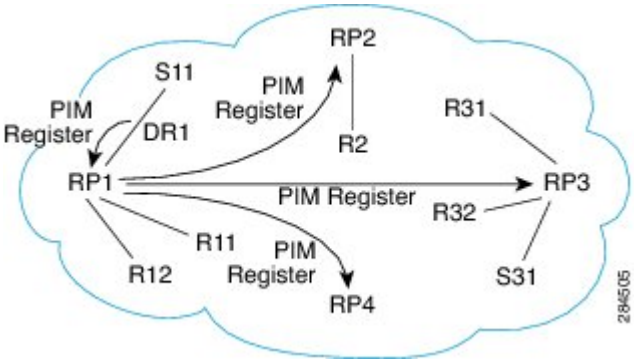
A unicast IP address is chosen as the RP address. This address is either statically configured or distributed using a dynamic protocol to all PIM devices throughout the domain. A set of devices in the domain is chosen to act as RPs for this RP address; these devices are called the anycast RP set. Each device in the anycast RP set is configured with a loopback interface using the RP address. Each device in the anycast RP set also needs a separate physical IP address to be used for communication between the RPs. Each device in the Anycast set must contain the list of all the devices in the Anycast set.

The RP address, or a prefix that covers the RP address, is injected into the unicast routing system inside of the domain. Each device in the anycast RP set is configured with the addresses of all other devices in the anycast RP set, and this configuration must be consistent in all RPs in the set. The IP address of the local device must be included in the set so that all devices in anycast set have the same IP addresses.

PIMv6 Anycast RP Normal Operation

The following illustration shows PIMv6 anycast RP normal operation and assumes the following:

- RP1, RP2, RP3, and RP4 are members in the same anycast RP group.
- S11 and S31 are sources that use RP1 and RP3, respectively, based on their unicast routing metric.
- R11, R12, R2, R31, and R32 are receivers. Based on their unicast routing metrics, R11 and R12 join to RP1, R2 joins to RP2 and R31, and R32 joins to RP3, respectively.

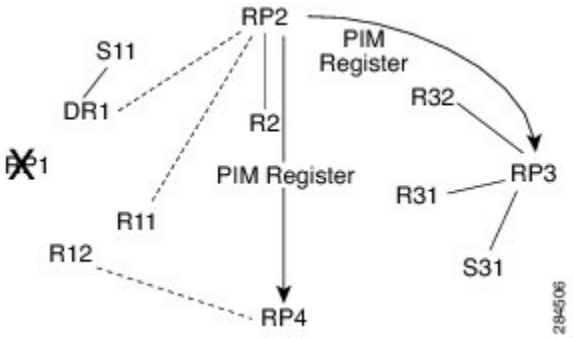


The following sequence of events occurs when S11 starts sending packets:

1. DR1 creates (S,G) states and sends a register to RP1. DR1 may also encapsulate the data packet in the register.
2. Upon receiving the register, RP1 performs normal PIM-SM RP functionality, and forwards the packets to R11 and R12.
3. RP1 also sends the register (which may encapsulate the data packets) to RP2, RP3, and RP4.
4. RP2, RP3, and RP4 do not further forward the register to each other.
5. RP2, RP3, and RP4 perform normal PIM-SM RP functionality, and if there is a data packet encapsulated, RP2 forwards the data packet to R2 and RP3 forwards the data packet to R31 and R32, respectively.
6. The previous five steps repeat for null registers sent by DR1.

PIMv6 Anycast RP Failover

The following illustration shows PIM anycast RP failover.



In failover, when RP1 is not reachable, the following occurs:

- Registers from DR1 will be routed transparently to RP2.
- R11 uses RP2 as the RP, and R12 uses RP4 as the RP.
- Registers from DR1 will be routed from RP2 to RP3 and RP4.

In this way, the loss of the RP (RP1 in this case) is transparent to DR1, R11, and R12, and the network can converge as soon as the IGP is converged.

How to Configure the PIMv6 Anycast RP Solution

Configuring PIMv6 Anycast RP

This task describes how to configure two PIMv6 anycast RP peers. Steps 3 through 11 show the configuration for RP1, and Steps 12 through 19 show the configuration for RP2.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 pim** [**vrf** *vrf-name*] **rp-address** *ipv6-address* [*group-address-list*] [**bidir**]
4. **interface** *type number*
5. **ipv6 address** {*ipv6-address*/*prefix-length* | *prefix-name sub-bits* /*prefix-length*}
6. **no shut**
7. **interface** *type number*
8. **ipv6 address** {*ipv6-address*/*prefix-length* | *prefix-name sub-bits* /*prefix-length*}
9. **no shut**
10. **exit**
11. **ipv6 pim anycast-RP** *rp-address peer-address*
12. **ipv6 pim** [**vrf** *vrf-name*] **rp-address** *ipv6-address* [*group-address-list*] [**bidir**]
13. **interface** *type number*
14. **ipv6 address** {*ipv6-address*/*prefix-length* | *prefix-name sub-bits* /*prefix-length*}
15. **no shut**
16. **interface** *type number*
17. **ipv6 address** {*ipv6-address*/*prefix-length* | *prefix-name sub-bits* /*prefix-length*}
18. **no shut**
19. **ipv6 pim anycast-RP** *rp-address peer-address*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 pim** [**vrf** *vrf-name*] **rp-address** *ipv6-address* [*group-address-list*] [**bidir**] **Example:** `Device(config)# ipv6 pim rp-address 2001:DB8::1:1 acl_sparse1`	Configures the address of a PIM RP for a particular group range.

	Command or Action	Purpose
Step 4	**interface** *type number* **Example:** `Device(config)# interface Loopback4`	Specifies an interface type and number, and places the device in interface configuration mode.
Step 5	**ipv6 address** {*ipv6-address*/*prefix-length* | *prefix-name sub-bits* /*prefix-length*} **Example:** `Device(config-if)# ipv6 address 2001:DB8::4:4/64`	Configures an IPv6 address based on an IPv6 general prefix and enable IPv6 processing on an interface.
Step 6	**no shut** **Example:** `Device(config-if)# no shut`	Enables an interface.
Step 7	**interface** *type number* **Example:** `Device(config-if)# interface Loopback5`	Specifies an interface type and number, and places the device in interface configuration mode.
Step 8	**ipv6 address** {*ipv6-address*/*prefix-length* | *prefix-name sub-bits* /*prefix-length*} **Example:** `Device(config-if)# ipv6 address 2001:DB8:0:ABCD::1/64`	Configures an IPv6 address based on an IPv6 general prefix and enable IPv6 processing on an interface.
Step 9	**no shut** **Example:** `Device(config-if)# no shut`	Enables an interface.
Step 10	**exit** **Example:** `Device(config-if)# exit`	Enter this command to exit interface configuration mode and enter global configuration mode.
Step 11	**ipv6 pim anycast-RP** *rp-address peer-address* **Example:** `Device(config)# ipv6 pim anycast-rp 2001:DB8:0:ABCD::1 2001:DB8::3:3`	Use this command to configure the address of the PIM RP for an anycast group range. • The IP address of the local device must be included in the set so that all devices in anycast set have the same IP addresses.

	Command or Action	Purpose
Step 12	**ipv6 pim** [**vrf** *vrf-name*] **rp-address** *ipv6-address* [*group-address-list*] [**bidir**] **Example:** `Device(config)# ipv6 pim rp-address 2001:DB8::1:1 acl_sparse1`	Configures the address of a PIM RP for a particular group range.
Step 13	**interface** *type number* **Example:** `Device(config)# interface Loopback4`	Specifies an interface type and number, and places the device in interface configuration mode.
Step 14	**ipv6 address** {*ipv6-address*/*prefix-length* | *prefix-name sub-bits* /*prefix-length*} **Example:** `Device(config-if)# ipv6 address 2001:DB8::3:3/64`	Configures an IPv6 address based on an IPv6 general prefix and enables IPv6 processing on an interface.
Step 15	**no shut** **Example:** `Device(config-if)# no shut`	Enables an interface.
Step 16	**interface** *type number* **Example:** `Device(config-if)# interface Loopback5`	Specifies an interface type and number, and places the device in interface configuration mode.
Step 17	**ipv6 address** {*ipv6-address*/*prefix-length* | *prefix-name sub-bits* /*prefix-length*} **Example:** `Device(config-if)# ipv6 address 2001:DB8:0:ABCD::1/64`	Configures an IPv6 address based on an IPv6 general prefix and enables IPv6 processing on an interface.
Step 18	**no shut** **Example:** `Device(config-if)# no shut`	Enables an interface
Step 19	**ipv6 pim anycast-RP** *rp-address peer-address* **Example:** `Device(config-if)# ipv6 pim anycast-rp 2001:DB8::1:1 2001:DB8::4:4`	Use this command to configure the address of the PIM RP for an anycast group range.

Configuration Examples for the PIMv6 Anycast RP Solution

Example: Configuring PIMv6 Anycast RP

```
RP1
Device1(config)# ipv6 pim rp-address 2001:DB8::1:1 acl_sparse1
Device1(config)# interface Loopback4
Device1(config-if)# ipv6 address 2001:DB8::4:4/64
Device1(config-if)# no shut

Device1(config)# interface Loopback5
Device1(config-if)# ipv6 address 2001:DB8:0:ABCD::1/64
Device1(config-if)# no shut
Device1(config-if)# exit
Device1(config)# ipv6 pim anycast-rp 2001:DB8:0:ABCD::1 2001:DB8::3:3

RP2 (Anycast RP Peer)
Device2(config)# ipv6 pim rp-address 2001:DB8::1:1 acl_sparse1
Device2(config)# interface Loopback4
Device2(config-if)# ipv6 address 2001:DB8::3:3/64
Device2(config-if)# no shut

Device2(config)# interface Loopback5
Device2(config-if)# ipv6 address 2001:DB8:0:ABCD::1/64
Device2(config-if)# no shut
Device2(config)# ipv6 pim anycast-rp 2001:DB8::1:1 2001:DB8::4:4
```

```
Device2 show ipv6 pim anycast-rp 2001:DB8::1:1

Anycast RP Peers For 2001:DB8::1:1   Last Register/Register-Stop received
  2001:DB8::3:3 00:00:00/00:00:00
  2001:DB8::4:4 00:00:00/00:00:00
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IPv6 commands	Cisco IOS IPv6 Command Reference
Cisco IOS IPv6 features	Cisco IOS IPv6 Feature Mapping

Standards and RFCs

Standard/RFC	Title
RFC 4610	*Anycast-RP Using Protocol Independent Multicast (PIM)*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for PIMv6 Anycast RP Solution

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 28: Feature Information for the PIMv6: Anycast RP Solution

Feature Name	Releases	Feature Information
PIMv6: Anycast RP Solution		The anycast RP solution in IPv6 PIM allows an IPv6 network to support anycast services for the PIM-SM RP. It allows anycast RP to be used inside a domain that runs PIM only. The following commands were introduced or modified: **ipv6 pim anycast-RP**, **show ipv6 pim anycast-RP**.

CHAPTER 26

MTR in VRF

The MTR in VRF feature extends to IPv4 VRF contexts the Cisco IOS software's capability that allows users to configure one or more non-congruent multicast topologies in global IPv4 routing context. These contexts can be used to forward unicast and multicast traffic over different links in the network, or in the case of non-base topologies to provide a Live-Live multicast service using multiple non-congruent multicast topologies mapped to different (S,G) groups.

- Finding Feature Information, page 351
- Information About MTR in VRF, page 351
- How to Configure VRF in MTR, page 352
- Configuring Examples for MTR in VRF, page 355
- Additional References for MTR in VRF, page 355
- Feature Information for MTR in VRF, page 356

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About MTR in VRF

MTR in VRF Overview

The MTR in VRF feature extends to IPv4 VRF contexts, Cisco IOS software's capability that allows users to configure one or more non-congruent multicast topologies in global IPv4 routing context. These contexts can

be used to forward unicast and multicast traffic over different links in the network, or in the case of non-base topologies to provide a Live-Live multicast service using multiple non-congruent multicast topologies mapped to different (S,G) groups.

The Cisco IOS Software allows a set of attributes, primarily used by BGP/MPLS L3VPNs, to be configured on a per-address family basis within a VRF. The MTR in VRF feature allows these attributes to be independently configured for the multicast sub-address families within a VRF address family.

How to Configure VRF in MTR

Configuring MTR in VRF

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vrf definition** *vrf-name*
4. **rd** *route-distinguisher*
5. **ipv4 multicast multitoplogy**
6. **address-family ipv4**
7. **exit-address-family**
8. **address-family ipv4 multicast**
9. **topology** *topology-instance-name*
10. **all-interfaces**
11. **exit**
12. **exit-address-family**
13. **exit**
14. **interface** *type number*
15. **interface** *type number*
16. **vrf forwarding** *vrf-name*
17. **ip address** *ip-address mask*
18. **ip pim sparse-dense-modeip**
19. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**vrf definition** *vrf-name* **Example:** `Device(config)# vrf definition vd1`	Configures a VRF routing table and enters VRF configuration mode.
Step 4	**rd** *route-distinguisher* **Example:** `Device(config-vrf)# rd 10:1`	Creates routing and forwarding tables for a VRF.
Step 5	**ipv4 multicast multitoplogy** **Example:** `Device(config-vrf)# ipv4 multicast multitoplogy`	Enables IPv4 multicast support for multi-topology routing (MTR) in a VRF instance.
Step 6	**address-family ipv4** **Example:** `Device(config-vrf)# address-family ipv4`	Specifies the IPv4 address family type and enters address family configuration mode.
Step 7	**exit-address-family** **Example:** `Device(config-vrf-af)# exit-address-family`	Exits address family configuration mode and removes the IPv4 address family.
Step 8	**address-family ipv4 multicast** **Example:** `Device(config-vrf)# address-family ipv4 multicast`	Specifies the IPv4 address family multicast type and enters VRF address family configuration mode.
Step 9	**topology** *topology-instance-name* **Example:** `Device(config-vrf-af)# topology red`	Specifies a topology instance and a name to it and enters VRF address family topology configuration mode.
Step 10	**all-interfaces** **Example:** `Device(config-vrf-af-topology)# all-interfaces`	Configure the topology instance to use all interfaces on the device.

	Command or Action	Purpose
Step 11	**exit** **Example:** `Device(config-vrf-af-topology)# exit`	Exits VRF address-family topology configuration mode and enters VRF address-family configuration mode.
Step 12	**exit-address-family** **Example:** `Device(config-vrf-af)# exit-address-family`	Exits address family configuration mode and removes the IPv4 address family.
Step 13	**exit** **Example:** `Device(config-vrf)# exit`	Exits VRF configuration mode and enters global configuration mode.
Step 14	**interface** *type number* **Example:** `Device(config)# interface ethernet 0/1`	Selects the Ethernet interface and enters the interface configuration mode.
Step 15	**interface** *type number* **Example:** `Device(config)# interface ethernet 0/1`	Selects the Ethernet interface and enters the interface configuration mode.
Step 16	**vrf forwarding** *vrf-name* **Example:** `Device(config-if)# vrf forwwarding vrf1`	Associates a VRF instance with the interface.
Step 17	**ip address** *ip-address mask* **Example:** `Device(config-if)# ip address 10.1.10.1 255.255.255.0`	Sets a primary or secondary IP address for an interface.
Step 18	**ip pim sparse-dense-modeip** **Example:** `Device(config-if)# ip pim sparse-dense-mode`	Enables Protocol Independent Multicast (PIM) on an interface.
Step 19	**end** **Example:** `Device(config-if)# end`	Exits the interface configuration mode and enters privileged EXEC mode.

Configuring Examples for MTR in VRF

Example for MTR in VRF

```
Device> enable
Device# configuration terminal
Device(config)# vrf definition vd1
Device(config-vrf)# rd 10:1
Device(config-vrf)# ipv4 multicast multitoplogy
Device(config-vrf)# address-family ipv4
Device(config-vrf)# exit-address-family
Device(config-vrf)# address-family ipv4 multicast
Device(config-vrf-af)# topology red
Device(config-vrf-af-topology)# all-interfaces
Device(config-vrf-af-topology)# exit
Device(config-vrf-af)# exit-address-family
Device(config-vrf)# exit
Device(config)# vrf forwarding vrf1
Device(config)# ip address 10.1.10.1 255.255.255.0
Device(config)# ip pim sparse-dense-mode
Device(config)# end
```

Additional References for MTR in VRF

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Multitopology Routing (MTR) commands	Cisco IOS Multitopology Routing Command Reference
IP multicast commands	Cisco IOS Multicast Command Reference
IP multicast concepts and tasks	*IP Multicast Configuration Guide Library*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for MTR in VRF

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 29: Feature Information for MTR in VRF

Feature Name	Releases	Feature Information
MTR in VRF		The MTR in VRF feature extends to IPv4 VRF contexts the Cisco IOS software's capability that allows users to configure one or more non-congruent multicast topologies in global IPv4 routing context. These contexts can be used to forward unicast and multicast traffic over different links in the network, or in the case of non-base topologies to provide a Live-Live multicast service using multiple non-congruent multicast topologies mapped to different (S,G) groups.