AOS-CX 10.08 Multicast Guide

6200, 6300, 6400, 8xxx Switch Series

a Hewlett Packard
Enterprise company

Published: August 2021
Edition: 1

Copyright Information

© Copyright 2021 Hewlett Packard Enterprise Development LP.

Open Source Code

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses. A complete machine-readable copy of the source code corresponding to such code is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett Packard Enterprise Company. To obtain such source code, send a check or money order in the amount of US $10.00 to:

Hewlett Packard Enterprise Company
6280 America Center Drive
San Jose, CA 95002
USA

Notices

The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use, or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Links to third-party websites take you outside the Hewlett Packard Enterprise website. Hewlett Packard Enterprise has no control over and is not responsible for information outside the Hewlett Packard Enterprise website.

Contents 3

About this document 11
Applicable products 11
Latest version available online 11
Command syntax notation conventions 11
About the examples 12
Identifying switch ports and interfaces 12
Identifying modular switch components 14

Multicast overview 15
Multicast protocols 15
Multicast addresses 16
Sub-interface recommendations and limitations 16

Internet Group Management Protocol (IGMP) 17
IGMP defaults, protocols, and supported configuration 17
How the IGMP protocol works 17
Considerations when configuring IGMP 18
IGMP configuration task list 19
Enabling or disabling IGMP 19
Specifying the IGMP version 19
Configuring IGMP static groups 20
Configuring IGMP query and response parameters 20
Disabling IGMP 21
Viewing IGMP information 21
IGMP configuration example 22
IGMP commands 23
ip igmp 23
ip igmp apply access-list 24
ip igmp last-member-query-interval 25
ip igmp querier 26
ip igmp querier interval 27
ip igmp querier query-max-response-time 29
ip igmp robustness 29
ip igmp router-alert-check 30
ip igmp static-group 31
ip igmp version 32
ip igmp version strict 32
no ip igmp 33
show ip igmp 34
show ip igmp counters 37
show ip igmp group 38
show ip igmp groups 40
show ip igmp interface 43
show ip igmp interface counters 44
show ip igmp interface group 46
show ip igmp interface groups 48

show ip igmp interface statistics 50
show ip igmp static-groups 51
show ip igmp statistics 52

IGMP snooping 55

IGMP snooping defaults, protocols, and supported configuration 55
How IGMP snooping works 56
IGMP snooping configuration task list 57
Enabling or disabling IGMP snooping 57
Specifying the IGMP snooping version 57
Configuring IGMP snooping static groups 58
Enabling drop-unknown filters 58
Configuring IGMP snooping fast learn ports globally 58
Configuring IGMP snooping per port filtering 59
Disabling IGMP snooping 59
Viewing IGMP snooping information 60
IGMP snooping commands 60
ip igmp snooping 60
ip igmp snooping apply access-list 61
ip igmp snooping auto vlan 62
ip igmp snooping blocked 63
ip igmp snooping drop-unknown 64
ip igmp snooping fastlearn 65
ip igmp snooping fastleave vlan 65
ip igmp snooping forced fastleave vlan 66
ip igmp snooping forward vlan 67
ip igmp snooping static-group 68
ip igmp snooping version 69
no ip igmp snooping 69
show ip igmp snooping 70
show ip igmp snooping counters 71
show ip igmp snooping groups 72
show ip igmp snooping static-groups 73
show ip igmp snooping statistics 73
show ip igmp snooping vlan 74
show ip igmp snooping vlan counters 76
show ip igmp snooping vlan group port 78
show ip igmp snooping vlan statistics 79

MLD snooping 80

MLD snooping functionality 80
MLD snooping global configuration commands 80
ipv6 mld snooping 80
MLD snooping VLAN configuration commands 81
ipv6 mld snooping 81
ipv6 mld snooping apply access-list 81
ipv6 mld snooping auto vlan 83
ipv6 mld snooping blocked vlan 83
ipv6 mld snooping fastlearn 84
ipv6 mld snooping fastleave vlan 85
ipv6 mld snooping forced fastleave vlan 86
ipv6 mld snooping forward vlan 87
ipv6 mld snooping version 87
ipv6 mld snooping static-group 88
MLD snooping show commands 89
show ipv6 mld snooping 89

show ipv6 mld snooping counters 89
show ipv6 mld snooping groups 91
show ipv6 mld snooping statistics 91
show ipv6 mld snooping vlan counters 92
show ipv6 mld snooping vlan group port 93
show ipv6 mld snooping vlan group source 94
show ipv6 mld snooping static-groups 96
show ipv6 mld snooping vlan statistics 97
MLD configuration commands for interface VLAN 97
ipv6 mld 98
ipv6 mld apply access-list 98
no ipv6 mld 99
ipv6 mld querier 100
ipv6 mld querier interval 100
ipv6 mld last-member-query-interval 101
ipv6 mld querier query-max-response-time 102
ipv6 mld robustness 102
ipv6 mld static-group 103
ipv6 mld version 104
ipv6 mld version strict 104
MLD show commands for interface VLAN 105
show ipv6 mld 105
show ipv6 mld interface vlan 106
show ipv6 mld vrf all-vrfs 107
show ipv6 mld interface vlan counters 108
show ipv6 mld interface vlan groups 110
show ipv6 mld interface vlan group source 111
show ipv6 mld groups 112
show ipv6 mld groups all-vrfs vrf 113
show ipv6 mld interface counters 114
show ipv6 mld interface statistics 116
show ipv6 mld interface groups 117
show ipv6 mld interface vlan group source 118
show ipv6 mld group all-vrfs vrf 119
show ipv6 mld group source all-vrfs vrf 121
show ipv6 mld interface vlan statistics 122
show ipv6 mld static-groups vrf all-vrfs 123
show ipv6 mld counters vrf 124
MLD configuration commands for interface 125
ipv6 mld 125
ipv6 mld apply access-list 126
no ipv6 mld 127
ipv6 mld querier 128
ipv6 mld querier interval 128
ipv6 mld last-member-query-interval 129
ipv6 mld querier query-max-response-time 129
ipv6 mld robustness 130
ipv6 mld static-group 131
ipv6 mld version 131
ipv6 mld version strict 132

Protocol Independent Multicast - Sparse Mode (V4 and V6) 134

Protocol Independent Multicast - Sparse Mode (PIM-SM) overview 134
PIM-SM defaults, protocols, and supported configuration 134
PIM-SM router types 135
How PIM-SM works 137

Enabling/disabling PIM-SM in an interface 139
Configuring PIM-SM options in an interface 140
Viewing PIM information 142
PIM-SM configuration example 143
PIM-SM configuration task list 145
Enabling or disabling PIM globally 146
Configuring join/prune interval 146
Enabling/disabling multicast traffic to SPT 147
Configuring an RP 147
Configuring a BSR 149
Configuring RPF override 151
Removing all PIM-SM related configurations on an interface 151
PIM VSX active-active 152
FAQ and best practices 153
PIM-SM commands for IPv4 155
accept-register access-list 155
accept-rp 156
active-active 157
bfd all-interfaces 158
bsr-candidate bsm-interval 159
bsr-candidate hash-mask-length 160
bsr-candidate priority 161
bsr-candidate source-ip-interface 161
disable 163
enable 163
ip pim-sparse 164
ip pim-sparse bfd 165
ip pim-sparse dr-priority 166
ip pim-sparse hello-delay 167
ip pim-sparse hello-interval 168
ip pim-sparse ip-addr 169
ip pim-sparse lan-prune-delay 170
ip pim-sparse override-interval 171
ip pim-sparse propagation-delay 172
join-prune-interval 173
multicast-route-limit 174
no ip pim-sparse 175
register-rate-limit 176
router pim 176
rp-address 177
rp-candidate group-prefix 178
rp-candidate hold-time 179
rp-candidate priority 180
rp-candidate source-ip-interface 181
rpf-override 182
show ip mroute 183
show ip mroute brief 184
show ip mroute group-addr 185
show ip pim 187
show ip pim bsr 188
show ip pim bsr elected 190
show ip pim bsr local 191
show ip pim interface 192
show ip pim interface interface-name 193
show ip pim interface interface-name counters 194
show ip pim neighbor 195

show ip pim pending 196
show ip pim rp-candidate 197
show ip pim rp-set 198
show ip pim rp-set learned 200
show ip pim rp-set static 201
show ip pim rpf-override 202
show ip pim rpf-override source 203
sources-per-group 204
spt-threshold 205
PIM-SM commands for IPv6 206
accept-register access-list 206
accept-rp 207
bsr-candidate bsm-interval 208
bsr-candidate hash-mask-length 209
bsr-candidate priority 210
bsr-candidate source-ip-interface 211
disable 212
enable 212
ipv6 pim6-sparse 213
ipv6 pim6-sparse bfd 214
ipv6 pim6-sparse dr-priority 215
ipv6 pim6-sparse hello-delay 216
ipv6 pim6-sparse hello-interval 217
ipv6 pim6-sparse ipv6-addr 218
ipv6 pim6-sparse lan-prune-delay 219
ipv6 pim6-sparse override-interval 220
ipv6 pim6-sparse propagation-delay 221
join-prune-interval 222
no ipv6 pim6-sparse 223
router pim6 223
rp-address 224
rp-candidate group-prefix 225
rp-candidate hold-time 226
rp-candidate priority 227
rp-candidate source-ip-interface 227
rpf-override 229
show ipv6 mroute grorp-addr 230
show ipv6 mroute 232
show ipv6 mroute brief 233
show ipv6 pim6 234
show ipv6 pim6 bsr 235
show ipv6 pim6 bsr elected 237
show ipv6 pim6 bsr local 238
show ipv6 pim6 interface interface-name 239
show ipv6 pim6 interface 240
show ipv6 pim6 neighbor 241
show ipv6 pim6 pending 242
show ipv6 pim6 rp-candidate 243
show ipv6 pim6 rpf-override 244
show ipv6 pim6 rpf-override source 245
show ipv6 pim6 rp-set 246
show ipv6 pim6 rp-set learned 248
show ipv6 pim6 rp-set static 249
spt-threshold 250

Protocol Independent Multicast - Dense Mode (V4 and V6) 251

Protocol Independent Multicast - Dense Mode (PIM-DM) overview 251
PIM-DM defaults, protocols, and supported configurations 251
PIM-DM configuration example 252
PIM-DM features 253
PIM-DM commands for IPv4 254
disable 254
enable 255
no ip pim-dense 255
ip pim-dense bfd 256
ip pim-dense graft-retry-interval 257
ip pim-dense hello-delay 258
ip pim-dense hello-interval 259
ip pim-dense ip-addr 261
ip pim-dense lan-prune-delay 262
ip pim-dense max-graft-retries 263
ip pim-dense override-interval 264
ip pim-dense propagation-delay 265
ip pim-dense ttl-threshold 266
router pim 267
show ip mroute 268
show ip mroute group-addr 269
show ip mroute brief 271
show ip pim 272
show ip pim interface 273
show ip pim interface interface-name 274
show ip pim interface interface-name counters 275
show ip pim neighbor 276
state-refresh-interval 277
PIM-DM commands for IPv6 278
disable 278
enable 279
ipv6 pim6-dense 279
ipv6 pim6-dense bfd 280
ipv6 pim6-dense graft-retry-interval 281
ipv6 pim6-dense hello-delay 282
ipv6 pim6-dense hello-interval 284
ipv6 pim6-dense ipv6-addr 285
ipv6 pim6-dense lan-prune-delay 286
ipv6 pim6-dense max-graft-retries 287
ipv6 pim6-dense override-interval 288
ipv6 pim6-dense propagation-delay 289
ipv6 pim6-dense ttl-threshold 290
no ipv6 pim6-dense 291
show ipv6 pim6 292
show ipv6 pim6 interface 293
show ipv6 pim6 interface interface-name 294
show ipv6 mroute 295
show ipv6 mroute brief 296
show ipv6 mroute group-addr 297
show ipv6 pim6 neighbor 299
router pim6 300
state-refresh-interval 301

Multicast Source Discovery Protocol (MSDP) 303
Multicast Source Discovery Protocol (MSDP) overview 303
MSDP router config commands 303

disable 303
enable 304
router msdp 305
sa-interval 305
MSDP peer configuration commands 306
connection-retry-interval 306
connect-source 307
clear ip msdp peer statistics 308
description 309
disable 309
enable 310
ip msdp peer 311
keepalive 312
mesh-group 312
password 313
sa-filter access-list 314
MSDP show commands 315
show ip msdp count 316
show ip msdp peer 316
show ip msdp sa-cache 318
show ip msdp summary 319

mDNS gateway 320
mDNS gateway overview 320
Configuring mDNS gateway 321
mDNS gateway commands 322
debug mdns 322
description 323
id 323
mdns-sd 324
mdns-sd apply-profile tx 325
mdns-sd enable 326
mdns-sd profile 327
mdns-sd service 327
clear mdns-sd statistics 328
sequence-number 329
show mdns-sd service-entries 330
show mdns-sd statistics 331
show mdns-sd statistics profile 332
show mdns-sd summary 333
show running-config interface 334
show running-config mdns-sd profile 335
show running-config mdns-sd service 335

Multicast VXLAN 337
Protocol and feature details 338
Broadcast, unknown unicast, multicast (BUM) traffic replication 338
Overlay multicast support 338
L2 multicast over VXLAN 338
L2 multicast over VXLAN enabled with IGMP snooping 339
Split horizon and L2 multicast 340
VSX and L2 multicast 340
Recommended configuration on the VSX VTEPs 343
IGMP querier positioning 344
L3 multicast over VXLAN 344
Centralized L3 gateway 344

Distributed L3 gateways 345
Border VTEP to external (non overlay) network 347
VSX and L3 Multicast 347
VSX Border VTEP with L3 connectivity to external (non overlay) network 348
RP placement and election 352
Supported platforms and standards 352
Scale 352
Supported RFCs and standards 353
Configuration task list 353
Multicast VXLAN and EVPN 353
VSX VTEP 353
IGMP snooping 353
PIM and IGMP on SVI with source and receivers 354
Static RP on VTEP 354
Overlay BSR/RP on VTEP 354
Considerations and best practices 355
Use cases 356
Use case 1: Campus network with centralized L3 gateway 356
Edge 357
Core-vsx-primary 361
Core-vsx-secondary 375
8320-vsx-pri 387
8320-vsx-sec 388
6300-VSF-VTEP1 390
6300-VTEP2 402
Use case 2: DC network with distributed L3 gateway 411
Spine01 412
Spine02 414
Leaf01-primary 416
Leaf01-secondary 427
Leaf02 439
8325-border-prim 449
8325-border-sec 462
Edge-primary 474
Edge-secondary 481
Multicast VXLAN commands 488
ip pim-sparse vsx-virtual-neighbor 488
show ip mroute 488
show ip pim neighbor 490
Debugging and troubleshooting 491
FAQ 498
References 500

Support and Other Resources 501

Accessing Aruba Support 501
Accessing Updates 501
Aruba Support Portal 501
My Networking 502
Warranty Information 502
Regulatory Information 502
Documentation Feedback 502

Chapter 1
About this document

This document describes features of the AOS-CX network operating system. It is intended for administrators responsible for installing, configuring, and managing Aruba switches on a network.

Applicable products

This document applies to the following products:

- Aruba 6200 Switch Series (JL724A, JL725A, JL726A, JL727A, JL728A)
- Aruba 6300 Switch Series (JL658A, JL659A, JL660A, JL661A, JL662A, JL663A, JL664A, JL665A, JL666A, JL667A, JL668A, JL762A)
- Aruba 6400 Switch Series (JL741A, R0X26A, R0X27A, R0X29A, R0X30A)
- Aruba 8320 Switch Series (JL479A, JL579A, JL581A)
- Aruba 8325 Switch Series (JL624A, JL625A, JL626A, JL627A)
- Aruba 8360 Switch Series (JL700A, JL701A, JL702A, JL703A, JL706A, JL707A, JL708A, JL709A, JL710A, JL711A)
- Aruba 8400 Switch Series (JL375A, JL376A)

Latest version available online

Updates to this document can occur after initial publication. For the latest versions of product documentation, see the links provided in Support and Other Resources.

Command syntax notation conventions

Convention	Usage
`example-text`	Identifies commands and their options and operands, code examples, filenames, pathnames, and output displayed in a command window. Items that appear like the example text in the previous column are to be entered exactly as shown and are required unless enclosed in brackets (`[ ]`).
example-text	In code and screen examples, indicates text entered by a user.
Any of the following: ■ *<example-text>* ■ <example-text> ■ *example-text* ■ *example-text*	Identifies a placeholder—such as a parameter or a variable—that you must substitute with an actual value in a command or in code: ■ For output formats where italic text cannot be displayed, variables are enclosed in angle brackets (< >). Substitute the text—including the enclosing angle brackets—with an actual value. ■ For output formats where italic text can be displayed, variables might or might not be enclosed in angle brackets. Substitute the text including the enclosing angle brackets, if any, with an actual value.

Convention	Usage
|	Vertical bar. A logical OR that separates multiple items from which you can choose only one. Any spaces that are on either side of the vertical bar are included for readability and are not a required part of the command syntax.
{ }	Braces. Indicates that at least one of the enclosed items is required.
[ ]	Brackets. Indicates that the enclosed item or items are optional.
... or . . .	Ellipsis: ■ In code and screen examples, a vertical or horizontal ellipsis indicates an omission of information. ■ In syntax using brackets and braces, an ellipsis indicates items that can be repeated. When an item followed by ellipses is enclosed in brackets, zero or more items can be specified.

About the examples

Examples in this document are representative and might not match your particular switch or environment.

The slot and port numbers in this document are for illustration only and might be unavailable on your switch.

Understanding the CLI prompts

When illustrating the prompts in the command line interface (CLI), this document uses the generic term `switch`, instead of the host name of the switch. For example:

```
switch>
```

The CLI prompt indicates the current command context. For example:

```
switch>
```

Indicates the operator command context.

```
switch#
```

Indicates the manager command context.

`switch(`*`CONTEXT-NAME`*`)#`

Indicates the configuration context for a feature. For example:

```
switch(config-if)#
```

Identifies the `interface` context.

Variable information in CLI prompts

In certain configuration contexts, the prompt may include variable information. For example, when in the VLAN configuration context, a VLAN number appears in the prompt:

```
switch(config-vlan-100)#
```

When referring to this context, this document uses the syntax:

`switch(config-vlan-<`*`VLAN-ID`*`>)#`

Where *<VLAN-ID>* is a variable representing the VLAN number.

Identifying switch ports and interfaces

Physical ports on the switch and their corresponding logical software interfaces are identified using the format:

member/slot/port

On the 6200 Switch Series

- *member*: Member number of the switch in a Virtual Switching Framework (VSF) stack. Range: 1 to 8. The primary switch is always member 1. If the switch is not a member of a VSF stack, then member is 1.
- *slot*: Always 1. This is not a modular switch, so there are no slots.
- *port*: Physical number of a port on the switch.

For example, the logical interface `1/1/4` in software is associated with physical port 4 in slot 1 on member 1.

On the 6300 Switch Series

- *member*: Member number of the switch in a Virtual Switching Framework (VSF) stack. Range: 1 to 10. The primary switch is always member 1. If the switch is not a member of a VSF stack, then member is 1.
- *slot*: Always 1. This is not a modular switch, so there are no slots.
- *port*: Physical number of a port on the switch.

For example, the logical interface `1/1/4` in software is associated with physical port 4 on member 1.

On the 6400 Switch Series

- *member*: Always 1. VSF is not supported on this switch.
- *slot*: Specifies physical location of a module in the switch chassis.
  - Management modules are on the front of the switch in slots 1/1 and 1/2.
  - Line modules are on the front of the switch starting in slot 1/3.
- *port*: Physical number of a port on a line module.

For example, the logical interface `1/3/4` in software is associated with physical port 4 in slot 3 on member 1.

On the 83xx Switch Series

- *member*: Always 1. VSF is not supported on this switch.
- *slot*: Always 1. This is not a modular switch, so there are no slots.
- *port*: Physical number of a port on the switch.

For example, the logical interface `1/1/4` in software is associated with physical port 4 on the switch.

If using breakout cables, the port designation changes to x:y, where x is the physical port and y is the lane when split to 4 x 10G or 4 x 25G. For example, the logical interface 1/1/4:2 in software is associated with lane 2 on physical port 4 in slot 1 on member 1.

On the 8400 Switch Series

- *member*: Always 1. VSF is not supported on this switch.
- *slot*: Specifies physical location of a module in the switch chassis.
  - Management modules are on the front of the switch in slots 1/5 and 1/6.
  - Line modules are on the front of the switch in slots 1/1 through 1/4, and 1/7 through 1/10.
- *port*: Physical number of a port on a line module

For example, the logical interface `1/1/4` in software is associated with physical port 4 in slot 1 on member 1.

Identifying modular switch components

- Power supplies are on the front of the switch behind the bezel above the management modules. Power supplies are labeled in software in the format: *member/power supply*:
  - *member*: 1.
  - *power supply*: 1 to 4.
- Fans are on the rear of the switch and are labeled in software as: *member/tray/fan*:
  - *member*: 1.
  - *tray*: 1 to 4.
  - *fan*: 1 to 4.
- Fabric modules are not labeled on the switch but are labeled in software in the format: *member/module*:
  - *member*: 1.
  - *member*: 1 or 2.
- The display module on the rear of the switch is not labeled with a member or slot number.

Multicast addressing allows one-to-many or many-to-many communication among hosts on a network. Typical applications of multicast communication include: audio and video streaming, desktop conferencing, collaborative computing, and similar applications.

In a network where IP multicast traffic is transmitted for multimedia applications, such traffic is blocked at routed interface (VLAN) boundaries unless a multicast routing protocol is running. Protocol Independent Multicast (PIM) is a family of routing protocols that form multicast trees to forward traffic from multicast sources to subnets that have used a protocol such as IGMP to request the traffic. PIM relies on the unicast routing tables created by any of several unicast routing protocols to identify the path back to a multicast source (Reverse Path Forwarding, or RPF). With this information, PIM sets up the distribution tree for the multicast traffic. IGMP provides the multicast traffic link between a host and a multicast router running PIM-SM. Both PIM-SM and IGMP must be enabled on VLANs whose member ports have directly connected hosts with a valid need to join multicast groups.

IGMP snooping (Internet Group Management Protocol controls) can be configured per-VLAN basis to reduce unnecessary bandwidth usage. In the factory default state (IGMP and IGMP snooping disabled), the switch simply floods all IP multicast traffic it receives on a given VLAN through all ports on that VLAN (except the port on which it received the traffic). This can result in significant and unnecessary bandwidth usage in networks where IP multicast traffic is a factor. Enabling IGMP allows the ports to detect IGMP queries and report packets and manage IP multicast traffic through the switch. IGMP will be configured on the hosts, and multicast traffic will be generated by one or more servers (inside or outside of the local network). Switches in the network (that support IGMP snooping) can then be configured to direct the multicast traffic to only the ports where needed. If multiple VLANs are configured, you can configure IGMP snooping on a per-VLAN basis.

Multicast Listener Discovery (MLD) is an IPv6 protocol used on a local link for multicast group management. MLD snooping is a subset of the MLD protocol that operates at the port level and conserves network bandwidth by reducing the flooding of multicast IPv6 packets.

Multicast protocols

Layer 3 multicast protocols include:

- IGMP (Internet Group Management Protocol) for last-hop multicast group management. Current RFCs include:
  - IGMPv2 (RFC 2236)
  - IGMPv3 (RFC 3376)
- PIM (Protocol Independent Multicast) for intra-domain multicast routing.
  - PIM-SM (Sparse mode) (RFC 4601)
  - PIM-DM (Dense mode) (RFC 3973)
  - BSR (Bootstrap router) (RFC 5059)
- MSDP (Multicast Source Discovery Protocol) (RFC 3618)

- MLD (Multicast Listener Discovery) v1 and v2
  - MLD v1 - RFC 2710
  - MLD v2 - RFC 3810

Layer 2 multicast protocol:

- IGMP snooping for IPv4 multicast filtering.
- MLD snooping for IPv6 multicast filtering.

Multicast addresses

Each multicast host group is identified by a single IP address in the range of 224.0.0.0 through 239.255.255.255.

- **For the 8320/8325 switch:** AOS-CX supports 4K IPv4 multicast flows.
- **For the 8400 switch:** AOS-CX supports 16K IPv4 multicast flows.
- **For the 6400/6300 switch:** AOS-CX supports 4K IPv4 multicast flows.
- **For the 6200 switch:** AOS-CX supports 1K IPv4 multicast flows.

For a list of all reserved and well known multicast addresses, see the standards document at the following links:

- https://www.iana.org/assignments/multicast-addresses/multicast-addresses.xhtml
- https://www.iana.org/assignments/ipv6-multicast-addresses/ipv6-multicast-addresses.xhtml

Sub-interface recommendations and limitations

(Supported only on the Aruba 6300, 6400, and 8360 Switch Series.)

The following recommendations and limitations apply:

- When ROP/sub-interface as uplink is used towards multicast source, a PIM-enabled point-to-point transit VLAN over ISL between VSX devices should be added to ensure an alternate path to reach the upstream multicast source. This transit VLAN is not carried on VSX LAGs. (A dedicated point-to-point link between VSX primary and secondary can also be used.)
- If KA is used for the P2P sub-interface link, KA has to be in a different VRF.
- BFD is not supported on sub-interfaces.

Chapter 3
Internet Group Management Protocol (IGMP)

In a network where IP multicast traffic is transmitted for various multimedia applications, you can use the switch to reduce unnecessary bandwidth usage on a per-port basis by configuring IGMP (Internet Group Management Protocol). IGMPv3 (RFC 3376) and IGMPv2 (RFC 2236) are the current RFCs for IGMP.

In the factory default state (IGMP disabled), the switch simply floods all IP multicast traffic it receives on a given VLAN through all ports on that VLAN (except the port on which it received the traffic). This can result in significant and unnecessary bandwidth usage in networks where IP multicast traffic is a factor. Enabling IGMP allows the ports to detect IGMP queries and report packets and manage IP multicast traffic through the switch.

IGMP is useful in multimedia applications such as LAN TV, desktop conferencing, and collaborative computing, where there is MultiPoint communication; that is, communication from one to many hosts, or communication originating from many hosts and destined for many other hosts.

In such MultiPoint applications, IGMP will be configured on the hosts, and multicast traffic will be generated by one or more servers (inside or outside of the local network). Switches in the network (that support IGMP) can then be configured to direct the multicast traffic to only the ports where needed. If multiple VLANs are configured, you can configure IGMP on a per-VLAN basis.

Enabling IGMP allows the router to become querier. If there is another querier in the LAN, the router will resume non querier functionality and will respond to query/report packets.

IGMP defaults, protocols, and supported configuration

IGMP default configuration:

- IGMP is disabled by default.
- The default IGMP version is IGMPv3.

IGMP supported protocols include:

- IGMPv2 (RFC 2236)
- IGMPv3 (RFC 3376)

Static groups:

You can configure a maximum of 32 IGMP static groups on the Aruba 6200 Switch Series.

How the IGMP protocol works

IGMP manages multicast group memberships based on the query and response mechanism.

IGMP is an internal protocol of the IP suite. IP manages multicast traffic by using switches, multicast routers, and hosts that support IGMP. A multicast router is not necessary as long as a switch is configured to support IGMP with the querier feature enabled. A set of hosts, routers, and/or switches that send or receive multicast data streams to or from the same sources, is called a multicast group. All devices in the group use the same multicast group address.

The multicast group uses three fundamental types of messages to communicate:

- Query: A message sent from the querier (multicast router or switch) asking for a response from each host belonging to the multicast group. If a multicast router supporting IGMP is not present, the switch must assume this function to elicit group membership information from the hosts on the network.
- Join: A message sent by a host to the querier to indicate that the host wants to be or is a member of a given group indicated in the join message.
- Leave group: A message sent by a host to the querier to indicate that the host has ceased to be a member of a specific multicast group.

An IP multicast packet includes the multicast group (address) to which the packet belongs. When an IGMP client connected to a switch port needs to receive multicast traffic from a specific group, it joins the group by sending an IGMP join request to the network. (The multicast group specified in the join request is determined by the requesting application running on the IGMP client.)

When the client is ready to leave the multicast group, it sends a Leave Group message to the network and ceases to be a group member. When the leave request is detected, the appropriate IGMP device ceases transmitting traffic for the designated multicast group through the port on which the leave request was received (as long as there are no other current members of that group on the affected port.)

Thus, IGMP identifies members of a multicast group (within a subnet) and allows IGMP-configured hosts (and routers) to join or leave multicast groups.

Considerations when configuring IGMP

With the factory default setting, multicast data transmitted from the sources will be flooded on all ports in the VLAN. Configuring IGMP snooping avoids flooding and causes the switch to forward data only to the receivers.

The function of the IGMP querier is to poll other IGMP-enabled devices in an IGMP-enabled interface to elicit group membership information. On enabling IGMP, the router performs this function if there is no other device in the interface to act as querier.

Basic steps to configure IGMP:

1. Configure VLANs.
2. Configure ports and assign them to the VLANs.
3. Configure the L3 interface (an interface VLAN/route only port/L3 LAG) and assign an IP address to the interface.
4. Enable IGMP.
5. Choose the desired IGMP version. The default is version 3.

IGMP configuration considerations:

- For IGMP to be operational, the interface has to be administratively up. For interface VLANs, the L2 VLAN has to be up and one of the ports in the VLAN has to be up.
- The IP address must be assigned for the interface to become querier. Without an IP address, the device will remain in a non querier state.
- A querier is required for proper IGMP operation. For this reason, you must enable IGMP on the L3 Interface. If the querier functionality is not configured or disabled, you must ensure that there is an IGMP querier in the same VLAN.
- For IGMP snooping to be operational on a VLAN, the VLAN has to be administratively up and at least one port in the VLAN has to be up.
- If IGMP snooping is enabled on the VLAN, and IGMP is enabled on the interface VLAN, and the configured version does not match, the lowest version is chosen as the operating version.

- If the switch becomes the querier for a particular interface, then subsequently detects queries transmitted from another device on the same VLAN, the switch ceases to operate as the querier for that interface.
- The switch automatically ceases querier operation in an IGMP-enabled interface if it detects another querier on the interface. You can also use the switch CLI to disable the querier capability.
- Multicast traffic will be flooded on the VLAN, if TTL=1 or TTL>255 regardless of IGMP joins and group membership within the VLAN.

IGMP configuration task list

Tasks at a glance.

- Enabling or disabling IGMP
- Specifying the IGMP version
- Configuring IGMP static groups
- Configuring IGMP query and response parameters
- Disabling IGMP
- Viewing IGMP information

Enabling or disabling IGMP

Prerequisites

You must be in an interface configuration context, as indicated by the `switch(config-if)#` prompt, `switch(config-if-vlan)#` prompt, or `switch(config-lag-if)#` prompt.

For IGMP to be operational, the interface has to be up. To become querier, the interface must have an IP address associated with it.

Procedure

IGMP is disabled by default. Enable IGMP on an interface using the following command.

```
ip igmp {enable | disable}
```

For example, the following command enables IGMP on interface VLAN 2:

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ip igmp enable
```

Use the `disable` parameter to disable IGMP on an interface.

Specifying the IGMP version

The version can be either 2 (IGMPv2) or 3 (IGMPv3). The default is 3. IGMPv2 supports filtering based on groups. IGMPv3 is more advanced and includes filtering based on source and groups.

If using the `strict` option, packets that do not match the configured version will be dropped.

Prerequisites

You must be in an interface configuration context, as indicated by the `switch(config-if)#` prompt, `switch(config-if-vlan)#` prompt, or `switch(config-lag-if)#` prompt.

Procedure

Specify the IGMP version for an interface using one of the following commands.

`ip igmp version <VERSION>`

`ip igmp version <VERSION> strict`

For example, the following command sets the IGMP version to 2 on interface VLAN 2:

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ip igmp version 2
```

And the following command sets IGMP strict version to 2 on interface VLAN 5:

```
switch(config)# interface vlan 5
switch(config-if-vlan)# ip igmp version 2 strict
switch(config-if-vlan)# no ip igmp version 2 strict
```

Configuring IGMP static groups

The switch will always flood the traffic destined for a group configured as static group. So the hosts will receive the traffic for static groups even if they have not subscribed for that group. You can configure a maximum of 32 IGMP static groups.

Prerequisites

You must be in an interface configuration context, as indicated by the `switch(config-if)#` prompt, `switch(config-if-vlan)#` prompt, or `switch(config-lag-if)#` prompt.

Procedure

Configure an IGMP static group on an interface using the following command.

`ip igmp static-group <MULTICAST-GROUP-IP>`

For example, the following command configures an IGMP static multicast group as 239.1.1.1 on interface VLAN 2:

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ip igmp static-group 239.1.1.1
```

The `no` form of the command removes an IGMP static group.

Configuring IGMP query and response parameters

Configure query and response parameters such as querier interval, last member query interval, max response time, and robustness.

Prerequisites

You must be in an interface configuration context, as indicated by the `switch(config-if)#` prompt, `switch(config-if-vlan)#` prompt, or `switch(config-lag-if)#` prompt.

Procedure

Configure IGMP query and response parameters on an interface using the following commands.

- Make sure that the IGMP querier is enabled. (In IGMPv3 the IGMP querier is enabled by default.) Configure the IGMP querier on an interface using the following command: `ip igmp querier`.
- Configure the IGMP querier interval on an interface using the following command: `ip igmp querier interval` *<INTERVAL-VALUE>*. The interval is from 5-300 seconds, with a default of 125.
- Configure the IGMP last member query interval value in seconds on an interface using the following command: `ip igmp last-member-query-interval` *<INTERVAL-VALUE>*. The interval is from 1-2 seconds, with a default of 1.
- Configure the IGMP max response time value in seconds on an interface using the following command: `ip igmp querier query-max-response-time` *<RESPONSE-TIME>*. The response time is from 10-128 seconds, with a default of 10.
- Configure the IGMP robustness (the number of times to retry a query) on an interface using the following command: `ip igmp robustness` *<VALUE>*. The robustness value is from 1-7 with default of 2.

For example, the following command configures the IGMP querier interface interval as 100 on interface VLAN 2. The `no` form of the command sets the interval to the default.

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ip igmp querier interval 100
switch(config-if-vlan)# no ip igmp querier interval
```

Disabling IGMP

Prerequisites

You must be in an interface configuration context, as indicated by the `switch(config-if)#` prompt, `switch(config-if-vlan)#` prompt, or `switch(config-lag-if)#` prompt.

Procedure

Remove IGMP from an interface using the following command.
`no ip igmp`
For example, the following command removes IGMP on interface VLAN 2:

```
switch(config)# interface vlan 2
switch(config-if-vlan)# no ip igmp
```

Viewing IGMP information

For some commands, you can specify viewing information by interface or by VRF.

Prerequisites

Use these show commands from the Operator (`>`) or Manager (`#`) context.

Procedure

To view IGMP information, use the following commands.

- To view IGMP configuration details and status, use: `show ip igmp` or use `show ip igmp interface`.
- To view IGMP statistics and groups joined, use: `show ip igmp statistics` or use `show ip igmp interface statistics`.
- To view IGMP counters, use: `show ip igmp counters` or use `show ip igmp interface counters`.
- To view IGMP static groups, use: `show ip igmp static-groups`.
- To view IGMP group information, use: `show ip igmp groups` or use `show ip igmp interface groups`.
- To view IGMP group details for a specific group and source, use: `show ip igmp group` or use `show ip igmp interface group`. Optionally you can also display joined group details by VRF.

IGMP configuration example

The output of the following `show running-config` command shows an example of an IGMP configuration with IGMP snooping.

On the 6400 Switch Series, interface identification differs.

```
switch# show running-config
Current configuration:
!
!
!
!
!
access-list ip mygroup
    10 permit any any 239.1.1.1/24
access-list ip mygroup1
    10 permit any any any
vlan 1
    no shutdown
vlan 2
    ip igmp snooping enable
    ip igmp snooping static group 239.1.1.10
    ip igmp snooping static group 239.1.1.11
! 'mygroup' will be ignored in this configuration as 'mygroup1' is configured in
'vlan2'.
    ip igmp snooping apply access-list mygroup
interface 1/1/1
    no shutdown
    ip address 100.1.1.1/24
    ip igmp enable
interface 1/1/1.1
    no shutdown
    routing
    ip address 100.100.100.1/24
    ip igmp enable
    ip igmp querier interval 5
    ip igmp last-member-query-interval 2
    ip igmp query-max-response-time 30
    ip igmp static-group 239.1.1.1
    ip igmp apply access-list mygroup1
interface 1/1/2
    no shutdown
    ip address 200.1.1.1/24
    ip igmp enable
    ip igmp querier interval 5
    ip igmp last-member-query-interval 2
```

```
    ip igmp query-max-response-time 50
    ip igmp static-group 239.1.1.1
    ip igmp apply access-list mygroup1
interface 1/1/3
    no shutdown
    no routing
    vlan access 2
    ip igmp snooping blocked vlan 2
interface 1/1/3
     no shutdown
     no routing
     vlan access 2
     ip igmp snooping forward vlan 2
interface vlan2
    no shutdown
    ip address 20.1.1.1/24
    ip igmp enable
    ip igmp querier interval 5
    ip igmp robustness 5
    ip igmp last-member-query-interval 2
    ip igmp query-max-response-time 50
    ip igmp static-group 239.1.1.1
    ip igmp apply access-list mygroup1
```

IGMP commands

For commands in the interface configuration context, the interface must be an L3 interface. The supported contexts include: `config-if`, `config-if-vlan`, `config-lag-if`, `config-sub-if`.

The sub-interface related configuration examples provided in this section apply only to the Aruba 6300, 6400, and 8360 Switch Series.

Only the default VRF is supported on the Aruba 6200 Switch Series.

ip igmp

```
ip igmp {enable | disable}
```

Description

Enables or disables IGMP on the current interface. IGMP is disabled by default.

Parameters

`enable`

Enable IGMP.

`disable`

Disable IGMP.

Examples

Enabling IGMP on interface VLAN 2:

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ip igmp enable
```

Disabling IGMP on interface VLAN 2:

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ip igmp disable
```

Enabling IGMP on interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# no shutdown
switch(config-if)# routing
switch(config-subif)# ip igmp enable
```

Disabling IGMP on interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-subif)# ip igmp disable
```

Enabling IGMP on sub-interface 1/1/1.1:

Applies only to the Aruba 6300, 6400, and 8360 Switch Series.

```
switch(config)# interface 1/1/1.1
switch(config-subif)# no shutdown
switch(config-subif)# ip igmp enable
```

Disabling IGMP on sub-interface 1/1/1.1:

Applies only to the Aruba 6300, 6400, and 8360 Switch Series.

```
switch(config)# interface 1/1/1.1
switch(config-subif)# ip igmp disable
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority

All platforms	`config-if-vlan`
	`config-if`
	`config-lag-if`
	`config-subif`
		Administrators or local user group members with execution rights for this command.

ip igmp apply access-list

```
ip igmp apply access-list <ACL-NAME>
no ip igmp apply access-list <ACL-NAME>
```

Description

Configures the ACL on a particular interface to filter the IGMP join or leave packets based on rules set in the particular ACL name.

The `no` form of this command unconfigures the rules set for the ACL.

This configuration will override the ACL associated with IGMP snooping on the corresponding L2 VLAN.

Parameters

`access-list`

Associates an ACL with the IGMP.

`<ACL-NAME>`

Specifies the name of the ACL.

Usage

Existing classifier commands are used to configure the ACL. In case an IGMPv3 packet with multiple group addresses is received, it will only process the permitted group addresses based on the ACL rule set, and any existing joins will time out. If there is no match or if there is a deny rule match, the packet is dropped.

Examples

Configuring the ACL on a VLAN to filter IGMP packets based on rules set in access list `mygroup`:

```
switch(config)# access-list ip mygroup
switch(config-acl-ip)# permit igmp any 239.1.1.1
switch(config-acl-ip)# exit
switch(config)# interface vlan 2
switch(config-if-vlan)# ip igmp apply access-list mygroup
```

Configuring the ACL to remove the rules set in access list `mygroup`:

```
switch(config-if-vlan)# no ip igmp apply access-list mygroup
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config-if-vlan`	Administrators or local user group members with execution rights for this command.

ip igmp last-member-query-interval

```
ip igmp last-member-query-interval <INTERVAL-VALUE>
```

```
no ip igmp last-member-query-interval <INTERVAL-VALUE>
```

Description

Configures an IGMP last member query interval value in seconds on an interface, depending on the command context you are in.

The `no` form of this command sets the value to a default of 1 second on an interface.

Parameters

<INTERVAL-VALUE>

Specifies an IGMP last-member-query-interval on the interface. Default: 1 second. Range: 1-2 seconds.

Examples

Configuring an IGMP last member query interval of 2 on interface VLAN 2:

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ip igmp last-member-query-interval 2
switch(config-if-vlan)# no ip igmp last-member-query-interval
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority

All platforms	`config-if-vlan`
	`config-if`
	`config-lag-if`
		Administrators or local user group members with execution rights for this command.

ip igmp querier

```
ip igmp querier
no ip igmp querier
```

Description

Configures an IGMP querier on an interface, depending on the command context you are in. This functionality will allow an interface to join in the querier-election process.

The `no` form of this command disables IGMP querier on an interface.

Examples

Configuring an IGMP querier on interface VLAN 2:

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ip igmp querier
```

Disabling an IGMP querier on interface VLAN 2:

```
switch(config)# interface vlan 2
switch(config-if-vlan)# no ip igmp querier
```

Configuring an IGMP querier on interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# no shutdown
switch(config-if)# routing
switch(config-subif)# ip igmp querier
```

Disabling an IGMP querier on interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-subif)# no ip igmp querier
```

Configuring an IGMP querier on sub-interface 1/1/1.1

Applies only to the Aruba 6300, 6400, and 8360 Switch Series.

```
switch(config)# interface 1/1/1.1
switch(config-subif)# no shutdown
switch(config-subif)# ip igmp querier
```

Disabling an IGMP querier on sub-interface 1/1/1.1:

Applies only to the Aruba 6300, 6400, and 8360 Switch Series.

```
switch(config)# interface 1/1/1.1
switch(config-subif)# no ip igmp querier
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if-vlan config-if config-lag-if config-subif	Administrators or local user group members with execution rights for this command.

ip igmp querier interval

```
ip igmp querier interval <INTERVAL-VALUE>
no ip igmp querier interval
```

Description

Configures the interval between IGMP queries on an interface, depending on the command context you are in.

The `no` form of this command sets the IGMP querier interval to the default value of 125 seconds on an interface.

Parameters

<INTERVAL-VALUE>

Specifies the IGMP querier interval in seconds on the interface. Default: 125 seconds. Range: 5-300.

Examples

Configuring an IGMP querier interface interval of 100 on interface VLAN 2:

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ip igmp querier interval 100
```

Resetting an IGMP querier interval to the default value:

```
switch(config-if-vlan)# no ip igmp querier interval
```

Configuring an IGMP querier interface interval of 100 on interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# no shutdown
switch(config-if)# routing
switch(config-subif)# ip igmp querier interval 100
```

Configuring an IGMP querier interface interval of 100 on sub-interface 1/1/1.1:

Applies only to the Aruba 6300, 6400, and 8360 Switch Series.

```
switch(config)# interface 1/1/1.1
switch(config-subif)# no shutdown
switch(config-subif)# ip igmp querier interval 100
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config-if-vlan` `config-if`	Administrators or local user group members with execution rights for this command.

Platforms	Command context	Authority
	config-lag-if config-subif	

ip igmp querier query-max-response-time

```
ip igmp querier query-max-response-time <RESPONSE-TIME>
no ip igmp querier query-max-response-time <RESPONSE-TIME>
```

Description

Configures the IGMP querier max response time value in seconds on an interface, depending on the command context you are in.

The no form of this command sets the querier max response time value to the default of 10 seconds on an interface.

Parameters

<RESPONSE-TIME>

Specifies the IGMP querier max response time value on the interface. Default: 10 seconds. Range: 10-128 seconds.

Examples

Configuring the IGMP querier maximum response time of 50 for interface VLAN 2:

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ip igmp query-max-response-time 50
```

Resetting an IGMP querier interval to the default value:

```
switch(config-if-vlan)# no ip igmp query-max-response-time
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if-vlan config-if config-lag-if	Administrators or local user group members with execution rights for this command.

ip igmp robustness

```
ip igmp robustness <VALUE>
no ip igmp robustness <VALUE>
```

Description

Configures IGMP robustness on an interface, depending on the command context. The robustness parameter allows tuning for the expected packet loss on a subnet.

The `no` form of this command sets the robustness value to the default of 2 on an interface.

Parameters

<VALUE>

Specifies an IGMP robustness value on the interface. Default: 2. Range: 1-7.

Examples

Configuring an IGMP robustness of 5 on interface VLAN 2:

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ip igmp robustness 5
```

Resetting the IGMP robustness to the default:

```
switch(config-if-vlan)# no ip igmp robustness
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority

All platforms	`config-if-vlan`
	`config-if`
	`config-lag-if`
		Administrators or local user group members with execution rights for this command.

ip igmp router-alert-check

```
ip igmp router-alert-check [enable | disable]
no ip igmp router-alert-check [enable | disable]
```

Description

Enables or disables IGMP router alert check for IGMP packets. IGMP packets without the router alert field set are dropped if router alert check is enabled. Router alert check is disabled by default.

The `no` form of this command disables router alert check for IGMP packets.

Parameters

`enable`

Enable IGMP router alert check.

`disable`

Disable IGMP router alert check.

Examples

Enabling IGMP router alert check on interface VLAN 2:

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ip igmp router-alert-check enable
```

Disabling IGMP router alert check on interface VLAN 2:

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ip igmp router-alert-check disable
```

Command History

Release	Modification
10.08	Command introduced.

Command Information

Platforms	Command context	Authority
All platforms	config-if-vlan config-if config-lag-if	Administrators or local user group members with execution rights for this command.

ip igmp static-group

```
ip igmp static-group <MULTICAST-GROUP-IP>
no ip igmp static-group <MULTICAST-GROUP-IP>
```

Description

Configures an IGMP static multicast group on an interface, depending on the command context you are in. You can configure a maximum of 32 IGMP static groups.

The no form of the command unconfigures IGMP static multicast group on an interface.

Parameters

<MULTICAST-GROUP-IP>

Specifies an IGMP static multicast group IP address on the interface. Format: A.B.C.D

Examples

Administrators or local user group members with execution rights for this command.

Configuring an IGMP static group on interface VLAN 2:

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ip igmp static-group 239.1.1.1
```

Resetting an IGMP static group on an interface to the default (none):

```
switch(config-if)# no ip igmp static-group 239.1.1.10
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority

All platforms	`config-if-vlan`
	`config-if`
	`config-lag-if`	

ip igmp version

`ip igmp version <VERSION>`

Description

Configures the IGMP version on an interface, depending on the command context you are in.

Parameters

<VERSION>

Specifies the IGMP version on the interface. Select 2 for IGMPv2 (RFC2236). Select 3 for IGMPv3 (RFC3376). Values: 2 or 3.

Examples

Configuring an IGMP version on interface VLAN 2:

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ip igmp version 2
```

Configuring an IGMP version on interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-if)# ip igmp version 2
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority

All platforms	`config-if-vlan`
	`config-if`
	`config-lag-if`
		Administrators or local user group members with execution rights for this command.

ip igmp version strict

```
ip igmp version <VERSION> strict
no ip igmp version <VERSION> strict
```

Description

Configures an IGMP strict version on an interface, depending on the command context you are in. Drops packets that do not match the configured version.

The `no` form of the command removes the strict version configuration from the interface.

Parameters

<VERSION>

Specifies the IGMP version on the interface. Select 2 for IGMPv2 (RFC2236). Select 3 for IGMPv3 (RFC3376). Values: 2 or 3.

Examples

Configuring the IGMP strict version to 2 on interface VLAN 2:

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ip igmp version 2 strict
```

Resetting the IGMP strict version to the default (none):

```
switch(config-if)# no ip igmp version 2 strict
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority

All platforms	`config-if-vlan`
	`config-if`
	`config-lag-if`
		Administrators or local user group members with execution rights for this command.

no ip igmp

```
no ip igmp
```

Description

Disables all IGMP configurations on an interface or sub-interface, depending on the command context you are in.

Examples

Removing IGMP on interface VLAN 2:

```
switch(config)# interface vlan 2
switch(config-if-vlan)# no ip igmp
```

Removing IGMP on interface 1/1/1:

```
switch(config)# interface 1/1/1
switch(config-subif)# no ip igmp
```

Removing IGMP on sub-interface 1/1/1.1:

Applies only to the Aruba 6300, 6400, and 8360 Switch Series.

```
switch(config)# interface 1/1/1.1
switch(config-subif)# no ip igmp
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority

All platforms	`config-if-vlan`
	`config-if`
	`config-lag-if`
	`config-subif`
		Administrators or local user group members with execution rights for this command.

show ip igmp

`show ip igmp [vrf <VRF-NAME> | all-vrfs] [vsx-peer]`

Description

Shows IGMP configuration information and status, or shows information by VRF.

Parameters

`vrf <VRF-NAME> | all-vrfs`

Optional. Used to show information by VRF. Specify the VRF by VRF name. With no `<VRF-NAME>` specified, the default VRF is implied. To show information for all VRFs, specify `all-vrfs`.

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing IGMP configuration and status:

```
switch# show ip igmp

VRF Name  : default
Interface : vlan2
IGMP Configured Version    : 3
IGMP Operating Version     : 3
Querier State              : Querier
Querier IP [this switch]   : 20.1.1.1
Querier Uptime             : 1m 4s
Querier Expiration Time    : 0m 1s
IGMP Snoop Enabled on VLAN : True
```

Showing IGMP information for VRF test:

```
switch# show ip igmp vrf test

VRF Name  : test
Interface  : 1/1/2
IGMP Configured Version  : 3
IGMP Operating Version   : 2
Querier State            : Querier
Querier IP [this switch] : 100.1.1.1
Querier Uptime           : 2m 55s
Querier Expiration Time  : 0m 16s

Active Group Address   Vers Mode Uptime    Expires
---------------------- ---- ---- --------- ---------
240.100.3.194          3    INC  0m 30s    3m 50s


IGMP is not enabled on interface 1/1/3


VRF Name  : test
Interface  : vlan2
IGMP Configured Version    : 3
IGMP Operating Version     : 3
Querier State              : Querier
Querier IP [this switch]   : 20.1.1.1
Querier Uptime             : 1m 4s
Querier Expiration Time    : 0m 1s
IGMP Snoop Enabled on VLAN : True

Active Group Address   Vers Mode Uptime    Expires
---------------------- ---- ---- --------- ---------
238.224.153.165        2         0m 38s    3m 42s


VRF Name  : test
Interface  : vlan10
IGMP Configured Version    : 3
IGMP Operating Version     : 3
Querier State              : Querier
Querier IP [this switch]   : 10.1.1.1
Querier Uptime             : 1m 4s
Querier Expiration Time    : 0m 1s
IGMP Snoop Enabled on VLAN : True

Active Group Address   Vers Mode Uptime    Expires
---------------------- ---- ---- --------- ---------
239.209.3.194          3    INC  0m 38s    3m 42s
```

Showing IGMP information for all VRFs:

```
switch# show ip igmp all-vrfs
VRF Name  : test
Interface  : 1/1/2
IGMP Configured Version  : 3
IGMP Operating Version   : 2
Querier State            : Querier
Querier IP [this switch] : 100.1.1.1
Querier Uptime           : 2m 55s
Querier Expiration Time  : 0m 16s

Active Group Address   Vers Mode Uptime    Expires
---------------------- ---- ---- --------- ---------
240.100.3.194          3    INC  0m 30s    3m 50s

VRF Name  : test
Interface  : vlan2
IGMP Configured Version    : 3
IGMP Operating Version     : 3
Querier State              : Querier
Querier IP [this switch]   : 20.1.1.1
Querier Uptime             : 1m 4s
Querier Expiration Time    : 0m 1s
IGMP Snoop Enabled on VLAN : True

Active Group Address   Vers Mode Uptime    Expires
---------------------- ---- ---- --------- ---------
238.224.153.165        2         0m 38s    3m 42s
VRF Name  : default
Interface  : vlan5
IGMP Configured Version    : 3
IGMP Operating Version     : 2
Querier State              : Querier
Querier IP [this switch]   : 50.1.1.1
Querier Uptime             : 1m 1s
Querier Expiration Time    : 0m 4s
IGMP Snoop Enabled on VLAN : False
VRF Name  : test
Interface  : vlan10
IGMP Configured Version    : 3
IGMP Operating Version     : 3
Querier State              : Querier
Querier IP [this switch]   : 10.1.1.1
Querier Uptime             : 1m 4s
Querier Expiration Time    : 0m 1s
IGMP Snoop Enabled on VLAN : True

Active Group Address   Vers Mode Uptime    Expires
---------------------- ---- ---- --------- ---------
239.209.3.194          3    INC  0m 38s    3m 42s
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip igmp counters

```
show ip igmp counters [vrf <VRF-NAME> | all-vrfs] [vsx-peer]
```

Description

Shows IGMP counter details, or shows counters by VRF.

Parameters

`vrf <VRF-NAME> | all-vrfs`

Optional. Used to show information by VRF. Specify the VRF by VRF name. With no *<VRF-NAME>* specified, the default VRF is implied. Specify `all-vrfs` to show information for all VRFs.

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing IGMP counters:

```
switch# show ip igmp counters

IGMP Counters

Interface Name      : vlan2
VRF Name            : default
Membership Timeout  : 0
                                              Rx             Tx
                                              -------------- --------------
V1 All Hosts Queries                          0              0
V2 All Hosts Queries                          0              12
V3 All Hosts Queries                          0              0
V2 Group Specific Queries                     0              0
V3 Group Specific Queries                     0              0
Group And Source Specific Queries             0              0
V3 Member Reports                             0              N/A
V2 Member Reports                             0              N/A
V1 Member Reports                             0              N/A
V2 Member Leaves                              0              N/A
Packets dropped by ACL                        0              N/A
```

Showing IGMP counters for the default VRF:

```
switch# show ip igmp counters vrf default

IGMP Counters

Interface Name      : vlan2
VRF Name            : default
Membership Timeout  : 0
```

```
                                          Rx            Tx
                                          ------------- -------------
V1 All Hosts Queries                      0             0
V2 All Hosts Queries                      0             12
V3 All Hosts Queries                      0             0
V2 Group Specific Queries                 0             0
V3 Group Specific Queries                 0             0
Group And Source Specific Queries         0             0
V3 Member Reports                         0             N/A
V2 Member Reports                         0             N/A
V1 Member Reports                         0             N/A
V2 Member Leaves                          0             N/A
Packets dropped by ACL                    0             N/A
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip igmp group

`show ip igmp group <GROUP-IP> [source <SOURCE-IP>] [vrf <VRF-NAME> | all-vrfs] [vsx-peer]`

Description

Shows IGMP joined group information for the specified group, or shows joined group source and display information by VRF.

Parameters

<GROUP-IP>

Specifies the IP address of the group. Format: A.B.C.D

`source` *<SOURCE-IP>*

Specifies the IP address of the source. Format: A.B.C.D

`vrf` *<VRF-NAME>* | `all-vrfs`

Optional. Used to show information by VRF. Specify the VRF by VRF name. With no *<VRF-NAME>* specified, the default VRF is implied. Specify `all-vrfs` to show information for all VRFs.

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing IGMP joined group details for group 239.1.1.10:

```
switch# show ip igmp group 239.1.1.10

IGMP group information for group 239.1.1.10

Interface Name   : vlan2
VRF Name         : default

Group Address    : 239.1.1.10
Last Reporter    : 100.1.1.10

                              V1        V2        Sources   Sources
Vers Mode Uptime    Expires   Timer     Timer     Forwarded Blocked
---- ---- --------- --------- --------- --------- --------- --------
3    EXC  16m 34s   2m 27s
```

Showing IGMP joined group details for group 239.1.1.10 and source 10.1.1.10:

```
switch# show ip igmp group 239.1.1.10 source 10.1.1.10

Interface Name  : vlan2
VRF Name  : default
Group Address  : 239.1.1.10
Source Address : 10.1.1.10

Mode Uptime    Expire
---- --------- -------
     0m 13s    4m 7s
```

Showing IGMP joined group details for group 239.1.1.10 for all VRFs:

```
switch# show ip igmp group 239.1.1.10 all-vrfs

IGMP group information for group 239.1.1.10

Interface Name   : vlan10
VRF Name         : default

Group Address    : 239.1.1.10
Last Reporter    : 100.1.1.10

                              V1        V2        Sources   Sources
Vers Mode Uptime    Expires   Timer     Timer     Forwarded Blocked
---- ---- --------- --------- --------- --------- --------- --------
3    EXC  17m 5s    4m 2s
```

Showing IGMP joined group details for group 239.1.1.10 source 10.1.1.10 for all VRFs:

```
switch# show ip igmp group 239.1.1.10 source 10.1.1.10 all-vrfs

Interface Name  : vlan10
VRF Name  : default
Group Address  : 239.1.1.10
Source Address : 10.1.1.10

Mode Uptime    Expire
```

```
---- --------- -------
     0m 39s    3m 41s
```

Showing IGMP joined group details group 239.1.1.10 for the default VRF:

```
switch# show ip igmp group 239.1.1.10 vrf default

IGMP group information for group 239.1.1.10

Interface Name   : vlan2
VRF Name         : default

Group Address    : 239.1.1.10
Last Reporter    : 100.1.1.10

                              V1        V2        Sources   Sources
Vers Mode Uptime    Expires   Timer     Timer     Forwarded Blocked
---- ---- --------- --------- --------- --------- --------- --------
3    EXC  17m 35s   3m 32s
```

Showing IGMP joined group details group 239.1.1.10 source 10.1.1.10 for the default VRF:

```
switch# show ip igmp group 239.1.1.10 source 10.1.1.10 vrf default

Interface Name  : vlan10
VRF Name  : default
Group Address  : 239.1.1.10
Source Address : 10.1.1.10

Mode Uptime    Expire
---- --------- -------
     0m 59s    3m 21s
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip igmp groups

`show ip igmp groups [vrf <VRF-NAME> | all-vrfs] [vsx-peer]`

Description

Shows IGMP group information, or you can display group information by VRF.

Parameters

`vrf <VRF-NAME> | all-vrfs`

Optional. Used to show information by VRF. Specify the VRF by VRF name. With no *<VRF-NAME>* specified, the default VRF is implied. Specify `all-vrfs` to show information for all VRFs.

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing IGMP group information:

```
switch# show ip igmp groups

IGMP group information for group 239.1.1.10

Interface Name   : vlan2
VRF Name         : default

Group Address    : 239.1.1.10
Last Reporter    : 100.1.1.10

                                 V1        V2        Sources   Sources
Vers Mode Uptime    Expires   Timer     Timer     Forwarded Blocked
---- ---- --------- --------- --------- --------- --------- --------
3    EXC  0m 36s    3m 44s

IGMP group information for group 239.1.1.11

Interface Name   : vlan2
VRF Name         : default

Group Address    : 239.1.1.11
Last Reporter    : 100.1.1.10

                                 V1        V2        Sources   Sources
Vers Mode Uptime    Expires   Timer     Timer     Forwarded Blocked
---- ---- --------- --------- --------- --------- --------- --------
3    EXC  0m 36s    3m 44s
```

Showing IGMP groups for all VRFs:

```
switch# show ip igmp groups all-vrfs
IGMP group information for group 239.1.1.1

Interface Name   : vlan10
VRF Name         : test

Group Address    : 239.1.1.1
Last Reporter    : 100.1.1.20

                                 V1        V2        Sources   Sources
Vers Mode Uptime    Expires   Timer     Timer     Forwarded Blocked
---- ---- --------- --------- --------- --------- --------- --------
3    EXC  0m 13s    4m 7s

IGMP group information for group 239.1.1.2

Interface Name   : vlan10
VRF Name         : test
```

```
Group Address    : 239.1.1.2
Last Reporter    : 100.1.1.20

                                V1        V2        Sources   Sources
Vers Mode Uptime    Expires     Timer     Timer     Forwarded Blocked
---- ---- --------- --------- --------- --------- --------- --------
3    EXC  0m 13s    4m 7s

IGMP group information for group 239.1.1.1

Interface Name   : vlan20
VRF Name         : default

Group Address    : 239.1.1.1
Last Reporter    : 200.1.1.10

                                V1        V2        Sources   Sources
Vers Mode Uptime    Expires     Timer     Timer     Forwarded Blocked
---- ---- --------- --------- --------- --------- --------- --------
3    EXC  0m 13s    4m 7s

IGMP group information for group 239.1.1.2

Interface Name   : vlan20
VRF Name         : default

Group Address    : 239.1.1.2
Last Reporter    : 200.1.1.10

                                V1        V2        Sources   Sources
Vers Mode Uptime    Expires     Timer     Timer     Forwarded Blocked
---- ---- --------- --------- --------- --------- --------- --------
3    EXC  0m 13s    4m 7s
```

Showing IGMP groups for the default VRF:

```
switch# show ip igmp groups vrf default

IGMP group information for group 239.1.1.10

Interface Name   : vlan2
VRF Name         : default

Group Address    : 239.1.1.10
Last Reporter    : 100.1.1.10

                                V1        V2        Sources   Sources
Vers Mode Uptime    Expires     Timer     Timer     Forwarded Blocked
---- ---- --------- --------- --------- --------- --------- --------
3    EXC  9m 23s    3m 20s

IGMP group information for group 239.1.1.11

Interface Name   : vlan2
VRF Name         : default

Group Address    : 239.1.1.11
Last Reporter    : 100.1.1.10

                                V1        V2        Sources   Sources
```

```
Vers Mode Uptime    Expires   Timer     Timer     Forwarded Blocked
---- ---- --------- --------- --------- --------- --------- --------
3    EXC  9m 23s    3m 20s
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip igmp interface

`show ip igmp interface {<INTF-ID> | <INTF-ID.ID> | vlan <VLAN-ID>} [vsx-peer]`

Description

Shows IGMP configuration information for a specific interface (VLAN, port or LAG).

Parameters

<INTF-ID>

Specifies an interface (such as 1/1/2 or LAG10).

<INTF-ID.ID>

Required. Specifies a sub-interface. (Applies only to the Aruba 6300, 6400, and 8360 Switch Series.)

`vlan` *<VLAN-ID>*

Specifies a VLAN. Values: 1-4094.

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing IGMP configuration information for interface VLAN 2:

```
switch# show ip igmp interface vlan 2

IGMP Configured Version   : 3
IGMP Operating Version    : 3
Querier State             : Querier
Querier IP [this switch] : 20.1.1.1
Querier Uptime            : 1m 46s
Querier Expiration Time   : 0m 1s
Snoop Enabled on VLAN     : True

switch# show ip igmp interface vlan  10
```

```
IGMP is not enabled
```

Showing IGMP configuration information for the specified interface 1/1/2:

```
switch# show ip igmp interface 1/1/2

IGMP Configured Version    : 3
IGMP Operating Version     : 3
Querier State              : Querier
Querier IP [this switch]   : 100.1.1.1
Querier Uptime             : 51m 44s
Querier Expiration Time    : 1m 51s
```

Showing IGMP configuration information for sub-interface 1/1/5.10:

Applies only to the Aruba 6300, 6400, and 8360 Switch Series.

```
switch# show ip igmp interface 1/1/5.10

IGMP Configured Version    : 3
IGMP Operating Version     : 3
Querier State              : Querier
Querier IP [this switch]   : 200.1.1.1
Querier Uptime             : 11m 44s
Querier Expiration Time    : 1m 51s
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip igmp interface counters

`show ip igmp interface {<INTF-ID> | <INTF-ID.ID>| vlan <VLAN-ID>} counters [vsx-peer]`

Description

Shows IGMP counter details for a specific interface or VLAN interface.

Parameters

<INTF-ID>

Specifies an interface (such as 1/1/2).

<INTF-ID.ID>

Required: Specifies a sub-interface. (Applies only to the Aruba 6300, 6400, and 8360 Switch Series.)

`vlan <VLAN-ID>`

Specifies a VLAN. Values: 1-4094.

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing IGMP counters for interface VLAN 2:

```
switch# show ip igmp interface vlan 2 counters

IGMP Counters

Interface Name      : vlan2
VRF Name            : default
Membership Timeout  : 0
                                          Rx             Tx
                                          -------------- --------------
V1 All Hosts Queries                      0              0
V2 All Hosts Queries                      0              0
V3 All Hosts Queries                      0              29
V2 Group Specific Queries                 0              0
V3 Group Specific Queries                 0              2
Group And Source Specific Queries         0              2
V3 Member Reports                         0              N/A
V2 Member Reports                         0              N/A
V1 Member Reports                         0              N/A
V2 Member Leaves                          0              N/A
Packets dropped by ACL                    0              N/A
```

Showing IGMP counters for sub-interface 10:

Applies only to the Aruba 6300, 6400, and 8360 Switch Series.

```
switch# show ip igmp interface 1/1/5.10 counters

IGMP Counters

Interface Name      : 1/1/5.10
VRF Name            : default
Membership Timeout  : 0
                                          Rx             Tx
                                          -------------- --------------
V1 All Hosts Queries                      0              0
V2 All Hosts Queries                      0              0
V3 All Hosts Queries                      0              9
V2 Group Specific Queries                 0              0
V3 Group Specific Queries                 0              0
Group And Source Specific Queries         0              0
V3 Member Reports                         3              N/A
V2 Member Reports                         4              N/A
V1 Member Reports                         0              N/A
V2 Member Leaves                          0              N/A
Packets dropped by ACL                    0              N/A
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip igmp interface group

```
show ip igmp [interface {<INTF-ID> | <INTF-ID.ID> | vlan <VLAN-ID>} [group <GROUP-IP>
[source <SOURCE-IP>] [vsx-peer]]]
```

Description

Shows IGMP joined group information for a specific interface or VLAN interface, or specify a source IP.

Parameters

<INTF-ID>

Specifies an interface (such as 1/1/2).

<INTF-ID.ID>

Required: Specifies the sub-interface. (Applies only to the Aruba 6300, 6400, and 8360 Switch Series.)

`vlan` *<VLAN-ID>*

Specifies a VLAN. Values: 1-4094.

<GROUP-IP>

Specifies the IP address of the group. Format: A.B.C.D

`source` *<SOURCE-IP>*

Specifies the IP address of the source. Format: A.B.C.D

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing IGMP joined group details for group 239.1.1.1 for interface VLAN 10:

```
switch# show ip igmp interface vlan 10 group 239.1.1.1

IGMP group information for group 239.1.1.1

Interface Name   : vlan10
VRF Name         : default

Group Address    : 239.1.1.1
Last Reporter    : 100.1.1.10

                                V1        V2        Sources   Sources
Vers Mode Uptime    Expires     Timer     Timer     Forwarded Blocked
---- ---- --------- --------- --------- --------- --------- --------
3    INC  8m 10s    2m 21s                        1
```

```
Group Address  : 239.1.1.1
Source Address : 10.1.1.1

Mode Uptime    Expire
---- --------- -------
INC  8m 10s    2m 21s
```

Showing IGMP joined group details for group 239.1.1.1 for interface VLAN 10 with source details for 10.1.1.1:

```
switch# show ip igmp interface vlan 10 group 239.1.1.1 source 10.1.1.1

Interface Name  : vlan10
VRF Name  : default
Group Address  : 239.1.1.1
Source Address : 10.1.1.1

Mode Uptime    Expire
---- --------- -------
INC  8m 52s    3m 51s
```

Showing IGMP joined group details for group 239.1.1.1 for sub-interface 1/1/1.10:

Applies only to the Aruba 6300, 6400, and 8360 Switch Series.

```
switch# show ip igmp interface 1/1/5.10 group 239.1.1.1

IGMP group information for group 239.1.1.1

Interface Name   : 1/1/5.10
VRF Name         : default

Group Address    : 239.1.1.1
Last Reporter    : 10.1.1.10

                                 V1        V2        Sources   Sources
Vers Mode Uptime    Expires      Timer     Timer     Forwarded Blocked
---- ---- --------- --------- --------- --------- --------- --------
3    INC  1m 49s    1m 31s                         1

Group Address  : 239.1.1.1
Source Address : 10.1.1.1

Mode Uptime    Expire
---- --------- -------
INC  1m 49s    1m 31s
```

Showing IGMP joined group details for group 239.1.1.1 for sub-interface 1/1/1.10 with source details for 10.1.1.1:

```
switch# show ip igmp interface 1/1/5.10 group 239.1.1.1 source 10.1.1.1

Interface Name  : 1/1/5.10
VRF Name  : default
```

```
Group Address  : 239.1.1.1
Source Address : 10.1.1.1

Mode Uptime    Expire
---- --------- -------
INC  1m 3s     4m 25s
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip igmp interface groups

`show ip igmp [interface {<INTF-ID> | <INTF-ID.ID> | vlan <VLAN-ID>} [groups] [vsx-peer]]`

Description

Shows IGMP group information for a specific interface or VLAN interface.

Parameters

<INTF-ID>
: Specifies an interface (such as 1/1/2).

<INTF-ID.ID>
: Specifies a sub-interface. (Applies only to the Aruba 6300, 6400, and 8360 Switch Series.)

vlan *<VLAN-ID>*
: Specifies a VLAN. Values: 1-4094.

vsx-peer
: Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing IGMP groups for interface VLAN 2:

```
switch# show ip igmp interface vlan 2 groups

IGMP group information for group 239.1.1.1

Interface Name   : vlan2
VRF Name         : default

Group Address    : 239.1.1.1
Last Reporter    : 100.1.1.10
```

```
                                V1        V2        Sources   Sources
Vers Mode Uptime    Expires     Timer     Timer     Forwarded Blocked
---- ---- --------- --------- --------- --------- --------- --------
3    INC  4m 40s    3m 51s                        1

Group Address  : 239.1.1.1
Source Address : 10.1.1.1

Mode Uptime    Expire
----------------------
INC  4m 40s    3m 51s

IGMP group information for group 239.1.1.2

Interface Name   : vlan2
VRF Name         : default

Group Address    : 239.1.1.2
Last Reporter    : 100.1.1.10

                                V1        V2        Sources   Sources
Vers Mode Uptime    Expires     Timer     Timer     Forwarded Blocked
---- ---- --------- --------- --------- --------- --------- --------
3    INC  4m 40s    3m 51s                        1

Group Address  : 239.1.1.2
Source Address : 10.1.1.1

Mode Uptime    Expire
---- --------- -------
INC  4m 40s    3m 51s
```

Showing IGMP groups for sub-interface:

Applies only to the Aruba 6300, 6400, and 8360 Switch Series.

```
switch# show ip igmp interface 1/1/5.10 groups

IGMP group information for group 239.1.1.1

Interface Name   : 1/1/5.10
VRF Name         : default

Group Address    : 239.1.1.10
Last Reporter    : 10.1.1.1

                                V1        V2        Sources   Sources
Vers Mode Uptime    Expires     Timer     Timer     Forwarded Blocked
---- ---- --------- --------- --------- --------- --------- --------
2         11m 59s   1m 44s              1m 44s

IGMP group information for group 239.1.1.2

Interface Name   : 1/1/5.10
VRF Name         : default

Group Address    : 239.1.1.20
Last Reporter    : 10.1.1.10
```

```
                                V1         V2         Sources   Sources
Vers Mode Uptime    Expires     Timer      Timer      Forwarded Blocked
---- ---- --------- --------- ---------- ---------- --------- --------
2         11m 59s   1m 44s               1m 44s
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip igmp interface statistics

`show ip igmp interface {<INTF-ID> | <INTF-ID.ID> | vlan <VLAN-ID>} statistics [vsx-peer]`

Description

Shows IGMP statistics for a specific interface or VLAN interface, including groups joined.

Parameters

<INTF-ID>

Specifies an interface (such as 1/1/2 or LAG1).

<INTF-ID.ID>

Required: Specifies a sub-interface. (Applies only to the Aruba 6300, 6400, and 8360 Switch Series.)

`vlan` *<VLAN-ID>*

Specifies a VLAN. Values: 1-4094.

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing IGMP statistics for interface VLAN 2:

```
switch# show ip igmp interface vlan 2 statistics

IGMP statistics

Interface Name : vlan2
VRF Name       : default

Number of Include Groups       :   2
Number of Exclude Groups       :   0
```

```
Number of Static Groups         :   0
Total Multicast Groups Joined   :   2
```

Showing IGMP statistics for the sub-interface:

Applies only to the Aruba 6300, 6400, and 8360 Switch Series.

```
switch# show ip igmp interface 1/1/5.10 statistics

IGMP statistics

Interface Name : 1/1/5.10
VRF Name       : default

Number of Include Groups        :   0
Number of Exclude Groups        :   2
Number of Static Groups         :   0
Total Multicast Groups Joined   :   2
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip igmp static-groups

`show ip igmp static-groups [vrf <VRF-NAME> | all-vrfs] [vsx-peer]`

Description

Shows IGMP static groups, or shows information by VRF.

Parameters

`vrf <VRF-NAME> | all-vrfs`

Optional. Used to show information by VRF. Specify the VRF by VRF name. With no `<VRF-NAME>` specified, the default VRF is implied. Specify `all-vrfs` to show information for all VRFs.

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing IGMP static-group information:

```
switch# show ip igmp static-groups

IGMP Static Group Address Information

VRF Name    default
Interface Name   Group Address
---------------- -----------------
vlan10            238.1.1.1
```

Showing IGMP statics-group information for all VRFs:

```
switch# show ip igmp static-groups all-vrfs

IGMP Static Group Address Information
VRF Name   :test
Interface Name   Group Address
---------------- -----------------
vlan20            239.1.1.1
VRF Name   :default
Interface Name   Group Address
---------------- -----------------
vlan10            238.1.1.1
```

Showing IGMP static-group information for VRF test:

```
switch# show ip igmp static-groups vrf test

IGMP Static Group Address Information

VRF Name   :test
Interface Name   Group Address
---------------- -----------------
vlan20            239.1.1.1
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip igmp statistics

`show ip igmp statistics [vrf <VRF-NAME> | all-vrfs] [vsx-peer]`

Description

Shows IGMP statistics, including groups joined, or shows statistics by VRF.

Parameters

`vrf <VRF-NAME> | all-vrfs`

Optional. Used to show information by VRF. Specify the VRF by VRF name. With no *<VRF-NAME>* specified, the default VRF is implied. Specify `all-vrfs` to show information for all VRFs.

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing IGMP statistics:

```
switch# show ip igmp statistics
IGMP statistics

VRF Name       : default

Number of Include Groups       :   1
Number of Exclude Groups       :   0
Number of Static Groups        :   0
Total Multicast Groups Joined  :   1
```

Showing IGMP statistics for all VRFs:

```
switch# show ip igmp statistics all-vrfs
IGMP statistics
VRF Name       : test

Number of Include Groups       :   2
Number of Exclude Groups       :   0
Number of Static Groups        :   0
Total Multicast Groups Joined  :   2
VRF Name       : default

Number of Include Groups       :   1
Number of Exclude Groups       :   0
Number of Static Groups        :   0
Total Multicast Groups Joined  :   1
```

Showing IGMP statistics for VRF test:

```
switch# show ip igmp statistics vrf test
IGMP statistics

VRF Name       : test

Number of Include Groups       :   2
Number of Exclude Groups       :   0
Number of Static Groups        :   0
Total Multicast Groups Joined  :   2
```

Command History

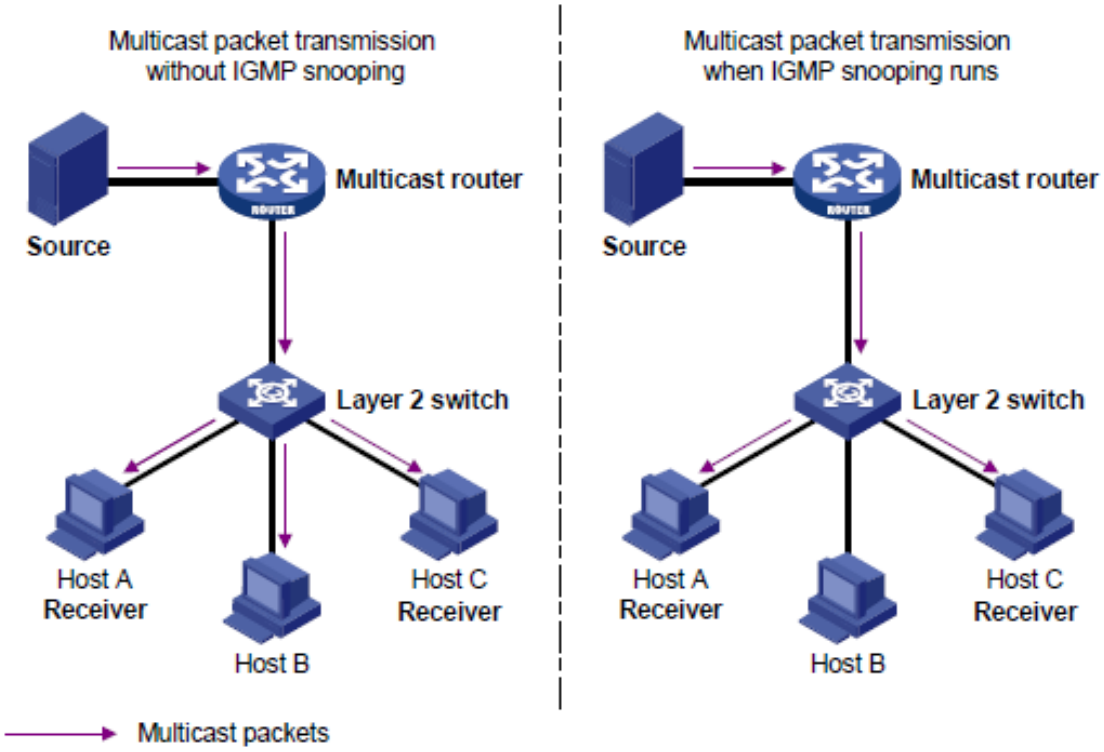
Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

IGMP snooping runs on a Layer 2 device as a multicast constraining mechanism to improve multicast forwarding efficiency. It creates Layer 2 multicast forwarding entries from IGMP packets that are exchanged between the hosts and the router.

When IGMP snooping is not enabled, the snooping switch floods multicast packets to all hosts in a VLAN. IGMP L2 snooping switch provides the benefit of conserving bandwidth on those segments of the network where no node has expressed interest in receiving packets addressed to the group address. When IGMP snooping is enabled, the L2 snooping switch forwards multicast packets of known multicast groups to only the receivers.



IGMP snooping defaults, protocols, and supported configuration

IGMP snooping default configuration:

- IGMP snooping is disabled by default.
- Version 3 is used by default.

IGMP snooping related protocols:

- IGMPv2 (RFC 2236)
- IGMPv3 (RFC 2276)

- Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches (RFC 4541)

Static groups:

You can configure a maximum of 32 IGMP snooping static groups.

How IGMP snooping works

IGMP message types include: Query, Report (Join), and Leave Group. An IGMP snooping enabled Layer 2 device performs differently depending on the message type.

Query

A message sent from the querier (multicast router or switch) asking for a response from each host belonging to the multicast group. If a multicast router supporting IGMP is not present, then the switch must assume this function in order to elicit group membership information from the hosts on the network.

The IGMP querier periodically sends IGMP general queries to all hosts and routers on the local subnet to check for the existence of multicast group members. After receiving an IGMP general query, the snooping switch forwards the query to all ports in the VLAN except the receiving port.

Report (Join)

A message sent by a host to the querier to indicate that the host wants to be or is a member of a given group indicated in the report message.

A host sends an IGMP report to the IGMP querier for the following purposes:

- Responds to queries if the host is a multicast group member.
- Applies for a multicast group membership.

After receiving an IGMP report from a host, the snooping switch forwards the report through all the router ports in the VLAN. It also looks up the forwarding table for a matching entry as follows:

- If no match is found, the snooping switch creates a forwarding entry with the receiving port as an outgoing interface. It also starts group membership expiry timer for the port to track the amount of time that must pass before a multicast router decides there are no more members of a group on a network.
- If a match is found but the matching forwarding entry does not contain the receiving port, the snooping switch adds the receiving port to the outgoing interface list. It also starts group membership expiry timer for the port.
- If a match is found and the matching forwarding entry contains the receiving port, the snooping switch restarts the group membership expiry timer for the port.

Leave Group

A message sent by a host to the querier to indicate that the host has ceased to be a member of a specific multicast group.

An IGMPv1 receiver host does not send any leave messages when it leaves a multicast group. The snooping switch cannot immediately update the status of the port that connects to the receiver host. The snooping switch does not remove the port from the outgoing interface list in the associated forwarding entry until the group membership timer expires.

An IGMPv2 or IGMPv3 host sends an IGMP leave message when it leaves a multicast group. Upon receiving leave message, the switch forwards the IGMP leave message to all router ports in the VLAN . IGMP querier

then sends an IGMP group-specific query to the multicast group to identify whether the group has active receivers attached to the receiving port.

After receiving the IGMP group-specific query, the switch forwards the query through all router ports and member ports of the group in the VLAN. Then, it waits for the responding IGMP report message from the directly connected hosts. If the port does not receive an IGMP report message when the group membership timer expires, the snooping switch removes the port from the forwarding entry for the multicast group.

IGMP snooping configuration task list

- Enabling or Disabling IGMP Snooping
- Specifying the IGMP snooping version
- Configuring IGMP snooping static groups
- Enabling Drop-Unknown Filters
- Configuring IGMP snooping fast learn ports globally
- Configuring IGMP snooping per port filtering
- Disabling IGMP Snooping
- Viewing IGMP snooping information

Enabling or disabling IGMP snooping

IGMP snooping is disabled by default. The default behavior is to flood multicast traffic in the VLAN. Use the following to enable IGMP snooping.

Prerequisites

You must be in the VLAN configuration context, as indicated by the `switch(config-vlan)#` prompt.

The VLAN has to be configured and up.

Procedure

Enable IGMP snooping on a VLAN using the following command.

```
ip igmp snooping {enable | disable}
```

For example, the following command enables IGMP snooping on VLAN 2:

```
switch(config)# vlan 2
switch(config-vlan)# ip igmp snooping enable
```

Use the `no` command to disable IGMP snooping on a VLAN.

Specifying the IGMP snooping version

The IGMP snooping version can be either 2 (IGMPv2) or 3 (IGMPv3). The default is 3. IGMPv2 supports filtering based on groups. IGMPv3 is more advanced and includes filtering based on source and groups.

Prerequisites

You must be in the VLAN configuration context, as indicated by the `switch(config-vlan)#` prompt.

Procedure

Specify the IGMP snooping version for a VLAN using the following command.

`ip igmp snooping version <VERSION>`

For example, the following command sets the IGMP snooping version to 2 on VLAN 2:

```
switch(config)# vlan 2
switch(config-vlan)# ip igmp snooping version 2
```

Configuring IGMP snooping static groups

Configure IGMP snooping static groups.

Prerequisites

You must be in the VLAN configuration context, as indicated by the `switch(config-vlan)#` prompt.

Procedure

Configure an IGMP snooping static group on a VLAN using the following command.

`ip igmp snooping static-group <MULTICAST-IP-ADDRESS>`

For example, the following command configures the IGMP snooping static multicast group as 239.1.1.1 on VLAN 2:

```
switch(config)# vlan 2
switch(config-vlan)# ip igmp snooping static-group 239.1.1.1
```

The `no` form of the command removes the IGMP snooping static group.

Enabling drop-unknown filters

While IGMP snooping is enabled, the traffic will be forwarded only to joined ports. Configuring drop unknown filters, ensures that packets are not forwarded to ports where a request for the traffic stream has not been received.

This could either be a filter across all VLANs (`vlan-shared`) or per VLAN (`vlan-exclusive`). The default is `vlan-shared`.

Prerequisites

You must be in the configuration context, as indicated by the `switch(config)#` prompt.

Procedure

Globally enable dropping multicast data using the following command.

`ip igmp snooping drop-unknown {vlan-shared | vlan-exclusive}`

For example, the following command configures a shared VLAN filter on the switch:

```
switch(config)# ip igmp snooping drop-unknown vlan-shared
```

Configuring IGMP snooping fast learn ports globally

Configuring fast learn on a port enables faster response to topology change notifications. When spanning tree changes the port state from blocked to forwarding, the device acting as querier will immediately send a

general query on the fast learn enabled port. Then the device acting as a non-querier will replay the joins. This will help in faster convergence of multicast flows.

Prerequisites

You must be in the configuration context, as indicated by the `switch(config)#` prompt.

Procedure

Configure one or more ports as IGMP snooping fast learn ports using the following command.

`ip igmp snooping fastlearn <PORT-LIST>`

For example, the following command configures ports 1/1/1-1/1/3 as fast learn ports:

```
switch(config)# ip igmp snooping fastlearn 1/1/1-1/1/3
```

Configuring IGMP snooping per port filtering

Configure IGMP snooping traffic handling by specifying auto, blocked, or forward for a port, list of ports or range of ports. In auto mode traffic flow is controlled by the IGMP joins/leaves. Auto mode is the default. In blocked mode, joins and traffic are always blocked on this port. In forward mode traffic is always forwarded on this port, irrespective of joins.

Prerequisites

You must be in the VLAN configuration context, as indicated by the `switch(config-vlan)#` prompt.

Procedure

Configure IGMP snooping traffic handling for ports on a VLAN using the following commands.

- Configure the specified ports in auto mode using the following command: `ip igmp snooping auto <PORT-LIST>`.
- Configure the specified ports in blocked mode using the following command: `ip igmp snooping blocked <PORT-LIST>`.
- Configure the specified ports in forward mode using the following command: `ip igmp snooping forward <PORT-LIST>`.

For example, the following command configures ports 1/1/1, 1/1/2, and 1/1/3 in auto mode for VLAN 2:

```
switch(config)# vlan 2
switch(config-vlan)# ip igmp snooping auto 1/1/1,1/1/2-1/1/3
```

Disabling IGMP snooping

Prerequisites

You must be in the VLAN configuration context, as indicated by the `switch(config-vlan)#` prompt.

Procedure

Disable IGMP snooping on a VLAN using the following command.

`no ip igmp snooping`

For example, the following command removes IGMP snooping on VLAN 2:

```
switch(config)# vlan 2
switch(config-vlan)# no ip igmp snooping
```

Viewing IGMP snooping information

Prerequisites

Use these show commands from the Operator (>) or Manager (#) context.

Procedure

To view IGMP snooping information, use the following commands.

- To view IGMP snooping configuration details and status, use: `show ip igmp snooping`.
- To view IGMP snooping query packet Tx, Rx, and Error packet counter details, use: `show ip igmp snooping counters`.
- To view IGMP snooping group information, use: `show ip igmp snooping groups`.
- To view IGMP snooping protocol information and the number of groups joined, use: `show ip igmp snooping statistics`.
- To view IGMP snooping query packet Tx, Rx, and Error packet counters for the specified VLAN, use: `show ip igmp snooping vlan counters`.
- To view IGMP snooping statistics details for the specified VLAN including the number of different groups joined for the VLAN, use: `show ip igmp snooping vlan statistics`.
- To view IGMP snooping group information for the specified VLAN, use: `show ip igmp snooping vlan`.
- To view IGMP snooping group details for the specified VLAN including information about all IGMP snooping groups or sources learned on a particular port, use: `show ip igmp snooping vlan group port`.
- To view IGMP snooping static groups details for the specified VLAN, use: `show ip igmp snooping static-groups`.

IGMP snooping commands

ip igmp snooping

`ip igmp snooping {enable | disable}`

Description

Enables or disables IGMP snooping on the VLAN. By default, IGMP snooping is disabled.

Parameters

`{enable | disable}`

Specifies enabling or disabling IGMP snooping on the VLAN. Default: disable.

Examples

Enable IGMP snooping on a VLAN:

```
switch(config)# vlan 2
switch(config-vlan)# ip igmp snooping enable
```

Disable IGMP snooping on a VLAN:

```
switch(config)# vlan 2
switch(config-vlan)# ip igmp snooping disable
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-vlan-*<VLAN-ID>*	Administrators or local user group members with execution rights for this command.

ip igmp snooping apply access-list

```
ip igmp snooping apply access-list <ACL-NAME>
no ip igmp snooping apply access-list <ACL-NAME>
```

Description

Configures the ACL on a particular interface to filter the IGMP join or leave packets based on rules set in the particular ACL name.

The no form of this command unconfigures the rules set for the ACL.

This configuration will override the ACL associated with IGMP snooping on the corresponding L2 VLAN.

Parameters

access-list

Associates an ACL with the IGMP.

<ACL-NAME>

Specifies the name of the ACL.

Usage

Existing classifier commands are used to configure the ACL. In case an IGMPv3 packet with multiple group addresses is received, it will only process the permitted group addresses based on the ACL rule set, and any existing joins will time out. If there is no match or if there is a deny rule match, the packet is dropped.

If the access list is configured for both L2 VLAN and L3 VLAN, the L3 VLAN configuration will be applied.

Examples

Configuring the ACL to filter IGMP packets based on rules set in access list mygroup:

```
switch(config)# access-list ip mygroup
switch(config-acl-ip)# permit igmp any 239.1.1.1
switch(config-acl-ip)# exit
switch(config)# interface vlan 2
switch(config-vlan)# ip igmp snooping apply access-list mygroup
```

Configuring the ACL to remove the rules set in access list `mygroup`:

```
switch(config-vlan)# no ip igmp snooping apply access-list mygroup
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-vlan-*<VLAN-ID>*	Administrators or local user group members with execution rights for this command.

ip igmp snooping auto vlan

```
ip igmp snooping [auto vlan <VLAN-LIST>]
no ip igmp snooping [auto vlan <VLAN-LIST>]
```

Description

Configures the specified ports in auto mode. In auto mode traffic flow is controlled by the IGMP joins/leaves. Auto mode is the default.

The `no` form of this command removes auto mode ports for the VLAN.

Parameters

<VLAN-LIST>

Required: Specifies a list of VLANs on which the port should be configured as an auto port. Specifies the number of a single VLAN or a series of numbers for a range of VLANs, separated by commas (10, 20, 30, 40), dashes (10-40), or both (10-40,60).

Example

On the 6400 Switch Series, interface identification differs.

Configure auto ports for VLAN on the interface:

```
switch# configure terminal
switch(config)# int 1/1/1
switch(config-if)# no shut
switch(config-if)# no routing
switch(config-if)# vlan trunk allowed 10-20
switch(config-if)# ip igmp snooping auto vlan 10
switch(config-if)# ip igmp snooping auto vlan 10-20
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config-if`	Administrators or local user group members with execution rights for this command.

ip igmp snooping blocked

```
ip igmp snooping [blocked vlan <VLAN-LIST>]
no ip igmp snooping [blocked vlan <VLAN-LIST>]
```

Description

Configures the specified ports in blocked mode for the specified VLAN list. In blocked mode, joins and traffic are always blocked on this port.

The `no` form of this command disables blocked ports.

Parameters

<VLAN-LIST>

Required: Specifies a list of VLANs on which the port should be configured as a blocked port. Specifies the number of a single VLAN or a series of numbers for a range of VLANs, separated by commas (10, 20, 30, 40), dashes (10-40), or both (10-40,60).

Examples

On the 6400 Switch Series, interface identification differs.

Configuring blocked ports for the VLAN on the interface:

```
switch# configure terminal
switch(config)# int 1/1/1
switch(config-if)# no shut
switch(config-if)# no routing
switch(config-if)# vlan trunk allowed 10-20
switch(config-if)# ip igmp snooping blocked vlan 10
switch(config-if)# ip igmp snooping blocked vlan 10-20
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if	Administrators or local user group members with execution rights for this command.

ip igmp snooping drop-unknown

```
ip igmp snooping drop-unknown {vlan-shared | vlan-exclusive}
no ip igmp snooping drop-unknown
```

Description

Configures drop-unknown mode. While IGMP snooping is enabled, the traffic will be forwarded only to ports that made an IGMP request for the multicast. Drop unknown filters ensure that packets are not forwarded to ports that did not make a request for the traffic stream. This could either be a filter across all VLANs (`vlan-shared`) or per VLAN (`vlan-exclusive`). The default is `vlan-shared`.

The `no` form of this command disables drop unknown on the switch.

Parameters

`vlan-shared`

Enables shared VLAN filter on the switch. Default: `vlan-shared`.

`vlan-exclusive`

Enables exclusive drop unknown filter per VLAN.

Examples

Configuring shared VLAN filter on the switch:

```
switch(config)# ip igmp snooping drop-unknown vlan-shared
```

Configuring exclusive drop unknown filter per VLAN:

```
switch(config)# ip igmp snooping drop-unknown vlan-exclusive
```

Disabling drop unknown on the switch:

```
switch(config)# no ip igmp snooping drop-unknown
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config	Administrators or local user group members with execution rights for this command.

ip igmp snooping fastlearn

```
ip igmp snooping fastlearn <PORT-LIST>
no ip igmp snooping fastlearn <PORT-LIST>
```

Description

Enables the port to learn group information when receiving a topology change notification. By default, fast learn is not enabled on ports.

The `no` form of this command disables fast learn on the specified ports.

Parameters

`fastlearn <PORT-LIST>`

Specifies a list of one or more ports to be configured as fast learn ports. You can specify a single port, a comma-separated list of ports or a range of ports such as 1/1/1-1/1/3. You may also enter an L2 LAG (1-128).

Examples

On the 6400 Switch Series, interface identification differs.

Configuring fast learn ports:

```
switch(config)# ip igmp snooping fastlearn 1/1/3
switch(config)# ip igmp snooping fastlearn 1/1/1-1/1/2
switch(config)# ip igmp snooping fastlearn 1/1/5,1/1/6
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config`	Administrators or local user group members with execution rights for this command.

ip igmp snooping fastleave vlan

```
ip igmp snooping [fastleave vlan <VLAN-LIST>]
no ip igmp snooping [fastleave vlan <VLAN-LIST>]
```

Description

Enables the switch to immediately remove the IGMP client from its IGMP table and cease transmitting multicast traffic to the client.

The `no` form of this command disables fastleave on the specified ports.

Parameters

`<VLAN-LIST>`

Specifies a list of VLANs on which the port should be configured as a fastleave port. Specifies the number of a single VLAN or a series of numbers for a range of VLANs, separated by commas (10, 20, 30, 40), dashes (10-40), or both (10-40,60).

Usage

IGMP fastleave is configured for ports on a per-VLAN basis. Upon receiving a Leave Group message, the querier sends an IGMP Group-Specific Query message out of the interface to ensure that no other receivers are connected to the interface. If receivers are directly attached to the switch, it is inefficient to send the membership query as the receiver wanting to leave is the only connected host.

When a fastleave-enabled switch port is connected to a single host and receives a leave, the switch does not wait for the querier status update interval, but instead immediately removes the IGMP client from its IGMP table and ceases transmitting multicast traffic to the client. (If the switch detects multiple end nodes on the port, Fastleave does not activate regardless of whether one or more of these end nodes are IGMP clients.) This processing speeds up the overall leave process and also eliminates the CPU overhead of having to generate an IGMP Group-Specific Query message.

Examples

On the 6400 Switch Series, interface identification differs.

Configuring fastleave ports for the VLAN on the interface:

```
switch# configure terminal
switch(config)# int 1/1/1
switch(config-if)# no shut
switch(config-if)# no routing
switch(config-if)# vlan trunk allowed 10-20
switch(config-if)# ip igmp snooping fastleave vlan 10
switch(config-if)# ip igmp snooping fastleave vlan 10-20
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if	Administrators or local user group members with execution rights for this command.

ip igmp snooping forced fastleave vlan

```
ip igmp snooping [forced-fastleave vlan <VLAN-LIST>]
no ip igmp snooping [forced-fastleave vlan <VLAN-LIST>]
```

Description

Configures the specified ports in forced fastleave mode.

The no form of this command disables forced fastleave on the specified ports.

Parameters

<VLAN-LIST>

Specifies a list of VLANs on which the port should be configured as a forced fastleave port. Specifies the number of a single VLAN or a series of numbers for a range of VLANs, separated by commas (10, 20, 30, 40), dashes (10-40), or both (10-40,60).

Usage

With forced fastleave enabled, IGMP speeds up the process of blocking unnecessary multicast traffic to a switch port that is connected to multiple end nodes. When a port having multiple end nodes receives a leave group request from one end node for a given multicast group, forced fastleave activates and waits for a second to receive a join request from any other member of the same group on that port. If the port does not receive a join request for that group within the forced fastleave interval, the switch then blocks any further traffic to that group on that port.

Examples

On the 6400 Switch Series, interface identification differs.

Configuring forced-fastleave ports for VLANs on the interface:

```
switch# configure terminal
switch(config)# int 1/1/1
switch(config-if)# no shut
switch(config-if)# no routing
switch(config-if)# vlan trunk allowed 10-20
switch(config-if)# ip igmp snooping forced-fastleave vlan 10
switch(config-if)# ip igmp snooping forced-fastleave vlan 10-20
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config-if`	Administrators or local user group members with execution rights for this command.

ip igmp snooping forward vlan

`ip igmp snooping forward [vlan <VLAN-LIST>]`
`no ip igmp snooping forward [vlan <VLAN-LIST>]`

Description

Configures the specified ports in forward mode in the given VLAN list. In forward mode, traffic is always forwarded on this port, irrespective of joins.

The `no` form of this command disables forward ports.

Parameters

<VLAN-LIST>

Required: Specifies a list of VLANs on which the port should be configured as a forward port. Specifies the number of a single VLAN or a series of numbers for a range of VLANs, separated by commas (10, 20, 30, 40), dashes (10-40), or both (10-40,60).

Examples

On the 6400 Switch Series, interface identification differs.

Configuring forward ports for the VLAN on the interface:

```
switch# configure terminal
switch(config)# int 1/1/1
switch(config-if)# no shut
switch(config-if)# no routing
switch(config-if)# vlan trunk allowed 10-20
switch(config-if)# ip igmp snooping forward vlan 10
switch(config-if)# ip igmp snooping forward vlan 10-20
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if	Administrators or local user group members with execution rights for this command.

ip igmp snooping static-group

```
ip igmp snooping static-group <MULTICAST-IP-ADDRESS>
no ip igmp snooping static-group <MULTICAST-IP-ADDRESS>
```

Description

Configures an IGMP snooping static multicast group. You can configure a maximum of 32 IGMP snooping static groups.

The no form of this command disables static multicast group.

Parameters

<MULTICAST-IP-ADDRESS>

Specifies the IGMP static multicast group IP address. Format: A.B.C.D

Examples

Configuring IGMP snooping static group:

```
switch(config)# vlan 2
switch(config-vlan)# ip igmp snooping static-group 239.1.1.1
switch(config-vlan)# no ip igmp snooping static-group 239.1.1.1
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config-vlan-<VLAN-ID>`	Administrators or local user group members with execution rights for this command.

ip igmp snooping version

`ip igmp snooping version <VERSION>`

Description

Configures the IGMP snooping version on the VLAN.

Parameters

<VERSION>

Specifies the IGMP snooping version. Select 2 for IGMPv2 (RFC2236). Select 3 for IGMPv3 (RFC3376). Values: 2 or 3.

Examples

Configuring IGMP snooping version on the VLAN:

```
switch(config)# vlan 2
switch(config-vlan)# ip igmp snooping version 2
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config-vlan-<VLAN-ID>`	Administrators or local user group members with execution rights for this command.

no ip igmp snooping

`no ip igmp snooping`

Description

Disables all IGMP snooping configurations on the VLAN.

Examples

Disabling all IGMP snooping configurations on the VLAN:

```
switch(config)# vlan 2
switch(config-vlan)# no ip igmp snooping
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-vlan-*<VLAN-ID>*	Administrators or local user group members with execution rights for this command.

show ip igmp snooping

```
show ip igmp snooping [vsx-peer]
```

Description

Shows IGMP snooping configuration information and status for all VLANs.

Parameters

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing IGMP snooping configuration and status:

```
switch# show ip igmp snooping

IGMP Snooping Protocol Info

Total VLANs with IGMP enabled             : 1
IGMP Drop Unknown Multicast               : Global


VLAN ID : 1
VLAN Name : DEFAULT_VLAN_1
IGMP Snooping is not enabled

VLAN ID : 2
VLAN Name : VLAN2
IGMP Configured Version : 3
IGMP Operating Version : 3
Querier Address [this switch] : 20.1.1.1
Querier Port :
```

```
Querier UpTime :0m 21s
Querier Expiration Time :0m 2s
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip igmp snooping counters

```
show ip igmp snooping counters [vsx-peer]
```

Description

Shows IGMP snooping query packet Tx, Rx, and Error packet counter details.

Parameters

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing IGMP snooping packet counters:

```
switch# show ip igmp snooping counters
IGMP Snooping VLAN Counters

Rx Counters :

V1 All Hosts Queries                          0
V2 All Hosts Queries                          0
V3 All Hosts Queries                          3
V2 Group Specific Queries                     0
V3 Group Specific Queries                     0
Group And Source Specific Queries             0
V1 Member Reports                             0
V2 Member Reports                             0
V3 Member Reports                             2
V2 Member Leaves                              0


Tx Counters :

Flood on vlan                                 44
```

```
V2 Group Specific Queries                          0
V3 Group Specific Queries                          0

Errors:

Unknown Message Type                               0
Malformed Packets                                  0
Bad Checksum                                       0
Packet received on IGMP-disabled Interface         0
Interface Wrong Version Queries                    0
Packets dropped by ACL                             0

Port Counters:

Membership Timeout                                 0
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip igmp snooping groups

```
show ip igmp snooping groups [vsx-peer]
```

Description

Shows IGMP snooping group information.

Parameters

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing IGMP snooping groups:

```
switch# show ip igmp snooping groups
IGMP Group Address Information

VLAN ID Group Address   Expires   UpTime    Last Reporter   Type
-----------------------------------------------------------------
2       239.1.1.3       0m 4s     0m 10s    10.1.1.1        Filter
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip igmp snooping static-groups

```
show ip igmp snooping static-groups [vsx-peer]
```

Description

Shows IGMP snooping static group details.

Parameters

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing IGMP snooping static group details:

```
switch# show ip igmp snooping static-groups

IGMP Static Group Address Information

VLAN ID Group Address
------------------------
10      239.1.1.10
10      239.1.1.11
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip igmp snooping statistics

```
show ip igmp snooping statistics [vsx-peer]
```

Description

Shows IGMP snooping protocol information and the joined group statistics.

Parameters

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing IGMP snooping statistics:

```
switch# show ip igmp snooping statistics
IGMP Snooping Protocol Info

Total VLANs with IGMP enabled             : 1
IGMP Drop Unknown Multicast               : Global

IGMP Snooping Joined Groups Statistics

VLAN ID VLAN Name         Total  Static INCLUDE  EXCLUDE
------- ----------------- ------ ------ -------  -------
1       DEFAULT_VLAN_1    0      0      0        0
2       VLAN10            2      2      0        0
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip igmp snooping vlan

```
show ip igmp snooping vlan <VLAN-ID> [group [<group-ip>]
     [source <source-ip>]] [vsx-peer]
```

Description

Shows IGMP snooping protocol information for the specified VLAN. You can also specify a group and source to show group and source information.

Parameters

<VLAN-ID>

Specifies a VLAN. Range: 1-4094.

`group <group-ip>`

Specifies a group to display port and group information. Format: A.B.C.D

`source <source-ip>`

Specifies a source to display source information for the group. Format: A.B.C.D

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing IGMP snooping protocol information for VLAN 2:

```
switch# show ip igmp snooping vlan 2

IGMP Snooping Protocol Info

Total VLANs with IGMP enabled             : 1
IGMP Drop Unknown Multicast               : Global

VLAN ID : 2
VLAN Name : VLAN2
IGMP Configured Version : 3
IGMP Operating Version : 3
Querier Address : 20.1.1.1
Querier Port : 1/1/1
Querier UpTime :
Querier Expiration Time :

Active Group Address   Tracking  Vers Mode Uptime    Expires
---------------------- ---------- ---- ---- --------- ----------
239.1.1.2              Filter    3    INC  0m 27s    0m 13s
```

Showing IGMP snooping group information for group 239.1.1.2 on VLAN 2:

```
switch# show ip igmp snooping vlan 2 group 239.1.1.2

IGMP ports and group information for group 239.1.1.2

VLAN ID   : 2
VLAN Name : VLAN2

Group Address : 239.1.1.2
Last Reporter : 10.1.1.1
Group Type    : Filter

                                        V1        V2        Sources   Sources
Port      Vers Mode Uptime    Expires   Timer     Timer     Forwarded Blocked
--------- ---- ---- --------- --------- --------- --------- --------- --------
1/1/6     3    INC  0m 41s    3m 39s                        3         0

Group Address  : 239.1.1.2
Source Address : 30.1.1.1
Source Type    : Filter

Port      Mode Uptime    Expires   Configured Mode
--------- ---- --------- --------- ----------------
1/1/6     INC  0m 41s    3m 39s    Auto
```

```
Group Address  : 239.1.1.2
Source Address : 30.1.1.2
Source Type    : Filter

Port      Mode Uptime    Expires   Configured Mode
--------- ---- --------- --------- ----------------
1/1/6     INC  0m 41s    3m 39s    Auto

Group Address  : 239.1.1.2
Source Address : 30.1.1.3
Source Type    : Filter

Port      Mode Uptime    Expires   Configured Mode
--------- ---- --------- --------- ----------------
1/1/6     INC  0m 41s    3m 39s    Auto
```

Showing IGMP snooping group information for group 239.1.1.2 on VLAN 2 and source 30.1.1.1:

```
switch# show ip igmp snooping vlan 2 group 239.1.1.2 source 30.1.1.1

VLAN ID   : 2
VLAN Name : VLAN2
Group Address  : 239.1.1.2
Source Address : 30.1.1.1
Source Type    : Filter

Port      Mode Uptime    Expires   Configured Mode
--------- ---- --------- --------- ----------------
1/1/6     INC  0m 41s    3m 39s    Auto
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip igmp snooping vlan counters

`show ip igmp snooping vlan <VLAN-ID> counters [vsx-peer]`

Description

Shows IGMP snooping query packet Tx, Rx, Error packet counters for the specified VLAN.

Parameters

<VLAN-ID>

Specifies a VLAN. Range: 1-4094.

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing IGMP snooping counters for VLAN 2:

```
Switch# show ip igmp snooping vlan 2 counters
IGMP Snooping VLAN Counters

VLAN ID   :   2
VLAN Name : VLAN2

Rx Counters :

V1 All Hosts Queries                          0
V2 All Hosts Queries                          0
V3 All Hosts Queries                          3
V2 Group Specific Queries                     0
V3 Group Specific Queries                     0
Group And Source Specific Queries             0
V1 Member Reports                             0
V2 Member Reports                             0
V3 Member Reports                             2
V2 Member Leaves                              0

Tx Counters :

Flood on vlan                                 71
V2 Group Specific Queries                     0
V3 Group Specific Queries                     0

Errors:

Unknown Message Type                          0
Malformed Packets                             0
Bad Checksum                                  0
Packet received on IGMP-disabled Interface    0
Interface Wrong Version Queries               0
Packet dropped by ACL                         0

Port Counters:

Membership Timeout                            0
Switch#
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip igmp snooping vlan group port

`show ip igmp snooping vlan <VLAN-ID> group port <PORT-ID> [vsx-peer]`

Description

Shows IGMP snooping group details for the specified VLAN. It shows information about all IGMP snooping groups or sources learned on a particular port.

Parameters

<VLAN-ID>

Specifies a VLAN. Range: 1-4094.

<PORT-ID>

Specifies a port of a VLAN to display information about all IGMPv3 snooping groups/sources learn on a particular port.

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing IGMP snooping group details for VLAN 2 port 1/1/6:

```
switch# show ip igmp snooping vlan 2 group port 1/1/6

VLAN ID   : 2
VLAN Name : VLAN2

Group Address : 239.1.1.1
Last Reporter : 10.1.1.1
Group Type    : Filter

                                        V1        V2        Sources   Sources
Port      Vers Mode Uptime    Expires   Timer     Timer     Forwarded Blocked
--------- ---- ---- --------- --------- --------- --------- --------- --------
1/1/6     2    EXC  0m 21s    1m 12s              2m 48s    0         0


VLAN ID   : 2
VLAN Name : VLAN2

Group Address : 239.1.1.2
Last Reporter : 10.1.1.1
Group Type    : Filter

                                        V1        V2        Sources   Sources
Port      Vers Mode Uptime    Expires   Timer     Timer     Forwarded Blocked
--------- ---- ---- --------- --------- --------- --------- --------- --------
1/1/6     2    EXC  0m 21s    1m 32s              2m 48s    0         0
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip igmp snooping vlan statistics

```
show ip igmp snooping vlan <VLAN-ID> statistics [vsx-peer]
```

Description

Shows IGMP snooping statistics details for the specified VLAN. It also shows information on the different groups joined in the VLAN.

Parameters

<VLAN-ID>

Specifies a VLAN. Range: 1-4094.

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing IGMP snooping statistics for VLAN 2:

```
switch# show ip igmp snooping vlan 2 statistics
IGMP Snooping statistics

VLAN ID   :   2
VLAN Name : VLAN2

Number of Include Groups       :   1
Number of Exclude Groups       :   0
Number of Static Groups        :   1
Total Multicast Groups Joined  :   2
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6200 6300 6400 8320 8325 8360 8400	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

MLD snooping functionality

Multicast Listener Discovery (MLD) snooping optimizes multicast traffic across the network to prevent traffic from flooding ports on a VLAN.

- For example, one of the features of MLD snooping lets you configure the network so that traffic is forwarded only to ports that initiate an MLD request for multicast.
- Another feature of MLD lets you enable a setting so that packets that do not match the configured version are dropped.
- You can also block ports from traffic.

MLD snooping global configuration commands

ipv6 mld snooping

```
ipv6 mld snooping [drop-unknown [vlan-shared | vlan-exclusive]]
[no] ipv6 mld snooping
```

Description

This command configures the drop unknown mode. While MLD snooping is enabled, the traffic will be forwarded only to ports that initiate an MLD request for multicast. Drop unknown mode can be a filter across all VLANs (vlan-shared) or per VLAN (exclusive-vlan). The default configuration is vlan-shared.

The `no` form of this command disables drop unknown mode on the switch.

Parameters

`vlan-shared`

Required: Enable shared VLAN filter on the switch.

`vlan-exclusive`

Required: Enable exclusive drop unknown filter per VLAN.

Example

```
switch(config)# ipv6 mld snooping drop-unknown vlan-shared
switch(config)# ipv6 mld snooping drop-unknown vlan-exclusive
switch(config)# no ipv6 mld snooping drop-unknown
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config`	Administrators or local user group members with execution rights for this command.

MLD snooping VLAN configuration commands

ipv6 mld snooping

```
ipv6 mld snooping {enable | disable}
```

Description

This command enables or disables MLD snooping on the VLAN.

The `no` form of this command disables all MLD snooping configurations on the VLAN.

Parameters

`enable`

Required: Enable MLD snooping on the VLAN.

`disable`

Required: Disable MLD snooping on the VLAN.

Example

Enable MLD snooping on VLAN 2:

```
switch(config)# vlan 2
switch(config-vlan)# ipv6 mld snooping enable
switch(config-vlan)# ipv6 mld snooping disable
```

Remove all MLD snooping configurations on VLAN 2:

```
switch(config)# vlan 2
switch(config-vlan)# no ipv6 mld snooping
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config-vlan-<VLAN-ID>`	Administrators or local user group members with execution rights for this command.

ipv6 mld snooping apply access-list

```
ipv6 mld snooping apply access-list <ACL-NAME>
no ipv6 mld snooping apply access-list <ACL-NAME>
```

Description

Configures the ACL on a particular interface to filter the MLD join or leave packets based on rules set in the particular ACL name.

The `no` form of this command disables the rules set for the ACL.

This configuration will override the ACL associated with IGMP snooping on the corresponding L2 VLAN.

Parameters

`access-list`

Associates an ACL with the IGMP.

`<ACL-NAME>`

Specifies the name of the ACL.

Usage

Existing classifier commands are used to configure the ACL. In case an MLDv2 packet with multiple group addresses is received, it will only process the permitted group addresses based on the ACL rule set, and any existing joins will time out. If there is no match or if there is a deny rule match, the packet is dropped.

If the access list is configured for both L2 VLAN and L3 VLAN, the L3 VLAN configuration will be applied.

Examples

Configuring the ACL to filter MLD packets based on rules set in access list `mygroup`:

```
switch(config)# access-list ipv6 mygroup
switch(config-acl-ip)# permit icmpv6 any ff55::1
switch(config-acl-ip)# exit
switch(config)# interface vlan 2
switch(config-vlan)# ipv6 mld snooping apply access-list mygroup
```

Configuring the ACL to remove the rules set in access list `mygroup`:

```
switch(config-vlan)# no ipv6 mld snooping apply access-list mygroup
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config-vlan`	Administrators or local user group members with execution rights for this command.

ipv6 mld snooping auto vlan

```
ipv6 mld snooping [auto vlan <VLAN-LIST>]
no ipv6 mld snooping [auto vlan <VLAN-LIST>]
```

Description

This command configures the given ports in auto mode, which is the default port mode.

The `no` form of this command disables auto ports.

Parameters

<VLAN-LIST>

Required: Specifies a list of VLANs on which the port should be configured as an auto port. Specifies the number of a single VLAN or a series of numbers for a range of VLANs, separated by commas (10, 20, 30, 40), dashes (10-40), or both (10-40,60).

Example

On the 6400 Switch Series, interface identification differs.

Configuring auto ports for VLANs on the interface:

```
switch# configure terminal
switch(config)# int 1/1/1
switch(config-vlan)# no shut
switch(config-vlan)# no routing
switch(config-vlan)# ipv6 mld snooping auto vlan 10
switch(config-vlan)# ipv6 mld snooping auto vlan 10-20
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config-vlan`	Administrators or local user group members with execution rights for this command.

ipv6 mld snooping blocked vlan

```
ipv6 mld snooping [blocked vlan <VLAN-LIST>]
no ipv6 mld snooping [blocked vlan <VLAN-LIST>]
```

Description

By default ports are configured in auto mode. This command configures the given ports in blocked mode.

The `no` form of this command removes blocked ports.

Parameters

<VLAN-LIST>

Required: Specifies a list of VLANs on which the port should be configured as an auto port. Specifies the number of a single VLAN or a series of numbers for a range of VLANs, separated by commas (10, 20, 30, 40), dashes (10-40), or both (10-40,60).

Example

On the 6400 Switch Series, interface identification differs.

Configuring blocked ports for the VLANs on the interface:

```
switch# configure terminal
switch(config)# int 1/1/1
switch(config-vlan)# no shut
switch(config-vlan)# no routing
switch(config-vlan)# ipv6 mld snooping blocked vlan 10
switch(config-vlan)# ipv6 mld snooping blocked vlan 10-20
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-vlan	Administrators or local user group members with execution rights for this command.

ipv6 mld snooping fastlearn

`ipv6 mld snooping fastlearn <port-list>`

Description

This command enables the port to learn group information on receiving topology change notification.

The `no` form of this command disables fastlearn on the ports.

Parameters

`port-list`

Required: 1/1/1-1/1/2, ports to be configured as fastlearn ports.

Example

On the 6400 Switch Series, interface identification differs.

```
switch(config)# ipv6 mld snooping fastlearn 1/1/3
switch(config)# ipv6 mld snooping fastlearn 1/1/1-1/1/2
switch(config)# ipv6 mld snooping fastlearn 1/1/5,1/1/6
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config`	Administrators or local user group members with execution rights for this command.

ipv6 mld snooping fastleave vlan

```
ipv6 mld snooping [fastleave vlan <VLAN-LIST>]
no ipv6 mld snooping [fastleave vlan <VLAN-LIST>]
```

Description

Configures the specified ports as fastleave ports. Enables the switch to immediately remove an interface from the bridge table upon receiving the leave group message.

The `no` form of this command disables fastleave configuration on the ports.

Parameters

<VLAN-LIST>

Required: Specifies a list of VLANs on which the port should be configured as an auto port. Specifies the number of a single VLAN or a series of numbers for a range of VLANs, separated by commas (10, 20, 30, 40), dashes (10-40), or both (10-40,60).

Usage

MLD fastleave is configured for ports on a per-VLAN basis. By default, the querier sends a MLD Group-Specific Query message out of the interface, upon which the leave group message is received to ensure that no other receivers are connected to the interface. If receivers are directly attached to the switch, it is inefficient to send the membership query as the receiver wanting to leave is the only connected host. Fastleave processing eliminates the MLD Group-Specific Query message. Thus, it allows the switch to immediately remove an interface from the bridge table upon receiving the leave Group message. This processing speeds up the overall leave process and also eliminates the CPU overhead of having to generate an MLD Group-Specific Query message.

Example

On the 6400 Switch Series, interface identification differs.

Configuring fastleave ports for the VLAN:

```
switch# configure terminal
switch(config)# int 1/1/1
switch(config-vlan)# no shut
switch(config-vlan)# no routing
switch(config-vlan)# ipv6 mld snooping fastleave vlan 10
switch(config-vlan)# ipv6 mld snooping fastleave vlan 10-20
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config-vlan`	Administrators or local user group members with execution rights for this command.

ipv6 mld snooping forced fastleave vlan

```
ipv6 mld snooping [forced-fastleave <VLAN-LIST>]
no ipv6 mld snooping [forced-fastleave <VLAN-LIST>]
```

Description

Configures the given ports in forced fastleave mode.

The `no` form of this command disables forced fastleave configuration on the ports.

Parameters

<VLAN-LIST>

Required: Specifies a list of VLANs on which the port should be configured as an auto port. Specifies the number of a single VLAN or a series of numbers for a range of VLANs, separated by commas (10, 20, 30, 40), dashes (10-40), or both (10-40,60).

Usage

With forced fastleave enabled, MLD speeds up the process of blocking unnecessary multicast traffic to a switch port that is connected to multiple end nodes. When a port having multiple end nodes receives a leave group request from one end node for a given multicast group, forced fastleave activates and waits a small amount of time to receive a join request from any other member of the same group on that port. If the port does not receive a join request for that group within the forced fastleave interval, the switch then blocks any further traffic to that group on that port.

Example

On the 6400 Switch Series, interface identification differs.

Configuring forced-fastleave ports for the VLAN:

```
switch# configure terminal
switch(config)# int 1/1/1
switch(config-vlan)# no shut
switch(config-vlan)# no routing
switch(config-vlan)# ipv6 mld snooping forced-fastleave vlan 10
switch(config-vlan)# ipv6 mld snooping forced-fastleave vlan 10-20
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-vlan	Administrators or local user group members with execution rights for this command.

ipv6 mld snooping forward vlan

```
ipv6 mld snooping [forward vlan <VLAN-LIST>]
no ipv6 mld snooping [forward vlan <VLAN-LIST>]
```

Description

By default ports are configured in auto mode. This command configures the given ports in forward mode.

The no form of this command disables forward ports.

Parameters

<VLAN-LIST>

Required: Specifies a list of VLANs on which the port should be configured as an auto port. Specifies the number of a single VLAN or a series of numbers for a range of VLANs, separated by commas (10, 20, 30, 40), dashes (10-40), or both (10-40,60).

Example

On the 6400 Switch Series, interface identification differs.

Configuring forward ports for VLANs on the interface:

```
switch# configureterminal
switch(config)# int 1/1/1
switch(config-vlan)# no shut
switch(config-vlan)# no routing
switch(config-vlan)# ipv6 mld snooping forward vlan 10
switch(config-vlan)# ipv6 mld snooping forward vlan 10-20
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-vlan	Administrators or local user group members with execution rights for this command.

ipv6 mld snooping version

```
ipv6 mld snooping [version <ver>]
```

Description

This command configures the MLD snooping version on the VLAN. MLD version 2 is the default.

Parameters

`ver`

Required: 1-2, MLD snooping version.

Example

```
switch(config)# vlan 2
switch(config-vlan)# ipv6 mld snooping version 2
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config-vlan-<VLAN-ID>`	Administrators or local user group members with execution rights for this command.

ipv6 mld snooping static-group

`ipv6 mld snooping [static-group <X:X::X:X>]`

Description

This command configures static multicast group.

The `no` form of this command disables static multicast group.

Parameters

`static-group`

Required: `<X:X::X:X>`, MLD static multicast group.

Example

```
switch(config)# vlan 2
switch(config-vlan)# ipv6 mld snooping static-group ff12::c
switch(config-vlan)# no ipv6 mld snooping static-group ff12::c
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-vlan-<*VLAN-ID*>	Administrators or local user group members with execution rights for this command.

MLD snooping show commands

show ipv6 mld snooping

```
show ipv6 mld snooping
```

Description

This command shows MLD snooping configuration details for all VLANs.

Example

```
switch# show ipv6 mld snooping

MLD Snooping Protocol Info

Total VLANs with MLD enabled             : 1
Current count of multicast groups joined : 0

MLD Drop Unknown Multicast               : Global


VLAN ID                                  : 1
VLAN Name                                : DEFAULT_VLAN_1
MLD Snooping is not enabled

VLAN ID                                  : 2
VLAN Name                                : VLAN2
MLD Configured Version                   : 2
MLD Operating Version                    : 2
Querier Address [this switch]            : fe80::218:71ff:fec4:2f00
Querier Port                             :
Querier UpTime                           :0m 21s
Querier Expiration Time                  :0m 2s
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 mld snooping counters

```
show ipv6 mld snooping [counters]
```

Description

This command shows MLD snooping query packet Tx, Rx, and Error packet counter details.

Parameters

`counters`

Optional, show MLD snooping counters.

Example

```
switch# show ipv6 mld snooping counters
MLD Snooping VLAN Counters

Rx Counters :

V1 All Hosts Queries                            0
V2 All Hosts Queries                            0
V2 Group Specific Queries                       0
Group And Source Specific Queries               0
V1 Member Reports                               0
V2 Member Reports                               0
V1 Member Leaves                                0


Tx Counters :

Flood on vlan                                   44
V1 Group Specific Queries                       0
V2 Group Specific Queries                       0

Errors:

Unknown Message Type                            0
Malformed Packets                               0
Bad Checksum                                    0
Packet received on MLD-disabled Interface       0
Interface Wrong Version Queries                 0
Packets dropped by ACL                          0

Port Counters:

Membership Timeout                              0
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 mld snooping groups

```
show ipv6 mld snooping [groups]
```

Description

This command shows MLD snooping group details for the specified VLAN.

Parameters

`groups`

Optional, show MLD snooping groups information.

Example

```
switch# show ipv6 mld snooping groups

MLD Group Address Information

VLAN ID Group Address     Expires   UpTime    Last Reporter                  Type
------- ----------------- --------- --------- ------------------------------ ----
10      ff12::c           3m 54s    0m 26s    2001::1                        Filter
10      ff12::d           4m 17s    0m 3s     2001::1
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 mld snooping statistics

```
show ipv6 mld snooping [statistics]
```

Description

This command shows MLD snooping statistics information.

Parameters

`statistics`

Optional, show MLD snooping statistics.

Example

```
switch# show ipv6 mld snooping statistics
MLD Snooping Protocol Info
```

```
Total VLANs with MLD enabled             : 1
Current count of multicast groups joined : 2

MLD Drop Unknown Multicast               : Global

MLD Snooping Joined Groups Statistics

VLAN ID VLAN Name        Total  Static INCLUDE  EXCLUDE
------- ---------------- ------ ------ -------  -------
1       DEFAULT_VLAN_1   0      0      0        0
2       VLAN2            2      2      0        0
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 mld snooping vlan counters

```
show ipv6 mld snooping [vlan <vlan-id> [counters]]
```

Description

This command shows MLD snooping protocol information and number of different groups joined for the VLAN.

Parameters

`vlan-id`

Required, 1-4094, shows MLD snooping information.

`counters`

Optional, shows MLD query packet Tx, Rx, Error packet counters on a specified VLAN.

Example

```
switch# show ipv6 mld snooping vlan 2 counters
MLD Snooping VLAN Counters

VLAN ID   :   2
VLAN Name :   VLAN2

Rx Counters :

V1 All Hosts Queries                          0
V2 All Hosts Queries                          0
V1 Group Specific Queries                     0
V2 Group Specific Queries                     0
```

```
Group And Source Specific Queries                0
V1 Member Reports                                0
V2 Member Reports                                0
V1 Member Leaves                                 0

Tx Counters :

Flood on vlan                                    71
V1 Group Specific Queries                        0
V2 Group Specific Queries                        0

Errors:

Unknown Message Type                             0
Malformed Packets                                0
Bad Checksum                                     0
Packet received on MLD-disabled Interface        0
Interface Wrong Version Queries                  0
Packets dropped by ACL                           0

Port Counters:

Membership Timeout                               0
switch#
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 mld snooping vlan group port

```
show ipv6 mld snooping [vlan <vlan-id> [group [port <port_id>]]
```

Description

This command shows MLD snooping details for the specified VLAN, including the number of different groups joined for the VLAN.

Parameters

`port-id`

Required: <PORT>, shows MLD protocol information for the specified port of a VLAN.

Example

```
switch# show ipv mld snooping vlan 2 group port 1/1/1
```

```
VLAN ID   : 2
VLAN Name : VLAN2

Group Address : ff05::2:1
Last Reporter : fe80::1
Group Type    : Filter

                                        V1        Sources   Sources
Port      Vers Mode Uptime    Expires   Timer     Forwarded Blocked
--------- ---- ---- --------- --------- --------- --------- --------
1/1/1     2    INC  1m 46s    2m 34s              3         0

Group Address  : ff05::2:1
Source Address : 3000::1
Source Type    : Filter

Port      Mode Uptime    Expires   Configured Mode
--------- ---- --------- --------- ----------------
1/1/1     INC  1m 46s    2m 34s    Auto

Group Address  : ff05::2:1
Source Address : 3000::2
Source Type    : Filter

Port      Mode Uptime    Expires   Configured Mode
--------- ---- --------- --------- ----------------
1/1/1     INC  1m 46s    2m 34s    Auto

Group Address  : ff05::2:1
Source Address : 3000::3
Source Type    : Filter

Port      Mode Uptime    Expires   Configured Mode
--------- ---- --------- --------- ----------------
1/1/1     INC  1m 46s    2m 34s    Auto
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 mld snooping vlan group source

`show ipv6 mld snooping [vlan <vlan-id> [group [<group-ip>] [source <source-ip>]]]`

Description

This command shows MLD snooping details for the specified VLAN, including the number of different groups joined for the VLAN.

Parameters

`vlan-id`

Required: 1-4094, shows MLD protocol information for the specified VLAN.

`group-ip`

Optional: X:X::X:X, MLD source information for the specified group.

`source-ip`

Optional: X:X::X:X, MLD source information for the specified group.

Example

```
switch# show ipv6 mld snooping vlan 2

MLD Snooping Protocol Info

Total VLANs with MLD enabled             : 2
Current count of multicast groups joined : 0

MLD Drop Unknown Multicast               : Global

VLAN ID                                  : 2
VLAN Name                                : VLAN2
MLD Configured Version                   : 2
MLD Operating Version                    : 2
Querier Address [this switch]            : fe80::218:71ff:fec4:2f00
Querier Port                             :
Querier UpTime                           :0m 21s
Querier Expiration Time                  :0m 2s

Active Group Address                          Tracking Vers Mode  Uptime    Expires
--------------------------------------------- -------- ---- ----- --------- ---------
ff05::2:1                                     Filter    2    EXC  0m 17s    4m 3s


switch# show ipv6 mld snooping vlan 2 group

MLD ports and group information for group ff05::2:1

VLAN ID                                  : 2
VLAN Name                                : VLAN2

Group Address                            : ff05::2:1
Last Reporter                            : 2001::1
Group Type                               : Filter

                                          V1        Sources   Sources
Port      Vers Mode Uptime    Expires     Timer     Forwarded Blocked
--------- ---- ---- --------- --------- --------- --------- --------
1/1/1     2    EXC  0m 5s     4m 15s    4m 15s    0         0


switch# show ipv6 mld snooping vlan 2 group ff05::2:1

MLD ports and group information for group ff05::2:1

VLAN ID                                  : 2
VLAN Name                                : VLAN2
```

```
Group Address                              : ff05::2:1
Last Reporter                              : 2001::1
Group Type                                 : Filter

                                          V1        Sources   Sources
Port      Vers Mode Uptime    Expires     Timer     Forwarded Blocked
--------- ---- ---- --------- --------- --------- --------- --------
1/1/1     2    EXC  0m 5s     4m 15s    4m 15s    0         0


switch# show ipv mld snooping vlan 2 group ff05::2:1 source 3000::3

VLAN ID                                    : 2
VLAN Name                                  : VLAN2
Group Address                              : ff05::2:1
Source Address                             : 3000::3
Source Type                                : Filter

Port      Mode Uptime    Expires   Configured Mode
--------- ---- --------- --------- ----------------
1/1/1     INC  0m 27s    3m 53s    Auto
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 mld snooping static-groups

```
show ipv6 mld snooping [static-groups]
```

Description

This command shows MLD snooping static group details, including the number of static groups joined.

Example

```
switch# show ipv6 mld snooping static-groups

MLD Static Group Address Information

VLAN ID Group Address
------- ----------------------------------------
10      ff12::1
10      ff12::2
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 mld snooping vlan statistics

```
show ipv6 mld snooping [vlan <vlan-id> [statistics]]
```

Description

This command shows MLD snooping statistics details for the specified VLAN, including the number of different groups joined for the VLAN.

Parameters

`vlan-id`

Required, 1-4094, shows MLD query packet Tx, Rx, error packet counters on VLAN.

Example

```
switch# show ipv6 mld snooping vlan 2 statistics
MLD Snooping statistics

VLAN ID   :   2
VLAN Name :   VLAN2

Number of Include Groups       :   1
Number of Exclude Groups       :   0
Number of Static Groups        :   1
Total Multicast Groups Joined  :   2
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

MLD configuration commands for interface VLAN

ipv6 mld

```
ipv6 mld {enable | disable}
```

Description

This command enables or disables MLD on the interface VLAN.

Parameters

`enable`

Required: Enable MLD on the interface VLAN.

`disable`

Required: Disable MLD on the interface VLAN.

Example

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ipv6 mld enable
switch(config-if-vlan)# ipv6 mld disable
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config-if-vlan`	Administrators or local user group members with execution rights for this command.

ipv6 mld apply access-list

```
ipv6 mld apply access-list <ACL-NAME>
no ipv6 mld apply access-list <ACL-NAME>
```

Description

Configures the ACL on a particular interface to filter the MLD join or leave packets based on rules set in the particular ACL name.

The `no` form of this command disables the rules set for the ACL.

Parameters

`access-list`

Associates an ACL with the IGMP.

<ACL-NAME>

Specifies the name of the ACL.

Usage

Existing classifier commands are used to configure the ACL. In case an MLDv2 packet with multiple group addresses is received, it will only process the permitted group addresses based on the ACL rule set, and any existing joins will time out. If there is no match or if there is a deny rule match, the packet is dropped.

Examples

Configuring the ACL to filter MLD packets based on rules set in access list `mygroup`:

```
switch(config)# access-list ipv6 mygroup
switch(config-acl-ip)# permit icmpv6 any ff55::1
switch(config-acl-ip)# exit
switch(config)# interface vlan 2
switch(config-vlan)# ipv6 mld apply access-list mygroup
```

Configuring the ACL to remove the rules set in access list `mygroup`:

```
switch(config-vlan)# no ipv6 mld apply access-list mygroup
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config-vlan`	Administrators or local user group members with execution rights for this command.

no ipv6 mld

`no ipv6 mld`

Description

This command removes all MLD configurations on the interface.

Example

On the 6400 Switch Series, interface identification differs.

```
switch(config)# interface 1/1/1interface vlan 1
switch(config-if)# no ipv6 mld
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config-if`	Administrators or local user group members with execution rights for this command.

ipv6 mld querier

`ipv6 mld querier`

Description

This command configures MLD querier.

The `no` form of this command disables MLD querier.

Example

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ipv6 mld querier
switch(config-if-vlan)# no ipv6 mld querier
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config-if-vlan`	Administrators or local user group members with execution rights for this command.

ipv6 mld querier interval

`ipv6 mld querier [interval <interval-value>]`

Description

This command configures MLD querier interval. The default interval-value is 125.

Parameters

`interval-value`

Required: 5-300, configures MLD querier interval.

Default interval-value is 125. Use the `no ipv6 mld querier interval` command to set interval-value to the default.

Example

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ipv6 mld querier interval 100
switch(config-if-vlan)# no ipv6 mld querier interval
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config-if-vlan`	Administrators or local user group members with execution rights for this command.

ipv6 mld last-member-query-interval

`ipv6 mld last-member-query-interval <interval-value>`

Description

This command configures MLD last member query interval value in seconds. The default interval-value is 1 second.

Parameters

`interval-value`

Required: 1-2, configures MLD last-member-query-interval.

Default interval-value is 1 second. Use the `no ipv6 mld last-member-query-interval` command to set interval-value to the default.

Example

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ipv6 mld last-member-query-interval 2
switch(config-if-vlan)# no ipv6 mld last-member-query-interval
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if-vlan	Administrators or local user group members with execution rights for this command.

ipv6 mld querier query-max-response-time

ipv6 mld querier query-max-response-time *<response-time>*

Description

This command configures MLD max response time value in seconds. The default max-response-time-value is 10 seconds.

Parameters

max-response-time-value

Required: 10-128, configures MLD querier max-response-time.

Default max-response-time-value is 10 seconds. Use the no ipv6 mld querier query-max-response-time command to set max-response-time-value to the default.

Example

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ipv6 mld query-max-response-time 50
switch(config-if-vlan)# no ipv6 mld query-max-response-time
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if-vlan	Administrators or local user group members with execution rights for this command.

ipv6 mld robustness

ipv6 mld robustness *<VALUE>*

Description

This command configures MLD robustness. The robustness value represents the number of times the querier retries queries on the connected subnets. The default robustness-value is 2 seconds.

Parameters

<VALUE>

Required: 1-7, configures MLD robustness.

Default robustness-value is 2 seconds. Use the `no ipv6 mld robustness` command to set robustness-value to the default.

Example

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ipv6 mld robustness 5
switch(config-if-vlan)# no ipv6 mld robustness
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config-if-vlan`	Administrators or local user group members with execution rights for this command.

ipv6 mld static-group

`ipv6 mld static-group <MULTICAST-GROUP-IP>`

Description

This command configures MLD static group.

Parameters

<MULTICAST-GROUP-IP>

Required: X:X::X:X, configures MLD static group.

Example

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ipv6 mld static-group ff12::c
switch(config-if-vlan)# no ipv6 mld static-group ff12::c
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config-if-vlan`	Administrators or local user group members with execution rights for this command.

ipv6 mld version

`ipv6 mld version <VERSION>`

Description

This command configures MLD version.

Parameters

<VERSION>

Required: 1-2, configures MLD version.

Example

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ipv6 mld version 2
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config-if-vlan`	Administrators or local user group members with execution rights for this command.

ipv6 mld version strict

`ipv6 mld version <VERSION> [strict]`

Description

This command configures MLD strict version. Packets that do not match the configured version will be dropped. By default, strict option is not enabled.

Parameters

<VERSION>

Required: 1-2, configures MLD version.

Example

```
switch(config)# interface vlan 2
switch(config-if-vlan)# ipv6 mld version 2 strict
switch(config-if-vlan)# no ipv6 mld version 2 strict
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config-if-vlan`	Administrators or local user group members with execution rights for this command.

MLD show commands for interface VLAN

Only the default VRF is supported on the Aruba 6200 Switch Series.

show ipv6 mld

`show ipv6 mld`

Description

This command shows MLD configuration on VLAN.

Example

```
switch# show ipv6 mld

VRF Name                    : default
Interface                   : vlan10
MLD Configured Version      : 2
MLD Operating Version       : 2
Querier State               : Querier
Querier IP [this switch]    : fe80::7272:cfff:fe96:d3ec
Querier Uptime              : 39m 44s
Querier Expiration Time     : 0m 31s
MLD Snoop Enabled on VLAN   : True
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 mld interface vlan

```
show ipv6 mld [interface <IFNAME> | <IFNAME.ID> | vlan <VLAN-ID>]
```

Description

This command shows MLD configuration on a specific VLAN.

Parameters

<VLAN-ID>

Required: 1-4094, shows MLD configuration on a specified VLAN.

<IFNAME>

Required: Shows MLD configuration on a specified interface.

<IFNAME.ID>

Required: Specifies a sub-interface. (Applies only to the Aruba 6300, 6400, and 8360 Switch Series.)

Examples

Showing MLD configuration on a specified interface:

```
switch# show ipv6 mld interface vlan 10

MLD Configured Version    : 2
MLD Operating Version     : 2
Querier State               : Querier
Querier IP [this switch]    : fe80::7272:cfff:fe96:d3ec
Querier Uptime              : 40m 42s
Querier Expiration Time     : 1m 39s
MLD Snoop Enabled on VLAN   : True

switch# show ipv6 mld interface 1/1/2

MLD Configured Version    : 2
MLD Operating Version     : 2
Querier State               : Querier
Querier IP [this switch]    : fe80::7272:cfff:fe96:d3ec
Querier Uptime              : 40m 42s
Querier Expiration Time     : 1m 39s
MLD Snoop Enabled on VLAN   : True
```

Showing MLD configuration on sub-interface 1/1/2.10:

Applies only to the Aruba 6300, 6400, and 8360 Switch Series.

```
switch# show ipv6 mld interface 1/1/2.10

MLD Configured Version    : 2
MLD Operating Version     : 2
Querier State               : Querier
```

```
Querier IP [this switch]   : fe80::7272:cfff:fe96:13ec
Querier Uptime             : 40m 42s
Querier Expiration Time    : 1m 39s
MLD Snoop Enabled on VLAN  : True
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 mld vrf all-vrfs

`show ipv6 mld [vrf <VRF-NAME> | all-vrfs ]`

Description

This command shows MLD information for the specified VRF.

Parameters

<VRF-NAME>

Optional: shows MLD information status in a specific VRF.

`all-vrfs`

Optional: shows MLD information status for all VRFs.

Example

```
switch(config)# show ipv6 mld all-vrfs
VRF Name   : default
Interface  : vlan2
MLD Configured Version   : 2
MLD Operating Version    : 2
Querier State              : Querier
Querier IP [this switch]   : fe80::a00:9ff:fe06:67cd
Querier Uptime             : 23m 53s
Querier Expiration Time    : 0m 17s
MLD Snoop Enabled on VLAN  : True

Active Group Address                          Vers Mode Uptime    Expires
--------------------------------------------- ---- ---- --------- ---------
ff05::2:1                                     2    INC  3m 56s    1m 47s

VRF Name   : red
Interface  : vlan3
MLD Configured Version   : 2
MLD Operating Version    : 2
Querier State              : Querier
```

```
Querier IP [this switch]   : fe80::a00:9ff:fe06:67cd
Querier Uptime             : 23m 53s
Querier Expiration Time    : 0m 17s
MLD Snoop Enabled on VLAN  : True

Active Group Address                          Vers Mode Uptime    Expires
--------------------------------------------- ---- ---- --------- ---------
ff05::2:1                                     2    INC  2m 30s    1m 50s
switch(config)# show ipv6 mld vrf red

VRF Name   : red
Interface  : vlan3
MLD Configured Version   : 2
MLD Operating Version    : 2
Querier State              : Querier
Querier IP [this switch]   : fe80::a00:9ff:fe06:67cd
Querier Uptime             : 24m 13s
Querier Expiration Time    : 2m 3s
MLD Snoop Enabled on VLAN  : True

Active Group Address                          Vers Mode Uptime    Expires
--------------------------------------------- ---- ---- --------- ---------
ff05::2:1                                     2    INC  2m 50s    1m 30s
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 mld interface vlan counters

`show ipv6 mld [interface <INTF-ID> | <INTF-ID.ID> | vlan <VLAN-ID>] [counters]]`

Description

This command shows MLD query packet Tx and Rx on a specific VLAN.

Parameters

<VLAN-ID>

Required: 1-4094, shows MLD configuration on a specified VLAN.

<INTF-ID>

Required: IFNAME, shows MLD configuration on a specified interface.

<INTF-ID.ID>

Required: IFNAME, shows MLD configuration on a specified sub-interface. (Applies only to the Aruba 6300, 6400, and 8360 Switch Series.)

`counters`

Optional: Shows MLD query packet counter Tx-Rx on a specified VLAN.

Example

Showing MLD query packet Tx and Rx on a specified interface:

```
switch# show ipv6 mld interface vlan 2 counters

MLD Counters

Interface Name      : vlan2
VRF Name            : default
Membership Timeout  : 0
                                          Rx             Tx
                                          -------------- --------------
V1 All Hosts Queries                      0              0
V2 All Hosts Queries                      0              0
V1 Group Specific Queries                 0              0
V2 Group Specific Queries                 0              2
Group And Source Specific Queries         0              2
V2 Member Reports                         0              N/A
V1 Member Reports                         0              N/A
V1 Member Leaves                          0              N/A
Packets dropped by ACL                    0              N/A


switch# show ipv6 mld interface 1/1/1 counters

MLD Counters

Interface Name      : 1/1/1
VRF Name            : default
Membership Timeout  : 0
                                          Rx             Tx
                                          -------------- --------------
V1 All Hosts Queries                      0              0
V2 All Hosts Queries                      0              0
V1 Group Specific Queries                 0              0
V2 Group Specific Queries                 0              0
Group And Source Specific Queries         0              0
V2 Member Reports                         0              N/A
V1 Member Reports                         0              N/A
V1 Member Leaves                          0              N/A
Packets dropped by ACL                    0              N/A
```

Showing MLD query packet Tx and Rx on a specified sub-interface:

Applies only to the Aruba 6300, 6400, and 8360 Switch Series.

```
switch# show ipv6 mld interface 1/1/1.10 counters

MLD Counters

Interface Name      : 1/1/1.10
VRF Name            : default
Membership Timeout  : 0
                                          Rx             Tx
                                          -------------- --------------
V1 All Hosts Queries                      0              0
V2 All Hosts Queries                      0              0
V1 Group Specific Queries                 0              0
V2 Group Specific Queries                 0              0
```

```
Group And Source Specific Queries            0             0
V2 Member Reports                            2             N/A
V1 Member Reports                            0             N/A
V1 Member Leaves                             0             N/A
Packets dropped by ACL                       0             N/A
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 mld interface vlan groups

`show ipv6 mld [interface <INTF-ID> | <INTF-ID.ID> | vlan <VLAN-ID>] [groups]]`

Description

This command shows MLD groups joined details.

Parameters

<INTF-ID>

Required: 1-4094, shows MLD information on a specified VLAN.

<INTF-ID.ID>

Required: IFNAME, shows MLD information on a specified interface. (Applies only to the Aruba 6300, 6400, and 8360 Switch Series.)

<VLAN-ID>

Required: 1-4094, shows MLD configuration on a specified VLAN.

`groups`

Optional: Shows MLD groups information on a specified interface.

Example

Showing MLD groups information on the specified VLAN:

```
switch# show ipv mld interface vlan 2 groups

MLD group information for group ff05::2:1

Interface Name    : vlan2
VRF Name          : default

Group Address     : ff05::2:1
Last Reporter     : fe80::1

                                V1        Sources    Sources
```

```
Vers Mode Uptime    Expires   Timer     Forwarded Blocked
---- ---- --------- --------- --------- --------- --------
2    INC  6m 2s     0m 4s               1

Group Address  : ff05::2:1
Source Address : 3000::1

Mode Uptime    Expire
---- -------- --------
INC  6m 2s     0m 4s
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 mld interface vlan group source

```
show ipv6 mld [interface (<intf-id> | <intf-id.id> | vlan <vlan-id>) [group <group_ip>]
[source <source_ip>]]]
```

Description

This command shows MLD joined group details on a specified interface.

Parameters

<VLAN-ID>

Required: 1-4094, shows MLD joined group details on a specified VLAN.

<INTF-ID>

Required: IFNAME, shows MLD joined group details on a specified interface.

<INTF-ID.ID>

Required: IFNAME, shows MLD joined group details on a specified sub-interface. (Applies only to the Aruba 6300, 6400, and 8360 Switch Series.)

group_ip

Required: X:X::X:X, shows MLD joined group details.

source_ip

Required: X:X::X:X, shows MLD joined group details for a specified source.

Example

```
switch# show ipv mld interface vlan 2 group ff55::5

MLD group information for group ff55::5
```

```
Interface Name   : vlan2
VRF Name         : default

Group Address    : ff55::5
Last Reporter    : fe80::1

                                V1        Sources   Sources
Vers Mode Uptime    Expires     Timer     Forwarded Blocked
---- ---- --------- --------- --------- --------- --------
2    INC  6m 2s     0m 4s               1

Group Address    : ff55::5
Source Address   : 3000::1

Mode Uptime    Expire
---- -------- --------
INC  6m 2s     0m 4s

switch# show ipv mld interface vlan 2 group ff55::5 source 3000::1

Interface Name   : vlan2
VRF Name         : default
Group Address    : ff55::5
Source Address   : 3000::1

Mode Uptime    Expire
---- -------- --------
INC  9m 37s    2m 0s
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 mld groups

```
show ipv6 mld [groups]
```

Description

This command shows MLD groups joined details.

Parameters

`groups`

Options: shows MLD groups information.

Example

```
switch# show ipv6 mld groups

MLD group information for group ff05::2:11

Interface Name    : vlan2
VRF Name          : default

Group Address     : ff05::2:11
Last Reporter     : 2001::1

                                 V1         Sources    Sources
Vers Mode Uptime     Expires     Timer      Forwarded  Blocked
---- ---- ---------- ---------- ---------- ---------- --------
1         2m 27s     1m 53s     1m 53s

MLD group information for group ff05::2:12

Interface Name    : vlan2
VRF Name          : default

Group Address     : ff05::2:12
Last Reporter     : 2001::1

                                 V1         Sources    Sources
Vers Mode Uptime     Expires     Timer      Forwarded  Blocked
---- ---- ---------- ---------- ---------- ---------- --------
1         0m 3s      4m 18s     4m 18s
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 mld groups all-vrfs vrf

```
show ipv6 mld groups [all-vrfs | vrf <vrf_name>]
```

Description

This command shows MLD groups joined details on VRFs.

Parameters

`all-vrfs`
Optional: shows MLD groups joined in all VRFs.

`vrf`
Optional: shows MLD groups joined in a specific VRF.

Example

```
switch# show ipv6 mld groups all-vrfs

MLD group information for group ff05::2:11

Interface Name   : vlan1
VRF Name         : default

Group Address    : ff05::2:11
Last Reporter    : 2001::1

                                V1        Sources   Sources
Vers Mode Uptime    Expires     Timer     Forwarded Blocked
---- ---- --------- --------- --------- --------- --------
1         4m 4s     2m 38s    2m 38s
MLD group information for group ff05::2:12
Interface Name   : vlan3
VRF Name         : red

Group Address    : ff05::2:12
Last Reporter    : 2001::1

                                V1        Sources   Sources
Vers Mode Uptime    Expires     Timer     Forwarded Blocked
---- ---- --------- --------- --------- --------- --------
1         1m 36s    2m 45s    2m 45s
switch# show ipv6 mld groups vrf default

MLD group information for group ff05::2:11

Interface Name   : vlan2
VRF Name         : default

Group Address    : ff05::2:11
Last Reporter    : 2001::1

                                V1        Sources   Sources
Vers Mode Uptime    Expires     Timer     Forwarded Blocked
---- ---- --------- --------- --------- --------- --------
1         5m 25s    1m 17s    1m 17s
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 mld interface counters

`show ipv6 mld [interface {<INTF-ID> | <INTF-ID.ID>}[counters]]`

Description

This command shows MLD query packet Tx and Rx on a specific interface.

Parameters

<INTF-ID>

Required: shows MLD configuration on a specified interface.

<INTF-ID.ID>

Required: shows MLD configuration on a specified sub-interface. (Applies only to the Aruba 6300, 6400, and 8360 Switch Series.)

counters

Optional: shows MLD query packet counter Tx-Rx on a specified interface.

Examples

Showing MLD configuration on a specified interface:

```
switch# show ipv6 mld interface 1/1/1 counters

MLD Counters

Interface Name      : 1/1/1
VRF Name            : default
Membership Timeout  : 0
                                          Rx             Tx
                                          -------------- --------------
V1 All Hosts Queries                      0              0
V2 All Hosts Queries                      0              9
V1 Group Specific Queries                 0              0
V2 Group Specific Queries                 0              0
Group And Source Specific Queries         0              0
V2 Member Reports                         0              N/A
V1 Member Reports                         0              N/A
V1 Member Leaves                          0              N/A
Packets dropped by ACL                    0              N/A
```

Showing MLD configuration on a specified sub-interface:

Applies only to the Aruba 6300, 6400, and 8360 Switch Series.

```
switch# show ipv6 mld interface 1/1/1.10 counters

MLD Counters

Interface Name      : 1/1/1.10
VRF Name            : default
Membership Timeout  : 0
                                          Rx             Tx
                                          -------------- --------------
V1 All Hosts Queries                      0              0
V2 All Hosts Queries                      0              9
V1 Group Specific Queries                 0              0
V2 Group Specific Queries                 0              0
Group And Source Specific Queries         0              0
V2 Member Reports                         0              N/A
V1 Member Reports                         0              N/A
V1 Member Leaves                          0              N/A
Packets dropped by ACL                    0              N/A
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 mld interface statistics

`show ipv6 mld [interface {<INTF-ID> | <INTF-ID.ID>} [statistics]]`

Description

This command shows MLD statistics on a specific interface.

Parameters

<INTF-ID>

Required: shows MLD statistics on a specified interface.

<INTF-ID.ID>

Required: shows MLD statistics on a specified sub-interface. (Applies only to the Aruba 6300, 6400, and 8360 Switch Series.)

`statistics`

Optional: shows MLD statistics on a specified interface.

Examples

Showing MLD statistics on a specified interface:

```
switch# show ipv6 mld interface 1/1/1 statistics

MLD statistics

Interface Name : 1/1/1
VRF Name       : default

Number of Include Groups       :   2
Number of Exclude Groups       :   0
Number of Static Groups        :   0
Total Multicast Groups Joined  :   2
```

Showing MLD statistics on a specified sub-interface:

Applies only to the Aruba 6300, 6400, and 8360 Switch Series.

```
switch# show ipv6 mld interface 1/1/1.10 statistics
```

```
MLD statistics

Interface Name : 1/1/1.10
VRF Name       : default

Number of Include Groups       :   2
Number of Exclude Groups       :   0
Number of Static Groups        :   0
Total Multicast Groups Joined  :   2
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 mld interface groups

`show ipv6 mld [interface {<INTF-ID> | <INTF-ID.ID>}[groups]]`

Description

This command shows MLD groups joined details.

Parameters

<INTF-ID>

Required: shows MLD configuration on a specified interface.

<INTF-ID.ID>

Required: shows MLD configuration on a specified sub-interface. (Applies only to the Aruba 6300, 6400, and 8360 Switch Series.)

`groups`

Optional: shows MLD groups information.

Example

Showing MLD groups information for a specified interface:

```
switch# show ipv6 mld interface 1/1/1 groups

MLD group information for group ff55::1

Interface Name   : 1/1/1
VRF Name         : default

Group Address    : ff55::1
Last Reporter    : fe80::a00:9ff:fe77:1062
```

```
                                V1        Sources   Sources
Vers Mode Uptime    Expires     Timer     Forwarded Blocked
---- ---- --------- --------- --------- --------- --------
2    EXC  0m 14s    4m 6s
```

Showing MLD groups information for a specified sub-interface:

```
switch# show ipv6 mld interface 1/1/1.10 groups

MLD group information for group ff56::1

Interface Name   : 1/1/1.10
VRF Name         : default

Group Address    : ff56::1
Last Reporter    : fe80::a00:9ff:fe77:1062

                                V1        Sources   Sources
Vers Mode Uptime    Expires     Timer     Forwarded Blocked
---- ---- --------- --------- --------- --------- --------
2    EXC  1m 14s    2m 6s
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 mld interface vlan group source

```
show ipv6 mld [interface (<intf-id> | <intf-id.id> | vlan <vlan-id>) [group <group_ip>]
[source <source_ip>]]]
```

Description

This command shows MLD joined group details on a specified interface.

Parameters

<VLAN-ID>

Required: 1-4094, shows MLD joined group details on a specified VLAN.

<INTF-ID>

Required: IFNAME, shows MLD joined group details on a specified interface.

<INTF-ID.ID>

Required: IFNAME, shows MLD joined group details on a specified sub-interface. (Applies only to the Aruba 6300, 6400, and 8360 Switch Series.)

group_ip

Required: X:X::X:X, shows MLD joined group details.

`source_ip`

Required: X:X::X:X, shows MLD joined group details for a specified source.

Example

```
switch# show ipv mld interface vlan 2 group ff55::5

MLD group information for group ff55::5

Interface Name   : vlan2
VRF Name         : default

Group Address    : ff55::5
Last Reporter    : fe80::1

                                V1        Sources   Sources
Vers Mode Uptime    Expires     Timer     Forwarded Blocked
---- ---- --------- --------- --------- --------- --------
2    INC  6m 2s     0m 4s               1

Group Address    : ff55::5
Source Address   : 3000::1

Mode Uptime    Expire
---- -------- --------
INC  6m 2s     0m 4s

switch# show ipv mld interface vlan 2 group ff55::5 source 3000::1

Interface Name   : vlan2
VRF Name         : default
Group Address    : ff55::5
Source Address   : 3000::1

Mode Uptime    Expire
---- -------- --------
INC  9m 37s    2m 0s
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 mld group all-vrfs vrf

`show ipv6 mld [group <group_ip> [all-vrfs | vrf <vrf_name>]]`

Description

This command shows MLD joined group details on VRF.

Parameters

`group_ip`

Required: X:X::X:X, shows MLD joined group details.

`all-vrfs`

Optional: shows MLD groups joined in all VRFs.

`vrf`

Optional: shows MLD groups joined in a specific VRF.

Example

```
switch# show ipv6 mld group ff55::1

MLD group information for group ff55::1

Interface Name   : 1/1/1
VRF Name         : default

Group Address    : ff55::1
Last Reporter    : fe80::a00:9ff:fe77:1062

                              V1        Sources   Sources
Vers Mode Uptime    Expires   Timer     Forwarded Blocked
---- ---- --------- --------- --------- --------- --------
2    EXC  3m 12s    3m 46s


switch# show ipv6 mld group ff05::2:11 all-vrfs

MLD group information for group ff05::2:11

Interface Name   : vlan2
VRF Name         : default

Group Address    : ff05::2:11
Last Reporter    : 2001::1

                              V1        Sources   Sources
Vers Mode Uptime    Expires   Timer     Forwarded Blocked
---- ---- --------- --------- --------- --------- --------
1         1m 16s    3m 4s     3m 4s
MLD group information for group ff05::2:11

Interface Name   : vlan3
VRF Name         : red

Group Address    : ff05::2:11
Last Reporter    : 2001::1

                              V1        Sources   Sources
Vers Mode Uptime    Expires   Timer     Forwarded Blocked
---- ---- --------- --------- --------- --------- --------
1         0m 52s    3m 28s    3m 28s

switch# show ipv6 mld group ff05::2:11 vrf red

MLD group information for group ff05::2:11

Interface Name   : vlan3
```

```
VRF Name         : red

Group Address    : ff05::2:11
Last Reporter    : 2001::1

                                 V1        Sources   Sources
Vers Mode Uptime    Expires      Timer     Forwarded Blocked
---- ---- --------- --------- --------- --------- --------
1         1m 24s    2m 56s    2m 56s
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 mld group source all-vrfs vrf

```
show ipv6 mld [group <group_ip> [source <source_ip> [all-vrfs | vrf <vrf_name>]]]
```

Description

This command shows MLD joined group details for a source on VRF.

Parameters

`group_ip`
Required: X:X::X:X, shows MLD joined group details.

`source_ip`
Required: X:X::X:X, shows MLD joined group details for a source.

`all-vrfs`
Optional: shows MLD groups joined in all VRFs.

`vrf`
Optional: shows MLD groups joined in a specific VRF.

Example

```
switch# show ipv6 mld group ff05::2:1 source 3000::1

Interface Name  : vlan2
VRF Name  : default
Group Address  : ff05::2:1
Source Address : 3000::1

Mode Uptime    Expire
---- -------- --------
INC  0m 53s    3m 27s
```

```
switch# show ipv6 mld group ff05::2:1 source 3000::1 all-vrfs

Interface Name  : vlan2
VRF Name  : default
Group Address  : ff05::2:1
Source Address : 3000::1

Mode Uptime    Expire
---- -------- --------
INC  1m 38s    4m 5s
Interface Name  : vlan3
VRF Name  : red
Group Address  : ff05::2:1
Source Address : 3000::1

Mode Uptime    Expire
---- -------- --------
INC  0m 12s    4m 8s

switch# show ipv6 mld group ff05::2:1 source 3000::1 vrf red

Interface Name  : vlan3
VRF Name  : red
Group Address  : ff05::2:1
Source Address : 3000::1

Mode Uptime    Expire
---- -------- --------
INC  0m 23s    3m 57s
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 mld interface vlan statistics

```
show ipv6 mld [interface vlan <vlan-id> [statistics]]
```

Description

This command shows MLD statistics on a specific interface VLAN.

Parameters

`vlan-id`

Required: 1-4094, shows MLD information on a specified VLAN.

`statistics`

Optional: shows MLD query packet Tx, Rx, Error packet counters on a specified VLAN.

Example

```
switch# show ipv6 mld interface vlan 2  statistics

MLD statistics

Interface Name : vlan2
VRF Name       : default

Number of Include Groups       :   2
Number of Exclude Groups       :   0
Number of Static Groups        :   0
Total Multicast Groups Joined  :   2
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 mld static-groups vrf all-vrfs

```
show ipv6 mld [static-groups [vrf <vrf_name> | all-vrfs]]
```

Description

This command shows MLD static groups.

Parameters

`all-vrfs`

Optional: shows MLD groups joined in all VRFs.

`vrf`

Optional: shows MLD groups joined in a specific VRF.

Example

```
switch# show ipv6 mld static-groups

MLD Static Group Address Information

VRF Name   :default
Interface Name   Group Address
---------------- ----------------------------------------
vlan2            ff12::c
vlan2            ff12::d

switch# show ipv6 mld static-groups vrf test
```

```
MLD Static Group Address Information

VRF Name   :test
Interface Name   Group Address
---------------- ----------------------------------------
vlan3            ff13::1
vlan3            ff13::2
switch# show ipv6 mld static-groups all-vrfs

MLD Static Group Address Information

VRF Name   :default
Interface Name   Group Address
---------------- ----------------------------------------
vlan2            ff12::c
vlan2            ff12::d
VRF Name   :test
Interface Name   Group Address
---------------- ----------------------------------------
vlan3            ff13::1
vlan3            ff13::2
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 mld counters vrf

```
show ipv6 mld [counters [ vrf <vrf_name> ]]
```

Description

This command shows MLD counters.

Parameters

`vrf`

Optional: shows MLD counter status in a specific VRF.

Example

```
switch# show ipv6 mld counters

MLD Counters

Interface Name      : vlan2
```

```
VRF Name            : default
Membership Timeout  : 0
                                                Rx             Tx
                                                -------------- --------------
V1 All Hosts Queries                            0              0
V2 All Hosts Queries                            0              12
V1 Group Specific Queries                       0              0
V2 Group Specific Queries                       0              0
Group And Source Specific Queries               0              0
V2 Member Reports                               0              N/A
V1 Member Reports                               0              N/A
V1 Member Leaves                                0              N/A
Packets dropped by ACL                          0              N/A

switch# show ipv6 mld counters vrf default

MLD Counters

Interface Name      : vlan2
VRF Name            : default
Membership Timeout  : 0
                                                Rx             Tx
                                                -------------- --------------
V1 All Hosts Queries                            0              0
V2 All Hosts Queries                            0              12
V1 Group Specific Queries                       0              0
V2 Group Specific Queries                       0              0
Group And Source Specific Queries               0              0
V2 Member Reports                               0              N/A
V1 Member Reports                               0              N/A
V1 Member Leaves                                0              N/A
Packets dropped by ACL                          0              N/A
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

MLD configuration commands for interface

ipv6 mld

```
ipv6 mld {enable | disable}
```

Description

This command enables or disables MLD on the interface.

Parameters

`enable`

Required: Enable MLD on the interface.

`disable`

Required: Disable MLD on the interface.

Example

On the 6400 Switch Series, interface identification differs.

```
switch(config)# interface 1/1/1interface vlan 1
switch(config-if)# ipv6 mld enable
switch(config-if)# ipv6 mld disable
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config-if`	Administrators or local user group members with execution rights for this command.

ipv6 mld apply access-list

`ipv6 mld apply access-list <ACL-NAME>`
`no ipv6 mld apply access-list <ACL-NAME>`

Description

Configures the ACL on a particular interface to filter the MLD join or leave packets based on rules set in the particular ACL name.

The `no` form of this command removes the rules set for the ACL.

Parameters

`access-list`

Associates an ACL with the IGMP.

<ACL-NAME>

Specifies the name of the ACL.

Usage

Existing classifier commands are used to configure the ACL. In case an MLDv2 packet with multiple group addresses is received, it will only process the permitted group addresses based on the ACL rule set, and any existing joins will time out. If there is no match or if there is a deny rule match, the packet is dropped.

Examples

On the 6400 Switch Series, interface identification differs.

Configuring the ACL to filter MLD packets based on rules set in access list `mygroup`:

```
switch(config)# access-list ipv6 mygroup
switch(config-acl-ip)# permit icmpv6 any ff55::1
switch(config-acl-ip)# exit
switch(config)# interface 1/1/1interface vlan 1
switch(config-vlan)# ipv6 mld apply access-list mygroup
```

Configuring the ACL to remove the rules set in access list `mygroup`:

```
switch(config-vlan)# no ipv6 mld apply access-list mygroup
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config-vlan`	Administrators or local user group members with execution rights for this command.

no ipv6 mld

`no ipv6 mld`

Description

This command removes all MLD configurations on the interface.

Example

On the 6400 Switch Series, interface identification differs.

```
switch(config)# interface 1/1/1interface vlan 1
switch(config-if)# no ipv6 mld
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config-if`	Administrators or local user group members with execution rights for this command.

ipv6 mld querier

```
ipv6 mld querier
```

Description

This command configures MLD querier. This functionality will allow the interface to join in the querier-election process.

Example

On the 6400 Switch Series, interface identification differs.

```
switch(config)# interface 1/1/1interface vlan 1
switch(config-if)# ipv6 mld querier
switch(config-if)# no ipv6 mld querier
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config-if`	Administrators or local user group members with execution rights for this command.

ipv6 mld querier interval

```
ipv6 mld querier [interval <interval-value>]
```

Description

This command configures MLD querier interval. The default interval-value is 125.

Parameters

`interval-value`

Required: 5-300, configures MLD querier interval.

Default interval-value is 125. Use the `no ipv6 mld querier interval` command to set interval-value to the default.

Example

On the 6400 Switch Series, interface identification differs.

```
switch(config)# interface 1/1/1interface vlan 1
switch(config-if)# ipv6 mld querier interval 100
switch(config-if)# no ipv6 mld querier interval
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config-if`	Administrators or local user group members with execution rights for this command.

ipv6 mld last-member-query-interval

`ipv6 mld last-member-query-interval <interval-value>`

Description

This command configures MLD last member query interval value in seconds. The default interval-value is 1 second.

Parameters

`interval-value`

Required: 1-2, configures MLD last-member-query-interval.

Default interval-value is 1 second. Use the `no ipv6 mld last-member-query-interval` command to set interval-value to the default.

Example

On the 6400 Switch Series, interface identification differs.

```
switch(config)# interface 1/1/1interface vlan 1
switch(config-if)# ipv6 mld last-member-query-interval 2
switch(config-if)# no ipv6 mld last-member-query-interval
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config-if`	Administrators or local user group members with execution rights for this command.

ipv6 mld querier query-max-response-time

`ipv6 mld querier query-max-response-time <response-time>`

Description

This command configures MLD max response time value in seconds. The default max-response-time-value is 10 seconds.

Parameters

`max-response-time-value`

Required: 10-128, configures MLD querier max-response-time.

Default max-response-time-value is 10 seconds. Use the `no ipv6 mld querier query-max-response-time` command to set max-response-time-value to the default.

Example

On the 6400 Switch Series, interface identification differs.

```
switch(config)# interface 1/1/1interface vlan 1
switch(config-if)# ipv6 mld query-max-response-time 50
switch(config-if)# no ipv6 mld query-max-response-time
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config-if`	Administrators or local user group members with execution rights for this command.

ipv6 mld robustness

`ipv6 mld robustness <value>`

Description

This command configures MLD robustness. The robustness value represents the number of times the querier retries queries on the connected subnets. The default robustness-value is 2 seconds.

Parameters

`robustness-value`

Required: 1-7, configures MLD robustness.

Default robustness-value is 2 seconds. Use the `no ipv6 mld robustness` command to set robustness-value to the default.

Example

On the 6400 Switch Series, interface identification differs.

```
switch(config)# interface 1/1l/1interface vlan 1
switch(config-if)# ipv6 mld robustness 5
switch(config-if)# no ipv6 mld robustness
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if	Administrators or local user group members with execution rights for this command.

ipv6 mld static-group

`ipv6 mld static-group <multicast-group-ip>`

Description

This command configures MLD static group.

Parameters

`multicast-group-ip`

Required: X:X::X:X, configures MLD static group.

Example

On the 6400 Switch Series, interface identification differs.

```
switch(config)# interface 1/1/1interface vlan 1
switch(config-if)# ipv6 mld static-group ff12::c
switch(config-if)# no ipv6 mld static-group ff12::c
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	config-if	Administrators or local user group members with execution rights for this command.

ipv6 mld version

`ipv6 mld version <version>`

Description

This command configures MLD version.

Parameters

`version`

Required: 1-2, configures MLD version.

Example

On the 6400 Switch Series, interface identification differs.

```
switch(config)# interface 1/1/1interface vlan 1
switch(config-if)# ipv6 mld version 2
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config-if`	Administrators or local user group members with execution rights for this command.

ipv6 mld version strict

`ipv6 mld version <version> [strict]`

Description

This command configures MLD strict version. Packets that do not match the configured version will be dropped. By default, strict option is not enabled.

Parameters

`version`

Required: 1-2, configures MLD version.

Example

On the 6400 Switch Series, interface identification differs.

```
switch(config)# interface 1/1/1interface vlan 1
switch(config-if)# ipv6 mld version 2 strict
switch(config-if)# no ipv6 mld version 2 strict
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config-if`	Administrators or local user group members with execution rights for this command.

In a network, IP multicast traffic transmitted for multimedia applications is blocked at routed interface boundaries unless a multicast routing protocol is running. Protocol Independent Multicast (PIM) is a family of routing protocols. It forms multicast trees to forward traffic from multicast sources to subnets which use protocols such as IGMP and MLD to request the traffic.

Protocol Independent Multicast - Sparse Mode (PIM-SM) overview

PIM relies on the unicast routing tables to identify the path back to a multicast source (reverse path forwarding (RPF)). The unicast routing protocols create the unicast routing tables. With this information, PIM sets up the distribution tree for the multicast traffic.

PIM-Sparse Mode (PIM-SM) can be configured on physical ports, VLAN interfaces, LAG interfaces, and loopback interfaces. All such configurations work in the mentioned interfaces context.

IGMP/MLD provides the multicast traffic link between a host and a multicast router running PIM-SM. Both PIM-SM and IGMP/MLD must be enabled on VLANs whose member ports have directly connected hosts with a valid need to join multicast groups.

PIM-SM uses the pull mode for multicast forwarding, and it is suitable for large and medium-sized networks with sparsely and widely distributed multicast group members.

PIM-SM assumes that most hosts do not want to receive multicast traffic. It uses a nonflooding multicast model to direct traffic from the source to the interface when there are multicast receivers in the group. As a result, this model sends traffic only to the routers that specifically request it.

PIM-SM defaults, protocols, and supported configuration

Default configuration

PIM-SM is disabled by default. When PIM-SM is enabled, switching to SPT and LAN prune delay are the default configuration activated.

PIM specification

Complies with PIM-SM specification (RFC 4061).

BSR implementation

Complies with RFC 5059 (scope zones are not supported).

Routing protocol support

PIM uses unicast routing information from any of the routing protocols that are running on the system, such as OSPFv2, OSPFv3, BGP. Static routes are also supported with Nexthop IP addresses.

Max interface support per flow

Up to 127 outbound interfaces (and 1 inbound interface) are supported in the multicast routing table at any given time. The sum of all outbound interfaces across all current flows on a router may not exceed 127.

PIM enabled interfaces (L3 and SVI)

The maximum PIM enabled interface is 1000 with an upper limit of 128 per VRF.

On the Aruba 6200 Switch Series, only 16 PIM enabled interfaces are supported.

IGMP and MLD compatibility

PIM-SM is compatible with IGMP version 2 and version 3, MLD version 1 and version 2, and is fully interoperable with IGMP/MLD for determining multicast flows.

VRRP

PIM-SM is fully interoperable with VRRP to quickly transition multicast routes in a failover.

VRF support

PIM-SM can run on multiple VRF instances in parallel. It is supported on all VRFs supported in the system.

On the Aruba 6200 Switch Series, PIM-SM only runs on the default VRF.

Static RPs count

PIM-SM supports a maximum of 8 static RPs per VRF.

PIM-SM router types

Within a PIM-SM domain, PIM-SM routers can be configured to fill one or more of the following roles:

- **Designated router (DR)**: A router performing this function forwards multicast traffic from a unicast source to the appropriate distribution (rendezvous) point.
- **Bootstrap router (BSR)**: A router elected to this function keeps all routers in a PIM-SM domain informed of the currently assigned rendezvous point (RP) for each multicast group currently known in the domain.
- **Rendezvous point (RP)**: A router elected as an RP for a multicast group receives requested multicast traffic from a DR and forwards it toward the multicast receivers requesting the traffic. An RP can be manually configured or dynamically elected through the BSR process.
- **Static RP**: This option forwards traffic in the same way as an RP, but requires manual configuration on all routers in the domain to be effective.
- **Candidate RP (C-RP)**: The C-RP periodically sends advertisement messages to the BSR, which collects RP-set information for RP election. The BSR starts a holdtime timer for a C-RP after it receives an advertisement message. If the BSR does not receive any advertisement message when the timer expires, it considers the C-RP failed or unreachable.

All of these can be enabled on each of several routers in a PIM-SM domain.

DR

In a LAN segment populated by one or more routers running PIM-SM, one such router is elected the DR for that LAN segment. When the DR receives a Join request from a multicast receiver on that LAN segment, it forwards the join toward the router operating as the RP for the requested multicast group.

Where multiple PIM-SM routers exist in a LAN segment, the following criteria is used to elect a DR:

1. The router configured with the highest DR priority in the LAN segment is elected.
2. If multiple routers in the LAN segment are configured with the same DR priority, the router having the highest IP address is elected.

In a given domain, each LAN segment capable of receiving multicast traffic from a unicast source should have at least one DR. (Enabling PIM-SM on a LAN segment automatically enables the router as a DR for that LAN segment.) Because there is an election process for DR on each LAN segment, all routers on a LAN segment must be enabled for DR. Where it is important to ensure that a particular router is elected as the DR for a given LAN segment, you can increase the DR priority on that LAN segment configuration for that router.

If it is necessary to prevent a router from operating as a DR on a given LAN segment, disable DR operation by configuring the DR priority as zero (0).

BSR

Before a DR can forward encapsulated packets for a specific multicast group to an RP, it must know which router in the domain is the elected RP for that multicast group. The BSR function enables this operation by doing the following:

1. Learns the group-to-RP mappings on the C-RPs in the domain by reading the periodic advertisements each one sends to the BSR.
2. Distributes the aggregate Candidate-RP (C-RP) information as an RP-set to the PIM-SM routers in the domain. This is followed by an election to assign a specific multicast group or range of groups to the C-RPs in the domain. The software supports assignment of up to four multicast addresses and/or ranges of multicast addresses to a Candidate Rendezvous Point.

The BSR periodically sends bootstrap messages to the other PIM-SM routers in the domain to maintain and update the RP-set data throughout the domain, and to maintain its status as the elected BSR.

RP

Instead of flooding multicast traffic as is done with PIM-DM, PIM-SM uses a set of multiple routers to operate as RPs. Each RP controls multicast traffic forwarding for one or more multicast groups as follows:

- Receives traffic from multicast sources (S) through a DR.
- Receives multicast joins from routers requesting multicast traffic.
- Forwards the requested multicast traffic to the requesting routers.

The routers requesting multicast traffic are either edge routers or intermediate routers. Edge routers are directly connected to specific multicast receivers using IGMP/MLD to request traffic. Intermediate routers are on the path between edge routers and the RP. This is known as an RP Tree (RPT) where only the multicast address appears in the routing table. For example:

`( *, G )`, where:

`*` = a variable (wildcard) representing the IP address of any multicast source

`G` = a particular multicast group address.

C-RP

Within a PIM-SM domain, different RPs support different multicast addresses or ranges of multicast addresses. That is, a given PIM-SM multicast group or range of groups is supported by only one active RP, although other C-RPs can also be configured with overlapping or identical support.

A C-RP's group-prefix configuration identifies the multicast groups the RP is enabled to support.

If multiple C-RPs have group-prefixes configured so that any of these RPs can support a given multicast group, then the following criteria are used to select the RP to support the group:

1. The C-RP configured with the longest group-prefix mask applicable to the multicast group is selected to support the group. Step 2 of this procedure applies if multiple RP candidates meet this criterion.
2. The C-RP configured with the highest priority is selected. Step 3 of this procedure applies if multiple RP candidates meet this criterion
3. A hash function (using the configured `bsr-candidate hash-mask-length` value) generates a series of mask length values that are individually assigned to the set of eligible C-RPs. If the hash function matches a single RP candidate to a longer mask length than the other candidates, that candidate is selected to support the group. Apply step 4 of this procedure if the hash function matches the longest mask length to multiple RP candidates.
4. The C-RP having the highest IP address is selected to support the group.

Also, within a PIM-SM domain, a router can be configured as a C-RP available for a given multicast group or range of groups and as the static RP for a given multicast group or range of groups. The recommended practice is to use C-RPs for all multicast groups unless there is a need to ensure that a specific group or range of groups is always supported by the same routing switch.

Loopback, Route Only Port (ROP), and Switched Virtual Interface (SVI) are interfaces that can be configured as RPs. Anycast RP is also supported with the help of MSDP mesh groups.

Static RP

Like C-RPs, static RPs control multicast forwarding of specific multicast groups or ranges of contiguous groups. However, static RPs are not dynamically learned, and increase the configuration and monitoring effort to maintain them. As a result, static RPs are not recommended for use except where one of the following conditions applies:

- It is desirable to designate a specific router interface as a backup RP for specific groups.
- Specific multicast groups are expected, and a static RP would help to avoid overloading a given RP with a high volume of multicast traffic.
- A C-RP for the same groups is less reliable than another RP that would not normally be elected to support the groups.
- Tighter traffic control or a higher priority is desired for specific multicast groups.

How PIM-SM works

PIM-SM (PIM Sparse Mode) assumes that most hosts do not want to receive multicast traffic. It uses a nonflooding multicast model to direct traffic from the source to the interface when there are multicast receivers in the group. As a result, this model sends traffic only to the routers that specifically request it.

In a given PIM-SM domain, routers identified as DRs, RPs, and a BSR participate in delivering multicast traffic to the IP multicast receivers that request it. This approach avoids the flooding method of distributing multicast traffic (employed by PIM-DM) and is best suited for lower bandwidth situations.

The software supports the following operation to enable multicast traffic delivery within a PIM-SM domain:

- From a pool of eligible DR candidates in each LAN segment, one DR is elected for each LAN segment interface having at least one PIM-SM router. In a multinetted domain, this DR supports multicast traffic from a source on any subnet in the LAN segment.
- From a pool of eligible BSR candidates in the domain, one BSR is elected for the entire domain.

- From a pool of eligible C-RPs, one is elected to support each multicast group or range of groups allowed in the domain, excluding any group supported only by static RPs. The multicast groups allowed in the domain are determined by the aggregation of the groups allowed by the individually configured RPs and any static RPs. C-RPs and static RPs can be configured with overlapping support for a given set of multicast groups.

Neighbor discovery

In a PIM domain, each PIM interface on a router periodically multicasts PIM hello messages to all other PIM routers (identified by the address 224.0.0.13 for V4 and ff02::d for V6) on the local subnet. Through the exchanging of hello messages, all PIM routers on the subnet determine their PIM neighbors, maintain PIM neighboring relationship with other routers, and build and maintain shortest path trees (SPTs).

DR election

A designated router (DR) is required on both the source-side network and receiver-side network. A source-side DR acts on behalf of the multicast source to send register messages to the RP. The receiver-side DR acts on behalf of the multicast receivers to send join messages to the RP.

The DR election process is as follows:

1. The routers on the shared-media LAN send hello messages to one another. The hello messages contain the DR priority for DR election. The router with the highest DR priority is elected as the DR.
2. The router with the highest IP address wins the DR election under one of following conditions:
   - All the routers have the same DR election priority.
   - A router does not support carrying the DR priority in hello messages.

If the DR fails, its PIM neighbor lifetime expires and the other routers will initiate to elect a new DR.

Rendezvous point tree (RPT)

When a DR in a VLAN receives traffic for a particular multicast group from a source on that VLAN, the DR encapsulates the traffic and forwards it to the RP elected to support that multicast group. The RP decapsulates the traffic and forwards it on toward the multicast receivers requesting that group. This forms an RPT extending from the DR through any intermediate PIM-SM routers leading to the PIM-SM edge routers for the multicast receivers requesting the traffic. (If the RP has no current join requests for the group, the traffic is dropped at the RP.)

Shortest path tree (SPT)

SPTs are especially useful in high data-rate applications where reducing unnecessary traffic concentrations and throughput delays are significant. In the default PIM-SM configuration, SPT operation is automatically enabled.

In the default PIM-SM configuration, after an edge router receives the first packet of traffic for a multicast group requested by a multicast receiver on that router, it uses Reverse Path Forwarding (RPF) to learn the shortest path to the group source. The edge router then stops using the RPT and begins using the shortest path tree (SPT) connecting the multicast source and the multicast receiver. In this case, when the edge router begins receiving group traffic from the multicast source through the SPT, it sends a prune message to the RP tree to terminate sending the requested group traffic on that route. (This results in entries for both the RP path and the STP in the routing table.) When completed, the switchover from the RPT to a shorter SPT can reduce unnecessary traffic concentrations in the network and reduce multicast traffic throughput delays.

The switchover from RPT to SPT is not instantaneous. For a short period, packets for a given multicast group may be received from both the RPT and the SPT. Also, in some topologies, the RPT and SPT to the same edge router may be identical.

Reverse Path Forward

Reverse Path Forward (RPF) checking is a core multicast routing mechanism that ensures that multicast traffic received arrived on the expected router interface before it is considered for further processing. If the RPF check fails for a multicast packet, the packet is discarded.

For traffic arriving on the SPT, the expected incoming interface for a given source/group multicast flow is the interface towards the source address of the traffic (as determined by the unicast routing system). For traffic arriving on the RP tree, the expected incoming interface is the interface towards the RP. PIM must be enabled on all paths where the unicast route points an ECMP path to the source.

RPF override is a feature that allows the override of the normal RPF lookup mechanism and indicates to the router that it may accept multicast traffic on an interface other than that which would be normally selected by the RPF lookup mechanism. This includes accepting traffic from a source directly connected to the router when the source IP address is invalid for the subnet or VLAN to which it is connected. Traffic may also be accepted from a valid PIM neighbor that is not on the reverse path towards the source of the received multicast traffic.

RPF checking is applied to all multicast traffic and is significant in preventing network loops. Up to eight manual RPF overrides can be specified.

The RPF-address indicates one of two distinct RPF candidates:

1. A valid PIM neighbor address from which forwarded multicast traffic is accepted with a source address of `<source-addr/src-mask>`.
2. A local router address on a PIM-enabled interface to which `<source-addr/src-mask>` is directly connected. The local router will assume the role of DR for this flow and registers the flow with an RP, if configured.

Enabling/disabling PIM-SM in an interface

Prerequisites

You must be in the interface configuration context, as indicated by the `switch(config-if)#` prompt, `switch(config-if-vlan)#` prompt, or `switch(config-lag-if)#` prompt.

Procedure

Enable or disable PIM-SM in an interface using the following command.

For example, the following command enables PIM-SM on interface vlan40:

For IPv4 configurations:

```
ip pim-sparse {enable|disable}
```

```
switch(config)# interface vlan40
switch(config-if-vlan)# ip address 40.0.0.4/24
switch(config-if-vlan)# ip pim-sparse enable
```

For IPv6 configurations:

```
ipv6 pim6-sparse {enable|disable}
```

```
switch(config)# interface vlan40
switch(config-if-vlan)# ip address 2001::01/64
switch(config-if-vlan)# ipv6 pim6-sparse enable
```

The `no` form of the command disables PIM-SM in an interface.

Configuring PIM-SM options in an interface

You can configure various PIM-SM options in an interface as described in the following steps.

Prerequisites

You mustce configuration context, as indicated by the `switch(config-if)#` prompt, `switch(config-if-vlan)#` prompt, or `switch(config-lag-if)#` prompt.

Procedure

1. Configure the frequency at which the router transmits PIM hello messages on the current interface using the following command.

   For IPv4 configurations:

   `ip pim-sparse hello-interval <INTERVAL-VALUE>`

   For example, the following command sets the V4 hello interval to 60 seconds on the 1/1/4 interface:

   ```
   switch(config)# interface 1/1/4
   switch(config-if)# ip pim-sparse hello-interval 60
   ```

   For IPv6 configurations:

   `ipv6 pim6-sparse hello-interval <INTERVAL-VALUE>`

   For example, the following command sets the V6 hello interval to 60 seconds on the 1/1/4 interface:

   ```
   switch(config)# interface 1/1/4
   switch(config-if)# ipv6 pim6-sparse hello-interval 60
   ```

2. Change the maximum time before the router transmits the initial PIM hello message on the interface using the following command.

   For IPv4 configurations:

   `ip pim-sparse hello-delay <DELAY-VALUE>`

   For example, the following command sets the hello delay to 4 seconds on the VLAN40 interface:

   ```
   switch(config)# interface vlan40
   switch(config-if-vlan)# ip pim-sparse hello-delay 4
   ```

   For IPv6 configurations:

   `ipv6 pim6-sparse hello-delay <DELAY-VALUE>`

   For example, the following command sets the hello delay to 4 seconds on the VLAN40 interface:

   ```
   switch(config)# interface vlan40
   switch(config-if-vlan)# ipv6 pim6-sparse hello-delay 4
   ```

3. Specify the priority value to use on the interface in the Designated Router (DR) election process using the following command.

   For IPv4 configurations:

   `ip pim-sparse dr-priority <PRIORITY-VALUE>`

   For example, the following command sets the DR priority to 4444 on the VLAN40 interface:

```
switch(config)# interface vlan40
switch(config-if-vlan)# ip pim-sparse dr-priority 4444
```

For IPv6 configurations:

```
ipv6 pim6-sparse dr-priority <PRIORITY-VALUE>
```

For example, the following command sets the DR priority to 4444 on the VLAN40 interface:

```
switch(config)# interface vlan40
switch(config-if-vlan)# ipv6 pim6-sparse dr-priority 4444
```

4. Enable the LAN prune delay option on the interface using the following command.

   For IPv4 configurations:

   ```
   ip pim-sparse lan-prune-delay
   ```

   For IPv6 configurations:

   ```
   ipv6 pim6-sparse lan-prune-delay
   ```

5. Configure the value inserted into the Override Interval field of a LAN Prune Delay option on the interface using the following command.

   For IPv4 configurations:

   ```
   ip pim-sparse override-interval <INTERVAL-VALUE>
   ```

   For example, the following command sets the override interval value to 4000 ms on interface VLAN40:

   ```
   switch(config)# interface vlan40
   switch(config-if-vlan)# ip pim-sparse override-interval 4000
   ```

   For IPv6 configurations:

   ```
   ipv6 pim6-sparse override-interval <INTERVAL-VALUE>
   ```

   For example, the following command sets the override interval value to 4000 ms on interface VLAN40:

   ```
   switch(config)# interface vlan40
   switch(config-if-vlan)# ipv6 pim6-sparse override-interval 4000
   ```

6. Configure the propagation delay value inserted into the LAN Prune Delay option on the interface using the following command.

   For IPv4 configurations:

   ```
   ip pim-sparse propagation-delay <DELAY-VALUE>
   ```

   For example, the following command sets the propagation delay value to 400 ms on interface VLAN40:

   ```
   switch(config)# interface vlan40
   switch(config-if-vlan)# ip pim-sparse propagation-delay 400
   ```

   For IPv6 configurations:

   ```
   ipv6 pim6-sparse propagation-delay <DELAY-VALUE>
   ```

For example, the following command sets the propagation delay value to 400 ms on interface VLAN40:

```
switch(config)# interface vlan40
switch(config-if-vlan)# ipv6 pim6-sparse propagation-delay 400
```

7. Configure the source IP address to be used in PIM packets transmitted from the interface using the following command.

   For IPv4 configurations:

   `ip pim-sparse ip-addr {<IP-ADDR-VALUE> | any}`

   For example, the following command specifies the IPv4 address 40.0.0.4:

   ```
   switch(config)# interface vlan40
   switch(config-if-vlan)# ip pim-sparse ip-addr 40.0.0.4
   ```

   For IPv6 configurations:

   `ipv6 pim6-sparse ipv6-addr {<IPv6-ADDR-VALUE> | any}`

   For example, the following command specifies the IPv6 address 2001::02:

   ```
   switch(config)# interface vlan40
   switch(config-if-vlan)# ipv6 pim6-sparse ipv6-addr 2001::02
   ```

Viewing PIM information

For some commands, you can specify viewing information by interface or VRF.

Prerequisites

Use these show commands from the Operator (>) or Manager (#) context.

Procedure

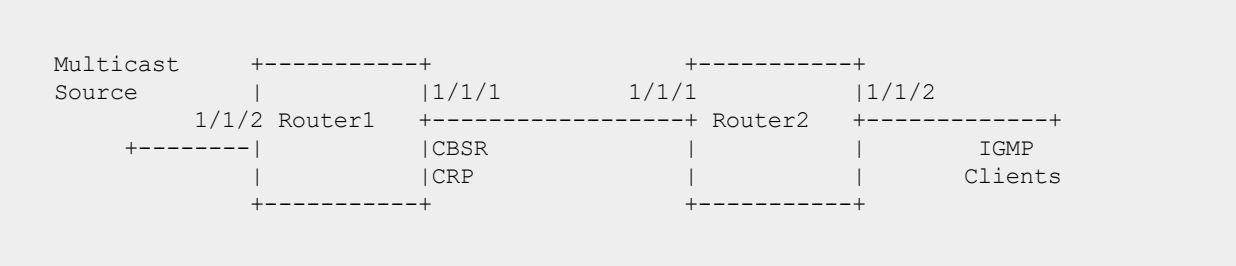
1. To display PIM information for an IPv4 configuration, use the following show commands.
   - To view PIM router information, use: `show ip pim`.
   - To view information about the PIM interfaces configured on the router, use: `show ip pim interface`.
   - To view information about a PIM interface, use: `show ip pim interface <INTERFACE-NAME>`.
   - To view PIM packet counter information for an interface, use: `show ip pim interface <INTERFACE-NAME> counters`.
   - To view PIM neighbor information, use: `show ip pim neighbor`.
   - To view RP information, use: `show ip pim rp-set`.
   - To view information for statically configured RP assignments, use: `show ip pim rp-set static`.
   - To view information for dynamically learned RP assignments, use: `show ip pim rp-set learned`.
   - To view candidate RP information, use: `show ip pim rp-candidate`.
   - To view information about BSR candidates in the domain, use: `show ip pim bsr`.
   - To view information about BSR candidates on the local router, use: `show ip pim bsr local`.
   - To view information about the elected BSR in the domain, use: `show ip pim bsr elected`.

- To view the RPF override configuration, use: `show ip pim rpf-override`.
- To view RPF override configuration for a source, use: `show ip pim rpf-override source`.
- To view pending joins on a PIM router, use: `show ip pim pending`.
- To view multicast routing information, use: `show ip mroute` or use `show ip mroute brief`.
- To view multicast routing information for a group address, use: `show ip mroute <GROUP-ADDR>`.

2. To display PIM information for an IPv6 configuration, use the following show commands.
   - To view PIM router information, use: `show ipv6 pim6`.
   - To view information about the PIM interfaces configured on the router, use: `show ipv6 pim6 interface`.
   - To view information about a PIM interface, use: `show ipv6 pimv6 interface <INTERFACE-NAME>`.
   - To view PIM neighbor information, use: `show ipv6 pim6 neighbor`.
   - To view RP information, use: `show ipv6 pim6 rp-set`.
   - To view information for statically configured RP assignments, use: `show ipv6 pim6 rp-set static`.
   - To view information for dynamically learned RP assignments, use: `show ipv6 pim6 rp-set learned`.
   - To view candidate RP information, use: `show ipv6 pim6 rp-candidate`.
   - To view information about BSR candidates in the domain, use: `show ipv6 pim6 bsr`.
   - To view information about BSR candidates on the local router, use: `show ipv6 pim6 bsr local`.
   - To view information about the elected BSR in the domain, use: `show ipv6 pim6 bsr elected`.
   - To view the RPF override configuration, use: `show ipv6 pim6 rpf-override`.
   - To view RPF override configuration for a source, use: `show ipv6 pim6 rpf-override source`.
   - To view pending joins on a PIM router, use: `show ipv6 pim6 pending`.
   - To view multicast routing information, use: `show ipv6 mroute` or use `show ipv6 mroute brief`.
   - To view multicast routing information for a group address, use: `show ipv6 mroute <GROUP-ADDR>`.

PIM-SM configuration example

The following is a sample topology diagram for a PIM-SM configuration.



In this topology, the multicast source is connected to Router1 and Clients are connected to Router2.

Router1 and Router2 are directly connected so you can verify the neighborship using the `show ip pim neighbor` command.

Secondly Router1 interface 1/1/1 is the BSR candidate and RP candidate in this domain. This information needs to be propagated across the network and needs to be consistent on all routers in the topology. To verify this, use the `show ip pim rp-set` command for group mapping information and the `show ip pim`

`bsr` command for elected BSR information. If they show inconsistent information, you could see possible multicast outages.

If the joins are seen by the routers before the streams can flow, both routes will display those requests in the `show ip pim pending` command output.

Once the multicast source streams start to flow, each router in the path will add multicast router (mroute) entries, which can be verified using the `show ip mroute` command.

The output of the following `show running-config` command shows an example of PIM-SM configuration for IPv4.

```
switch# show running-config
Current configuration:
!
!
!
!
!
Router1
---------------

router ospf 1
    redistribute connected
    area 0.0.0.0
router pim
    enable
    bsr-candidate source-ip-interface 1/1/1
    rp-candidate source-ip-interface 1/1/1
    rp-candidate group-prefix 224.0.0.0/4
interface 1/1/1
    ip address 10.10.10.1/24
    ip ospf 1 area 0.0.0.0
    ip pim-sparse enable
interface 1/1/2
    ip address 20.20.20.1/24
    ip pim-sparse enable


Router2
---------------
router ospf 1
    redistribute connected
    area 0.0.0.0
router pim
    enable
interface 1/1/1
    ip address 10.10.10.2/24
    ip ospf 1 area 0.0.0.0
    ip pim-sparse enable
interface 1/1/2
    ip address 30.30.30.1/24
    ip pim-sparse enable
    ip igmp enable
```

The output of the following `show running-config` command shows an example of PIM-SM configuration for IPv6.

```
switch# show running-config
Current configuration:
!
```

```
!
!
!
!
Router1
---------------
router ospfv3 1
redistribute connected
area 0.0.0.0

router pim6
bsr-candidate source-ip-interface loopback1
rp-candidate source-ip-interface loopback1
rp-candidate group-prefix ff00::/8
enable


interface loopback 1
ipv6 address 1000::1000/64
ipv6 ospfv3 1 area 0.0.0.0
ipv6 pim6-sparse enable

interface 1/1/1
ipv6 address 2000::1/64
ipv6 ospfv3 1 area 0.0.0.0
ipv6 pim6-sparse enable

interface 1/1/2
ipv6 address 4000::1/64
ipv6 pim6-sparse enable

Router2
---------------
router ospfv3 1
redistribute connected
area 0.0.0.0

router pim6
enable

interface 1/1/1
ipv6 address 2000::2/64
ipv6 ospfv3 1 area 0.0.0.0
ipv6 pim6-sparse enable

interface 1/1/2
ipv6 address 5000::1/64
ipv6 pim-sparse enable
ipv6 mld enable
```

PIM-SM configuration task list

Tasks at a glance.

- Enabling or disabling PIM globally
- Configuring join/prune interval
- Enabling/disabling multicast traffic to SPT
- Configuring an RP
- Configuring a BSR

- Configuring RPF override
- Enabling/disabling PIM-SM in an interface
- Configuring PIM-SM options in an interface
- Removing all PIM-SM related configurations on an interface
- Viewing PIM information
- PIM VSX active-active

Enabling or disabling PIM globally

Prerequisites

You must be in the PIM configuration context, as indicated by the `switch(config-pim)#` prompt for IPv4 or the `switch(config-pim6)#` prompt for IPv6.

Procedure

Enable PIM globally on a router using the following command.
`enable`

For example, the following command enables PIM globally:

For IPv4 configurations:

```
switch# configure terminal
switch(config)# router pim
switch(config-pim)# enable
```

For IPv6 configurations:

```
switch# configure terminal
switch(config)# router pim6
switch(config-pim6)# enable
```

You can enable PIM globally and enable PIM-SM at the interface level. When PIM-SM is not enabled on the interface, irrespective of the global PIM status, unknown multicast traffic does not get routed. When PIM-SM is enabled on the interface, multicast traffic is routed to the interface where there are clients joined, provided PIM is enabled globally.

Use the `disable` command to disable PIM globally on a router. You could use this command to temporarily disable PIM globally without removing the individual interface configuration.

Configuring join/prune interval

Configure the interval at which the router will send periodic PIM-SM join or prune interval messages.

Prerequisites

You must be in the PIM configuration context, as indicated by the `switch(config-pim)#` prompt for IPv4 or the `switch(config-pim6)#` prompt for IPv6.

Procedure

Configure the join/prune interval using the following command.
`join-prune-interval <INTERVAL-VALUE>`

For example, the following command sets the join/prune interval to 400 seconds:

For IPv4 configurations:

```
switch# configure terminal
switch(config)# router pim
switch(config-pim)# join-prune-interval 400
```

For IPv6 configurations:

```
switch# configure terminal
switch(config)# router pim6
switch(config-pim6)# join-prune-interval 400
```

The `no` form of the command sets the interval to the default of 60 seconds.

Enabling/disabling multicast traffic to SPT

Switching to SPT is enabled by default.

Prerequisites

You must be in the PIM configuration context, as indicated by the `switch(config-pim)#` prompt for IPv4 or the `switch(config-pim6)#` prompt for IPv6.

Procedure

Enable or disable the router's ability to switch multicast traffic flows to the Shortest Path Tree (SPT) using the following command.
`spt-threshold`

For example, the following command enables switching traffic flows to the SPT:

For IPv4 configurations:

```
switch(config)# router pim
switch(config-pim)# spt-threshold
```

For IPv6 configurations:

```
switch(config)# router pim6
switch(config-pim6)# spt-threshold
```

The `no` form of the command disables switching to SPT.

Configuring an RP

An RP can be manually configured (static RP) or dynamically elected through the Bootstrap Router (BSR) mechanism (Candidate RP or C-RP).

Prerequisites

You must be in the PIM configuration context, as indicated by the `switch(config-pim)#` prompt for IPv4 or the `switch(config-pim6)#` prompt for IPv6.

- A Rendezvous Point (RP) can provide services for multiple or all multicast groups. However, only one RP can forward multicast traffic for a multicast group at a time.

- For a large-scaled PIM network, configuring static RPs is a tedious job. Generally, static RPs are backups for dynamic RPs to enhance the robustness and operational manageability on a multicast network.
- When configuring a static RP, you must configure the same static RP on all routers in the PIM-SM domain.
- When you configure a Candidate RP (C-RP), reserve a relatively large bandwidth between the C-RP and other devices in the PIM-SM domain.

Procedure

1. Configure a static RP using the following command.

   `rp-address <IP-ADDR> [<GRP-ADDR/GRP-MASK>] [override]`

   For example, the following command configures a static RP of 40.0.0.8 for the multicast group:

   For IPv4 configurations:

   ```
   switch(config)# router pim
   switch(config-pim)# rp-address 40.0.0.8 226.0.0.4/24
   ```

   For IPv6 configurations:

   ```
   switch(config)# router pim6
   switch(config-pim6)# rp-address 2002::02 ff08::1:4/64
   ```

2. Configure a C-RP using the following command.

   `rp-candidate source-ip-interface <INTERFACE-NAME> [group-prefix <GRP-ADDR/GRP-MASK>]`

   For example, the following command configures a C-RP using loopback1 as the source for the C-RP router IP address and associates the multicast group with the C-RP router:

   For IPv4 configurations:

   ```
   switch(config)# router pim
   switch(config-pim)# rp-candidate source-ip-interface loopback1 group-prefix
   230.0.0.4/24
   ```

   For IPv6 configurations:

   ```
   switch(config)# router pim6
   switch(config-pim6)# rp-candidate source-ip-interface loopback1 group-prefix
   ff08::1:3/64
   ```

   For a C-RP, you can configure various options as shown in the following steps. C-RP can be configured on an SVI or ROP interface also.

3. Add or remove multicast groups for the C-RP, as needed, using the following command.

   `rp-candidate group-prefix <GRP-ADDR/GRP-MASK>`

   For example, the following commands configure a C-RP using VLAN 40 as the source for the C-RP router IP address and then adds the multicast group to the C-RP:

   For IPv4 configurations:

```
switch(config)# router pim
switch(config-pim)# rp-candidate source-ip-interface vlan40
switch(config-pim)# rp-candidate group-prefix 230.0.0.4/24
```

For IPv6 configurations:

```
switch(config)# router pim6
switch(config-pim6)# rp-candidate source-ip-interface vlan40
switch(config-pim6)# rp-candidate group-prefix ff08::1:3/64
```

4. Configure the hold-time a C-RP includes in its advertisements to the BSR using the following command.

   `rp-candidate hold-time <TIME-VALUE>`

   For example, the following command sets the hold-time to 250 seconds:

   For IPv4 configurations:

   ```
   switch(config)# router pim
   switch(config-pim)# rp-candidate hold-time 250
   ```

   For IPv6 configurations:

   ```
   switch(config)# router pim6
   switch(config-pim6)# rp-candidate hold-time 250
   ```

5. Set the priority for a C-RP using the following command.

   `rp-candidate priority <PRIORITY-VALUE>`

   For example, the following command sets the priority to 250:

   For IPv4 configurations:

   ```
   switch(config)# router pim
   switch(config-pim)# rp-candidate priority 250
   ```

   For IPv6 configurations:

   ```
   switch(config)# router pim6
   switch(config-pim6)# rp-candidate priority 250
   ```

Configuring a BSR

Configure the router to advertise itself as the Candidate Bootstrap Router (Candidate-BSR) for the PIM-SM domain.

Prerequisites

You must be in the PIM configuration context, as indicated by the `switch(config-pim)#` prompt for IPv4 or the `switch(config-pim6)#` prompt for IPv6.

PIM-SM must be enabled on the interface used as the source IP interface.

Procedure

1. Configure a Candidate-BSR using the following command.

   ```
   bsr-candidate source-ip-interface <INTERFACE-NAME>
   ```

   For example, the following command configures a Candidate-BSR using interface 1/1/4 as the source for the router IP address. This command can also be applied to an L3 VLAN or L3 LAG. (L3 LAG is not supported on the Aruba 6200 Switch Series.)

   For IPv4 configurations:

   ```
   switch(config)# router pim
   switch(config-pim)# bsr-candidate source-ip-interface 1/1/4
   ```

   For IPv6 configurations:

   ```
   switch(config)# router pim6
   switch(config-pim6)# bsr-candidate source-ip-interface 1/1/4
   ```

   Candidate-BSR can be enabled on a loopback interface as well. For a Candidate-BSR, you can configure various options as shown in the following steps.

2. Configure the bootstrap message (BSM) interval for sending periodic RP-Set messages using the following command.

   ```
   bsr-candidate bsm-interval <INTERVAL-VALUE>
   ```

   For example, the following command configures a bootstrap message interval of 150 seconds:

   For IPv4 configurations:

   ```
   switch(config)# router pim
   switch(config-pim)# bsr-candidate bsm-interval 150
   ```

   For IPv6 configurations:

   ```
   switch(config)# router pim6
   switch(config-pim6)# bsr-candidate bsm-interval 150
   ```

3. Set the priority to apply to the router when a BSR election process occurs in the PIM-SM domain using the following command.

   ```
   bsr-candidate priority <PRIORITY-VALUE>
   ```

   For example, the following command configures the priority as 250:

   For IPv4 configurations:

   ```
   switch(config)# router pim
   switch(config-pim)# bsr-candidate priority 250
   ```

   For IPv6 configurations:

   ```
   switch(config)# router pim6
   switch(config-pim6)# bsr-candidate priority 250
   ```

4. Configure the length (in bits) of the hash-mask using the following command. Used to control the distribution of multicast groups among the C-RP in a domain where there is overlapping coverage of the groups among the RPs.

   `bsr-candidate hash-mask-length <LENGTH-VALUE>`

   For example, the following command configures the hash-mask length to 4:

   For IPv4 configurations:

```
switch(config)# router pim
switch(config-pim)# bsr-candidate hash-mask-length 4
```

```
For IPv6 configurations:

switch(config)# router pim6
switch(config-pim6)# bsr-candidate hash-mask-length 4
```

Configuring RPF override

Configure Reverse Path Forward (RPF) override to allow the override of the normal RPF lookup mechanism, indicating to the router that it may accept multicast traffic on an interface other than the one that would normally be selected by the RPF lookup mechanism.

RPF checking ensures that multicast traffic received arrived on the expected router interface before it is considered for further processing. If the RPF check fails for a multicast packet, the packet is discarded.

RPF override entry gets precedence over routes learned from routing protocols or static routes. It must also be noted that PIM will not switch to an alternate path if the configured RPF neighbor is not reachable.

Prerequisites

You must be in the PIM configuration context, as indicated by the `switch(config-pim)#` prompt for IPv4 or the `switch(config-pim6)#` prompt for IPv6.

Procedure

Add, edit, or delete RPF overrides using the following command.

`rpf-override <SRC-ADDR/SRC-MASK><RPF-ADDR|INTERFACE-NAME>`

For IPv4 configurations:

```
switch(config)# router pim
switch(config-pim)# rpf-override 40.0.0.4/24 30.0.0.4
```

For IPv6 configurations:

```
switch(config)# router pim6
switch(config-pim6)# rpf-override 50::4/24 40::1
```

Removing all PIM-SM related configurations on an interface

Prerequisites

You must be in the interface configuration context, as indicated by the `switch(config-if)#` prompt, `switch(config-if-vlan)#` prompt, or `switch(config-lag-if)#` prompt.

Procedure

Remove all PIM-SM related configurations for the interface using the following command.

For IPv4 configurations:

```
no ip pim-sparse
```

For IPv6 configurations:

```
no ipv6 pim6-sparse
```

PIM VSX active-active

Not supported on the 6200 and 6300 Switch Series.

The PIM active-active solution makes one of the VSX devices act as DR and other device as proxy-DR for each of the downstream VLANs. Both the VSX peers behave the same as far as the protocol is concerned with only the DR forwarding the multicast traffic to downstream routers. The PIM active-active feature is enabled on VSX devices connected to access switches on one side with hosts behind the access switches. The DR election depends on the IP address and a single VSX device doesn't be the DR for all of the downstream VLANs.

When a VSX device which is acting as DR for some of the downstream VLANs starts rebooting, traffic loss would be seen for the multicast streams in those downstream VLANs for few seconds. The VSX software upgrade process involves rebooting each VSX device with new software. The secondary VSX device is upgraded before primary VSX device. If the secondary is acting as DR for some of downstream VLANs then after the VSX software upgrade is triggered multicast traffic loss will be seen twice for the streams present in those VLANs; once during secondary VSX device reboot and then during primary VSX device reboot.

With graceful shutdown traffic loss is not seen for any of multicast streams. Instead, some duplicates are expected for 1-3 seconds for each stream.

The sequence of events during each VSX device upgrade is outlined below:

1. The first step is based on device role and is applicable only to the primary device. According to VSX software upgrade process, the device upgrade is triggered in the primary after the secondary upgrade. The secondary should already have all the multicast routes before taking over the DR role from the primary. After the secondary device reboots the primary device waits for few minutes so that the secondary learns the multicast routes and is ready to take over the DR role. The wait time in primary device depends on the number of multicast routes present.
2. DR roles of all the downstream VLANs are offloaded to its peer. At the end of this step the device which is going to reboot will be a proxy-DR for all the downstream VLANs.
3. After the interface role change, each multicast flow in the hardware is changed simultaneously in both the DR and proxy-DR based on the new roles they have taken. The new DR converts bridge entries to route entries and the proxy-DR converts route entries to bridge entries in the hardware.

The wait times for the primary upgrade before multicast graceful shutdown process starts are listed below:

Number of MRoutes	Timer value
0	0
< 1024	120 seconds
< 2048	150 seconds
< 4096	210 seconds

Number of MRoutes	Timer value
< 8192	300 seconds
< 16284	360 seconds
> 16384	480 seconds

The recommended configurations for graceful shutdown are as follows:

1. The multicast graceful shutdown is applicable only to the topologies which are supported for the PIM active-active solution. Other topologies will experience multicast traffic loss during a VSX software upgrade.
2. The robustness timer for IGMP/MLD protocol should be increased. The robustness timer helps to increase the expiration time of IGMP/MLD joins. This is needed during VSX device reboot so that joins don't expire. The configured value depends on how much time the VSX device reboot takes. If the robustness value is configured at the maximum value of 8, then the expiration time of multicast joins can increase up to 16 minutes with default query-interval. Use the below command to configure robustness timer:

   ```
   switch(config-if)#ip igmp robustness <2-7>
   ```

3. If OSPF v2/v3 is enabled, it is recommended not to configure the VSX device as OSPF v2/v3 DR for any of the interfaces. Use following commands to configure the other routers as DR for an interface:

   ```
   ip ospf priority <0-255>
   ipv6 ospfv3 priority <0-255>
   ```

4. If BGP is enabled, it is recommended to increase BGP graceful restart timer for every BGP-enabled interface. The recommended value of BGP graceful restart timer should be the same as the wait time in the primary before the multicast graceful shutdown process starts. Refer to the table in previous section which mentions the wait times. Use following command to reconfigure the BGP graceful restart timer:

   ```
   bgp graceful restart restart-time <1-3600>
   ```

PIM Active-Active configuration is not recommended when downstream connectivity is not via MCLAG.

FAQ and best practices

Though both DR and Proxy DR router receive the data from the source, only the DR router forwards the streams to the outgoing interface list. Since the outgoing interface list is a shared SVI between VSX pairs, the ProxyDR router also receives a copy of the stream via ISL link on the same outgoing VLANs. Thus the ProxyDR router creates a bridge entry for all these flows with the incoming interface as that of the same downstream host VLANs. If there are many client VLANs that subscribe to the same streams, the ProxyDR router will create a bridge entry on all those client VLANs. This is one of the reasons for the overall scale to go down in an Active-Active setup.

When Active-Active is configured, DR priority is internally used for its pre-empting functionality and a user-configured DR priority will not take effect. Therefore, it is not recommended to modify DR priority on the host VLANs when PIM Active-Active is configured.

PIM Active-Active is designed to improve the failover time where the multicast clients are located and hence it is only limited to those SVI where IGMP (ip igmp) is enabled and member of MCLAG. PIM Active-Active functionality, like the DR and ProxyDR roles, are only applicable on these VLANs.

In a PIM Active-Active solution more than one ProxyDR is not supported as that would cause additional bandwidth to fetch the source traffic to all Proxy DR routers. If the protocol detects more than one neighbor on the client SVIs (IGMP enabled) an error will be logged. Therefore, it is not a supported configuration.

RMON LOG: `More than one PIM Neighbor detected on Active-Active interface %s. Configuration not supported.`

As explained above PIM Active-Active solution assumes that there are two PIM routers in the host connected SVI segment, where one takes the DR and other the Proxy DR role. If it detects more than one neighbor on those SVIs an error will be logged and traffic outages can be seen. Therefore, it is not a recommended configuration.

RMON LOG: `More than one PIM Neighbor detected on Active-Active interface %s. Configuration not supported.`

PIM active-active is supported on multi-tier VSX deployments, however it must be noted that the feature is required to be only enabled on the VSX tier where IGMP clients are connected. Also it is not advisable to enable IGMP (ip igmp) on the infrastructure links which connect the VSX tiers together. If IGMP is enabled on those inter VSX links, PIM detects multiple neighbors and throws a warning.

It is recommended to configure a non-PIM Active-Active router as RP or BSR. The guidelines for RP are explained in the RP section above.

The Proxy DR router can detect MM failover and will take up the DR role when MM failover happens. The failed router then becomes the ProxyDR router.

Though PIM Active-Active is enabled from the VRF's context, the SVIs that it picks to run are based on the following criteria. If any of the conditions is not met, active-active will not run on them.

- PIM-SM must be enabled on the SVI.
- SVI should be a member VLAN of one of the MCLAG links.
- IGMP (ip igmp enable) must be enabled on the SVI.

We are working on a command to manually change the DR Role. It should be available on the newer releases.

PIM Active-Active does not guarantee RP redundancies. This is primarily used for downstream host redundancy when VSX is used as an L3-L2 split. This should not be confused with Active Forwarding for Unicast.

As mentioned in previous sections PIM Active-Active minimizes the traffic loss when the DR is down or there is a role change. It does not guarantee a zero traffic loss for multicast but reduces the downtime from 105

seconds to 2-3 seconds.

PIM-DM does not have a concept of DR and works in flood-prune manner. PIM-DM is not expected to be enabled on a VSX topology. PIM Active-Active is not supported for PIM-DM.

The PIM Active-Active feature is applicable only to last hop routers where IGMP joins are present; therefore, ideally it should not be enabled on any other intermediate routers.

General recommendations

- PIM Active/Active configuration is recommended for multicast clients connected to downstream VSX LAGs. PIM Active/Active does not provide DR redundancy for downstream receivers connected over ROP or sub-interfaces (i.e. multicast traffic impact when DR fails).
- When RP is configured on a VSX, anycast RP with MSDP is recommended. For BSR/C-RP, a PIM peering over a point-to-point transit VLAN between VSX devices is needed. In case of BSR/C-RP, convergence time is higher than anycast RP configuration when active RP fails.

PIM-SM commands for IPv4

Only the default VRF is supported on the Aruba 6200 Switch Series.

accept-register access-list

```
accept-register access-list <ACL-RULE>
no accept-register access-list <ACL-RULE>
```

Description

Configures ACL on RP to filter PIM Register packets from unauthorized sources. The ACL specified will contain the (S,G) traffic in register packets to permitted or denied.

The `no` form of this command removes the currently configured ACL rule.

Parameters

<ACL-RULE>

Specifies the ACL rule name.

Usage

When register ACL is associated with a PIM Router, PIM protocol will store the source and destination address details along with the action (permit or deny). If there are any existing flows, the user will need to disable and enable PIM on the interface to apply the ACL.

Upon receiving the register messages, a look up is made to check if the S and G in the packet is in the permitted list. If there is no match or if there is a deny rule match, a register stop message is immediately sent and the packet is dropped and no further action is taken. Permitted packets will go through the normal flow.

Loopback interfaces are special interfaces where only unicast PIM messages are updated. This includes Register, Register Stop, and Candidate RP Advertisements.

When a loopback interface is configured as the RP, the ACL drop counters will be updated on the interface on which the packets are received.

Examples

Configuring ACL on RP with an ACL rule named `pim_reg_acl`:

```
switch(config)# access-list ip pim_reg_acl
switch(config-acl-ip)# 10 permit any 20.1.1.1 225.1.1.2
switch(config-acl-ip)# 20 deny any 30.1.1.1 225.1.1.3
switch(config)# router pim
switch(config-pim)# accept-register access-list pim_reg_acl
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config-pim	Administrators or local user group members with execution rights for this command.

accept-rp

```
accept-rp <IP-ADDR> access-list <ACL-RULE>
no accept-rp <IP-ADDR> access-list <ACL-RULE>
```

Description

Enables PIM router to filter PIM join/prune messages destined for a specific RP and specific groups. The ACL specifies the group addresses which are allowed or denied. Up to 8 RP addresses and group ACL can be associated with the PIM router.

The `no` form of this command removes the currently configured ACL rule.

Parameters

<IP-ADDR>

Specifies the IPv4 address of the static RP. Format: A.B.C.D

<ACL-RULE>

Specifies the ACL rule name.

Usage

PIM will store the accepted RP address and the associated group ACL. When a join or prune message is received, a RP look up is made for the packet. If the RP is in the configured list and if the group in the join/prune packet is allowed in the ACL, the packet is allowed. Otherwise the packet is dropped.

To allow join/prune message from any groups, group address in the ACL can be wild-carded. In this case, only RP address check is performed.

This command impacts only (*,G) join/prune messages. If there are any existing flows, the user will need to disable and enable PIM on the interface to apply the ACL.

Loopback interfaces are special interfaces where only unicast PIM messages are updated. This includes Register, Register Stop, and Candidate RP Advertisements.

When a loopback interface is configured as the RP, the ACL drop counters will be updated on the interface on which the packets are received.

If there is an active flow which is in the SPT, the traffic flow through the SPT will continue. Only (*,G) join/prune messages are dropped. (S,G) join/prune messages will not be impacted.

Examples

Configuring ACL on a RP with an ACL rule named `pim_rp_grp_acl` to filter join/prune messages:

```
switch(config)# access-list ip pim_rp_grp_acl
switch(config-acl-ip)# 10 permit any any 225.1.1.2/255.255.255.0
switch(config-acl-ip)# 20 permit any any 239.1.1.2/255.255.255.0
switch(config)-acl-ip# router pim
switch(config-pim)# accept-rp 30.1.1.1 access-list pim_rp_grp_acl
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	`config-pim`	Administrators or local user group members with execution rights for this command.

active-active

```
active-active
no active-active
```

Description

Enables the PIM active-active mechanism per VRF on VSX. The default is disabled.

The `no` form of this command disables the PIM active-active mechanism.

Usage

PIM active-active keeps the multicast forwarding state synchronized on both VSX peer devices. Synchronization is achieved by electing the VSX peer that has the highest IP address as a designated router (DR) and the other as Proxy-DR.

If you want the multicast traffic to flow through VSX primary, assign higher IP addresses to the interfaces in VSX primary. When the VSX peer that is acting as the DR goes down, traffic is recovered faster since the multicast routes are synchronized.

Recommendations:

- Do not configure the DR priority of interfaces when `active-active` is enabled. The DR priority will be set to high on DR and default on Proxy-DR and any user-configured DR priority will be ignored.
- Always configure `keepalive` between VSX peers. If the ISL goes down when `keepalive` is not configured, both VSX peers start acting independently as DRs, resulting in duplicate traffic.
- Do not configure IGMP joins on transit VLANS.
- RP redundancy is not supported on the `active-active` mechanism. If one of the VSX peers is configured as RP and it goes down, the new traffic flows will not be converged until the RP is elected. For a static RP, new flows will never be converged until the VSX peer is back up.

Examples

Enabling the PIM active-active mechanism:

```
switch(config)# router pim
switch(config-pim)# active-active
```

Disabling the PIM active-active mechanism:

```
switch(config)# router pim
switch(config-pim)# no active-active
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	`config-pim`	Administrators or local user group members with execution rights for this command.

bfd all-interfaces

Not supported on the Aruba 6200 Switch Series.

```
bfd all-interfaces
no bfd all-interfaces
```

Description

Enables BFD on all PIM interfaces. BFD can be disabled at individual PIM interface using the `ip pim-sparse bfd disable` command.

The `no` form of this command disables BFD for all the interfaces.

Examples

Enabling and disabling BFD on all PIM interfaces:

```
switch(config)# router pim
switch(config-pim)# bfd all-interfaces
switch(config-pim)# no bfd all-interfaces
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config-pim	Administrators or local user group members with execution rights for this command.

bsr-candidate bsm-interval

```
bsr-candidate bsm-interval <INTERVAL-VALUE>
no bsr-candidate bsm-interval
```

Description

Configures the interval in seconds to send periodic RP-Set messages to all PIM-SM interfaces on a router that operates as the BSR in a domain. This setting must be smaller than the `rp-candidate hold-time` settings (range of 30 to 255; default 150) configured in the RPs operating in the domain.

The `no` form of this command removes the currently configured value and sets it to the default of 60 seconds.

Parameters

<INTERVAL-VALUE>

Specifies the BSR-candidate BSM interval in seconds. Default: 60 seconds. Range: 5-300.

Example

Configuring and removing BSR-candidate BSM-interval:

```
switch(config)# router pim
switch(config-pim)# bsr-candidate bsm-interval 150
switch(config-pim)# no bsr-candidate bsm-interval
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	`config-pim`	Administrators or local user group members with execution rights for this command.

bsr-candidate hash-mask-length

```
bsr-candidate hash-mask-length <LENGTH-VALUE>
no bsr-candidate hash-mask-length
```

Description

Controls the distribution of multicast groups among the C-RP, in a domain where there is overlapping coverage of the groups among the RPs. This value specifies the length (number of significant bits) when allocating this distribution. A longer hash-mask-length results in fewer multicast groups, for each block of group addresses assigned to the RPs. Multiple blocks of addresses assigned to each C-RP results in wider dispersal of addresses. Includes enhanced load-sharing for the multicast traffic for the different groups that are used in the domain at the same time.

The `no` form of this command removes currently configured value and sets to the default of 30.

Parameters

<LENGTH-VALUE>

Specifies the length (in bits) of the hash mask. Default: 30. Range: 1-32.

Example

Configuring and removing the BSR-candidate hash-mask-length:

```
switch(config)# router pim
switch(config-pim)# bsr-candidate hash-mask-length 4
switch(config-pim)# no bsr-candidate hash-mask-length
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config-pim	Administrators or local user group members with execution rights for this command.

bsr-candidate priority

```
bsr-candidate priority <PRIORITY-VALUE>
no bsr-candidate priority
```

Description

Configures the priority to apply to the router when a BSR election process occurs in the PIM-SM domain. The candidate with the highest priority becomes the BSR for the domain. If the highest priority is shared by multiple routers, the candidate having the highest IP address becomes the BSR of the domain. Zero (0) is the lowest priority. To make BSR selection easily predictable, use this command to assign a different priority to each candidate BSR in the PIM-SM domain.

The `no` form of this command removes currently configured value and sets to the default of 0.

Parameters

<PRIORITY-VALUE>

Specifies the priority for the Candidate Bootstrap router. Default: 0. Range: 0-255

Example

Configuring and removing the BSR-candidate priority:

```
switch(config)# router pim
switch(config-pim)# bsr-candidate priority 250
switch(config-pim)# no bsr-candidate priority
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config-pim	Administrators or local user group members with execution rights for this command.

bsr-candidate source-ip-interface

```
bsr-candidate source-ip-interface <INTERFACE-NAME>
no bsr-candidate source-ip-interface <INTERFACE-NAME>
```

Description

Configures the router to advertise itself as a candidate PIM-SM BSR on the interface specified, and enables BSR candidate operation. The result makes the router eligible to be elected as the BSR for the PIM-SM domain in which it operates. One BSR candidate interface is allowed per-router.

The `no` form of this command removes the Candidate BSR configuration.

Parameters

<INTERFACE-NAME>

Specifies the interface to use as a source for Candidate-BSR router IP address. Interface can be a VLAN interface (such as vlan15) or routed interfaces (such as lag 1 or 1 / 1 / 19). PIM-SM must be enabled on this interface (use the `ip pim-sparse enable` command).

Example

On the 6400 Switch Series, interface identification differs.

Configuring and removing the BSR-candidate interface:

```
switch(config)# router pim
switch(config-pim)# bsr-candidate source-ip-interface 1/1/4
switch(config-pim)# bsr-candidate source-ip-interface vlan5
switch(config-pim)# no rp-candidate source-ip-interface 1/1/4
```

Configuring and removing sub-interface 1/1/4.10 as the BSR-candidate:

Applies only to the Aruba 6300, 6400, and 8360 Switch Series.

```
switch(config)# router pim
switch(config-pim)# bsr-candidate source-ip-interface 1/1/4.10
switch(config-pim)#
switch(config-pim)# no rp-candidate source-ip-interface 1/1/4.10
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	`config-pim`	Administrators or local user group members with execution rights for this command.

disable

`disable`

Description

Disables PIM globally on the router. PIM is disabled by default.

Using the `disable` command will cause all the multicast routes to be erased from hardware.

Example

Disabling PIM router:

```
switch(config)# router pim
switch(config-pim)# disable
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	`config-pim`	Administrators or local user group members with execution rights for this command.

enable

`enable`

Description

Enables PIM globally on the router.

Example

Enabling PIM router:

```
switch(config)# router pim
switch(config-pim)# enable
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	`config-pim`	Administrators or local user group members with execution rights for this command.

ip pim-sparse

`ip pim-sparse {enable|disable}`

Description

Enables or disables PIM-SM in the current interface. PIM-SM is disabled by default on an interface. IP address must be configured on the interface to enable PIM-SM.

Parameters

`enable`

Specifies PIM SM on the interface. IP address must be configured on the interface to enable PIM-SM.

`disable`

Disables PIM SM on the interface.

Examples

Enabling and disabling PIM-SM:

```
switch(config)# interface vlan 40
switch(config-if-vlan)# ip address 40.0.0.4/24
switch(config-if-vlan)# ip pim-sparse enable
switch(config-if-vlan)# ip pim-sparse disable
```

Configuring and disabling PIM-SM on the sub-interface:

Applies only to the Aruba 6300, 6400, and 8360 Switch Series.

```
switch(config-if)# interface 1/1/10.10
switch(config-subif)# ip add 100.100.1.1/24
switch(config-subif)# ip pim-sparse enable
switch(config-subif)# switch(config-subif)# ip pim-sparse disable
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority

6300
6400
8320
8325
8360
8400
	`config-if`
	`config-if-vlan`
	`config-lag-if`
	`config-subif`
		Administrators or local user group members with execution rights for this command.

ip pim-sparse bfd

Not supported on the Aruba 6200 Switch Series.

```
ip pim-sparse bfd [disable]
no ip pim-sparse bfd
```

Description

Configures BFD on a per-interface basis for one interface associated with the PIM process.

The `no` form of this command removes the BFD configuration on the interface and sets it to the default configuration.

If BFD is enabled globally, it will be enabled by default on all interfaces. The only exception is when it is disabled specifically on an interface using the `ip pim-sparse bfd disable` command.
If BFD is disabled globally, it will be disabled by default on all interfaces. The only exception is when it is enabled specifically on an interface using the `ip pim-sparse bfd` command.

Parameters

`disable`

Disables the BFD configuration on the interface.

Examples

Enabling the BFD configuration on the interface:

```
switch(config)# interface vlan 40
switch(config-if-vlan)# ip pim-sparse bfd
```

Removing the BFD configuration on the interface:

```
switch(config-if-vlan)# no ip pim-sparse bfd
```

Disabling the BFD configuration on the interface and overriding the global setting:

```
switch(config-if-vlan)# ip pim-sparse bfd disable
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config-if config-if-vlan	Administrators or local user group members with execution rights for this command.

ip pim-sparse dr-priority

```
ip pim-sparse dr-priority <PRIORITY-VALUE>
no ip pim-sparse dr-priority
```

Description

Changes the router priority for the designated router (DR) election process in the current interface.

A numerically higher value means a higher priority. If multiple routes share the highest priority, the router with the highest IP address is selected as the DR.

The no form of this command removes currently configured value and sets to the default of 1.

Parameters

<PRIORITY-VALUE>

Specifies the priority value to use on the interface in the DR election process. Required. Default: 1. Range: 0- to 294967295.

Examples

Configuring and removing the interface priority value:

```
switch(config)# interface vlan 40
switch(config-if-vlan)# ip pim-sparse dr-priority 4444
switch(config-if-vlan)# no ip pim-sparse dr-priority
```

Configuring and removing the interface priority value in the sub-interface:

Applies only to the Aruba 6300, 6400, and 8360 Switch Series.

```
switch(config-if)# interface 1/1/10.10
switch(config-subif)# ip pim-sparse dr-priority 1000
```

```
switch(config-subif)#
switch(config-subif)# no ip pim-sparse dr-priority
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config-if config-if-vlan config-lag-if config-subif	Administrators or local user group members with execution rights for this command.

ip pim-sparse hello-delay

```
ip pim-sparse hello-delay <DELAY-VALUE>
no ip pim-sparse hello-delay
```

Description

Configures the maximum time in seconds before the router actually transmits the initial PIM hello message on the current interface.

The no form of this command removes currently configured value and sets to the default of 5 seconds.

Parameters

<DELAY-VALUE>

Specifies the hello-delay in seconds, which is the maximum time before a triggered PIM Hello message is transmitted on this interface. Default: 5. Range: 0 to 5.

Usage

- In cases where a new interface activates connections with multiple routers. If all the connected routers sent hello packets at the same time, the receiving router could become momentarily overloaded.
- This command randomizes the transmission delay to a time between zero and the hello delay setting. Using zero means no delay. After the router sends the initial hello packet to a newly detected interface, it sends subsequent hello packets according to the current hello interval setting.

Example

Configuring and removing hello-delay interface:

```
switch(config)# interface vlan 40
switch(config-if-vlan)# ip pim-sparse hello-delay 4
switch(config-if-vlan)# no ip pim-sparse hello-delay
```

Configuring and removing hello-delay on the sub-interface:

Applies only to the Aruba 6300, 6400, and 8360 Switch Series.

```
switch(config-if)# interface 1/1/10.10
switch(config-subif)# ip pim-sparse hello-delay 4
switch(config-subif)#
switch(config-subif)# no ip pim-sparse hello-delay
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config-if config-if-vlan config-lag-if config-subif	Administrators or local user group members with execution rights for this command.

ip pim-sparse hello-interval

```
ip pim-sparse hello-interval <INTERVAL-VALUE>
no ip pim-sparse hello-interval
```

Description

Configures the frequency at which the router transmits PIM hello messages on the current interface.

The no form of this command removes the currently configured value and sets to the default of 30 seconds.

Parameters

<INTERVAL-VALUE>

Specifies the frequency at which PIM Hello messages are transmitted on this interface. Range: 5 to 300. Default: 30.

Usage

- The router uses hello packets to inform neighbor routers of its presence.
- The router also uses this setting to compute the hello holdtime, which is included in hello packets sent to neighbor routers.
- Hello holdtime tells neighbor routers how long to wait for the next hello packet from the router. If another packet does not arrive within that time, the router removes the neighbor adjacency on that interface from the PIM adjacency table, which removes any flows running on that interface.
- Shortening the hello interval reduces the hello holdtime. If they do not receive a new hello packet when expected, it changes how quickly other routers stop sending traffic to the router.

Example

Configuring and removing sparse hello-interval:

```
switch(config)# interface vlan 20
switch(config-if-vlan)# ip pim-sparse hello-interval 60
switch(config-if-vlan)# no ip pim-sparse hello-interval
```

Configuring and removing sparse hello-interval on the sub-interface:

Applies only to the Aruba 6300, 6400, and 8360 Switch Series.

```
switch(config-if)# interface 1/1/10.10
switch(config-subif)# ip pim-sparse hello-interval 60
switch(config-subif)#
switch(config-subif)# no ip pim-sparse hello-interval
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config-if config-if-vlan config-lag-if config-subif	Administrators or local user group members with execution rights for this command.

ip pim-sparse ip-addr

```
ip pim-sparse ip-addr {<IP-ADDR-VALUE> | any}
no ip pim-sparse ip-addr
```

Description

Enables the router to dynamically determine the source IP address to use for PIM-SM packets sent from the interface or to use the specific IP address.

The `no` form of this command removes the currently configured value and sets to the default of `any`.

Parameters

<IP-ADDR-VALUE>

Specifies an IP address as the source IP for the interface.

`any`

Specifies dynamically determining the source IP from the current IP address of the interface.

Examples

Configuring and removing source IP address:

```
switch(config)# interface vlan 40
switch(config-if-vlan)# ip pim-sparse ip-addr 40.0.0.4
switch(config-if-vlan)# no ip pim-sparse ip-addr
```

Configuring and removing source IP address on the sub-interface:

Applies only to the Aruba 6300, 6400, and 8360 Switch Series.

```
switch(config-if)# interface 1/1/10.10
switch(config-subif)# ip pim-sparse ip-addr 10.0.0.1
switch(config-subif)#
switch(config-subif)# no ip pim-sparse ip-addr
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority

6300
6400
8320
8325
8360
8400
	`config-if`
	`config-if-vlan`
	`config-lag-if`
	`config-subif`
		Administrators or local user group members with execution rights for this command.

ip pim-sparse lan-prune-delay

```
ip pim-sparse lan-prune-delay
no ip pim-sparse lan-prune-delay
```

Description

Enables the LAN prune delay option on the current interface. The default is enabled.

With LAN-prune-delay enabled, the router informs downstream neighbors how long it will wait before pruning a flow after receiving a prune request. Other downstream routers on the same interface must send a join to override the prune before the LAN-prune-delay time to continue the flow. Prompts any downstream neighbors with multicast receivers continuing to belong to the flow to reply with a join. If no joins are received after the LAN-prune-delay period, the router prunes the flow. The propagation-delay and override-interval settings determine the LAN-prune-delay setting.

The `no` form of this command disables the LAN prune delay option.

Example

Enabling and disabling the LAN prune delay:

```
switch(config)# interface vlan 40
switch(config-if-vlan)# ip pim-sparse lan-prune-delay
switch(config-if-vlan)# no ip pim-sparse lan-prune-delay
```

Enabling and disabling the LAN prune delay on the sub-interface:

Applies only to the Aruba 6300, 6400, and 8360 Switch Series.

```
switch(config-if)# interface 1/1/10.10
switch(config-subif)# no ip pim-sparse lan-prune-delay
switch(config-subif)#
switch(config-subif)# ip pim-sparse lan-prune-delay
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config-if config-if-vlan config-lag-if config-subif	Administrators or local user group members with execution rights for this command.

ip pim-sparse override-interval

```
ip pim-sparse override-interval <INTERVAL-VALUE>
no ip pim-sparse override-interval
```

Description

Configures the override interval that gets inserted into the Override Interval field of a LAN Prune Delay option.

The no form of this command removes the currently configured value and sets the value to the default of 2500 ms.

Parameters

<INTERVAL-VALUE>

Specifies the override interval of a LAN Prune Delay option in ms. Range: 500 to 6000. Default: 2500.

Usage

A router sharing a VLAN with other multicast routers uses the override-interval value along with the propagation-delay value to compute the lan-prune-delay setting. The setting specifies how long to wait for a PIM-SM join after receiving a prune packet from downstream for a particular multicast group.

Example scenario:

A network may have multiple routers sharing VLAN X. When an upstream router is forwarding traffic from multicast group X to VLAN Y, if one of the routers on VLAN Y does not want this traffic, it issues a prune response to the upstream neighbor. The upstream neighbor then goes into a prune pending state for group X on VLAN Y. During this period, the upstream neighbor continues to forward the traffic. During the pending period, another router on VLAN Y can send a group X join to the upstream neighbor. If this happens, the upstream neighbor drops the prune pending status and continues forwarding the traffic. But if no routers on the VLAN send a join, the upstream router prunes.

Example

Configuring and removing the override interval:

```
switch(config)# interface vlan 40
switch(config-if-vlan)# ip pim-sparse override-interval 4000
switch(config-if-vlan)# no ip pim-sparse override-interval
```

Configuring and removing the override interval on the sub-interface:

Applies only to the Aruba 6300, 6400, and 8360 Switch Series.

```
switch(config-if)# interface 1/1/10.10
switch(config-subif)# ip pim-sparse override-interval 4000
switch(config-subif)#
switch(config-subif)# no ip pim-sparse override-interval
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config-if config-if-vlan config-lag-if config-subif	Administrators or local user group members with execution rights for this command.

ip pim-sparse propagation-delay

```
ip pim-sparse propagation-delay <DELAY-VALUE>
no ip pim-sparse propagation-delay
```

Description

Configures the propagation delay that gets inserted into the LAN prune delay field of a LAN Prune Delay option.

The no form of this command removes currently configured value and sets to the default of 500 ms.

Parameters

<DELAY-VALUE>

Specifies the propagation delay value in ms. Range: 250 to 2000. Default: 500.

Examples

Configuring and removing the propagation delay:

```
switch(config)# interface vlan 40
switch(config-if-vlan)# ip pim-sparse propagation-delay 400
switch(config-if-vlan)# no ip pim-sparse propagation-delay
```

Configuring and removing the propagation delay on the sub-interface:

Applies only to the Aruba 6300, 6400, and 8360 Switch Series.

```
switch(config-if)# interface 1/1/10.10
switch(config-subif)# ip pim-sparse propagation-delay 400
switch(config-subif)#
switch(config-subif)# no ip pim-sparse propagation-delay
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config-if config-if-vlan config-lag-if config-subif	Administrators or local user group members with execution rights for this command.

join-prune-interval

```
join-prune-interval <INTERVAL-VALUE>
no join-prune-interval
```

Description

Configures the frequency at which the router will send periodic join or prune-interval messages.

The no form of this command sets the interval to the default value of 60 seconds.

Parameters

<INTERVAL-VALUE>

Specifies the join-prune-interval in seconds. Range 5 to 65535 Default: 60.

Examples

Configuring join prune interval:

```
switch(config)# router pim
switch(config-pim)# join-prune-interval 400
switch(config-pim)# no join-prune-interval
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config-pim	Administrators or local user group members with execution rights for this command.

multicast-route-limit

```
multicast-route-limit <limit>
no multicast-route-limit <limit>
```

Description

Configures the limit on the maximum number of multicast route entries that can be programmed. When the limit is configured, multicast route entries created because of IGMP or MLD membership reports, and multicast route entries created because of multicast streams are restricted to the configured limit.

The no form of this command removes the currently configured limit value.

Parameters

<limit>

Specifies the value to be configured as the multicast route limit. Range: 1 to 4294967295.

Usage

Flows exceeding the configured multicast route limit will be programmed as a bridge entry and will not have the outgoing interfaces list populated. This configuration prevents creation of new multicast routes when limits are reached. At the time of configuration, if the device has more multicast routes than the configured limit, existing multicast routes continue to exist until they are removed.

The flows are programmed in the HW on a FCFS basis. There could be scenarios where the flow is forwarded in neighbor router, but it may not be forwarded on the current router because of exceeding the limits configured on the current router. In such cases, it is recommended to configure higher limits to avoid traffic outage.

Examples

Configuring and removing the multicast route rate limit:

```
switch(config)# router pim
switch(config-pim)# multicast-route-limit 1024
switch(config-pim)# no multicast-route-limit
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config-pim	Administrators or local user group members with execution rights for this command.

no ip pim-sparse

```
no ip pim-sparse
```

Description

Removes all the PIM-SM related configurations for the interface.

Example

Removing PIM-SM configuration:

```
switch(config)# interface vlan 40
switch(config-if-vlan)# no ip pim-sparse
```

Removing PIM-SM configuration on the sub-interface:

Applies only to the Aruba 6300, 6400, and 8360 Switch Series.

```
switch(config)# interface 1/1/10.10
switch(config-subif)# no ip pim-sparse
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config-if config-if-vlan config-lag-if config-subif	Administrators or local user group members with execution rights for this command.

register-rate-limit

```
register-rate-limit <limit>
no register-rate-limit <limit>
```

Description

Configures the limit on the maximum number of register messages sent per second for every unique (S,G) entry. By default, there is no maximum rate set. When the limit is configured, register messages generation is limited to the configured value.

The no form of this command removes the currently configured limit value.

Parameters

<limit>

Specifies the value to be configured as the register rate limit. Range: 1 to 4294967295.

Examples

Configuring and removing the register rate limit:

```
switch(config)# router pim
switch(config-pim)# register-rate-limit 10
switch(config-pim)# no register-rate-limit
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config-pim	Administrators or local user group members with execution rights for this command.

router pim

```
router pim [vrf <VRF-NAME>]
no router pim [vrf <VRF-NAME>]
```

Description

Changes the current context to the PIM configuration context. If no VRF is specified, the default VRF is assumed.

The `no` form of this command removes the PIM configuration from the specified context or the default VRF.

Parameters

`vrf <VRF-NAME>`

Specifies the name of a VRF.

Examples

Configuring default router PIM:

```
switch(config)# router pim
switch(config-pim)#
```

Configuring specified router PIM:

```
switch(config)# router pim vrf green
switch(config-pim)#
```

Removing router PIM:

```
switch(config)# no router pim
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Administrators or local user group members with execution rights for this command.

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config	

rp-address

```
rp-address <IP-ADDR> [<GRP-ADDR/GRP-MASK>] [override]
no rp-address <IP-ADDR> [<GRP-ADDR/GRP-MASK>] [override]
```

Description

Statically configures the router as the RP for a specified multicast group or range of multicast groups. This must be configured on all PIM-SM routers in the domain. If group address is not specified, it applies to all

IPv4 multicast addresses (224.0.0.0 - 239.255.255.255). PIM-SM supports a maximum of 8 static RPs per VRF.

The `no` form of this command removes static RP configuration and its precedence.

Parameters

<IP-ADDR>

Specifies the address of the static RP in IPv4 format (`x.x.x.x`), where `x` is a decimal number from 0 to 255.

<GRP-ADDR>

Specifies the multicast group address in IPv4 format (`x.x.x.x`), where `x` is a decimal number from 0 to 255.

<GRP-MASK>

Specifies the address mask in CIDR format (`x`), where `x` is a decimal number from 0 to 128.

`override`

Specifies higher precedence to static RP over Candidate RP.

Usage

Where a static RP and a C-RP are configured to support the same multicast groups and the multicast group mask for the static RP is equal to or greater than the same mask for the applicable C-RPs, this command assigns the higher precedence to the static RP, resulting in the C-RP operating only as a backup RP for the configured group. Without override, the C-RP has precedence over a static RP configured for the same multicast group or groups.

Examples

```
switch(config)# router pim
switch(config-pim)# rp-address 40.0.0.4 230.0.0.4/24 ovverride
switch(config-pim)# rp-address 40.0.0.8 222.0.0.4/24
switch(config-pim)# no rp-address 40.0.0.4 230.0.0.4/24
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	`config-pim`	Administrators or local user group members with execution rights for this command.

rp-candidate group-prefix

`rp-candidate group-prefix <GRP-ADDR/GRP-MASK>`
`no rp-candidate group-prefix <GRP-ADDR/GRP-MASK>`

Description

Adds multicast group address to the current Candidate Rendezvous Point (C-RP) configuration.

The `no` form of this command removes C-RP multicast group address.

Parameters

<GRP-ADDR>

Specifies the multicast group address in IPv4 format (`x.x.x.x`), where `x` is a decimal number from 0 to 255.

<GRP-MASK>

Specifies the address mask in CIDR format (`x`), where `x` is a decimal number from 0 to 128.

Examples

Configuring and removing candidate group prefix:

```
switch(config)# router pim
switch(config-pim)# rp-candidate group-prefix 230.0.0.4/24
switch(config-pim)# no rp-candidate group-prefix 230.0.0.4/24
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	`config-pim`	Administrators or local user group members with execution rights for this command.

rp-candidate hold-time

```
rp-candidate hold-time <TIME-VALUE>
no rp-candidate hold-time
```

Description

Changes the hold-time a C-RP includes in its advertisements to the BSR.

Hold-time is included in the advertisements the C-RP periodically sends to the elected BSR for the domain. Also updates the BSR on how long to wait after the last advertisement from the reporting RP before assuming it has become unavailable.

The `no` form of this command removes the currently configured value and sets it to the default value 150 seconds.

Parameters

<TIME-VALUE>

Specifies the hold-time value in seconds to be sent in C-RP-Adv messages. Range: 30 to 250. Default: 150.

Example

Setting and removing the candidate holdtime:

```
switch(config)# router pim
switch(config-pim)# rp-candidate hold-time 250
switch(config-pim)# no rp-candidate hold-time
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config-pim	Administrators or local user group members with execution rights for this command.

rp-candidate priority

```
rp-candidate priority <PRIORITY-VALUE>
no rp-candidate priority
```

Description

Changes the current priority setting for a C-RP. Where multiple C-RP configurations are used to support the same multicast groups, the candidate having the highest priority is elected. Zero (0) is the highest priority, and 255 is the lowest priority.

The no form of this command removes the currently configured value and sets it to the default of 192.

Parameters

<PRIORITY-VALUE>

Specifies the priority value for the Candidate-RP router. Range: 0 to 255. Default: 192.

Example

Configuring and removing candidate priority:

```
switch(config)# router pim
switch(config-pim)# rp-candidate priority 250
switch(config-pim)# no rp-candidate priority
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config-pim	Administrators or local user group members with execution rights for this command.

rp-candidate source-ip-interface

```
rp-candidate source-ip-interface <INTERFACE-NAME> [group-prefix <GRP-ADDR/GRP-MASK>]
no rp-candidate source-ip-interface <INTERFACE-NAME> [group-prefix <GRP-ADDR/GRP-MASK>]
```

Description

Enables the Candidate Rendezvous Point (C-RP) operation, and configures the router to advertise itself as a C-RP to the Bootstrap Router (BSR) for the current domain.

This step includes the option to allow the C-RP to be a candidate for all possible multicast groups, or for up to four multicast groups, or ranges of groups. If group-prefix is not given, it considers for all multicast group addresses.

The `no` form of this command removes the C-RP configuration.

Parameters

<INTERFACE-NAME>

Specifies the interface to use as a source for the C-RP router IP address.

<GRP-ADDR>

Specifies the multicast group address in IPv4 format (`x.x.x.x`), where `x` is a decimal number from 0 to 255.

<GRP-MASK>

Specifies the address mask in CIDR format (`x`), where `x` is a decimal number from 0 to 128.

Examples

Configuring and removing candidate source IP interface:

```
switch(config)# router pim
switch(config-pim)# rp-candidate source-ip-interface vlan40 group-prefix
230.0.0.4/24
switch(config-pim)# no rp-candidate source-ip-interface vlan20
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config-pim	Administrators or local user group members with execution rights for this command.

rpf-override

```
rpf-override <SRC-ADDR/SRC-MASK> <RPF-ADDR|INTERFACE-NAME>
no rpf-override <SRC-ADDR/SRC-MASK> <RPF-ADDR|INTERFACE-NAME>
```

Description

The Reverse Path Forward (RPF) override, allows overriding the normal RPF lookup mechanism, and indicates to the router that it may accept multicast traffic on an interface other than the one that the RPF lookup mechanism would normally select. This includes accepting traffic from an invalid source IP address for the subnet or VLAN that is directly connected to the router. Traffic may also be accepted from a valid PIM neighbor that is not on the reverse path towards the source of the received multicast traffic.

The `no` form of this command removes currently configured RPF entry.

Parameters

<SRC-ADDR/SRC-MASK>

Specifies the multicast source IPv4 address in IPv4 format (`x.x.x.x`), where `x` is a decimal number from 0 to 255. And the number of bits in the address mask in CIDR format (`x`), where `x` is a decimal number from 0 to 128.

<RPF-ADDR>

Specifies the RPF address in IPv4 format (`x.x.x.x`), where `x` is a decimal number from 0 to 255.

<INTERFACE-NAME>

Specifies the RPF interface name.

Usage

- Reverse Path Forward (RPF) checking is a core multicast routing mechanism. The RPF ensures that the multicast traffic received arrives on the expected router interface before further processing. If the RPF check fails for a multicast packet, the packet is discarded. For multicast traffic flow that arrives on the SPT, the expected incoming interface for a given source or group is the interface towards the source address of the traffic (determined by the unicast routing system). For traffic arriving on the RP tree, the expected incoming interface is the interface towards the RP.
- RPF checking is applied to all multicast traffic and is significant in preventing network loops. Up to eight manual RPF overrides can be specified. The RPF-address indicates one of two distinct RPF candidates:
  1. A valid PIM neighbor address from which forwarded multicast traffic is accepted with a source address of *<source-addr/src-mask>*.
  2. A local router address on a PIM-enabled interface to which *<source-addr/src-mask>* is directly connected. If configured, the local router will assume the role of DR for this flow and registers the flow with an RP.

Example

Configuring and removing RPF override:

```
switch(config)# router pim
switch(config-pim)# rpf-override 40.0.0.4/24 30.0.0.4
switch(config-pim)# no rpf-override 40.0.0.4/24 30.0.0.4
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config-pim	Administrators or local user group members with execution rights for this command.

show ip mroute

```
show ip mroute [all-vrfs | vrf <VRF-NAME>] [vsx-peer]
```

Description

Shows multicast routing information. Optionally, you can show specific information by VRF. If no options are specified, it shows information for the default VRF.

Parameters

`all-vrfs`

Shows mroute information for all VRFs.

`vrf <VRF-NAME>`

Specifies the name of a VRF. Default: default.

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing IP mroute for all VRFs:

```
switch# show ip mroute  all-vrfs
VRF : blue
Total number of entries : 1

Group Address           : 239.1.1.1
Source Address          : 40.0.0.5
Incoming interface      : vlan3
Downstream Interface
Interface   State
---------   -----
```

```
vlan2       forwarding

VRF : green
Total number of entries : 2

Group Address           : 239.1.1.1
Source Address          : 40.0.0.4
Neighbor                : 10.1.1.1
Incoming interface      : vlan2
Downstream Interface
Interface   State
---------   -----
vlan5       forwarding

Group Address           : 239.1.1.1
Source Address          : 40.0.0.5
Neighbor                : 10.1.1.2
Incoming interface      : vlan1
Downstream Interface
Interface   State
---------   -----
vlan6       forwarding

VRF : default
Total number of entries : 1

Group Address           : 10.1.1.14
Source Address          : 40.0.0.6
Neighbor                : 10.1.1.2
Incoming interface      : 1/1/5
Downstream Interface
Interface   State
---------   -----
1/1/3       forwarding
1/1/1       pruned
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip mroute brief

`show ip mroute brief [al-vrfs | vrf <VRF-NAME>] [vsx-peer]`

Description

Shows brief version of the multicast routing information. Optionally, you can specify the display information by VRF. If no options are specified, it shows information for the default VRF.

Parameters

`all-vrfs`

Shows mroute information briefly for all VRFs.

`vrf <VRF-NAME>`

Specifies the name of a VRF. Default: default.

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing the IP mroute brief:

```
switch# show ip mroute  brief
VRF : default
Total number of entries : 1

Group Address      Source Address     Neighbor          Interface
-------------      --------------     --------          ---------
239.1.1.1          40.0.0.6           10.1.1.2          vlan5
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip mroute group-addr

`show ip mroute <GROUP-ADDR> [<SOURCE-ADDR>] [all-vrfs | vrf <vrf-name>] [vsx-peer]`

Description

Shows the multicast routing information for the given group address. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameters

`<GROUP-ADDR>`

Specifies a group address in IPv4 format (`x.x.x.x`), where `x` is a decimal number from 0 to 255.

<SOURCE-ADDR>

Specifies show information for the group from this source in IPv4 format (`x.x.x.x`), where `x` is a decimal number from 0 to 255.

`all-vrfs`

Shows mroute information for the group for all VRFs.

`vrf` *<VRF-NAME>*

Specifies the name of a VRF.

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing information for group 239.1.1.1 and VRF green:

```
switch# show ip mroute 239.1.1.1 vrf green

VRF : green

Group Address                 : 239.1.1.1
Source Address                : 40.0.0.5
Neighbor                      : 10.1.1.2
Incoming interface            : vlan1
Unicast Routing Protocol      : connected
Metric                        : 1234
Metric  Pref                  : 1234
Downstream Interface
Interface   State
---------   -----
vlan6       forwarding
```

Showing information for group 239.1.1.1 from source 40.0.0.5 and all VRFs:

```
switch# show ip mroute 239.1.1.1 40.0.0.5 all-vrfs

VRF : blue

Group Address                 : 239.1.1.1
Source Address                : 40.0.0.5
Incoming interface            : vlan3
Unicast Routing Protocol      : connected
Metric                        : 1234
Metric  Pref                  : 1234
Downstream Interface
Interface   State
---------   -----
vlan2       forwarding


VRF : green

Group Address                 : 239.1.1.1
Source Address                : 40.0.0.5
Neighbor                      : 10.1.1.2
Incoming interface            : vlan1
Unicast Routing Protocol      : connected
Metric                        : 1234
```

```
Metric  Pref                  : 1234
Downstream Interface
Interface   State
---------   -----
vlan6       forwarding
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip pim

`show ip pim [all-vrfs | vrf <VRF-NAME>] [vsx-peer]`

Description

Shows the PIM router information. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameters

`all-vrfs`

Shows PIM router information on all VRFs.

`vrf <VRF-NAME>`

Specify the name of a VRF. Default: default.

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing IP PIM router:

```
switch# show ip pim

PIM Global Parameters

VRF                          :  default
PIM Status                   :  enable
SPT Threshold                :  enabled
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip pim bsr

```
show ip pim bsr [all-vrfs | vrf <VRF-NAME>] [vsx-peer]
```

Description

Shows the information about BSR candidates in the domain and multicast groups it supports. Optionally, you can specify the display information by VRF. If no options are specified, it shows information for the default VRF.

Parameters

`all-vrfs`

Optional. Shows PIM candidate BSR information for all VRFs.

`vrf <VRF-NAME>`

Optional. Shows PIM candidate BSR information for a particular VRF. If the *<VRF-NAME>* is not specified, it shows information for the default VRF.

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing information about BSR candidates:

```
switch# show ip pim bsr all-vrfs

Status and Counters- PIM-SM Bootstrap Router Information

VRF                         : default
E-BSR Address               : 10.0.0.1
E-BSR Priority              : 0
E-BSR Hash Mask Length      : 30
E-BSR Up Time               : 3000 secs
Next Bootstrap Message      : 80 secs

C-BSR Admin Status          : This system is a Candidate-BSR
C-BSR Address               : 2.2.2.2/24
```

```
C-BSR Priority            : 34
C-BSR Hash Mask Length    : 30
C-BSR Message Interval    : 76
C-BSR Source IP Interface : vlan10

C-RP Admin Status         : This system is a Candidate-RP
C-RP Address              : 2.2.2.2
C-RP Hold Time            : 150
C-RP Advertise Period     : 60
C-RP Priority             : 192
C-RP Source IP Interface  : vlan10

Group Address    Group Mask
---------------  ---------------
226.2.2.2        255.255.255.255
228.2.2.2        255.255.255.255
232.2.2.2        255.255.255.255

VRF                       : green
E-BSR Address             : 2.2.2.2
E-BSR Priority            : 0
E-BSR Hash Mask Length    : 30
E-BSR Up Time             : 3000 secs
Next Bootstrap Message    : 80 secs

C-BSR Admin Status        : This system is a Candidate-BSR
C-BSR Address             : 2.2.2.2/24
C-BSR Priority            : 34
C-BSR Hash Mask Length    : 32
C-BSR Message Interval    : 60
C-BSR Source IP Interface : vlan10

C-RP Admin Status         : This system is a Candidate-RP
C-RP Address              : 2.2.2.2
C-RP Hold Time            : 150
C-RP Advertise Period     : 60
C-RP Priority             : 192
C-RP Source IP Interface  : vlan10

Group Address    Group Mask
---------------  ---------------
231.2.2.2        255.255.255.255
232.2.2.2        255.255.255.255
235.2.2.2        255.255.255.255
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

Platforms	Command context	Authority
8360 8400		

show ip pim bsr elected

```
show ip  pim bsr elected [all-vrfs | vrf <VRF-NAME>] [vsx-peer]
```

Description

Shows information about the elected BSR in the domain and multicast groups it supports. Optionally you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameters

`all-vrfs`

Selects all VRFs.

`vrf <VRF-NAME>`

Specifies the name of a VRF. Default: default.

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing PIM elected bootstrap router information:

```
switch# show ip pim bsr elected all-vrfs

Status and Counters- PIM-SM Elected Bootstrap Router Information

VRF                         : default
E-BSR Address               : 10.0.0.1
E-BSR Priority              : 0
E-BSR Hash Mask Length      : 30
E-BSR Up Time               : 3000 secs
Next Bootstrap Message      : 80 secs

VRF                         : green
E-BSR Address               : 20.0.0.1
E-BSR Priority              : 0
E-BSR Hash Mask Length      : 30
E-BSR Up Time               : 3000 secs
Next Bootstrap Message      : 80 secs
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip pim bsr local

```
show ip pim bsr local [all-vrfs | vrf <VRF-NAME>] [vsx-peer]
```

Description

Shows the information about BSR candidates on the local router and multicast groups it supports. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameters

`all-vrfs`

Selects all VRFs.

`vrf <VRF-NAME>`

Specifies the name of a VRF. Default: default.

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing local Candidate BSR:

```
switch# show ip pim bsr local all-vrfs

Status and Counters - PIM-SM Local Candidate-BSR Information

VRF                       : default
C-BSR Admin Status        : This system is a Candidate-BSR
C-BSR Address             : 2.2.2.2/24
C-BSR Priority            : 34
C-BSR Hash Mask Length    : 30
C-BSR Message Interval    : 76
C-BSR Source IP Interface : vlan10

VRF                       : green
C-BSR Admin Status        : This system is a Candidate-BSR
C-BSR Address             : 2.2.2.2/24
C-BSR Priority            : 34
C-BSR Hash Mask Length    : 32
C-BSR Message Interval    : 60
C-BSR Source IP Interface : vlan10
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip pim interface

```
show ip pim interface [all-vrfs | vrf <VRF-NAME>] [vsx-peer]
```

Description

Shows the information about PIM interfaces currently configured in the router. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameters

`all-vrfs`

Selects all VRFs.

`vrf <VRF-NAME>`

Specifies the name of a VRF. Default: default.

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing PIM interface:

```
switch# show ip pim interface

PIM Interfaces

VRF: default

Interface           IP Address          mode
------------------- ------------------  ----------
1/1/1               40.0.0.4/24         sparse
1/1/2               50.0.0.4/24         sparse
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip pim interface interface-name

```
show ip pim interface <INTERFACE-NAME> [vsx-peer]
```

Description

Shows detailed information about the PIM interface currently configured.

Parameters

<INTERFACE-NAME>

Specifies an interface for showing PIM interface information. Interface can also be a LAG or VLAN.

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing PIM interface information for interface 1/1/2:

```
switch# show ip pim interface 1/1/2

PIM Interfaces

VRF: default

Interface  : 1/1/2
IP Address : 50.0.0.4/24
Mode       : sparse

Designated Router :
Hello Interval (sec)  : 30
Hello Delay (sec)     : 5

Override Interval (msec)  : 2500              Lan Prune Delay     : Yes
Propagation Delay (msec)  : 500               DR Priority         : 1
Neighbor Timeout          : 105
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip pim interface interface-name counters

```
show ip pim interface <INTERFACE-NAME> counters [vsx-peer]
```

Description

Shows the PIM packet counters information for the specified interface.

Parameters

<INTERFACE-NAME>

Specifies the interface to show packet counter information.

vsx-peer

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Usage

Loopback interfaces are special interfaces where only unicast PIM messages are updated. This includes Register, Register Stop, and Candidate RP Advertisements.

When a loopback interface is configured as the RP, the ACL drop counters will be updated on the interface on which the packets are received.

Example

Showing PIM packet counters:

```
switch# show ip pim interface vlan1 counters

Interface           : vlan1
VRF                 : default

Rx Counters :

Hello                                4
State Refresh                        0
Join/Prune                           1
RPadv                                0
Graft                                0
GraftAck                             0
Assert                               0
Bsm                                  0
Register                             0
Register Stop                        0
Register Drops(Register ACL hitcount)  10
Join/Prune Drops(RP ACL hitcount)      5
```

```
Tx Counters :

Hello                9
State Refresh        0
Join/Prune           0
RPadv                0
Graft                0
GraftAck             0
Assert               0
Bsm                  0
Register             0
Register Stop        0

Invalid Rx Counters :

Hello                0
State Refresh        0
Join/Prune           0
RPadv                0
Graft                0
GraftAck             0
Assert               0
Bsm                  0
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip pim neighbor

`show ip pim neighbor [<IP-ADDR>] [all-vrfs | vrf <VRF-NAME>] [vsx-peer]`

Description

Shows PIM neighbor information. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameters

`all-vrfs`

Selects all VRFs.

`vrf <VRF-NAME>`

Specifies the name of a VRF. Default: default.

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing PIM neighbor information:

```
switch# show ip pim neighbor

PIM Neighbor

VRF                 : default
IP Address          : 40.0.0.44
Interface           : 1/1/1
Up Time (sec)       : 544
Expire Time (sec)   : 80
DR Priority         : 40
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip pim pending

`show ip pim pending [<GROUP-ADDR>] [all-vrfs | vrf <VRF-NAME>] [vsx-peer]`

Description

Shows the pending joins on a PIM router. Optionally you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Use this command to determine what flows are being requested on the PIM network. If data availability for a flow is expected, and a join for the flow is pending, the troubleshooting search moves to the source of that flow, since the routers are verified to be seeing the request for data.

Parameters

<GROUP-ADDR>

Specifies a group address in IPv4 format (`x.x.x.x`), where `x` is a decimal number from 0 to 255.

`all-vrfs`

Selects all VRFs.

`vrf <VRF-NAME>`

Specifies the name of a VRF. Default: default.

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

On the 6400 Switch Series, interface identification differs.

Showing pending PIM joins:

```
switch# show ip pim pending
Join Pending
VRF : default
   Group 234.0.20.4
       (*,G) Pending
            Incoming Interface:  1/1/32
   Group 234.0.20.5
       (*,G) Pending
            Incoming Interface:  1/2/32
   Group 234.0.20.6
       (*,G) Pending
            Incoming Interface:  1/1/32
   Group 234.0.20.7
       (*,G) Pending
            Incoming Interface:  1/1/2
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip pim rp-candidate

`show ip pim rp-candidate [all-vrfs | vrf <VRF-NAME>] [vsx-peer]`

Description

Shows the candidate RP operational and configuration information. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameters

`all-vrfs`

Selects all VRFs.

`vrf <VRF-NAME>`

Specifies the name of a VRF. Default: default.

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing PIM RP candidate:

```
switch# show ip pim rp-candidate all-vrfs

 Status and Counters- PIM-SM Candidate-RP Information

 VRF                      : Green
 C-RP Admin Status        : This system is a Candidate-RP
 C-RP Address             : 10.1.1.27
 C-RP Hold Time           : 150
 C-RP Advertise Period    : 60
 C-RP Priority            : 192
 C-RP Source IP Interface : Vlan10

 Group Address   Group Mask
 --------------- ---------------
 239.10.10.240   255.255.255.252
 236.0.0.0       255.255.255.0

 VRF                      : Red
 C-RP Admin Status        : This system is a Candidate-RP
 C-RP Address             : 20.1.1.27
 C-RP Hold Time           : 150
 C-RP Advertise Period    : 60
 C-RP Priority            : 192
 C-RP Source IP Interface : Vlan20

 Group Address   Group Mask
 --------------- ---------------
 239.10.10.240   255.255.255.252
 236.0.0.0       255.255.255.0
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip pim rp-set

```
show ip pim rp-set [all-vrfs | vrf <VRF-NAME>] [vsx-peer]
```

Description

Shows the multicast group support for both the learned C-RP assignments and any statically configured RP assignments. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameters

`all-vrfs`

Selects all VRFs.

`vrf <VRF-NAME>`

Specifies the name of a VRF. Default: default.

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing PIM RP set information:

```
switch# show ip pim rp-set all-vrfs

VRF: default

Status and Counters - PIM-SM Static RP-Set Information
Group Address    Group Mask       RP Address       Override
---------------  ---------------  ---------------  --------
233.100.128.255  255.255.255.255  100.10.10.1      Yes
238.100.128.255  255.255.255.255  100.10.10.3      Yes

Status and Counters - PIM-SM Learned RP-Set Information
Group Address    Group Mask       RP Address       Hold Time  Expire Time
---------------  ---------------  ---------------  ---------  -----------
223.2.2.34       255.0.0.0        9.0.0.25         12         0

VRF: green

Status and Counters - PIM-SM Static RP-Set Information
Group Address    Group Mask       RP Address       Override
---------------  ---------------  ---------------  --------
226.102.128.255  255.255.255.255  105.10.10.3      Yes
234.102.128.255  255.255.255.255  110.10.10.3      Yes

Status and Counters - PIM-SM Learned RP-Set Information
Group Address    Group Mask       RP Address       Hold Time  Expire Time
---------------  ---------------  ---------------  ---------  -----------
223.2.2.34       255.0.0.0        9.0.0.25         12         0
229.2.2.34       255.0.0.0        9.0.0.25         10         0
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip pim rp-set learned

```
show ip pim rp-set learned [all-vrfs | vrf <VRF-NAME>] [vsx-peer]
```

Description

Shows the multicast group support for dynamically learned RP assignments. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameters

`all-vrfs`

Selects all VRFs.

`vrf <VRF-NAME>`

Specifies the name of a VRF. Default: default.

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing PIM RP set learned information:

```
switch# show ip pim rp-set learned all-vrfs

VRF: default

Status and Counters - PIM-SM Learned RP-Set Information
Group Address    Group Mask       RP Address       Hold Time  Expire Time
---------------  ---------------  ---------------  ---------  -----------
223.2.2.34       255.0.0.0        9.0.0.25         12         0

VRF: green

Status and Counters - PIM-SM Learned RP-Set Information
Group Address    Group Mask       RP Address       Hold Time  Expire Time
---------------  ---------------  ---------------  ---------  -----------
223.2.2.34       255.0.0.0        9.0.0.25         12         0
229.2.2.34       255.0.0.0        9.0.0.25         10         0
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip pim rp-set static

```
show ip pim rp-set static [all-vrfs | vrf <VRF-NAME>] [vsx-peer]
```

Description

Shows the multicast group support for statically configured RP assignments. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameters

`all-vrfs`

Selects all VRFs.

`vrf <VRF-NAME>`

Specifies the name of a VRF. Default: default.

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing PIM Static RP set information:

```
switch# show ip pim rp-set static all-vrfs

VRF: default

Status and Counters - PIM-SM Static RP-Set Information
Group Address    Group Mask       RP Address       Override
---------------  ---------------  ---------------  --------
233.100.128.255  255.255.255.255  100.10.10.1      Yes
238.100.128.255  255.255.255.255  100.10.10.3      Yes

VRF: green

Status and Counters - PIM-SM Static RP-Set Information
Group Address    Group Mask       RP Address       Override
---------------  ---------------  ---------------  --------
226.102.128.255  255.255.255.255  105.10.10.3      Yes
234.102.128.255  255.255.255.255  110.10.10.3      Yes
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip pim rpf-override

`show ip pim rpf-override [all-vrfs | vrf <VRF-NAME>] [vsx-peer]`

Description

Shows the RPF override configuration, which can be useful information when troubleshooting potential RPF misconfigurations. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF

Parameters

`all-vrfs`

Optional. Shows PIM RPF override information for all VRFs.

`vrf <VRF-NAME>`

Optional. Shows PIM RPF override information for a particular VRF. If the *<VRF-NAME>* is not specified, it shows information for the default VRF

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

On the 6400 Switch Series, interface identification differs.

Showing PIM RPF override:

```
switch# show ip pim rpf-override all-vrfs

VRF                 : default
Static RPF Override
Multicast Source RPF IP Address
------------------- ------------------
10.0.0.2/32          1.1.1.1

VRF                 : green
Static RPF Override
Multicast Source RPF IP Address
------------------- ------------------
10.0.0.2/32          1.1.1.1
10.1.1.1/32          1.1.1.2
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip pim rpf-override source

`show ip pim rpf-override source <IP-ADDR> [all-vrfs | vrf <VRF-NAME>] [vsx-peer]`

Description

Shows the RPF override configuration for the specified source. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameters

`source <IP-ADDR>`

Specifies the RPF source address in IPv4 format (`x.x.x.x`), where `x` is a decimal number from 0 to 255.

`all-vrfs`

Selects all VRFs.

`vrf <VRF-NAME>`

Specifies the name of a VRF. Default: default.

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

On the 6400 Switch Series, interface identification differs.

Showing PIM RPF override source:

```
switch# show ip pim rpf-override source 10.0.0.2

VRF                 : default
Static RPF Override
Multicast Source RPF IP Address
------------------- ------------------
10.0.0.2             1.1.1.1
```

Showing PIM RPF override source for all VRFs:

```
switch# show ip pim rpf-override source 10.0.0.2 all-vrfs
```

```
VRF                 : default
Static RPF Override
Multicast Source RPF IP Address
------------------- ------------------
10.0.0.2             1.1.1.1

VRF                 : green
Static RPF Override
Multicast Source RPF IP Address
------------------- ------------------
10.0.0.2             1.1.1.1
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

sources-per-group

```
sources-per-group <limit>
no sources-per-group <limit>
```

Description

Configures the total number of sources allowed for a group on the router. By default, there is no limit on the number of sources for a group. When the number of sources for a group exceeds the configured limit, multicast traffic from additional sources will be dropped.

The `no` form of this command removes the currently configured limit value.

Parameters

<limit>

Specifies the value to be configured as the sources allowed per group. Range: 1 to 4294967295.

Usage

Flows exceeding the limit will be programmed as a bridge entry and will not have the outgoing interfaces list populated. This configuration does not allow new sources for the group. At the time of configuration, if the device has more sources for the given group than the configured value, already allowed sources continue to exist until they are removed.

The flows are programmed in the HW on a FCFS basis. There could be scenarios where the flow is forwarded in neighbor router, but it may not be forwarded on the current router because of exceeding the limits

configured on the current router. In such cases, it is recommended to configure higher limits to avoid traffic outage.

Examples

Configuring and removing the sources allowed per group:

```
switch(config)# router pim
switch(config-pim)# sources-per-group 4
switch(config-pim)# no sources-per-group
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config-pim	Administrators or local user group members with execution rights for this command.

spt-threshold

```
spt-threshold
no spt-threshold
```

Description

Enables the router to switch the multicast traffic flows to the shortest path tree. Default is enabled.

The no form of this command disables the routers ability to switch the multicast traffic flows to the shortest path tree.

To apply this configuration a user needs to apply disable/enable PIM globally.

Example

Enabling and disabling the SPT threshold:

```
switch(config)# router pim
switch(config-pim)# spt-threshold
switch(config-pim)# no spt-threshold
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	`config-pim`	Administrators or local user group members with execution rights for this command.

PIM-SM commands for IPv6

Only the default VRF is supported on the Aruba 6200 Switch Series.

accept-register access-list

```
accept-register access-list <ACL-RULE>
no accept-register access-list <ACL-RULE>
```

Description

Configures ACL on RP to filter PIM Register packets from unauthorized sources. The ACL specified will contain the (S,G) traffic in register packets to permitted or denied.

The `no` form of this command removes the currently configured ACL rule.

Parameters

<ACL-RULE>

Specifies the ACL rule name.

Usage

When register ACL is associated with a PIM Router, PIM protocol will store the source and destination address details along with the action (permit or deny).

Upon receiving the register messages, a look up is made to check if the S and G in the packet is in the permitted list. If there is no match or if there is a deny rule match, a register stop message is immediately sent and the packet is dropped and no further action is taken. Permitted packets will go through the normal flow.

Loopback interfaces are special interfaces where only unicast PIM messages are updated. This includes Register, Register Stop, and Candidate RP Advertisements.

When a loopback interface is configured as the RP, the ACL drop counters will be updated on the interface on which the packets are received.

Examples

Configuring ACL on RP with an ACL rule named `pim_regv6_acl`:

```
switch(config)# access-list ipv6 pim_regv6_acl
switch(config-acl-ipv6)# 10 permit any 20.::1 ff1e::1
switch(config-acl-ipv6)# 20 deny any 30::1 ff1e::3
```

```
switch(config)# router pim6
switch(config-pim6)# accept-register access-list pim_regv6_acl
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config-pim6	Administrators or local user group members with execution rights for this command.

accept-rp

```
accept-rp <IPv6-ADDR> access-list <ACL-RULE>
no accept-rp <IPv6-ADDR> access-list <ACL-RULE>
```

Description

Enables PIM router to filter PIM join/prune messages destined for a specific RP and specific groups. The ACL specifies the group addresses which are allowed or denied. Up to 8 RP addresses and group ACL can be associated with the PIM router.

The no form of this command removes the currently configured ACL rule.

Parameters

<IPv6-ADDR>

Specifies an address in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F.

<ACL-RULE>

Specifies the ACL rule name.

Usage

PIM will store the accepted RP address and the associated group ACL. When a join or prune message is received, a RP look up is made for the packet. If the RP is in the configured list and if the group in the join/prune packet is allowed in the ACL, the packet is allowed. Otherwise the packet is dropped.

To allow join/prune message from any groups, group address in the ACL can be wild-carded. In this case, only RP address check is performed.

This command impacts only (*,G) join/prune messages. If there are any existing flows, the user will need to disable and enable PIM on the interface to apply the ACL.

Loopback interfaces are special interfaces where only unicast PIM messages are updated. This includes Register, Register Stop, and Candidate RP Advertisements.

When a loopback interface is configured as the RP, the ACL drop counters will be updated on the interface on which the packets are received.

If there is an active flow which is in the SPT, the traffic flow through the SPT will continue. Only (*,G) join/prune messages are dropped. (S,G) join/prune messages will not be impacted.

Examples

Configuring ACL on RP with an ACL rule named `pim_rpv6_grp_acl` to filter join/prune messages:

```
switch(config-pim)# access-list ip pim_rpv6_grp_acl
switch(config-acl-ipv6)# 10 permit any any ff2e::2/64
switch(config-acl-ipv6)# 20 permit any any ff1e::1/64
switch(config-acl-ipv6)# router pim6
switch(config-pim6)# accept-rp 30::1 access-list pim_rpv6_grp_acl
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	`config-pim6`	Administrators or local user group members with execution rights for this command.

bsr-candidate bsm-interval

```
bsr-candidate bsm-interval <INTERVAL-VALUE>
no bsr-candidate bsm-interval
```

Description

Configures the interval in seconds to send periodic RP-Set messages to all PIM-SM interfaces on a router that operates as the BSR in a domain. This setting must be smaller than the `rp-candidate hold-time` settings (range of 30 to 255; default 150) configured in the RPs operating in the domain.

The `no` form of this command removes the currently configured value and sets it to the default of 60 seconds.

Parameters

<INTERVAL-VALUE>

Specifies the BSR-candidate BSM interval in seconds. Range: 5 to 300. Default: 60.

Example

Configuring and removing BSR-candidate BSM-interval:

```
switch(config)# router pim6
switch(config-pim6)# bsr-candidate bsm-interval 150
switch(config-pim6)# no bsr-candidate bsm-interval
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config-pim6	Administrators or local user group members with execution rights for this command.

bsr-candidate hash-mask-length

```
bsr-candidate hash-mask-length <LENGTH-VALUE>
no bsr-candidate hash-mask-length
```

Description

Controls the distribution of multicast groups among the C-RP, in a domain where there is overlapping coverage of the groups among the RPs. This value specifies the length (number of significant bits) when allocating this distribution. A longer hash-mask-length results in fewer multicast groups, for each block of group addresses assigned to the RPs. Multiple blocks of addresses assigned to each C-RP results in wider dispersal of addresses. Includes enhanced load-sharing for the multicast traffic for the different groups that are used in the domain at the same time.

The no form of this command removes currently configured value and sets to the default of 126.

Parameters

<LENGTH-VALUE>

Specifies the length (in bits) of the hash mask. Range: 1 to 128. Default: 126.

Example

Configuring and removing the BSR-candidate hash-mask-length:

```
switch(config)# router pim6
switch(config-pim6)# bsr-candidate hash-mask-length 4
switch(config-pim6)# no bsr-candidate hash-mask-length
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config-pim6	Administrators or local user group members with execution rights for this command.

bsr-candidate priority

```
bsr-candidate priority <PRIORITY-VALUE>
no bsr-candidate priority
```

Description

Configures the priority to apply to the router when a BSR election process occurs in the PIM-SM domain. The candidate with the highest priority becomes the BSR for the domain. If the highest priority is shared by multiple routers, the candidate having the highest IP address becomes the BSR of the domain. Zero (0) is the lowest priority. To make BSR selection easily predictable, use this command to assign a different priority to each candidate BSR in the PIM-SM domain.

The no form of this command removes currently configured value and sets to the default of 0.

Parameters

<PRIORITY-VALUE>

Specifies the priority for the Candidate Bootstrap router. Range: 0 to 255. Default: 0.

Example

Configuring and removing the BSR-candidate priority:

```
switch(config)# router pim6
switch(config-pim6)# bsr-candidate priority 250
switch(config-pim6)# no bsr-candidate priority
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300	config-pim6	Administrators or local user group members with execution rights

Platforms	Command context	Authority
6400 8320 8325 8360 8400		for this command.

bsr-candidate source-ip-interface

```
bsr-candidate source-ip-interface <INTERFACE-NAME>
no bsr-candidate source-ip-interface <INTERFACE-NAME>
```

Description

Configures the router to advertise itself as a candidate PIM-SM BSR on the interface specified, and enables BSR candidate operation. The result makes the router eligible to be elected as the BSR for the PIM-SM domain in which it operates. One BSR candidate interface is allowed per-router.

The `no` form of this command removes the Candidate BSR configuration.

Parameters

<INTERFACE-NAME>

Specifies the interface to use as a source for Candidate-BSR router IP address. Interface can be a VLAN interface, routed interface, or LAG. PIM-SM must be enabled on this interface with the command `ipv6 pimv6-sparse enable`.

Example

On the 6400 Switch Series, interface identification differs.

Configuring and removing the BSR-candidate interface:

```
switch(config)# router pim6
switch(config-pim6)# bsr-candidate source-ip-interface 1/1/4
switch(config-pim6)# no rp-candidate source-ip-interface 1/1/4
```

Configuring and removing the BSR-candidate sub-interface:

```
switch(config)# router pim6
switch(config-pim6)# bsr-candidate source-ip-interface 1/1/4
switch(config-pim6)# no rp-candidate source-ip-interface 1/1/4
```

Configuring sub-interface 1/1/19/10 as Candidate BSR:

```
switch(config)# router pim6
switch(config-pim6)# bsr-candidate source-ip-interface 1/1/19.10
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	`config-pim6`	Administrators or local user group members with execution rights for this command.

disable

`disable`

Description

Disables PIMv6 globally on the router.

Using the `disable` command will cause all the multicast routes to be erased from hardware.

Example

Disabling PIM router:

```
switch(config)# router pim6
switch(config-pim6)# disable
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	`config-pim6`	Administrators or local user group members with execution rights for this command.

enable

`enable`

Description

Enables PIMv6 globally on the router.

Example

Enabling PIM router:

```
switch(config)# router pim6
switch(config-pim6)# enable
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config-pim6	Administrators or local user group members with execution rights for this command.

ipv6 pim6-sparse

```
ipv6 pim6-sparse {enable | disable}
```

Description

Enables or disables PIM-SM on the current interface. PIM-SM is disabled by default on an interface. An IPv6 address must be configured on the interface to enable PIM-SM.

Parameters

`enable`

Enables PIM-SM on the interface. IPv6 address must be configured on the interface to enable PIM-SM (use the `ipv6 address <X:X::X:X/M>` command).

`disable`

Disables PIM SM on the interface.

Examples

Enabling and disabling PIM-SM on an interface:

```
switch(config)# interface vlan40
switch(config-if-vlan)# ipv6 address 2001::01/64
switch(config-if-vlan)# ipv6 pim6-sparse enable
switch(config-if-vlan)# ipv6 pim6-sparse disable
```

Enabling and disabling PIM-SM on a sub-interface:

```
switch(config)# interface 1/1/19.10
switch(config-subif)# ipv6 address 90::1/64
```

```
switch(config-subif)# ipv6 pim6-sparse enable
switch(config-subif)# ipv6 pim6-sparse disable
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config-if config-if-vlan config-lag-if config-subif	Administrators or local user group members with execution rights for this command.

ipv6 pim6-sparse bfd

Not supported on the Aruba 6200 Switch Series.

```
ipv6 pim6-sparse bfd [disable]
no ipv6 pim6-sparse bfd
```

Description

Configures BFD on a per-interface basis for an interface associated with the PIM process.

The no form of this command removes the BFD configuration on the interface and sets it to the default configuration.

If BFD is enabled globally, it will be enabled by default on all interfaces. The only exception is when it is disabled specifically on an interface using the ipv6 pim6-sparse bfd disable command.
If BFD is disabled globally, it will be disabled by default on all interfaces. The only exception is when it is enabled specifically on an interface using the ipv6 pim6-sparse bfd command.

Parameters

disable

Disables the BFD configuration on the interface.

Examples

Enabling the BFD configuration on the interface:

```
switch(config)# interface vlan 40
switch(config-if-vlan)# ipv6 pim6-sparse bfd
```

Disabling the BFD configuration on the interface:

```
switch(config-if-vlan)# ipv6 pim6-sparse bfd disable
```

Removing the BFD configuration on the interface:

```
switch(config-if-vlan)# no ipv6 pim6-sparse bfd
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config-if config-if-vlan config-lag-if	Administrators or local user group members with execution rights for this command.

ipv6 pim6-sparse dr-priority

```
ipv6 pim6-sparse dr-priority <PRIORITY-VALUE>
no ipv6 pim6-sparse dr-priority
```

Description

Changes the router priority for the designated router (DR) election process in the current interface.

A numerically higher value means a higher priority. If multiple routes share the highest priority, the router with the highest IP address is selected as the DR.

The `no` form of this command removes currently configured value and sets to the default of 1.

Parameters

<PRIORITY-VALUE>

Specifies the priority value to use on the interface in the DR election process. Range: 0 to 4294967295. Default: 1.

Examples

Configuring and removing the interface priority value:

```
switch(config)# interface vlan 40
switch(config-if-vlan)# ipv6 pim6-sparse dr-priority 4444
switch(config-if-vlan)# no ipv6 pim6-sparse dr-priority
```

Configuring and removing the interface priority value:

```
switch(config)# interface 1/1/19.10
switch(config-if-vlan)# ipv6 pim6-sparse dr-priority 2000
switch(config-if-vlan)# no ipv6 pim6-sparse dr-priority
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config-if config-if-vlan config-lag-if config-subif	Administrators or local user group members with execution rights for this command.

ipv6 pim6-sparse hello-delay

```
ipv6 pim6-sparse hello-delay <DELAY-VALUE>
no ipv6 pim6-sparse hello-delay
```

Description

Configures the maximum time in seconds before the router actually transmits the initial PIM hello message on the current interface.

The no form of this command removes currently configured value and sets to the default of 5 seconds.

Parameters

<DELAY-VALUE>

Specifies the hello-delay in seconds, which is the maximum time before a triggered PIM Hello message is transmitted on this interface. Range: 0 to 5. Default: 5.

Usage

- In cases where a new interface activates connections with multiple routers. If all the connected routers sent hello packets at the same time, the receiving router could become momentarily overloaded.
- This command randomizes the transmission delay to a time between zero and the hello delay setting. Using zero means no delay. After the router sends the initial hello packet to a newly detected interface, it sends subsequent hello packets according to the current hello interval setting.

Example

Configuring and removing hello-delay interface:

```
switch(config)# interface vlan 40
switch(config-if-vlan)# ipv6 pim6-sparse hello-delay 4
switch(config-if-vlan)# no ipv6 pim6-sparse hello-delay
```

Configuring and removing hello-delay on a sub-interface:

```
switch(config)# interface 1/1/19.10
switch(config-subif)# ipv6 pim6-sparse hello-delay 4
switch(config-subif)# no ipv6 pim6-sparse hello-delay
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config-if config-if-vlan config-lag-if config-subif	Administrators or local user group members with execution rights for this command.

ipv6 pim6-sparse hello-interval

```
ipv6 pim6-sparse hello-interval <INTERVAL-VALUE>
no ipv6 pim6-sparse hello-interval
```

Description

Configures the frequency at which the router transmits PIM hello messages on the current interface.

The no form of this command removes the currently configured value and sets to the default of 30 seconds.

Parameters

<INTERVAL-VALUE>

Specifies the frequency at which PIM Hello messages are transmitted on this interface in seconds. Range: 5 to 300. Default: 30.

Usage

- The router uses hello packets to inform neighbor routers of its presence.
- The router also uses this setting to compute the hello holdtime, which is included in hello packets sent to neighbor routers.
- Hello holdtime tells neighbor routers how long to wait for the next hello packet from the router. If another packet does not arrive within that time, the router removes the neighbor adjacency on that interface from the PIM adjacency table, which removes any flows running on that interface.
- Shortening the hello interval reduces the hello holdtime. If they do not receive a new hello packet when expected, it changes how quickly other routers stop sending traffic to the router.

Example

Configuring and removing sparse hello-interval:

```
switch(config-if)# ipv6 pim6-sparse hello-interval 60
switch(config-if)# no ipv6 pim6-sparse hello-interval
```

Configuring and removing sparse hello-interval on a sub-interface:

```
switch)config)# interface 1/1/19.10
switch(config-subif)# ipv6 pim6-sparse hello-interval 100
switch(config-subif)# no ipv6 pim6-sparse hello-interval
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config-if config-if-vlan config-lag-if config-subif	Administrators or local user group members with execution rights for this command.

ipv6 pim6-sparse ipv6-addr

```
ipv6 pim6-sparse ipv6-addr {<IPv6-ADDR-VALUE> | any}
no ipv6 pim6-sparse ipv6-addr
```

Description

Enables the router to dynamically determine the source IP address to use for PIM-SM packets sent from the interface or to use the specific IPv6 address.

The `no` form of this command removes the currently configured value and sets to the default of `any`.

Parameters

<IP-ADDR-VALUE>

Specifies the source IP address in IPv6 format (`xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx`), where `x` is a hexadecimal number from 0 to F.

`any`

Specifies dynamically determining the source IP from the current IP address of the interface.

Examples

Configuring and removing source IP address:

```
switch(config)# interface vlan40
switch(config-if-vlan)# ipv6 pim6-sparse ipv6-addr 2001::02
switch(config-if-vlan)# no ipv6 pim6-sparse ipv6-addr
```

Configuring and removing source IP address on a sub-interface:

```
switch(config)# interface 1/1/19.10
switch(config-subif)# ipv6 pim6-sparse ipv6-addr 2001:1::1
switch(config-if-vlan)# no ipv6 pim6-sparse ipv6-addr 2001:1::1
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config-if config-if-vlan config-lag-if config-subif	Administrators or local user group members with execution rights for this command.

ipv6 pim6-sparse lan-prune-delay

```
ipv6 pim6-sparse lan-prune-delay
no ipv6 pim6-sparse lan-prune-delay
```

Description

Enables the LAN prune delay option on the current interface. The default is enabled.

With LAN-prune-delay enabled, the router informs downstream neighbors how long it will wait before pruning a flow after receiving a prune request. Other downstream routers on the same interface must send a join to override the prune before the LAN-prune-delay time to continue the flow. Prompts any downstream neighbors with multicast receivers continuing to belong to the flow to reply with a join. If no joins are received after the LAN-prune-delay period, the router prunes the flow. The propagation-delay and override-interval settings determine the LAN-prune-delay setting.

The `no` form of this command disables the LAN prune delay option.

Example

Enabling and disabling the LAN prune delay:

```
switch(config)# interface vlan40
switch(config-if-vlan)# ipv6 pim6-sparse lan-prune-delay
switch(config-if-vlan)# no ipv6 pim6-sparse lan-prune-delay
```

Enabling and disabling the LAN prune delay on a sub-interface:

```
switch(config)# interface 1/1/19.10
switch(config-subif)# ipv6 pim6-sparse lan-prune-delay
switch(config-subif)# no ipv6 pim6-sparse lan-prune-delay
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority

6300
6400
8320
8325
8360
8400
	`config-if`
	`config-if-vlan`
	`config-lag-if`
	`config-subif`
		Administrators or local user group members with execution rights for this command.

ipv6 pim6-sparse override-interval

```
ipv6 pim6-sparse override-interval <INTERVAL-VALUE>
no ipv6 pim6-sparse override-interval
```

Description

Configures the override interval that gets inserted into the Override Interval field of a LAN Prune Delay option.

The `no` form of this command removes the currently configured value and sets the value to the default of 2500 ms.

Parameters

<INTERVAL-VALUE>

Specifies the override interval of a LAN Prune Delay option in ms. Range: 500 to 6000. Default: 2500.

Usage

A router sharing a VLAN with other multicast routers uses the override-interval value along with the propagation-delay value to compute the `lan-prune-delay` setting. The setting specifies how long to wait for a PIM-SM join after receiving a prune packet from downstream for a particular multicast group.

Example scenario:

A network may have multiple routers sharing VLAN X. When an upstream router is forwarding traffic from multicast group X to VLAN Y, if one of the routers on VLAN Y does not want this traffic, it issues a prune response to the upstream neighbor. The upstream neighbor then goes into a prune pending state for group X on VLAN Y. During this period, the upstream neighbor continues to forward the traffic. During the pending period, another router on VLAN Y can send a group X join to the upstream neighbor. If this happens, the upstream neighbor drops the prune pending status and continues forwarding the traffic. But if no routers on the VLAN send a join, the upstream router prunes.

Example

Configuring and removing the override interval:

```
switch(config)# interface vlan40
switch(config-if-vlan)# ipv6 pim6-sparse override-interval 4000
switch(config-if-vlan)# no ipv6 pim6-sparse override-interval
```

Configuring and removing the override interval on a sub-interface:

```
switch(config)# interface 1/1/19.10
switch(config-subif)# ipv6 pim6-sparse override-interval 5000
switch(config-subif)# no ipv6 pim6-sparse override-interval
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config-if config-if-vlan config-lag-if config-subif	Administrators or local user group members with execution rights for this command.

ipv6 pim6-sparse propagation-delay

```
ipv6 pim6-sparse propagation-delay <DELAY-VALUE>
no ipv6 pim6-sparse propagation-delay
```

Description

Configures the propagation delay that gets inserted into the LAN prune delay field of a LAN Prune Delay option.

The no form of this command removes currently configured value and sets to the default of 500 ms.

Parameters

<DELAY-VALUE>

Specifies the propagation delay value in ms. Range: 250 to 2000. Default: 500.

Examples

Configuring and removing the propagation delay:

```
switch(config)# interface vlan 40
switch(config-if-vlan)# ipv6 pim6-sparse propagation-delay 400
switch(config-if-vlan)# no ipv6 pim6-sparse propagation-delay
```

Configuring and removing the propagation delay on a sub-interface:

```
switch(config)# interface 1/1/19.10
switch(config-subif)# ipv6 pim6-sparse propagation-delay 1000
switch(config-subif)# no ipv6 pim6-sparse propagation-delay
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority

6300
6400
8320
8325
8360
8400
	`config-if`
	`config-if-vlan`
	`config-lag-if`
	`config-subif`
		Administrators or local user group members with execution rights for this command.

join-prune-interval

```
join-prune-interval <INTERVAL-VALUE>
no join-prune-interval
```

Description

Configures the frequency at which the router will send periodic join or prune-interval messages.

The `no` form of this command sets the interval to the default value of 60 seconds.

Parameters

<INTERVAL-VALUE>

Specifies the join-prune-interval in seconds. Range 5 to 65535. Default: 60.

Examples

Configuring join prune interval:

```
switch(config)# router pim6
switch(config-pim6)# join-prune-interval 400
switch(config-pim6)# no join-prune-interval
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	`config-pim6`	Administrators or local user group members with execution rights for this command.

no ipv6 pim6-sparse

```
no ipv6 pim6-sparse
```

Description

Removes all the PIM-SM related IPv6 configurations for the interface.

Example

Removing PIM-SM configuration:

```
switch(config)# interface vlan40
switch(config-if-vlan)# no ipv6 pim6-sparse
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config-if config-if-vlan config-lag-if	Administrators or local user group members with execution rights for this command.

router pim6

```
router pim6 [vrf <VRF-NAME>]
no router pim6 [vrf <VRF-NAME>]
```

Description

Changes the current context to the PIMv6 configuration context. If no VRF is specified, the default VRF is assumed.

The no form of this command removes the PIM configuration from the specified context or the default VRF.

Parameters

`vrf <VRF-NAME>`

Specifies the name of a VRF. Default: default.

Examples

Configuring default router PIM:

```
switch(config)# router pim6
switch(config-pim6)#
```

Configuring specified router PIM:

```
switch(config)# router pim6 vrf Green
switch(config-pim6)#
```

Removing router PIM:

```
switch(config)# no router pim6
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config	Administrators or local user group members with execution rights for this command.

rp-address

```
rp-address <IPv6-ADDR> [<GRP-ADDR/GRP-MASK>] [override]
no rp-address <IPv6-ADDR> [<GRP-ADDR/GRP-MASK>] [override]
```

Description

Statically configures the router as the RP for a specified multicast group or range of multicast groups. This must be configured on all PIM-SM routers in the domain. If group address is not specified, it applies to all IPv6 multicast addresses.

The no form of this command removes static RP configuration and its precedence.

Parameters

<IPv6-ADDR>

Specifies an address in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F.

<GRP-ADDR>

Specifies the range of multicast group addresses in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F.

<GRP-MASK>

Specifies the number of bits in the address mask in CIDR format (x), where x is a decimal number from 0 to 128.

override

Specifies higher precedence to static RP over Candidate RP.

Usage

Where a static RP and a C-RP are configured to support the same multicast groups and the multicast group mask for the static RP is equal to or greater than the same mask for the applicable C-RPs, this command assigns the higher precedence to the static RP, resulting in the C-RP operating only as a backup RP for the configured group. Without override, the C-RP has precedence over a static RP configured for the same multicast group or groups.

Examples

```
switch(config)# router pim6
switch(config-pim6)# rp-address 2001::01 ff08::1:3/64 ovverride
switch(config-pim6)# rp-address 2002::02 ff08::1:4/64
switch(config-pim6)# no rp-address 2002::02 ff08::1:4/64
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config-pim	Administrators or local user group members with execution rights for this command.

rp-candidate group-prefix

```
rp-candidate group-prefix <GRP-ADDR/GRP-MASK>
no rp-candidate group-prefix <GRP-ADDR/GRP-MASK>
```

Description

Adds multicast group address to the current Candidate Rendezvous Point (C-RP) configuration.

The no form of this command removes C-RP multicast group address.

Parameters

<GRP-ADDR>

Specifies the multicast group address in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F.

<GRP-MASK>

Specifies the number of bits in the address mask in CIDR format (x), where x is a decimal number from 0 to 128.

Examples

Configuring and removing candidate group prefix:

```
switch(config)# router pim6
switch(config-pim6)# rp-candidate group-prefix ff08::1:3/64
switch(config-pim6)# no rp-candidate group-prefix ff08::1:3/64
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config-pim6	Administrators or local user group members with execution rights for this command.

rp-candidate hold-time

```
rp-candidate hold-time <TIME-VALUE>
no rp-candidate hold-time
```

Description

Changes the hold-time a C-RP includes in its advertisements to the BSR.

Hold-time is included in the advertisements the C-RP periodically sends to the elected BSR for the domain. Also updates the BSR on how long to wait after the last advertisement from the reporting RP before assuming it has become unavailable.

The no form of this command removes the currently configured value and sets it to the default value 150 seconds.

Parameters

<TIME-VALUE>

Specifies the hold-time value in seconds to be sent in C-RP-Adv messages. Range: 30 - 255. Default: 150.

Example

Setting and removing the candidate holdtime:

```
switch(config)# router pim6
switch(config-pim6)# rp-candidate hold-time 250
switch(config-pim6)# no rp-candidate hold-time
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config-pim6	Administrators or local user group members with execution rights for this command.

rp-candidate priority

```
rp-candidate priority <PRIORITY-VALUE>
no rp-candidate priority
```

Description

Changes the current priority setting for a C-RP. Where multiple C-RP configurations are used to support the same multicast groups, the candidate having the highest priority is elected. Zero (0) is the highest priority, and 255 is the lowest priority.

The no form of this command removes the currently configured value and sets it to the default of 192.

Parameters

<PRIORITY-VALUE>

Specifies the priority value for the Candidate-RP router. Range: 0 to 255. Default: 192.

Example

Configuring and removing candidate priority:

```
switch(config)# router pim6
switch(config-pim6)# rp-candidate priority 250
switch(config-pim6)# no rp-candidate priority
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config-pim	Administrators or local user group members with execution rights for this command.

rp-candidate source-ip-interface

```
rp-candidate source-ip-interface <INTERFACE-NAME> [group-prefix <GRP-ADDR/GRP-MASK>]
no rp-candidate source-ip-interface <INTERFACE-NAME> [group-prefix <GRP-ADDR/GRP-MASK>]
```

Description

Enables the Candidate Rendezvous Point (C-RP) operation, and configures the router to advertise itself as a C-RP to the Bootstrap Router (BSR) for the current domain.

This step includes the option to allow the C-RP to be a candidate for all possible multicast groups, or for up to four multicast groups, or ranges of groups. If group-prefix is not given, it considers for all multicast group addresses.

The `no` form of this command removes the C-RP configuration.

Parameters

<INTERFACE-NAME>

Specifies the interface to use as a source for the C-RP router IP address.

`group-prefix` *<GRP-ADDR/GRP-MASK>*

Specifies the multicast group address in IPv6 format (`xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx`), where `x` is a hexadecimal number from 0 to F. And the number of bits in the address mask in CIDR format (`x`), where `x` is a decimal number from 0 to 128.

Examples

Configuring a C-RP using VLAN 40 as the source for the C-RP router IP address and associating the ff08::1:3/64 multicast group with the C-RP router:

```
switch(config)# router pim6
switch(config-pim6)# rp-candidate source-ip-interface vlan40 group-prefix
ff08::1:3/64
```

Configuring a C-RP using loopback1 as the source for the C-RP router IP address and associating the ff08::1:3/64 multicast group with the C-RP router:

```
switch(config)# router pim6
switch(config-pim6)# rp-candidate source-ip-interface loopback1 group-prefix
ff08::1:3/64
```

Configuring sub-interface 1/1/19.10 as candidate RP:

```
switch(config)# router pim6
switch(config-pim6)# rp-candidate source-ip-interface 1/1/19.10
```

Removing the candidate source IP interface:

```
switch(config-pim6)# no rp-candidate source-ip-interface vlan20
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config-pim6	Administrators or local user group members with execution rights for this command.

rpf-override

```
rpf-override <SRC-ADDR/SRC-MASK> <RPF-ADDR|INTERFACE-NAME>
no rpf-override <SRC-ADDR/SRC-MASK> <RPF-ADDR|INTERFACE-NAME>
```

Description

The Reverse Path Forward (RPF) override, allows overriding the normal RPF lookup mechanism, and indicates to the router that it may accept multicast traffic on an interface other than the one that the RPF lookup mechanism would normally select. This includes accepting traffic from an invalid source IP address for the subnet or VLAN that is directly connected to the router. Traffic may also be accepted from a valid PIM neighbor that is not on the reverse path towards the source of the received multicast traffic.

The no form of this command removes currently configured RPF entry.

Parameters

<SRC-ADDR>

Specifies the multicast source address in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F.

<SRC-MASK>

Specifies the number of bits in the address mask in CIDR format (x), where x is a decimal number from 0 to 128.

<RPF-ADDR>

Specifies the RPF address in IPv6 format (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx), where x is a hexadecimal number from 0 to F.

<INTERFACE-NAME>

Specifies the RPF interface name.

Usage

- Reverse Path Forward (RPF) checking is a core multicast routing mechanism. The RPF ensures that the multicast traffic received arrives on the expected router interface before further processing. If the RPF check fails for a multicast packet, the packet is discarded. For multicast traffic flow that arrives on the SPT, the expected incoming interface for a given source or group is the interface towards the source address of the traffic (determined by the unicast routing system). For traffic arriving on the RP tree, the expected incoming interface is the interface towards the RP.
- RPF checking is applied to all multicast traffic and is significant in preventing network loops. Up to eight manual RPF overrides can be specified. The RPF-address indicates one of two distinct RPF candidates:
    1. A valid PIM neighbor address from which forwarded multicast traffic is accepted with a source address of *<source-addr/src-mask>*.

2. A local router address on a PIM-enabled interface to which *<source-addr/src-mask>* is directly connected. If configured, the local router will assume the role of DR for this flow and registers the flow with an RP.

Example

Configuring and removing RPF override:

```
switch(config)# router pim6
switch(config-pim6)# rpf-override 50::4/24 40::1
switch(config-pim)# no rpf-override 50::4/24 40::1
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config-pim6	Administrators or local user group members with execution rights for this command.

show ipv6 mroute grorp-addr

`show ipv6 mroute <GROUP-ADDR> [<SOURCE-ADDR>] [all-vrfs | vrf <vrf-name>] [vsx-peer]`

Description

Shows the multicast routing information for the given group address. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameters

<GROUP-ADDR>

Specifies a group address in IPv6 format (`xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx`), where `x` is a hexadecimal number from 0 to F.

<SOURCE-ADDR>

Specifies a source IP address in IPv6 format (`xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx`), where `x` is a hexadecimal number from 0 to F.

`all-vrfs`

Shows information for all VRFs.

`vrf <VRF-NAME>`

Specifies the name of a VRF. Default: default.

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing information for group ff08::1:3 and VRF green:

```
switch# show ipv6 mroute  ff08::1:3 vrf green

VRF : green

Group Address           : ff08::1:3
Source Address          : 2001::03
Neighbor                : 2003::04
Incoming interface      : 1/1/1
Outgoing Interface List :
Interface      State
---------      -----
1/1/4          pruned
```

Showing information for group ff08::1:3 from source 2001::03 and all VRFs:

```
switch# show ipv6 mroute  ff08::1:3 2001::03 all-vrfs

VRF : blue

Group Address           : ff08::1:3
Source Address          : 2001::03
Neighbor                : 2003::04
Incoming interface      : 1/1/1
Outgoing Interface List :
Interface      State
---------      -----
1/1/4          pruned


VRF : green

Group Address           : ff08::1:3
Source Address          : 2001::03
Neighbor                : 2003::04
Incoming interface      : 1/1/2
Outgoing Interface List :
Interface      State
---------      -----
1/1/4          pruned
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

Platforms	Command context	Authority
8325 8360 8400		

show ipv6 mroute

```
show ipv6 mroute [all-vrfs | vrf <VRF-NAME>] [vsx-peer]
```

Description

Shows multicast routing information. Optionally, you can show specific information by VRF. If no options are specified, it shows information for the default VRF.

Parameters

`all-vrfs`

Shows information for all VRFs.

`vrf <VRF-NAME>`

Specifies the name of a VRF. Default: default.

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing IPv6 mroute:

```
switch# show ipv6 mroute  all-vrfs
IP Multicast Route Entries

VRF : blu
Total number of entries : 2

Group Address           : ff08::1:3
Source Address          : 2002::04
Neighbor                : 2001::04
Incoming interface      : 1/1/2
Outgoing Interface List :
Interface      State
---------      -----
1/1/3          pruned
1/1/4          forwarding

Group Address           : ff08::1:4
Source Address          : 2003::04
Neighbor                : 2001::04
Incoming interface      : 1/1/2
Outgoing Interface List :
Interface      State
---------      -----
1/1/3          pruned

VRF : default
Total number of entries : 1

Group Address           : ff08::1:5
```

```
Source Address          : 2001::03
Neighbor                : 2003::04
Incoming interface      : 1/1/1
Outgoing Interface List :
Interface      State
---------      -----
1/1/4          pruned
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 mroute brief

`show ipv6 mroute brief [all-vrfs | vrf <VRF-NAME>] [vsx-peer]`

Description

Shows brief version of the multicast routing information. Optionally, you can specify the display information by VRF. If no options are specified, it shows information for the default VRF.

Parameters

`all-vrfs`

Shows information for all VRFs.

`vrf <VRF-NAME>`

Specifies the name of a VRF. Default: default.

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing the IPv6 mroute brief:

```
switch# show ipv6 mroute brief all-vrfs
IP Multicast Route Entries

VRF : blu
Total number of entries : 2
```

```
Group Address  : ff08::1:3
Source Address : 2002::04
Neighbor       : 2003::04
Interface       : 1/1/2

Group Address  : ff08::1:4
Source Address : 2002::03
Neighbor       : 2003::05
Interface       : 1/1/3

VRF : default
Total number of entries : 1

Group Address  : ff08::1:5
Source Address : 2001::03
Neighbor       : 2002::01
Interface       : 1/1/1
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 pim6

`show ipv6 pim6 [all-vrfs | vrf <VRF-NAME>] [vsx-peer]`

Description

Shows the PIM router information. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameters

`all-vrfs`

Shows information for all VRFs.

`vrf <VRF-NAME>`

Specifies the name of a VRF. Default: default.

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing the IPv6 PIM router:

```
switch# show ipv6 pim6

PIM Global Parameters

VRF                           :  default
PIM Status                    :  Enabled
Join/Prune Interval (sec)     :  46
SPT Threshold                 :  Disabled
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 pim6 bsr

`show ipv6 pim6 bsr [all-vrfs | vrf <VRF-NAME>] [vsx-peer]`

Description

Shows the information about BSR candidates in the domain and multicast groups it supports. Optionally, you can specify the display information by VRF. If no options are specified, it shows information for the default VRF.

Parameters

`all-vrfs`

Shows information for all VRFs.

`vrf <VRF-NAME>`

Specifies the name of a VRF. Default: default.

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing information about BSR candidates:

```
switch# show ipv6 pim6 bsr all-vrfs

Status and Counters- PIM-SM(IPv6) Bootstrap Router Information

VRF                        : blu
E-BSR Address              : 2006::06
E-BSR Priority             : 0
E-BSR Hash Mask Length     : 0
E-BSR Up Time              : 0 secs
Next Bootstrap Message     : 0 secs

C-BSR Admin Status         : This system is a Candidate-BSR
C-BSR Address              : 2007::01
C-BSR Priority             : 40
C-BSR Hash Mask Length     : 36
C-BSR Message Interval     : 50
C-BSR Source IP Interface  : lag1

C-RP Admin Status          : This system is a Candidate-RP
C-RP Address               : 2007::01
C-RP Hold Time             : 60
C-RP Advertise Period      : 60
C-RP Priority              : 46
C-RP Source IP Interface   : lag1

Group Prefix    : ff00::/8
Group Prefix    : ff08::1:3/64
Group Prefix    : ff08::1:4/64

VRF                        : default
E-BSR Address              : 2001::01
E-BSR Priority             : 40
E-BSR Hash Mask Length     : 36
E-BSR Up Time              : 53 mins
Next Bootstrap Message     : 88 secs

C-BSR Admin Status         : This system is a Candidate-BSR
C-BSR Address              : 2001::01
C-BSR Priority             : 40
C-BSR Hash Mask Length     : 36
C-BSR Message Interval     : 50
C-BSR Source IP Interface  : 1/1/1

C-RP Admin Status          : This system is a Candidate-RP
C-RP Address               : 2001::01
C-RP Hold Time             : 60
C-RP Advertise Period      : 60
C-RP Priority              : 46
C-RP Source IP Interface   : 1/1/1

Group Prefix    : ff00::/8
Group Prefix    : ff08::1:5/64
Group Prefix    : ff08::1:6/64
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 pim6 bsr elected

```
show ipv6 pim6 bsr elected [all-vrfs | vrf <VRF-NAME>] [vsx-peer]
```

Description

Shows information about the elected BSR in the domain and multicast groups it supports. Optionally you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameters

`all-vrfs`

Shows information for all VRFs.

`vrf <VRF-NAME>`

Specifies the name of a VRF. Default: default.

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing PIM elected bootstrap router information:

```
switch# show ipv6 pim6 bsr elected all-vrfs

Status and Counters - PIM-SM(IPv6) Elected Bootstrap Router Information

VRF                         : blu
E-BSR Address               : 2005::05
E-BSR Priority              : 0
E-BSR Hash Mask Length      : 0
E-BSR Up Time               : 0 secs
Next Bootstrap Message      : 0 secs

VRF                         : default
E-BSR Address               : 2002::02
E-BSR Priority              : 0
E-BSR Hash Mask Length      : 30
E-BSR Up Time               : 50 mins
Next Bootstrap Message      : 88 secs
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 pim6 bsr local

`show ipv6 pim6 bsr local [all-vrfs | vrf <VRF-NAME>] [vsx-peer]`

Description

Shows the information about BSR candidates on the local router and multicast groups it supports. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameters

`all-vrfs`

Shows information for all VRFs.

`vrf <VRF-NAME>`

Specifies the name of a VRF. Default: default.

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing local Candidate BSR:

```
switch# show ipv6 pim6 bsr local all-vrfs

Status and Counters - PIM-SM(IPv6) Local Candidate-BSR Information

VRF                       : blu
C-BSR Admin Status        : This system is a Candidate-BSR
C-BSR Address             : 2007::01
C-BSR Priority            : 40
C-BSR Hash Mask Length    : 36
C-BSR Message Interval    : 50
C-BSR Source IP Interface : lag1

VRF                       : default
C-BSR Admin Status        : This system is a Candidate-BSR
C-BSR Address             : 2001::01
C-BSR Priority            : 40
C-BSR Hash Mask Length    : 36
C-BSR Message Interval    : 50
C-BSR Source IP Interface : 1/1/1
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 pim6 interface interface-name

`show ipv6 pim6 interface <INTERFACE-NAME> [vsx-peer]`

Description

Shows detailed information about the PIM interface currently configured.

Parameters

<INTERFACE-NAME>

Specifies an interface for showing PIM interface information. Interface can also be a LAG or VLAN.

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

On the 6400 Switch Series, interface identification differs.

Showing PIM interface information for interface 1/1/1:

```
switch# show ipv6 pim6 interface 1/1/1

PIM Interfaces

VRF: default

Interface  : 1/1/1
IPv6 Address : fe80::a00:9ff:feec:dc0e/64
Mode       : sparse

Designated Router :
Hello Interval (sec)   : 30
Hello Delay (sec)      : 4

Override Interval (msec)   : 500              Lan Prune Delay     : Yes
Propagation Delay (msec)   : 350              DR Priority         : 3
Neighbor Timeout           : 0
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 pim6 interface

`show ipv6 pim6 interface [all-vrfs | vrf <VRF-NAME>] [vsx-peer]`

Description

Shows the information about PIM interfaces currently configured in the router. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameters

`all-vrfs`

Shows information for all VRFs.

`vrf <VRF-NAME>`

Specifies the name of a VRF. Default: default.

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing PIM interface:

```
switch# show ipv6 pim6 interface
PIM Interfaces

VRF: default

Interface          IP Address
mode
------------------ ------------------------------------------------------------  -
---------
1/1/1              fe80::a00:9ff:feec:dc0e/64
sparse
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 pim6 neighbor

`show ipv6 pim6 neighbor [<IPv6-ADDR>] [all-vrfs | vrf <VRF-NAME>] [vsx-peer]`

Description

Shows PIM neighbor information. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameters

<IPv6-ADDR>

Specifies a neighbor address in IPv6 format (`xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx`), where `x` is a hexadecimal number from 0 to F.

`all-vrfs`

Shows information for all VRFs.

`vrf <VRF-NAME>`

Specifies the name of a VRF. Default: default.

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

On the 6400 Switch Series, interface identification differs.

Showing PIM neighbor information:

```
switch# show ipv6 pim6 neighbor

PIM Neighbor

VRF                 : default
IP Address          : 2001::02
Interface           : 1/1/1
Up Time (sec)       : 0
Expire Time (sec)   : 0
DR Priority         : 44
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 pim6 pending

`show ipv6 pim6 pending [<GROUP-ADDR>] [all-vrfs | vrf <VRF-NAME>] [vsx-peer]`

Description

Shows the pending joins on a PIM router. Optionally you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Use this command to determine what flows are being requested on the PIM network. If data availability for a flow is expected, and a join for the flow is pending, the troubleshooting search moves to the source of that flow, since the routers are verified to be seeing the request for data.

Parameters

<GROUP-ADDR>

Specifies a group addressin IPv6 format (`xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx`), where `x` is a hexadecimal number from 0 to F.

`all-vrfs`

Shows information for all VRFs.

`vrf <VRF-NAME>`

Specifies the name of a VRF. Default: default.

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

On the 6400 Switch Series, interface identification differs.

Showing pending PIM joins:

```
switch# show ipv6 pim6 pending
Join Pending

VRF : default
   Group ff08::1:3
        (*,G) Pending
             Incoming Interface:  1/1/1
   Group ff08::1:4
        (*,G) Pending
             Incoming Interface:  1/1/1
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 pim6 rp-candidate

```
show ipv6 pim6 rp-candidate [all-vrfs | vrf <VRF-NAME>] [vsx-peer]
```

Description

Shows the candidate RP operational and configuration information. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameters

`all-vrfs`

Shows information for all VRFs.

`vrf <VRF-NAME>`

Specifies the name of a VRF. Default: default.

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing PIM RP candidate:

```
switch# show ipv6 pim6 rp-candidate all-vrfs

 Status and Counters- PIM-SM(IPv6) Candidate-RP Information

VRF                       : blu
C-RP Admin Status         : This system is a Candidate-RP
C-RP Address              : 2007::01
C-RP Hold Time            : 60
C-RP Advertise Period     : 60
C-RP Priority             : 46
C-RP Source IP Interface  : lag1

Group Prefix   : ff00::/8
Group Prefix   : ff08::1:3/64
Group Prefix   : ff08::1:4/64


VRF                       : default
```

```
C-RP Admin Status         : This system is a Candidate-RP
C-RP Address              : 2001::01
C-RP Hold Time            : 60
C-RP Advertise Period     : 60
C-RP Priority             : 46
C-RP Source IP Interface  : 1/1/1

Group Prefix   : ff00::/8
Group Prefix   : ff08::1:5/64
Group Prefix   : ff08::1:6/64
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 pim6 rpf-override

`show ipv6 pim6 rpf-override [all-vrfs | vrf <VRF-NAME>] [vsx-peer]`

Description

Shows the RPF override configuration, which can be useful information when troubleshooting potential RPF misconfigurations. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF

Parameters

`all-vrfs`

Shows information for all VRFs.

`vrf <VRF-NAME>`

Specifies the name of a VRF. Default: default.

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing PIM RPF override:

```
switch# show ipv6 pim6 rpf-override all-vrfs

VRF : Green
Static RPF Override
Multicast Source : 2003::1/128
RPF IPv6 Address : 2001::01
Multicast Source : 2005::1/128
RPF IPv6 Address : 2007::01
VRF : Red
Static RPF Override
Multicast Source : 2004::02/128
RPF IPv6 Address : 2002::02
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 pim6 rpf-override source

`show ipv6 pim6 rpf-override source <IPv6-ADDR> [all-vrfs | vrf <VRF-NAME>] [vsx-peer]`

Description

Shows the RPF override configuration for the specified source. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameters

`source <IPv6-ADDR>`

Specifies the RPF source address in IPv6 format (`xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx`), where `x` is a hexadecimal number from 0 to F.

`all-vrfs`

Shows information for all VRFs.

`vrf <VRF-NAME>`

Specifies the name of a VRF. Default: default.

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing PIM RPF override source:

```
switch# show ipv6 pim6 rpf-override source 2004::02

VRF : default
Static RPF Override
Multicast Source : 2004::02/128
RPF IPv6 Address : 2002::02
```

Showing PIM RPF override source for all VRFs:

```
switch# show ipv6 pim6 rpf-override source 2004::02 all-vrfs

VRF : Red
Static RPF Override
Multicast Source : 2004::02/128
RPF IPv6 Address : 2002::02
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 pim6 rp-set

`show ipv6 pim6 rp-set [all-vrfs | vrf <VRF-NAME>] [vsx-peer]`

Description

Shows the multicast group support for both the learned C-RP assignments and any statically configured RP assignments. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameters

`all-vrfs`

Shows information for all VRFs.

`vrf <VRF-NAME>`

Specifies the name of a VRF. Default: default.

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing PIM RP set information:

```
switch# show ipv6 pim6 rp-set all-vrfs

VRF: blu

Status and Counters - PIM-SM(IPv6) Static RP-Set Information

Group Prefix  : ff00::/8
RP Address    : 2004::04
Override [No] : No

Status and Counters - PIM-SM(IPv6) Learned RP-Set Information

Group Prefix       : ff08::1:3/64
RP Address         : 2007::01
Hold Time (sec)    : 60
Expire Time (sec)  : 0
Group Prefix       : ff08::1:4/64
RP Address         : 2007::01
Hold Time (sec)    : 60
Expire Time (sec)  : 92

VRF: default

Status and Counters - PIM-SM(IPv6) Static RP-Set Information

Group Prefix  : ff00::/8
RP Address    : 2003::03
Override [No] : No

Status and Counters - PIM-SM(IPv6) Learned RP-Set Information

Group Prefix       : ff08::1:5/64
RP Address         : 2001::01
Hold Time (sec)    : 60
Expire Time (sec)  : 0
Group Prefix       : ff08::1:6/64
RP Address         : 2002::01
Hold Time (sec)    : 60
Expire Time (sec)  : 92
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 pim6 rp-set learned

```
show ipv6 pim6 rp-set learned [all-vrfs | vrf <VRF-NAME>] [vsx-peer]
```

Description

Shows the multicast group support for dynamically learned RP assignments. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameters

`all-vrfs`

Shows information for all VRFs.

`vrf <VRF-NAME>`

Specifies the name of a VRF. Default: default.

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing PIM RP set learned information:

```
switch# show ipv6 pim6 rp-set learned all-vrfs

VRF: blu

Status and Counters - PIM-SM(IPv6) Learned RP-Set Information
Group Prefix       : ff08::1:3/64
RP Address         : 2007::01
Hold Time (sec)    : 60
Expire Time (sec)  : 0
Group Prefix       : ff08::1:4/64
RP Address         : 2007::01
Hold Time (sec)    : 60
Expire Time (sec)  : 92

VRF: default

Status and Counters - PIM-SM(IPv6) Learned RP-Set Information
Group Prefix       : ff08::1:5/64
RP Address         : 2001::01
Hold Time (sec)    : 60
Expire Time (sec)  : 0
Group Prefix       : ff08::1:6/64
RP Address         : 2002::01
Hold Time (sec)    : 60
Expire Time (sec)  : 92
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 pim6 rp-set static

```
show ipv6 pim6 rp-set static [all-vrfs | vrf <VRF-NAME>] [vsx-peer]
```

Description

Shows the multicast group support for statically configured RP assignments. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameters

`all-vrfs`

Shows information for all VRFs.

`vrf <VRF-NAME>`

Specifies the name of a VRF. Default: default.

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing PIM Static RP set information:

```
switch# show ipv6 pim6 rp-set static all-vrfs

VRF: blu

Status and Counters - PIM-SM(IPv6) Static RP-Set Information

Group Prefix  : ff00::/8
RP Address    : 2004::04
Override [No] : No

VRF: default

Status and Counters - PIM-SM(IPv6) Static RP-Set Information

Group Prefix  : ff00::/8
RP Address    : 2003::03
Override [No] : No
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

spt-threshold

```
spt-threshold
no spt-threshold
```

Description

Enables the router to switch the multicast traffic flows to the shortest path tree. Default is enabled.

The `no` form of this command disables the routers ability to switch the multicast traffic flows to the shortest path tree.

To apply this configuration a user needs to apply disable/enable PIM globally.

Example

Enabling and disabling the SPT threshold:

```
switch(config)# router pim6
switch(config-pim6)# spt-threshold
switch(config-pim6)# no spt-threshold
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	`config-pim6`	Administrators or local user group members with execution rights for this command.

Chapter 7
Protocol Independent Multicast - Dense Mode (V4 and V6)

In a network, IP multicast traffic transmitted for multimedia applications is blocked at routed interface boundaries unless a multicast routing protocol is running. Protocol Independent Multicast (PIM) is a family of routing protocols. It forms multicast trees to forward traffic from multicast sources to subnets which use protocols such as IGMP and MLD to request the traffic.

Protocol Independent Multicast - Dense Mode (PIM-DM) overview

PIM relies on the unicast routing tables to identify the path back to a multicast source. This routing method is known as reverse path forwarding (RPF). The unicast routing protocols create the unicast routing tables. With this information, PIM sets up the distribution tree for the multicast traffic.

PIM-DM operates at the router level to direct traffic for a particular multicast group along the most efficient path to the network which has hosts that have joined that group. A unicast source address and a multicast group address comprise a given source/group (S/G) pair. Multicast traffic moving from a source to a multicast group address creates a flow to one or more areas of the network requiring the traffic. The flow destination is the multicast group address and not a specific host or VLAN. A single multicast flow has one source and one multicast group address (destination), but may reach many hosts in different subnets, depending on which hosts have issued joins for the same multicast group.

PIM routes the multicast traffic for a particular S/G pair on paths between the source unicast address and to the interfaces where it is requested (by joins from hosts connected to those subnets.) Physical destinations for a particular multicast group can be hosts in different networks. Individual hosts use IGMP/MLD configured per-subnet to send joins requesting membership in a particular multicast group. All hosts that have joined a given multicast group (defined by a multicast address) remain in that group as long as they continue to issue periodic joins.

PIM-DM interoperates with IGMP/MLD and the switch's routing protocols. PIM operates independently of the routing protocol that is chosen to run on the switches. So PIM-DM can be used with RIP, OSPF, BGP, or static routes configured. PIM-DM uses a unicast routing table to find the path to the originator of the multicast traffic and sets up multicast trees for distributing multicast traffic.

PIM-DM defaults, protocols, and supported configurations

Default configuration

PIM-DM is disabled by default. Either PIM-SM or PIM-DM can be configured within a VRF at a time. All the interfaces within the VRF must run with same mode.

Routing protocol support

PIM uses unicast routing information from any of the routing protocols that are running on the system, such as OSPFv2, OSPFv3, BGP. Static routes are also supported with Nexthop IP addresses.

PIM enabled interfaces (L3 and SVI)

PIM can be enabled across all VRFs on a maximum of 1,000 interfaces with an upper limit of 128 per VRF.

Although up to 128 PIM DM enabled interfaces can be configured, when configuring trunk interfaces with multiple Dense enabled SVIs, the trunk interfaces must have sufficient bandwidth or have only the required number of trunks it can support. This ensures that the link utilization is not exceeded due to the initial flooding nature of the protocol.

IGMP and MLD compatibility

PIM-DM is compatible with IGMP version 2 and version 3, MLD version 1 and version 2, and is fully interoperable with IGMP/MLD for determining multicast flows.

VRRP

PIM-DM is fully interoperable with VRRP to quickly transition multicast routes in a failover.

VRF support

PIM-DM can run on multiple VRF instances in parallel. It is supported on all VRFs supported in the system.

Limitations

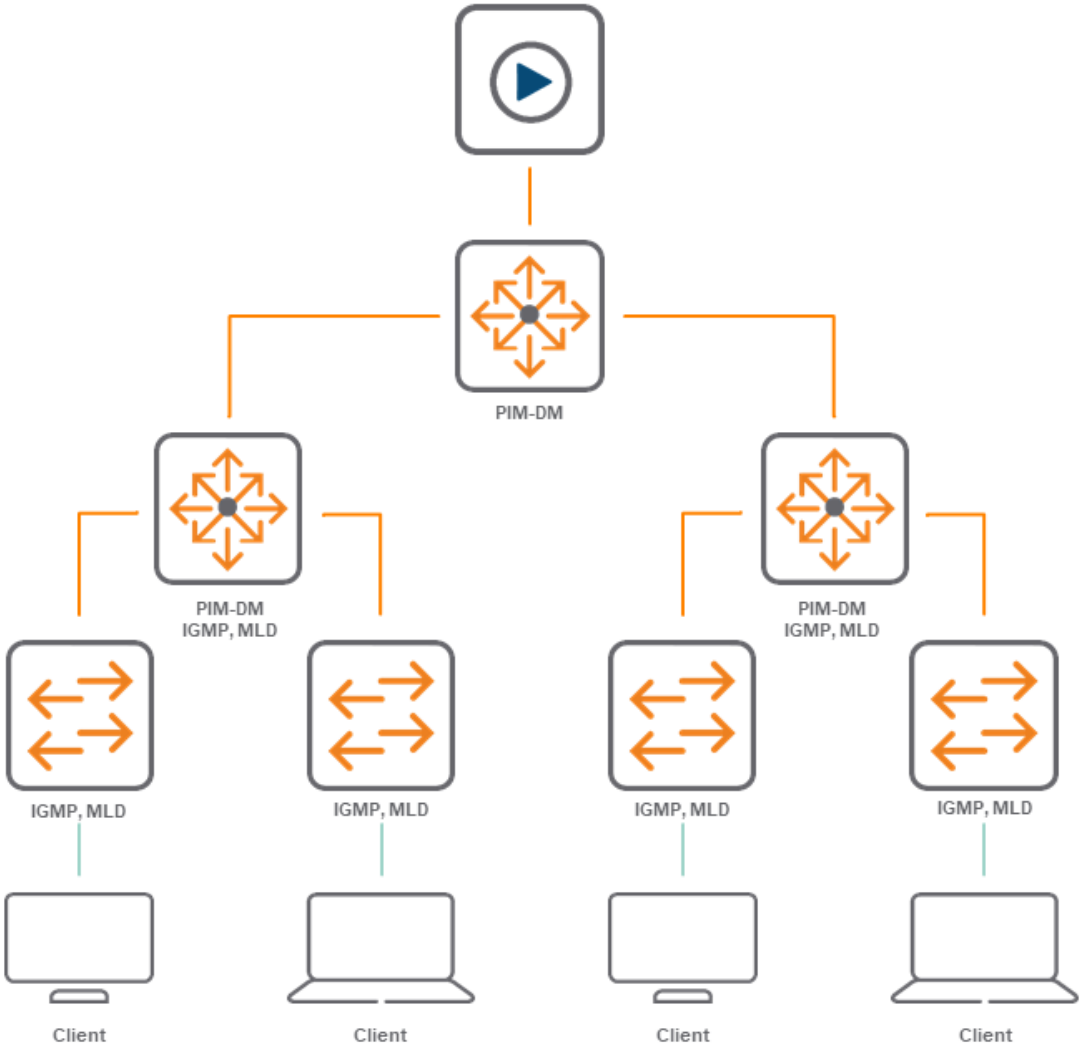
PIM-DM currently does not support the following:

- VxLAN, 6in4, 6in6, and GRE interfaces
- PIM-DM cannot be enabled on VSX deployments.

PIM-DM configuration example

When the routing switch detects a new multicast flow, it initially floods the traffic throughout the PIM-DM domain, then it prunes the traffic on the branches (network paths) where joins have not been received from individual hosts. The following is a sample topology diagram for a PIM-DM configuration.

Figure 1 *PM-DM Configuration Examples*



The routing switch maintains individual branches in the multicast tree as long as there is at least one host maintaining a membership in the multicast group. When all the hosts in a particular subnet drop out of the group, PIM-DM prunes that interface from the multicast tree. Similarly, if the routing switch detects a join from a host in a pruned interface, it adds that branch back into the tree.

Unlike PIM-SM, the number of mroutes created with dense mode is typically high since the source router floods the traffic initially to all the PIM neighbors. If we have two routers connected with many VLAN trunks, the resulting mroutes on the receiver router will be proportional to the number of SVIs configured. Ensure that the given flows are within the limits of the receiver router's mroute scale.

PIM-DM features

Multicast flow management

Multicast flow management refers to how the routing switch manages forwarding and pruned flows. This is useful when planning topologies to include multicast support and when viewing and interpreting the show command output for PIM-DM features.

Initial flood and prune

When a router running PIM-DM receives a new multicast flow, it initially floods the traffic to all downstream multicast routers. Branches that do not have members send Prune messages toward the source to prune off the unwanted/unnecessary traffic.

Maintaining the prune state

For a multicast group "X" on a given interface, when the last host belonging to group "X" leaves the group, PIM places that interface in a prune state. Multicast traffic from group "X" is now blocked to that interface. The prune state remains until a host on the same interface issues a join for group "X", in which case the router cancels the prune state and changes the flow to the forwarding state.

State-refresh packets and bandwidth conservation

A multicast switch, if directly connected to a multicast source (such as a video conference application), periodically transmits state-refresh packets to downstream multicast routers. On routers that have pruned the multicast flow, the state-refresh packets keep the pruned state alive. On routers that have been added to the network after the initial flooding and pruning of a multicast group, the state-refresh packets inform the newly added router of the current state of that branch. So if all multicast routers in a network support the state-refresh packet, the multicast router directly connected to the multicast source performs only one flood-prune cycle to the edge of the network when a new flow (multicast group) is introduced and preserves bandwidth for other uses.

PIM-DM commands for IPv4

Only the default VRF is supported on the Aruba 6200 Switch Series.

disable

`disable`

Description

Disables PIM globally on the router. PIM is disabled by default.

Using the `disable` command will cause all the multicast routes to be erased from hardware.

Example

Disabling PIM router:

```
switch(config)# router pim
switch(config-pim)# disable
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	`config-pim`	Administrators or local user group members with execution rights for this command.

enable

```
enable
```

Description

Enables PIM globally on the router.

Example

Enabling PIM router:

```
switch(config)# router pim
switch(config-pim)# enable
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	`config-pim`	Administrators or local user group members with execution rights for this command.

no ip pim-dense

```
no ip pim-dense {enable|disable}
```

Description

Enables or disables PIM-DM in the current interface. PIM-DM is disabled by default on an interface. IP address must be configured on the interface to enable PIM-DM.

Parameters

`enable`

Specifies PIM-DM on the interface. IP address must be configured on the interface to enable PIM-DM (use the `ip address <A.B.C.D/M>` command).

`disable`

Disables PIM-DM on the interface.

Examples

Enabling and disabling PIM-DM in an interface:

```
switch(config)# interface vlan40
switch(config-if-vlan)# ip address 40.0.0.4/24
switch(config-if-vlan)# ip pim-dense enable
switch(config-if-vlan)#
switch(config-if-vlan)# ip pim-dense disable
```

Enabling and disabling PIM-DM in a sub-interface:

Applies only to the Aruba 6300, 6400, and 8360 Switch Series.

```
switch(config)# interface 1/1/1.10
switch(config-subif)# ip address 10.0.0.1/24
switch(config-subif)# ip pim-dense enable
switch(config-subif)#
switch(config-subif)# ip pim-dense disable
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config-if config-if-vlan config-lag-if config-subif	Administrators or local user group members with execution rights for this command.

ip pim-dense bfd

Not supported on the Aruba 6200 Switch Series.

```
ip pim-dense bfd [disable]
no ip pim-dense bfd
```

Description

Configures BFD on a per-interface basis for an interface associated with the PIM process.

The no form of this command removes the BFD configuration on the interface and sets it to the default configuration.

If BFD is enabled globally, it will be enabled by default on all interfaces. The only exception is when it is disabled specifically on an interface using the `ip pim-dense bfd disable` command.
If BFD is disabled globally, it will be disabled by default on all interfaces. The only exception is when it is enabled specifically on an interface using the `ip pim-dense bfd` command.

Parameters

`disable`

Disables the BFD configuration on the interface.

Examples

Enabling the BFD configuration on the interface:

```
switch(config)# interface vlan40
switch(config-if-vlan)# ip pim-dense bfd
```

Removing the BFD configuration on the interface:

```
switch(config-if-vlan)# no ip pim-dense bfd
```

Disabling the BFD configuration on the interface and overriding the global setting:

```
switch(config-if-vlan)# ip pim-dense bfd disable
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	`config-if` `config-if-vlan`	Administrators or local user group members with execution rights for this command.

ip pim-dense graft-retry-interval

```
ip pim-dense graft-retry-interval <INTERVAL-VALUE>
no ip pim-dense graft-retry-interval
```

Description

Configures the interval for which the routing switch waits for the graft acknowledgment from another router before resending the graft request.

The no form of this command removes the currently configured value and sets to the default of 3 seconds.

Parameters

<INTERVAL-VALUE>

Specifies the interval the routing switch waits for the graft acknowledgement. Default: 3 seconds. Range: 1-10 seconds.

Usage

Graft packets result when a downstream router transmits a request to join a flow. The upstream router responds with a graft acknowledgment packet. If the graft acknowledgment is not received within the time period of the graft-retry-interval, it resends the graft packet.

Example

Configuring and removing dense graft retry interval on the interface:

```
switch(config)# interface vlan40
switch(config-if-vlan)# ip pim-dense graft-retry-interval 5
switch(config-if-vlan)# no ip pim-dense graft-retry-interval
```

Configuring and removing dense graft retry interval on the sub-interface:

Applies only to the Aruba 6300, 6400, and 8360 Switch Series.

```
switch(config)# interface 1/1/1.10
switch(config-subif)# ip pim-dense graft-retry-interval 5
switch(config-subif)#
switch(config-subif)# no ip pim-dense graft-retry-interval
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config-if config-if-vlan config-lag-if config-subif	Administrators or local user group members with execution rights for this command.

ip pim-dense hello-delay

```
ip pim-dense hello-delay <DELAY-VALUE>
no ip pim-dense hello-delay
```

Description

Configures the maximum time in seconds before the router actually transmits the initial PIM hello message on the current interface.

The `no` form of this command removes currently configured value and sets to the default of 5 seconds.

Parameters

<DELAY-VALUE>

Specifies the hello-delay in seconds, which is the maximum time before a triggered PIM Hello message is transmitted on this interface. Default: 5 seconds. Range: 0-5 seconds.

Usage

In cases where a new interface activates connections with multiple routers, if all the connected routers send hello packets at the same time, the receiving router could become momentarily overloaded. This command randomizes the transmission delay to a time between zero and the hello delay setting. Using zero means no delay. After the router sends the initial hello packet to a newly detected interface, it sends subsequent hello packets according to the current hello interval setting.

Example

Configuring and removing hello-delay on the interface:

```
switch(config)# interface vlan40
switch(config-if-vlan)# ip pim-dense hello-delay 4
switch(config-if-vlan)# no ip pim-dense hello-delay
```

Configuring and removing hello-delay on the sub-interface:

Applies only to the Aruba 6300, 6400, and 8360 Switch Series.

```
switch(config)# interface 1/1/1.10
switch(config-subif)# ip pim-dense hello-delay 4
switch(config-subif)#
switch(config-subif)# no ip pim-dense hello-delay
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority

6300
6400
8320
8325
8360
8400
	`config-if`
	`config-if-vlan`
	`config-lag-if`
	`config-subif`
		Administrators or local user group members with execution rights for this command.

ip pim-dense hello-interval

```
ip pim-dense hello-interval <INTERVAL-VALUE>
no ip pim-dense hello-interval
```

Description

Configures the frequency at which the router transmits PIM hello messages on the current interface.

The `no` form of this command removes the currently configured value and sets to the default of 30 seconds.

Parameters

<INTERVAL-VALUE>

Required: Specifies the frequency at which PIM Hello messages are transmitted on this interface. Default: 30 seconds. Range: 5-300 seconds.

Usage

- The router uses hello packets to inform neighbor routers of its presence.
- The router also uses this setting to compute the hello holdtime, which is included in hello packets sent to neighbor routers.
- Hello holdtime tells neighbor routers how long to wait for the next hello packet from the router. If another packet does not arrive within that time, the router removes the neighbor adjacency on that interface from the PIM adjacency table, which removes any flows running on that interface.
- Shortening the hello interval reduces the hello holdtime. If they do not receive a new hello packet when expected, it changes how quickly other routers stop sending traffic to the router.

Example

Configuring and removing dense hello-interval:

```
switch(config)# interface 1/1/4
switch(config-if)# ip pim-dense hello-interval 60
switch(config-if)# no ip pim-dense hello-interval
```

Configuring and removing dense hello-interval on the sub-interface:

Applies only to the Aruba 6300, 6400, and 8360 Switch Series.

```
switch(config-subif)# interface 1/1/10.10
switch(config-subif)# ip pim-dense hello-interval 60
switch(config-subif)#
switch(config-subif)# no ip pim-dense hello-interval
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority

6300
6400
8320
8325
8360
8400
	`config-if`
	`config-if-vlan`
	`config-lag-if`
	`config-subif`
		Administrators or local user group members with execution rights for this command.

ip pim-dense ip-addr

```
ip pim-dense ip-addr {<IP-ADDR-VALUE> | any}
no ip pim-dense ip-addr
```

Description

Enables the router to dynamically determine the source IP address to use for PIM packets sent from the interface or to use the specific IP address.

The `no` form of this command removes the currently configured value and sets to the default of `any`.

Parameters

`<IP-ADDR-VALUE>`

Specifies an IP address as the source IP for the interface.

`any`

Specifies dynamically determining the source IP from the current IP address of the interface.

Examples

Configuring and removing source IP address:

```
switch(config)# interface vlan40
switch(config-if-vlan)# ip pim-dense ip-addr 40.0.0.4
switch(config-if-vlan)# no ip pim-dense ip-addr
```

Configuring and removing source IP address on the sub-interface:

Applies only to the Aruba 6300, 6400, and 8360 Switch Series.

```
switch(config)# interface 1/1/1.10
switch(config-subif)# ip pim-dense ip-addr 10.1.1.1
switch(config-subif)#
switch(config-subif)# no ip pim-dense ip-addr
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority

6300
6400
8320
8325
8360
8400
	`config-if`
	`config-if-vlan`
	`config-lag-if`
	`config-subif`
		Administrators or local user group members with execution rights for this command.

ip pim-dense lan-prune-delay

```
ip pim-dense lan-prune-delay
no ip pim-dense lan-prune-delay
```

Description

Enables the LAN prune delay option on the current interface. The default status is enabled.

The `no` form of this command disables the LAN prune delay option.

Usage

With LAN-prune-delay enabled, the router informs downstream neighbors how long it will wait before pruning a flow after receiving a prune request. Other downstream routers on the same interface must send a join to override the prune before the LAN-prune-delay time to continue the flow. Prompts any downstream neighbors with multicast receivers continuing to belong to the flow to reply with a join. If no joins are received after the LAN-prune-delay period, the router prunes the flow. The propagation-delay and override-interval settings determine the LAN-prune-delay setting.

Example

Enabling and disabling the LAN prune delay:

```
switch(config)# interface vlan40
switch(config-if-vlan)# ip pim-dense lan-prune-delay
switch(config-if-vlan)# no ip pim-dense lan-prune-delay
```

Enabling and disabling the LAN prune delay on the sub-interface:

Applies only to the Aruba 6300, 6400, and 8360 Switch Series.

```
switch(config)# interface 1/1/1.10
switch(config-subif)# ip pim-dense lan-prune-delay
switch(config-subif)# no ip pim-dense lan-prune-delay
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config-if config-if-vlan config-lag-if config-subif	Administrators or local user group members with execution rights for this command.

ip pim-dense max-graft-retries

```
ip pim-dense max-graft-retries <ATTEMPT-VALUE>
no ip pim-dense max-graft-retries
```

Description

Configures the number of attempts the routing switch will retry sending the same graft packet to join a flow.

The no form of this command removes the currently configured value and sets to the default of 3 attempts.

Parameters

<INTERVAL-VALUE>

Specifies the number of retries for the routing switch to resend the graft packet. Default: 3 attempts. Range: 1-10 attempts.

Usage

If a graft acknowledgment response is not received after the specified number of retries, the routing switch ceases trying to join the flow. In this case the flow is removed until either a state-refresh from upstream re-initiates the flow or an upstream router floods the flow. Increasing this value helps to improve multicast reliability.

Example

Configuring and removing dense graft retry interval:

```
switch(config)# interface vlan40
switch(config-if-vlan)# ip pim-dense max-graft-retries 6
switch(config-if-vlan)# no ip pim-dense max-graft-retries
```

Configuring and removing dense graft retry interval on the sub-interface:

Applies only to the Aruba 6300, 6400, and 8360 Switch Series.

```
switch(config)# interface 1/1/1.10
switch(config-subif)# ip pim-dense max-graft-retries 6
switch(config-subif)#
switch(config-subif)# no ip pim-dense max-graft-retries
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority

6300
6400
8320
8325
8360
8400
	`config-if`
	`config-if-vlan`
	`config-lag-if`
	`config-subif`
		Administrators or local user group members with execution rights for this command.

ip pim-dense override-interval

```
ip pim-dense override-interval <INTERVAL-VALUE>
no ip pim-dense override-interval
```

Description

Configures the override interval that gets inserted into the Override Interval field of a LAN Prune Delay option.

The `no` form of this command removes the currently configured value and sets the value to the default of 2500 ms.

Parameters

<INTERVAL-VALUE>

Specifies the override interval of a LAN Prune Delay option in ms. Default: 2500 ms. Range: 500-6000.

Usage

Each router on the LAN expresses its view of the amount of randomization necessary in the Override Interval field of the LAN Prune Delay option. When all routers on a LAN use the LAN Prune Delay Option, all routers on the LAN MUST set their Override_Interval to the largest Override value on the LAN.

Example

Configuring and removing the override interval:

```
switch(config)# interface vlan40
switch(config-if-vlan)# ip pim-dense override-interval 4000
switch(config-if-vlan)# no ip pim-dense override-interval
```

Configuring and removing the override interval on the sub-interface:

Applies only to the Aruba 6300, 6400, and 8360 Switch Series.

```
switch(config)# interface 1/1/1.10
switch(config-subif)# ip pim-dense override-interval 4000
switch(config-subif)# no ip pim-dense override-interval
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority

6300
6400
8320
8325
8360
8400
	`config-if`
	`config-if-vlan`
	`config-lag-if`
	`config-subif`
		Administrators or local user group members with execution rights for this command.

ip pim-dense propagation-delay

```
ip pim-dense propagation-delay <DELAY-VALUE>
no ip pim-dense propagation-delay
```

Description

Configures the propagation delay that gets inserted into the LAN prune delay field of a LAN Prune Delay option.

The `no` form of this command removes currently configured value and sets to the default of 500 ms.

Parameters

<DELAY-VALUE>

Specifies the propagation delay value in ms. Default: 500 ms. Range: 250-2000 ms.

Usage

The LAN Delay inserted by a router in the LAN Prune Delay option expresses the expected message propagation delay on the link. When all routers on a link use the LAN Prune Delay Option, all routers on the LAN MUST set Propagation Delay to the largest LAN Delay on the LAN.

Examples

Configuring and removing the propagation delay:

```
switch(config)# interface vlan40
switch(config-if-vlan)# ip pim-dense propagation-delay 400
switch(config-if-vlan)# no ip pim-dense propagation-delay
```

Configuring and removing the propagation delay on the sub-interface:

Applies only to the Aruba 6300, 6400, and 8360 Switch Series.

```
switch(config)# interface 1/1/1.10
switch(config-subif)# ip pim-dense propagation-delay 400
switch(config-subif)# no ip pim-dense propagation-delay
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority

6300
6400
8320
8325
8360
8400
	`config-if`
	`config-if-vlan`
	`config-lag-if`
	`config-subif`
		Administrators or local user group members with execution rights for this command.

ip pim-dense ttl-threshold

```
ip pim-dense ttl-threshold <THRESHOLD-VALUE>
no ip pim-dense ttl-threshold
```

Description

Configures the multicast datagram time-to-live (router hop-count) threshold for the interface. A state-refresh packet with a TTL less than this threshold will not be forwarded out the interface.

The `no` form of this command removes the currently configured value and sets to the default of 3 attempts.

Parameters

<THRESHOLD-VALUE>

Specifies the time to live threshold. Default: 3 attempts. Range: 0-255.

Usage

The interface connected to the multicast source does not receive state refresh packets and thus is not state-refresh capable. Downstream VLANs in the switches are state-refresh capable. This parameter provides a method for containing multicast traffic within a network, or even within specific areas of a network. Initially, the multicast traffic source sets a TTL value in the packets it transmits. Each time one of these packets passes through a multicast routing device, the TTL setting decrements by 1. If the packet arrives with a TTL lower than the ttl-threshold, the routing switch does not forward the packet. The following aspects of the TTL setting of incoming multicast packets must be considered, before changing this parameter on a routing switch:

- A value that is too high will allow multicast traffic to go beyond the internal network.
- A value that is too low may prevent some intended hosts from receiving the desired multicast traffic.
- A value of 0 will forward multicast traffic regardless of the packet TTL setting.

Example

Configuring and removing the time-to-live threshold:

```
switch(config)# interface vlan40
switch(config-if-vlan)# ip pim-dense ttl-threshold 8
switch(config-if-vlan)# no ip pim-dense ttl-threshold
```

Configuring and removing the time-to-live threshold on the sub-interface:

Applies only to the Aruba 6300, 6400, and 8360 Switch Series.

```
switch(config)# interface 1/1/1.10
switch(config-subif)# ip pim-dense ttl-threshold 8
switch(config-subif)#
switch(config-subif)# no ip pim-dense ttl-threshold
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config-if config-if-vlan config-lag-if config-subif	Administrators or local user group members with execution rights for this command.

router pim

```
router pim [vrf <VRF-NAME>]
no router pim [vrf <VRF-NAME>]
```

Description

Changes the current context to the PIM configuration context. If no VRF is specified, the default VRF is assumed.

The no form of this command removes the PIM configuration from the specified context or the default VRF.

Parameters

`vrf <VRF-NAME>`

Specifies the name of a VRF.

Examples

Configuring default router PIM:

```
switch(config)# router pim
switch(config-pim)#
```

Configuring specified router PIM:

```
switch(config)# router pim vrf green
switch(config-pim)#
```

Removing router PIM:

```
switch(config)# no router pim
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Administrators or local user group members with execution rights for this command.

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config	

show ip mroute

`show ip mroute [all-vrfs | vrf <VRF-NAME>] [vsx-peer]`

Description

Shows multicast routing information. Optionally, you can show specific information by VRF. If no options are specified, it shows information for the default VRF.

Parameters

`all-vrfs`

Shows mroute information for all VRFs. Optional.

`vrf <VRF-NAME>`

Shows mroute information for a particular VRF. If the *<VRF-NAME>* is not specified, it shows information for the default VRF. Optional.

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing IP mroute for all VRFs:

```
switch# show ip mroute  all-vrfs
VRF : blue
Total number of entries : 1

Group Address           : 239.1.1.1
Source Address          : 40.0.0.5
Incoming interface      : vlan3
```

```
Downstream Interface
Interface   State
---------   -----
vlan2       forwarding

VRF : green
Total number of entries : 2

Group Address           : 239.1.1.1
Source Address          : 40.0.0.4
Neighbor                : 10.1.1.1
Incoming interface      : vlan2
Downstream Interface
Interface   State
---------   -----
vlan5       forwarding

Group Address           : 239.1.1.1
Source Address          : 40.0.0.5
Neighbor                : 10.1.1.2
Incoming interface      : vlan1
Downstream Interface
Interface   State
---------   -----
vlan6       forwarding

VRF : default
Total number of entries : 1

Group Address           : 10.1.1.14
Source Address          : 40.0.0.6
Neighbor                : 10.1.1.2
Incoming interface      : 1/1/5
Downstream Interface
Interface   State
---------   -----
1/1/3       forwarding
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip mroute group-addr

`show ip mroute <GROUP-ADDR> [<SOURCE-ADDR>] [all-vrfs | vrf <vrf-name>] [vsx-peer]`

Description

Shows the multicast routing information for the given group address. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameters

<GROUP-ADDR>

Specifies a group address in IPv4 format (`x.x.x.x`), where `x` is a decimal number from 0 to 255.

<SOURCE-ADDR>

Specifies show information for the group from this source in IPv4 format (`x.x.x.x`), where `x` is a decimal number from 0 to 255.

`all-vrfs`

Shows mroute information for the group for all VRFs.

`vrf` *<VRF-NAME>*

Specifies the name of a VRF.

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing information for group 239.1.1.1 and VRF green:

```
switch# show ip mroute 239.1.1.1 vrf green

VRF : green

Group Address                 : 239.1.1.1
Source Address                : 40.0.0.5
Neighbor                      : 10.1.1.2
Incoming interface            : vlan1
Unicast Routing Protocol      : connected
Metric                        : 1234
Metric  Pref                  : 1234
Downstream Interface
Interface   State
---------   -----
vlan6       forwarding
```

Showing information for group 239.1.1.1 from source 40.0.0.5 and all VRFs:

```
switch# show ip mroute 239.1.1.1 40.0.0.5 all-vrfs

VRF : blue

Group Address                 : 239.1.1.1
Source Address                : 40.0.0.5
Incoming interface            : vlan3
Unicast Routing Protocol      : connected
Metric                        : 1234
Metric  Pref                  : 1234
Downstream Interface
Interface   State
---------   -----
vlan2       forwarding
```

```
VRF : green

Group Address                 : 239.1.1.1
Source Address                : 40.0.0.5
Neighbor                      : 10.1.1.2
Incoming interface            : vlan1
Unicast Routing Protocol      : connected
Metric                        : 1234
Metric  Pref                  : 1234
Downstream Interface
Interface   State
---------   -----
vlan6       forwarding
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip mroute brief

```
show ip mroute brief [al-vrfs | vrf <VRF-NAME>] [vsx-peer]
```

Description

Shows brief version of the multicast routing information. Optionally, you can specify the display information by VRF. If no options are specified, it shows information for the default VRF.

Parameters

`all-vrfs`

Shows mroute information briefly for all VRFs.

`vrf <VRF-NAME>`

Specifies the name of a VRF. Default: default.

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing the IP mroute brief:

```
switch# show ip mroute  brief
VRF : default
Total number of entries : 1

Group Address      Source Address     Neighbor          Interface
-------------      --------------     --------          ---------
239.1.1.1          40.0.0.6           10.1.1.2          vlan5
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip pim

`show ip pim [all-vrfs | vrf <VRF-NAME>] [vsx-peer]`

Description

Shows the PIM router information. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameters

`all-vrfs`

Optional. Shows PIM router information on all VRFs.

`vrf <VRF-NAME>`

Optional. Shows PIM router information for a particular VRF. If the *<VRF-NAME>* is not specified, it shows information for the default VRF.

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing IP PIM router:

```
switch# show ip pim

PIM Global Parameters
```

```
VRF                           :  default
PIM Status                    :  Enabled
Join/Prune Interval (sec)     :  60
SPT Threshold                 :  Enabled
State Refresh Interval (sec)  :  60
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip pim interface

`show ip pim interface [all-vrfs | vrf <VRF-NAME>] [vsx-peer]`

Description

Shows the information about PIM interfaces currently configured in the router. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameters

`all-vrfs`

Optional. Shows PIM interface information for all VRFs.

`vrf <VRF-NAME>`

Optional. Shows PIM interface information for a particular VRF. If the *<VRF-NAME>* is not specified, it shows the default VRF information.

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing PIM interface:

```
switch# show ip pim interface

PIM Interfaces

VRF: default
```

```
Interface          IP Address         mode
------------------ ------------------ ----------
1/1/1              40.0.0.4/24        dense
1/1/2              50.0.0.4/24        dense
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip pim interface interface-name

`show ip pim interface <INTERFACE-NAME> [vsx-peer]`

Description

Shows detailed information about the PIM interface currently configured.

Parameters

<INTERFACE-NAME>

Specifies an interface for showing PIM interface information. Interface can also be a LAG or VLAN.

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing PIM interface information for interface 1/1/2:

```
switch# show ip pim interface 1/1/2

PIM Interfaces

VRF: default

Interface  : 1/1/2
IP Address : 50.0.0.4/24
Mode       : dense

Designated Router :
Hello Interval (sec)      : 30
```

```
Hello Delay (sec)          : 5
Graft Retry Interval(sec)  : 3
Max Graft Retries          : 5
SR TTL Threshold           : 8

Override Interval (msec)   : 2500              Lan Prune Delay      : Yes
Propagation Delay (msec)   : 500               DR Priority          : 1
Neighbor Timeout           : 105
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip pim interface interface-name counters

`show ip pim interface <INTERFACE-NAME> counters [vsx-peer]`

Description

Shows the PIM packet counters information for the specified interface.

Parameters

<INTERFACE-NAME>

Specifies the interface to show packet counter information.

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing PIM packet counters:

```
switch# show ip pim interface vlan1 counters

Interface           : vlan1
VRF                 : default

Rx Counters :

Hello               4
```

```
State Refresh       0
Join/Prune          1
RPadv               0
Graft               0
GraftAck            0
Assert              0
Bsm                 0

Tx Counters :

Hello               9
State Refresh       0
Join/Prune          0
RPadv               0
Graft               0
GraftAck            0
Assert              0
Bsm                 0

Invalid Rx Counters :

Hello               0
State Refresh       0
Join/Prune          0
RPadv               0
Graft               0
GraftAck            0
Assert              0
Bsm                 0
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip pim neighbor

`show ip pim neighbor [<IP-ADDR>] [all-vrfs | vrf <VRF-NAME>] [vsx-peer]`

Description

Shows PIM neighbor information. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameters

`all-vrfs`

Selects all VRFs.

`vrf <VRF-NAME>`

Specifies the name of a VRF. Default: default.

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing PIM neighbor information:

```
switch# show ip pim neighbor

PIM Neighbor

VRF                 : default
IP Address          : 40.0.0.44
Interface           : 1/1/1
Up Time (sec)       : 544
Expire Time (sec)   : 80
DR Priority         : 40
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

state-refresh-interval

```
state-refresh <INTERVAL-VALUE>
no state-refresh
```

Description

Configures the interval between successive state-refresh messages originated by the routing switch. Only the routing switch connected directly to the multicast source initiates state-refresh packets. All other PIM routers in the network only propagate these state-refresh packets.

The `no` form of this command sets the interval to the default value of 60 seconds.

Parameters

`<INTERVAL-VALUE>`

Specifies the state refresh interval in seconds. Default: 60 seconds. Range 10-100.

Examples

Configuring the state refresh interval:

```
switch(config)# router pim
switch(config-pim)# state-refresh 30
switch(config-pim)# no state-refresh
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config-pim	Administrators or local user group members with execution rights for this command.

PIM-DM commands for IPv6

Only the default VRF is supported on the Aruba 6200 Switch Series.

disable

`disable`

Description

Disables PIMv6 globally on the router.

Using the `disable` command will cause all the multicast routes to be erased from hardware.

Example

Disabling PIM router:

```
switch(config)# router pim6
switch(config-pim6)# disable
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	`config-pim6`	Administrators or local user group members with execution rights for this command.

enable

`enable`

Description

Enables PIMv6 globally on the router.

Example

Enabling PIM router:

```
switch(config)# router pim6
switch(config-pim6)# enable
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	`config-pim6`	Administrators or local user group members with execution rights for this command.

ipv6 pim6-dense

`ipv6 pim6-dense {enable | disable}`

Description

Enables or disables PIM-DM on the current interface. PIM-DM is disabled by default on an interface. An IPv6 address must be configured on the interface to enable PIM-DM.

Parameters

`enable`

Enables PIM-DM on the interface. IPv6 address must be configured on the interface to enable PIM-SM (use the `ipv6 address <X:X::X:X/M>` command).

`disable`

Disables PIM-DM on the interface.

Examples

Enabling and disabling PIM-DM on an interface:

```
switch(config)# interface vlan40
switch(config-if-vlan)# ipv6 address 2001::01/64
switch(config-if-vlan)# ipv6 pim6-dense enable
switch(config-if-vlan)# ipv6 pim6-dense disable
```

Enabling and disabling PIM-DM on a sub-interface:

Applies only to the Aruba 6300, 6400, and 8360 Switch Series.

```
switch(config)# interface 1/1/1.10
switch(config-subif)# ipv6 address 1001::01/64
switch(config-subif)# ipv6 pim6-dense enable
switch(config-subif)# ipv6 pim6-dense disable
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority

6300
6400
8320
8325
8360
8400
	`config-if`
	`config-if-vlan`
	`config-lag-if`
	`config-subif`
		Administrators or local user group members with execution rights for this command.

ipv6 pim6-dense bfd

Not supported on the Aruba 6200 Switch Series.

```
ipv6 pim6-dense bfd [disable]
no ipv6 pim6-dense bfd
```

Description

Configures BFD on a per-interface basis for an interface associated with the PIM process.

The `no` form of this command removes the BFD configuration on the interface and sets it to the default configuration.

If BFD is enabled globally, it will be enabled by default on all interfaces. The only exception is when it is disabled specifically on an interface using the `ipv6 pim6-dense bfd disable` command.
If BFD is disabled globally, it will be disabled by default on all interfaces. The only exception is when it is enabled specifically on an interface using the `ipv6 pim6-dense bfd` command.

Parameters

`disable`

Disables the BFD configuration on the interface.

Examples

Enabling the BFD configuration on the interface:

```
switch(config)# interface vlan40
switch(config-if-vlan)# ipv6 pim6-dense bfd
```

Disabling the BFD configuration on the interface:

```
switch(config-if-vlan)# ipv6 pim6-dense bfd disable
```

Removing the BFD configuration on the interface:

```
switch(config-if-vlan)# no ipv6 pim6-dense bfd
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority

6300
6400
8320
8325
8360
8400
	`config-if`
	`config-if-vlan`
	`config-lag-if`
		Administrators or local user group members with execution rights for this command.

ipv6 pim6-dense graft-retry-interval

`ipv6 pim6-dense graft-retry-interval <INTERVAL-VALUE>`
`no ipv6 pim6-dense graft-retry-interval`

Description

Configures the interval for which the routing switch waits for the graft acknowledgment from another router before resending the graft request.

The `no` form of this command removes the currently configured value and sets to the default of 3 seconds.

Parameters

<INTERVAL-VALUE>

Specifies the interval the routing switch waits for the graft acknowledgement. Default: 3 seconds. Range: 1-10.

Usage

Graft packets result when a downstream router transmits a request to join a flow. The upstream router responds with a graft acknowledgment packet. If the graft acknowledgment is not received within the time period of the graft-retry-interval, it resends the graft packet.

Example

Configuring and removing dense graft retry interval:

```
switch(config)# interface vlan40
switch(config-if-vlan)# ipv6 pim6-dense graft-retry-interval 5
switch(config-if-vlan)# no ipv6 pim6-dense graft-retry-interval
```

Configuring and removing dense graft retry interval on the sub-interface:

Applies only to the Aruba 6300, 6400, and 8360 Switch Series.

```
switch(config)# interface 1/1/1.10
switch(config-subif)# ipv6 pim6-dense graft-retry-interval 5
switch(config-subif)#
switch(config-subif)# no ipv6 pim6-dense graft-retry-interval
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config-if config-if-vlan config-lag-if config-subif	Administrators or local user group members with execution rights for this command.

ipv6 pim6-dense hello-delay

```
ipv6 pim6-dense hello-delay <DELAY-VALUE>
no ipv6 pim6-dense hello-delay
```

Description

Configures the maximum time in seconds before the router actually transmits the initial PIM hello message on the current interface.

The `no` form of this command removes currently configured value and sets to the default of 5 seconds.

Parameters

<DELAY-VALUE>

Specifies the hello-delay in seconds, which is the maximum time before a triggered PIM Hello message is transmitted on this interface. Default: 5 seconds. Range: 0-5.

Usage

- In cases where a new interface activates connections with multiple routers, if all the connected routers sent hello packets at the same time, the receiving router could become momentarily overloaded.
- This command randomizes the transmission delay to a time between zero and the hello delay setting. Using zero means no delay. After the router sends the initial hello packet to a newly detected interface, it sends subsequent hello packets according to the current hello interval setting.

Example

Configuring and removing hello-delay on the interface:

```
switch(config)# interface vlan40
switch(config-if-vlan)# ipv6 pim6-dense hello-delay 4
switch(config-if-vlan)# no ipv6 pim6-dense hello-delay
```

Configuring and removing hello-delay on the sub-interface:

Applies only to the Aruba 6300, 6400, and 8360 Switch Series.

```
switch(config)# interface 1/1/1.10
switch(config-subif)# ipv6 pim6-dense hello-delay 4
switch(config-subif)#
switch(config-subif)# no ipv6 pim6-dense hello-delay
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority

6300
6400
8320
8325
8360
8400
	`config-if`
	`config-if-vlan`
	`config-lag-if`
	`config-subif`
		Administrators or local user group members with execution rights for this command.

ipv6 pim6-dense hello-interval

```
ipv6 pim6-dense hello-interval <INTERVAL-VALUE>
no ipv6 pim6-dense hello-interval
```

Description

Configures the frequency at which the router transmits PIM hello messages on the current interface.

The `no` form of this command removes the currently configured value and sets to the default of 30 seconds.

Parameters

<INTERVAL-VALUE>

Specifies the frequency at which PIM Hello messages are transmitted on this interface. Default: 30 seconds. Range: 5-300.

Usage

- The router uses hello packets to inform neighbor routers of its presence.
- The router also uses this setting to compute the hello holdtime, which is included in hello packets sent to neighbor routers.
- Hello holdtime tells neighbor routers how long to wait for the next hello packet from the router. If another packet does not arrive within that time, the router removes the neighbor adjacency on that interface from the PIM adjacency table, which removes any flows running on that interface.
- Shortening the hello interval reduces the hello holdtime. If they do not receive a new hello packet when expected, it changes how quickly other routers stop sending traffic to the router.

Example

Configuring and removing dense hello-interval:

```
switch(config)# interface 1/1/4
switch(config-if)# ipv6 pim6-dense hello-interval 60
switch(config-if)# no ipv6 pim6-dense hello-interval
```

Configuring and removing dense hello-interval on the sub-interface:

Applies only to the Aruba 6300, 6400, and 8360 Switch Series.

```
switch(config-subif)# interface 1/1/10.10
switch(config-subif)# ipv6 pim6-dense hello-interval 60
switch(config-subif)#
switch(config-subif)# no ipv6 pim6-dense hello-interval
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config-if config-if-vlan config-lag-if config-subif	Administrators or local user group members with execution rights for this command.

ipv6 pim6-dense ipv6-addr

```
ipv6 pim6-dense ipv6-addr {<IPV6-ADDR-VALUE> | any}
no ipv6 pim6-dense ipv6-addr
```

Description

Enables the router to dynamically determine the source IP address to use for PIM packets sent from the interface or to use the specific IP address.

The `no` form of this command removes the currently configured value and sets to the default of `any`.

Parameters

<IPV6-ADDR-VALUE>

Specifies an IPv6 address as the source IP for the interface.

`any`

Specifies dynamically determining the source IP from the current IPv6 address of the interface.

Examples

Configuring and removing the source IP address:

```
switch(config)# interface vlan40
switch(config-if-vlan)# ipv6 pim6-dense ip-addr 2001::02
switch(config-if-vlan)# no ipv6 pim6-dense ipv6-addr
```

Configuring and removing the source IP address for the sub-interface:

Applies only to the Aruba 6300, 6400, and 8360 Switch Series.

```
switch(config)# interface 1/1/1.10
switch(config-subif)# ipv6 pim6-dense ipv6-addr 1001::01
switch(config-subif)#
switch(config-subif)# no ipv6 pim6-dense ipv6-addr
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config-if config-if-vlan config-lag-if config-subif	Administrators or local user group members with execution rights for this command.

ipv6 pim6-dense lan-prune-delay

```
ipv6 pim6-dense lan-prune-delay
no ipv6 pim6-dense lan-prune-delay
```

Description

Enables the LAN prune delay option on the current interface. The default status is enabled.

The no form of this command disables the LAN prune delay option.

Usage

With LAN-prune-delay enabled, the router informs downstream neighbors how long it will wait before pruning a flow after receiving a prune request. Other downstream routers on the same interface must send a join to override the prune before the LAN-prune-delay time to continue the flow. Prompts any downstream neighbors with multicast receivers continuing to belong to the flow to reply with a join. If no joins are received after the LAN-prune-delay period, the router prunes the flow. The propagation-delay and override-interval settings determine the LAN-prune-delay setting.

Example

Enabling and disabling the LAN prune delay:

```
switch(config)# interface vlan40
switch(config-if-vlan)# ipv6 pim6-dense lan-prune-delay
switch(config-if-vlan)# no ipv6 pim6-dense lan-prune-delay
```

Enabling and disabling the LAN prune delay on the sub-interface:

Applies only to the Aruba 6300, 6400, and 8360 Switch Series.

```
switch(config)# interface 1/1/1.10
switch(config-subif)# no ipv6 pim6-dense lan-prune-delay
switch(config-subif)#
switch(config-subif)# ipv6 pim6-dense lan-prune-delay
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config-if config-if-vlan config-lag-if config-subif	Administrators or local user group members with execution rights for this command.

ipv6 pim6-dense max-graft-retries

```
ipv6 pim6-dense max-graft-retries <ATTEMPT-VALUE>
no ipv6 pim6-dense max-graft-retries
```

Description

Configures the number of attempts the routing switch will retry sending the same graft packet to join a flow.

The no form of this command removes the currently configured value and sets to the default of 3 attempts.

Parameters

<INTERVAL-VALUE>

Specifies the number of retries for the routing switch to resend the graft packet. Default: 3 attempts. Range: 1-10.

Usage

If a graft acknowledgment response is not received after the specified number of retries, the routing switch ceases trying to join the flow. In this case the flow is removed until either a state-refresh from upstream re-initiates the flow or an upstream router floods the flow. Increasing this value helps to improve multicast reliability.

Example

Configuring and removing the dense graft retry interval:

```
switch(config)# interface vlan40
switch(config-if-vlan)# ipv6 pim6-dense max-graft-retries 6
switch(config-if-vlan)# no ipv6 pim6-dense max-graft-retries
```

Configuring and removing the dense graft retry interval on the sub-interface:

Applies only to the Aruba 6300, 6400, and 8360 Switch Series.

```
switch(config)# interface 1/1/1.10
switch(config-subif)# ipv6 pim6-dense max-graft-retries 6
switch(config-subif)# no ipv6 pim6-dense max-graft-retries
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority

6300
6400
8320
8325
8360
8400
	`config-if`
	`config-if-vlan`
	`config-lag-if`
	`config-subif`
		Administrators or local user group members with execution rights for this command.

ipv6 pim6-dense override-interval

```
ipv6 pim6-dense override-interval <INTERVAL-VALUE>
no ipv6 pim6-dense override-interval
```

Description

Configures the override interval that gets inserted into the Override Interval field of a LAN Prune Delay option.

The `no` form of this command removes the currently configured value and sets the value to the default of 2500 ms.

Parameters

<INTERVAL-VALUE>

Specifies the override interval of a LAN Prune Delay option in ms. Default: 2500 ms. Range: 500-6000.

Usage

Each router on the LAN expresses its view of the amount of randomization necessary in the Override Interval field of the LAN Prune Delay option. When all routers on a LAN use the LAN Prune Delay Option, all routers on the LAN MUST set their Override_Interval to the largest Override value on the LAN.

Example

Configuring and removing the override interval:

```
switch(config)# interface vlan40
switch(config-if-vlan)# ipv6 pim6-dense override-interval 4000
switch(config-if-vlan)# no ipv6 pim6-dense override-interval
```

Configuring and removing the override interval on the sub-interface:

Applies only to the Aruba 6300, 6400, and 8360 Switch Series.

```
switch(config)# interface 1/1/1.10
switch(config-subif)# ipv6 pim6-dense override-interval 4000
switch(config-subif)#
switch(config-subif)# no ipv6 pim6-dense override-interval
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority

6300
6400
8320
8325
8360
8400
	`config-if`
	`config-if-vlan`
	`config-lag-if`
	`config-subif`
		Administrators or local user group members with execution rights for this command.

ipv6 pim6-dense propagation-delay

```
ipv6 pim6-dense propagation-delay <DELAY-VALUE>
no ipv6 pim6-dense propagation-delay
```

Description

Configures the propagation delay that gets inserted into the LAN prune delay field of a LAN Prune Delay option.

The `no` form of this command removes currently configured value and sets to the default of 500 ms.

Parameters

<DELAY-VALUE>

Specifies the propagation delay value in ms. Default: 500 ms. Range: 250-2000.

Usage

The LAN Delay inserted by a router in the LAN Prune Delay option expresses the expected message propagation delay on the link. When all routers on a link use the LAN Prune Delay Option, all routers on the LAN MUST set Propagation Delay to the largest LAN Delay on the LAN.

Examples

Configuring and removing the propagation delay:

```
switch(config)# interface vlan40
switch(config-if-vlan)# ipv6 pim6-dense propagation-delay 400
switch(config-if-vlan)# no ipv6 pim6-dense propagation-delay
```

Configuring and removing the propagation delay on the sub-interface:

Applies only to the Aruba 6300, 6400, and 8360 Switch Series.

```
switch(config)# interface 1/1/1.10
switch(config-subif)# ipv6 pim6-dense propagation-delay 400
switch(config-subif)#
switch(config-subif)# no ipv6 pim6-dense propagation-delay
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority

6300
6400
8320
8325
8360
8400
	`config-if`
	`config-if-vlan`
	`config-lag-if`
	`config-subif`
		Administrators or local user group members with execution rights for this command.

ipv6 pim6-dense ttl-threshold

```
ipv6 pim6-dense ttl-threshold <THRESHOLD-VALUE>
no ipv6 pim6-dense ttl-threshold
```

Description

Configures the multicast datagram time-to-live (router hop-count) threshold for the interface. Any IP multicast datagrams or state-refresh packets with a TTL less than this threshold will not be forwarded out the interface.

The `no` form of this command removes the currently configured value and sets to the default of 3 attempts.

Parameters

<THRESHOLD-VALUE>

Specifies the time-to-live threshold. Default: 3 attempts. Range: 0-255.

Usage

The VLAN connected to the multicast source does not receive state refresh packets and thus is not state-refresh capable. Downstream VLANs in the switches are state-refresh capable. This parameter provides a method for containing multicast traffic within a network, or even within specific areas of a network. Initially, the multicast traffic source sets a TTL value in the packets it transmits. Each time one of these packets passes through a multicast routing device, the TTL setting decrements by 1. If the packet arrives with a TTL lower than the ttl-threshold, the routing switch does not forward the packet. The following aspects of the TTL setting of incoming multicast packets must be considered, before changing this parameter on a routing switch:

- A value that is too high will allow multicast traffic to go beyond the internal network.
- A value that is too low may prevent some intended hosts from receiving the desired multicast traffic.
- A value of 0 will forward multicast traffic regardless of the packet TTL setting.

Example

Configuring and removing the time-to-live threshold:

```
switch(config)# interface vlan40
switch(config-if-vlan)# ipv6 pim6-dense ttl-threshold 8
switch(config-if-vlan)# no ipv6 pim6-dense ttl-threshold
```

Configuring and removing the time-to-live threshold on the sub-interface:

Applies only to the Aruba 6300, 6400, and 8360 Switch Series.

```
switch(config)# interface 1/1/1.10
switch(config-subif)# ipv6 pim6-dense ttl-threshold 8
switch(config-subif)# no ipv6 pim6-dense ttl-threshold
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config-if config-if-vlan config-lag-if config-subif	Administrators or local user group members with execution rights for this command.

no ipv6 pim6-dense

no ip pim-dense

Description

Removes PIM-DM for all IPv6 related configurations for the interface.

Examples

Removing all PIM-DM configurations on an interface:

```
switch(config)# interface vlan40
switch(config-if-vlan)# no ipv6 pim6-dense
```

Removing all PIM-DM configurations on a sub-interface:

Applies only to the Aruba 6300, 6400, and 8360 Switch Series.

```
switch(config)# interface 1/1/1.10
switch(config-subif)# no ipv6 pim6-dense
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority

6300
6400
8320
8325
8360
8400
	`config-if`
	`config-if-vlan`
	`config-lag-if`
	`config-subif`
		Administrators or local user group members with execution rights for this command.

show ipv6 pim6

`show ipv6 pim6 [all-vrfs | vrf <VRF-NAME>] [vsx-peer]`

Description

Shows the PIM router information. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameters

`all-vrfs`

Shows information for all VRFs.

`vrf <VRF-NAME>`

Specifies the name of a VRF. Default: default.

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing the IPv6 PIM router:

```
switch# show ipv6 pim6

PIM Global Parameters

VRF                          :  default
PIM Status                   :  Enabled
Join/Prune Interval (sec)    :  46
SPT Threshold                :  Disabled
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 pim6 interface

`show ipv6 pim6 interface [all-vrfs | vrf <VRF-NAME>] [vsx-peer]`

Description

Shows the information about PIM interfaces currently configured in the router. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameters

`all-vrfs`

Optional. Shows PIM interface information for all VRFs.

`vrf <VRF-NAME>`

Optional. Shows PIM interface information for a particular VRF. If the `<VRF-NAME>` is not specified, it shows the default VRF information.

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing PIM interface:

```
switch# show ipv6 pim6 interface
PIM Interfaces

VRF: default

Interface          IP Address
mode
------------------ ------------------------------------------------------------  -
---------
1/1/1              fe80::a00:9ff:feec:dc0e/64
dense
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 pim6 interface interface-name

```
show ipv6 pim6 interface <INTERFACE-NAME> [vsx-peer]
```

Description

Shows detailed information about the PIM interface currently configured.

Parameters

<INTERFACE-NAME>

Specifies an interface for showing PIM interface information. Interface can also be a LAG or VLAN.

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing PIM interface information for interface 1/1/1:

```
switch# show ipv6 pim6 interface 1/1/1

PIM Interfaces

VRF: default

Interface             : 1/1/1
IPv6 Address          : fe80::a00:9ff:feec:dc0e/64
Mode                  : dense

Designated Router     : fe80::a00:9ff:febd:8364
Hello Interval        : 30 sec
Hello Delay           : 4 sec

Override Interval     : 500 msec              LAN Prune Delay     : Yes
Propagation Delay     : 350 msec              DR Priority         : 3
Neighbor Timeout      : 0                     TTL Threshold       : 250
Graft Retry Interval  : 9                     Max Graft Retries   : 9
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 mroute

```
show ipv6 mroute [all-vrfs | vrf <VRF-NAME>] [vsx-peer]
```

Description

Shows multicast routing information. Optionally, you can show specific information by VRF. If no options are specified, it shows information for the default VRF.

Parameters

`all-vrfs`

Shows information for all VRFs.

`vrf <VRF-NAME>`

Specifies the name of a VRF. Default: default.

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing IPv6 mroute:

```
switch# show ipv6 mroute  all-vrfs
IP Multicast Route Entries

VRF : blu
Total number of entries : 2

Group Address           : ff08::1:3
Source Address          : 2002::04
Neighbor                : 2001::04
Incoming interface      : 1/1/2
Outgoing Interface List :
Interface      State
---------      -----
1/1/3          pruned
1/1/4          forwarding

Group Address           : ff08::1:4
Source Address          : 2003::04
Neighbor                : 2001::04
Incoming interface      : 1/1/2
Outgoing Interface List :
Interface      State
---------      -----
1/1/3          pruned

VRF : default
```

```
Total number of entries : 1

Group Address           : ff08::1:5
Source Address          : 2001::03
Neighbor                : 2003::04
Incoming interface      : 1/1/1
Outgoing Interface List :
Interface      State
---------      -----
1/1/4          pruned
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 mroute brief

```
show ipv6 mroute brief [all-vrfs | vrf <VRF-NAME>] [vsx-peer]
```

Description

Shows brief version of the multicast routing information. Optionally, you can specify the display information by VRF. If no options are specified, it shows information for the default VRF.

Parameters

`all-vrfs`

Shows information for all VRFs.

`vrf <VRF-NAME>`

Specifies the name of a VRF. Default: default.

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

Showing the IPv6 mroute brief:

```
switch# show ipv6 mroute brief all-vrfs
IP Multicast Route Entries
```

```
VRF : blu
Total number of entries : 2

Group Address  : ff08::1:3
Source Address : 2002::04
Neighbor       : 2003::04
Interface       : 1/1/2

Group Address  : ff08::1:4
Source Address : 2002::03
Neighbor       : 2003::05
Interface       : 1/1/3

VRF : default
Total number of entries : 1

Group Address  : ff08::1:5
Source Address : 2001::03
Neighbor       : 2002::01
Interface       : 1/1/1
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 mroute group-addr

```
show ipv6 mroute <GROUP-ADDR> [<SOURCE-ADDR>]
     [all-vrfs | vrf <vrf-name>] [vsx-peer]
```

Description

Shows the multicast routing information for the given group address. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameters

<GROUP-ADDR>

Specifies show information for the group address. Format: X:X::X:X

<SOURCE-ADDR>

Optional. Specifies show information for the group from this source. Format: X:X::X:X

`all-vrfs`

Optional. Shows mroute information for the group for all VRFs.

`vrf` *<VRF-NAME>*

Optional. Shows mroute information for the group for a particular VRF. If the *<VRF-NAME>* is not specified, it shows information for the default VRF.

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Showing information for group ff08::1:3 and VRF green:

```
switch# show ipv6 mroute  ff08::1:3 vrf green

IP Multicast Route Entries

VRF : green

Group Address                 : ff08::1:3
Source Address                : 2001::03
Neighbor                      : 2003::04
Incoming Interface            : 1/1/1
Multicast Routing Protocol    : PIM-DM
Unicast Routing Protocol      : connected
Metric                        : 0
Metric  Pref                  : 0

Downstream Interface
Interface      State
---------      -----
1/1/4          pruned
```

Showing information for group ff08::1:3 from source 2001::03 and all VRFs:

```
switch# show ipv6 mroute  ff08::1:3 2001::03 all-vrfs

IP Multicast Route Entries

VRF : blue

Group Address                 : ff08::1:3
Source Address                : 2001::03
Neighbor                      : 2003::04
Incoming Interface            : 1/1/1
Multicast Routing Protocol    : PIM-DM
Unicast Routing Protocol      : connected
Metric                        : 0
Metric  Pref                  : 0

Downstream Interface
Interface      State
---------      -----
1/1/4          pruned

VRF : green

Group Address                 : ff08::1:3
Source Address                : 2001::03
Neighbor                      : 2003::04
Incoming Interface            : 1/1/2
Multicast Routing Protocol    : PIM-DM
```

```
Unicast Routing Protocol      : connected
Metric                        : 0
Metric  Pref                  : 0

Downstream Interface
Interface      State
---------      -----
1/1/4          pruned

VRF : red

Group Address                 : ff08::1:6
Source Address                : 2001::04
Neighbor                      : 2003::04
Incoming Interface            : 1/1/2
Multicast Routing Protocol    : PIM-DM
Unicast Routing Protocol      : connected
Metric                        : 0
Metric  Pref                  : 0

Downstream Interface
Interface      State               By_Proxy_Dr
---------      -----               -----------
vlan10         forwarding          false
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ipv6 pim6 neighbor

`show ipv6 pim6 neighbor [<IPv6-ADDR>] [all-vrfs | vrf <VRF-NAME>] [vsx-peer]`

Description

Shows PIM neighbor information. Optionally, you can specify display information by VRF. If no options are specified, it shows information for the default VRF.

Parameters

<IPv6-ADDR>

Specifies a neighbor address in IPv6 format (`xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx`), where `x` is a hexadecimal number from 0 to F.

`all-vrfs`

Shows information for all VRFs.

`vrf <VRF-NAME>`

Specifies the name of a VRF. Default: default.

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Example

On the 6400 Switch Series, interface identification differs.

Showing PIM neighbor information:

```
switch# show ipv6 pim6 neighbor

PIM Neighbor

VRF                 : default
IP Address          : 2001::02
Interface           : 1/1/1
Up Time (sec)       : 0
Expire Time (sec)   : 0
DR Priority         : 44
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

router pim6

`router pim6 [vrf <VRF-NAME>]`
`no router pim6 [vrf <VRF-NAME>]`

Description

Changes the current context to the PIMv6 configuration context. If no VRF is specified, the default VRF is assumed.

The `no` form of this command removes the PIM configuration from the specified context or the default VRF.

Parameters

`vrf <VRF-NAME>`

Specifies the name of a VRF. Default: default.

Examples

Configuring default router PIM:

```
switch(config)# router pim6
switch(config-pim6)#
```

Configuring specified router PIM:

```
switch(config)# router pim6 vrf Green
switch(config-pim6)#
```

Removing router PIM:

```
switch(config)# no router pim6
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config	Administrators or local user group members with execution rights for this command.

state-refresh-interval

```
state-refresh <INTERVAL-VALUE>
no state-refresh
```

Description

Configures the interval between successive state-refresh messages originated by the routing switch. Only the routing switch connected directly to the unicast source initiates state-refresh packets. All other PIM routers in the network only propagate these state-refresh packets.

The no form of this command sets the interval to the default value of 60 seconds.

Parameters

<INTERVAL-VALUE>

Specifies the state refresh interval in seconds. Default: 60 seconds. Range 10-100.

Examples

Configuring the state refresh interval:

```
switch(config)# router pim6
switch(config-pim6)# state-refresh 30
switch(config-pim6)# no state-refresh
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config-pim6	Administrators or local user group members with execution rights for this command.

Chapter 8
Multicast Source Discovery Protocol (MSDP)

Multicast Source Discovery Protocol (MSDP) is a mechanism to connect multiple Protocol Independent Multicast sparse mode (PIM-SM) domains. MSDP allows multicast sources for a group to be known to all rendezvous points (RPs) in different domains. An RP runs MSDP over TCP to discover multicast sources in other 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).

Not supported on the Aruba 6200 Switch Series.

Multicast Source Discovery Protocol (MSDP) overview

When MSDP is configured in a network, RPs running MSDP exchange source information with MSDP enabled 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 device 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, which behaves similar to a local PIM register packet.

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 and thus provides administrative independence.
- Allows filtering.

PIM Anycast RP is supported with the help of MSDP mesh groups. The main purpose of an Anycast RP implementation is that the downstream multicast routers will see just one address for an RP.

Currently, only intra-domain MSDP deployments are supported; inter-domain MSDP deployments are not supported.

MSDP router config commands

disable

```
disable
```

Description

Disables MSDP on the VRF.

Example

Disabling MSDP:

```
switch(config)# router msdp
switch(config-msdp)# disable
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config-msdp	Administrators or local user group members with execution rights for this command.

enable

enable

Description

Enables MSDP on the VRF.

Example

Enabling MSDP:

```
switch(config)# router msdp
switch(config-msdp)# enable
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config-msdp	Administrators or local user group members with execution rights for this command.

router msdp

```
router msdp [vrf <VRF-NAME>]
no router msdp [vrf <VRF-NAME>]
```

Description

Changes the current context to the MSDP router context. If no VRF is specified, the default VRF MSDP context of the router is assumed.

The `no` form of this command removes the MSDP configuration from the specified context or the default VRF.

Parameters

`vrf <VRF-NAME>`

Specifies the context to the specified VRF.

Examples

Configuring default MSDP router context:

```
switch(config)# router msdp
switch(config-msdp)#
```

Configuring specified router MSDP:

```
switch(config-msdp)# router msdp vrf red
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	`config`	Administrators or local user group members with execution rights for this command.

sa-interval

```
sa-interval <INTERVAL-VALUE>
no sa-interval
```

Description

Configures the sa-interval for the frequency at which MSDP source-active messages are sent.

The `no` form of this command sets the interval to the default value of 60 seconds.

Parameters

<INTERVAL-VALUE>

Specifies the sa-interval in seconds. Default: 60 seconds. Range 60-65535.

Examples

Configuring the sa-interval:

```
switch(config)# router msdp
switch(config-msdp)# sa-interval 400
switch(config-msdp)# no sa-interval
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config-msdp	Administrators or local user group members with execution rights for this command.

MSDP peer configuration commands

connection-retry-interval

```
connection-retry-interval <INTERVAL-VALUE>
no connection-retry-interval
```

Description

Configures the connection-retry-interval for which MSDP peers will wait after peering sessions are reset, before attempting to re-establish the peering sessions.

The no form of this command removes the currently configured value and sets it to the default value of 30 seconds.

Parameters

<INTERVAL-VALUE>

Specify connection-retry-interval in seconds. Range: 1-65535.

Example

Configuring the connection-retry-interval:

```
switch(config-msdp-peer)# connection-retry-interval 120
switch(config-msdp-peer)# no connection-retry-interval
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config-msdp-peer	Administrators or local user group members with execution rights for this command.

connect-source

`connect-source <INTERFACE-NAME>`

Description

Configures the connection source interface for the MSDP Peer.

The `no` form of this command removes the existing connection source interface and resets the peer connection.

Parameters

<INTERFACE-NAME>

Specifies the interface to use as a source.

Examples

Configuring the connection source interface:

```
switch(config-msdp-peer)# connect-source 1/1/1
```

Configuring the connection source as ROP:

```
switch(config)# router msdp
switch(config-msdp)# ip msdp peer 10.1.1.1
switch(config-msdp-peer)# connect-source 1/1/1
```

Configuring the connection source as a sub-interface:

Supported only on the Aruba 6300, 6400, and 8360 Switch Series.

```
switch(config)# router msdp
switch(config-msdp)# ip msdp peer 20.1.1.1
switch(config-msdp-peer)# connect-source 1/1/10.10
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config-msdp-peer	Administrators or local user group members with execution rights for this command.

clear ip msdp peer statistics

`clear ip msdp peer [all-vrfs | vrf <VRF-NAME> | <PEER-IP>]`

Description

Clears MSDP SA counters of peer information for the given VRF. If VRF is not specified, it clears SA counters of peers in the default VRF. It also clears MSDP SA counters for a specified peer address.

Parameters

`all-vrfs`

Clears MSDP peer information for all VRFs. Optional.

`vrf <VRF-NAME>`

Clears MSDP peer information for a particular VRF. If the *<VRF-NAME>* is not specified, it clears information for the default VRF. Optional.

`<PEER-IP>`

Clears MSDP peer information for the specified Peer IP. Format: A.B.C.D. Optional.

Examples

Showing MSDP peer information for VRFs:

```
switch# clear ip msdp peer statistics all-vrfs
switch# clear ip msdp peer statistics 2.2.2.2
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	Operator (>) or Manager (#)	Auditors or Administrators or local user group members with execution rights for this command. Auditors can execute this command from the auditor context (auditor>) only.

description

```
description <TEXT>
no description
```

Description

Configures a description for a specified MSDP peer to make it easier to identify in a configuration or show command output.

The `no` form of this command removes the peer description.

Parameters

<TEXT>

Specifies a description for the MSDP Peer.

Example

Configuring the MSDP peer description:

```
switch(config-msdp)# ip msdp peer 10.1.1.1
switch(config-msdp-peer)#
switch(config-msdp-peer)# description Peer_1
switch(config-msdp-peer)# no description
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	`config-msdp-peer`	Administrators or local user group members with execution rights for this command.

disable

```
disable
```

Description

Disables MSDP peer on the L3 interface.

Example

Disabling MSDP peering:

```
switch(config)# router msdp
switch(config-msdp)#
switch(config-msdp)# ip msdp peer 10.1.1.1
switch(config-msdp-peer)#
switch(config-msdp-peer)# disable
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	`config-msdp-peer`	Administrators or local user group members with execution rights for this command.

enable

`enable`

Description

Enables MSDP peer on the L3 interface.

Only one MSDP peering session per VRF should be configured between two routers to avoid loops.

Example

Enabling MSDP peering:

```
switch(config)# router msdp
switch(config-msdp)#
switch(config-msdp)# ip msdp peer 10.1.1.1
switch(config-msdp-peer)#
switch(config-msdp-peer)# enable
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	`config-msdp-peer`	Administrators or local user group members with execution rights for this command.

ip msdp peer

```
ip msdp peer <IP-ADDR>
no ip msdp peer
```

Description

Changes the current context to the MSDP peer context.

The `no` form of this command removes the MSDP peer configuration from the specified context.

Parameters

<IP-ADDR>

Specifies the IPv4 address of the MSDP peer. Format: A.B.C.D

Examples

Enabling the MSDP peer context:

```
switch(config)# router msdp
switch(config-msdp)#
switch(config-msdp)# ip msdp peer 10.1.1.1
switch(config-msdp-peer)#
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	`config-msdp`	Administrators or local user group members with execution rights for this command.

keepalive

```
keepalive <KEEPALIVE-INTERVAL> <HOLD-TIME>
no keepalive
```

Description

Configures the interval at which a 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.

The `no` form of this command removes the currently configured value and sets it to the default value.

Parameters

<KEEPALIVE-INTERVAL>

Specifies the value for the keepalive interval.

<HOLD-TIME>

Specifies the value for the hold time.

Example

Configuring the keepalive interval and the hold time for MSDP peer:

```
switch(config-msdp-peer)# keepalive 30 45
switch(config-msdp-peer)# no keepalive
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config-msdp-peer	Administrators or local user group members with execution rights for this command.

mesh-group

```
mesh-group <MESH-NAME>
no mesh-group <MESH-NAME>
```

Description

Associates the given mesh group with the MSDP peer. This feature is used to reduce the amount of SA traffic in an intra-domain setting.

The `no` form of this command removes the peer from the currently configured mesh.

Parameters

<MESH-NAME>

Specifies the MSDP mesh group name.

Usage

All MSDP peers on the router that participate in the mesh group must be fully meshed with all other peers in the mesh group. When MSDP mesh groups are used, SA messages are not flooded to other mesh group peers. It also eliminates RPF checks on arriving SA messages. With MSDP mesh group configured, SA messages are always accepted from mesh group peers.

Example

Associating a mesh group with an MSDP peer:

```
switch(config-msdp-peer)# mesh-group test-mesh-group
```

Removing the MSDP peer from the configured mesh:

```
switch(config-msdp-peer)# no mesh-group test-mesh-group
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	`config-msdp-peer`	Administrators or local user group members with execution rights for this command.

password

```
password [{ciphertext | plaintext} <PASSWD>]
no password
```

Description

Enables MD5 password encryption for a TCP connection between two MSDP peers.

The `no` form of this command removes MD5 password encryption.

Parameters

`{ciphertext | plaintext}`

Selects the password type.

`<PASSWD>`

Specifies the password.

When the password is not provided on the command line, plaintext password prompting occurs upon pressing Enter. The entered password characters are masked with asterisks.

Examples

Configuring MD5 password encryption with a provided plaintext password:

```
switch(config)# router msdp
switch(config-msdp)#
switch(config-msdp)# ip msdp peer 10.1.1.1
switch(config-msdp-peer)#
switch(config-msdp-peer)# password plaintext F82#4eva
```

Configuring MD5 password encryption with a prompted plaintext password:

```
switch(config)# router msdp
switch(config-msdp)#
switch(config-msdp)# ip msdp peer 10.1.1.1
switch(config-msdp-peer)#
switch(config-msdp-peer)# password
Enter the MD5 password: ********
Re-Enter the MD5 password: ********
```

Removing MD5 password encryption:

```
switch(config)# router msdp
switch(config-msdp)#
switch(config-msdp)# ip msdp peer 10.1.1.1
switch(config-msdp-peer)#
switch(config-msdp-peer)# no password
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config-msdp-peer	Administrators or local user group members with execution rights for this command.

sa-filter access-list

```
sa-filter {in|out} access-list <ACL-RULE>
no sa-filter {in|out} access-list <ACL-RULE>
```

Description

Associates the given ACL to filter MSDP SA messages on the peer.

The `no` form of this command removes the currently configured ACL entry.

Parameters

`{in|out}`

Enables the filter for incoming or outgoing SA messages.

`<ACL-RULE>`

Specifies the ACL rule name.

Usage

By default, the MSDP enabled router forwards all the SA messages, and the peer router processes all the received messages. This command allows the user to configure an ACL on the MSDP peer to filter SA messages. User can prevent the incoming/outgoing SA messages on MSDP router by creating incoming/outgoing filter lists using an ACL.

Example

Filtering incoming SA messages on the MSDP peer for the specified ACL:

```
switch(config-msdp-peer)# sa-filter in access-list msdp_sa_filter1
```

Filtering outgoing SA messages on the MSDP peer for the specified ACL:

```
switch(config-msdp-peer)# sa-filter out access-list msdp_sa_filter2
```

Removing filter on the MSDP peer for the specified ACL:

```
switch(config-msdp-peer)# no sa-filter in access-list msdp_sa_filter2
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	`config-msdp-peer`	Administrators or local user group members with execution rights for this command.

MSDP show commands

show ip msdp count

```
show ip msdp count [all-vrfs | vrf <VRF-NAME>]
```

Description

Shows MSDP Peer (S,G) learnt count for a given VRF. If no options are specified, it shows information for the default VRF.

Parameters

`all-vrfs`

Shows MSDP (S,G) entries count for all VRFs. Optional.

`vrf <VRF-NAME>`

Shows MSDP (S,G) entries count for a particular VRF. If the *<VRF-NAME>* is not specified, it shows information for the default VRF. Optional.

Examples

Showing the MSDP learnt count:

```
switch# show ip msdp count

VRF: default
SA state per Peer counters
<Peer>:<#SA learned>
10.1.1.1: 30
20.1.1.1: 100
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

show ip msdp peer

```
show ip msdp peer [all-vrfs | vrf <VRF-NAME> | <PEER-IP>]
```

Description

Shows MSDP Peer information for the given VRF. Optionally, you can show specific information by VRF.

Parameters

`all-vrfs`

Shows MSDP peer information for all VRFs. Optional.

`vrf <VRF-NAME>`

Shows MSDP peer information for a particular VRF. If the *<VRF-NAME>* is not specified, it shows information for the default VRF. Optional.

<PEER-IP>

Shows MSDP Peer information for specified Peer IP. Format: A.B.C.D. Optional.

Examples

Showing MSDP peer information for VRFs:

(Sub-interface is supported only on the Aruba 6300, 6400, 8360 Switch Series)

```
switch# show ip msdp peer

VRF: default

MSDP Peer: 10.1.1.1
Connection status
State: up  Resets: 0  Connection Source: 1/1/1
Uptime(Downtime): 0m 25s    SA Messages sent: 0
SA's learned from this peer: 0
SA Filtering
Input (S,G) filter: msdp_sa_filter1  (S,G) entries dropped: 0
Output (S,G) filter: msdp_sa_filter2  (S,G) entries dropped: 30
Mesh group: test-mesh-group


MSDP Peer: 30.1.1.1
Connection status
State: up  Resets: 0  Connection Source: 1/1/10.10(30.1.1.2)
Uptime(Downtime): 0m 25s    SA Messages sent: 0
SA's learned from this peer: 0
Peer Keepalive interval: 70
Peer Hold time: 90
Peer Connection Retry interval: 40
SA Filtering
Input (S,G) filter: msdp_sa_filter1  (S,G) entries dropped: 0
Output (S,G) filter: msdp_sa_filter2  (S,G) entries dropped: 30
Mesh group: test-mesh-group1

switch# show ip msdp peer 20.1.1.1

VRF: default

MSDP Peer: 20.1.1.1
Connection status
State: down  Resets: 0  Connection Source: 1/1/2
Uptime(Downtime): 1m 25s    SA Messages sent: 0
SA's learned from this peer: 0
SA Filtering
Input (S,G) filter: msdp_sa_filter1  (S,G) entries dropped: 0
Output (S,G) filter: msdp_sa_filter2  (S,G) entries dropped: 20
Mesh group: test-mesh-group
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

show ip msdp sa-cache

`show ip msdp sa-cache [all-vrfs | vrf <VRF-NAME> | <SRC-OR-GRP-IP>]`

Description

Shows MSDP Peer SA-Cache information for the given VRF. Optionally, you can show specific information by VRF. The SA-Cache output can be filtered based on the source or group IPv4 address.

Parameters

`all-vrfs`

Shows MSDP SA-Cache information for all VRFs. Optional.

`vrf <VRF-NAME>`

Shows MSDP SA-Cache information for a particular VRF. If the <*VRF-NAME*> is not specified, it shows information for the default VRF. Optional.

`<SRC-OR-GRP-IP>`

Shows the filtered SA-cache output for the specified source or group IPv4 address. Format: A.B.C.D. Optional.

Examples

Showing MSDP SA-Cache information for VRFs:

```
switch# show ip msdp sa-cache

VRF: default
(30.0.0.1, 230.1.1.1)  RP: 10.1.1.1  Peer: 10.1.1.2
(20.0.0.1, 229.1.1.1)  RP: 10.1.1.1  Peer: 10.1.1.2
(10.0.0.1, 229.1.1.1)  RP: 10.1.1.1  Peer: 10.1.1.2

Total entries: 3

switch# show ip msdp sa-cache 229.1.1.1
(20.0.0.1, 229.1.1.1)  RP: 10.1.1.1  Peer: 10.1.1.2
(10.0.0.1, 229.1.1.1)  RP: 10.1.1.1  Peer: 10.1.1.2

Total entries: 2
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

show ip msdp summary

```
show ip msdp summary [all-vrfs | vrf <VRF-NAME>]
```

Description

Shows MSDP peer summary for a given VRF. If no options are specified, it shows information for the default VRF.

Parameters

`all-vrfs`

Shows the MSDP peer summary for all VRFs. Optional.

`vrf <VRF-NAME>`

Shows the MSDP peer summary for a particular VRF. If the <*VRF-NAME*> is not specified, it shows information for the default VRF. Optional.

Examples

Showing the MSDP peer summary:

```
switch# show ip msdp summary

VRF: default

MSDP Peer Status Summary
Peer address    State    Uptime(Downtime)      Reset Count     SA Count

10.1.1.1        down     34m 34s               0               0
20.1.1.1        up       50m 24s               0               50
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	Operator (>) or Manager (#)	Administrators or local user group members with execution rights for this command.

Chapter 9
mDNS gateway

Multicast DNS (mDNS) gateway helps users to discover various servers such as printers and Apple TV, across VLANs. mDNS gateway uses the reflection mechanism to achieve service discovery across VLANS.

This feature is supported on the 6200, 6300, and 6400 Switch Series only.

mDNS gateway overview

Reflection mechanism

With the reflection mechanism, the mDNS packets received in one VLAN are reflected to all the other mDNS gateway-enabled VLANs based on filters. Only the packets containing the following records are supported for reflection:

- PTR record—Contains service-name to service-instance-name mapping.
- SRV record—Contains service-instance-name to UDP/TCP port number and hostname mapping.
- TXT record—Contains more information about the service-instance, such as, vendor information.
- A record—Contains hostname to host IP address mapping.

Filters

Filters are used to control the service discovery both within and across VLANs. You can configure filter rules in the service profiles based on service-name and service-instance-names. If a profile is configured for a VLAN, then the filter rules in the profile will be used to filter packets transmitted out of the VLAN interface.

Filtering is performed based on parameters extracted from the first record.

Example of mDNS service discovery

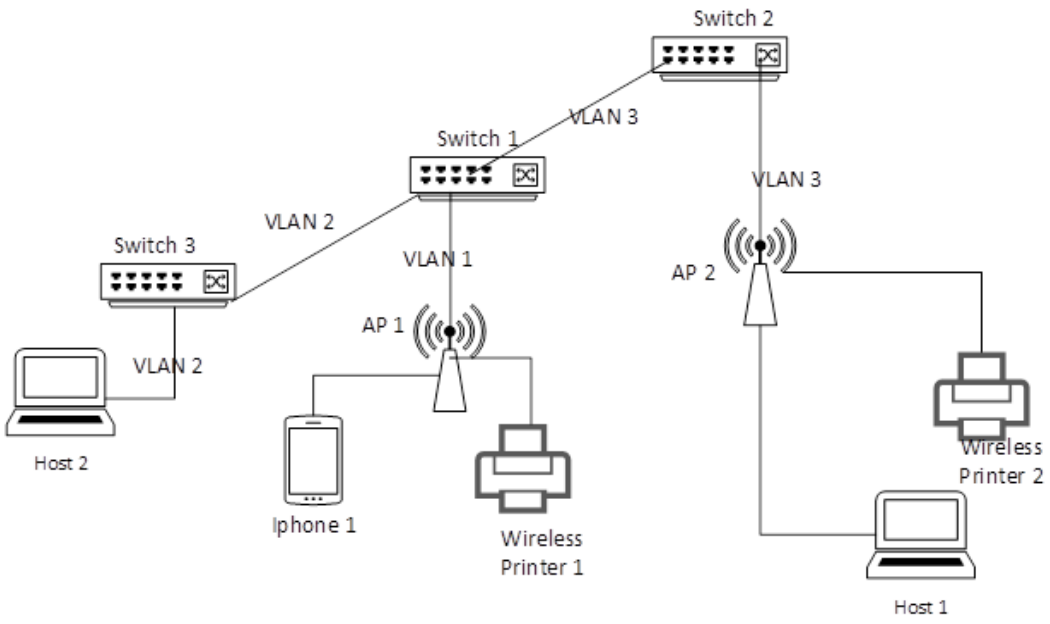
The following figure shows an example topology where mDNS gateway is useful. Consider the following:

- Enable mDNS only on Switch 1 in VLAN 1, 2, and 3.
- Create a configuration rule in Switch 1 for VLAN 3—No host in VLAN 3 must discover any external printers.

When Host 1 in VLAN 3 sends an mDNS query to Switch 1, the query is reflected in VLAN 1 and VLAN 2. The Wireless Printer 1 in VLAN 1 generates a response that the Switch 1 receives and reflects to VLAN 2 and not to VLAN 3, because a rule is configured for VLAN 3 to not allow any printer service.

However, Host 1 will still be able to access Wireless Printer 2, because it is present in the same VLAN 3.

Figure 1 *Example of mDNS service discovery*



Limitations

Following are a few limitations when configuring mDNS gateway:

- Filtering is performed only based on parameters extracted in the first mDNS record.
- Filtering is applied only on the egress mDNS packets.
- Only IPv4 mDNS packets are supported.
- mDNS gateway is recommended for deployments where mDNS is enabled on lesser VLANs. This is because the switch allows the mDNS packets to be reflected to a maximum of 256 VLANs for the 6300 and 6400 Switch Series, and 128 VLANs for the 6200 Switch Series, in incremental order of VLAN IDs, and in the VLAN from where the packet was initiated.
- mDNS packets are rate limited at 150 packets per second.
- When switches are connected directly with each other, you must enable mDNS only on one switch to prevent a reflection loop.
- You must enable debug logging only for troubleshooting an issue. Enabling debug logging on a high scale mDNS configuration might lead to high CPU utilization and the system may slow down.

Configuring mDNS gateway

Perform the following steps to configure mDNS gateway:

Procedure

1. Create a service for the mDNS gateway with the `mdns-sd service` command.
   You can group multiple service IDs into a single service.
   Add description to the service and create service IDs with the following commands:

a. Add a description to the service with the `description` command.
b. Create unique service IDs with the `id` command.

2. Create a profile to be applied on a VLAN with the `mdns-sd profile` command.

   Add rules to the profile with the `<sequence-number>` command.
3. Enable mDNS gateway on a VLAN with the `mdns-sd` command.
4. Apply a profile on the VLAN with the `mdns-sd apply-profile tx` command.
5. Enable mDNS gateway globally with the `mdns-sd enable`command.

mDNS gateway commands

Supported on the 6200, 6300, and 6400 Switch Series only.

debug mdns

```
debug mdns {all | config | init | packet | timer}
```

Description

Enables mDNS gateway debug logs for all or specific debug modules.

Parameters

`all`
Enables debug logs for all mDNS gateway modules.

`config`
Enables debug logs to trace mDNS gateway configuration changes.

`init`
Enables debug logs to trace mDNS gateway initialization.

`packet`
Enables debug logs to trace mDNS gateway packet processing.

`timer`
Enables debug logs to trace mDNS gateway timer events.

Examples

Enabling debug logs for all modules:

```
switch# debug mdns all
```

Enabling debug logs for config module:

```
switch# debug mdns config
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	Manager (#)	Administrators or local user group members with execution rights for this command.

description

```
description <SERVICE-DESCRIPTION>
no description <SERVICE-DESCRIPTION>
```

Description

Adds description to a service.

The `no` form of this command deletes the description of a service.

Parameters

<SERVICE-DESCRIPTION>

Specifies the service description. Maximum 128 characters.

Examples

Add a service description:

```
switch(config-mdns-sd-service)# description students-airplay-service
```

Remove the service description from a service:

```
switch(config-mdns-sd-service)# no description students-airplay-service
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config-mdns-sd-service	Administrators or local user group members with execution rights for this command.

id

```
id <SERVICE-ID>
```

```
no id <SERVICE-ID>
```

Description

Adds a service identifier to a service. The service ID configured here must be same as the service ID that is present in the packet.

The `no` form of this command removes a service ID from the service.

Parameters

<SERVICE-ID>

Specifies the service ID. Maximum 128 characters.

Examples

Add a service ID:

```
switch(config-mdns-sd-service)# id _appletv-v2._tcp
```

Remove a service ID from a service:

```
switch(config-mdns-sd-service)# no id _appletv-v2._tcp
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	`config-mdns-sd-service`	Administrators or local user group members with execution rights for this command.

mdns-sd

```
mdns-sd
no mdns-sd
```

Description

Enables mDNS gateway on a VLAN interface.

The `no` form of this command disables mDNS gateway on a VLAN interface.

This command is applicable only to VLAN interfaces.
The switch will not process mDNS packets until the mDNS gateway is enabled globally.

Examples

Enabling mDNS gateway on VLAN 10:

```
switch(config)# interface vlan 10
switch(config-if-vlan)# mdns-sd
```

Disabling mDNS gateway on VLAN 10:

```
switch(config)# interface vlan 10
switch(config-if-vlan)# no mdns-sd
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config-if-vlan	Administrators or local user group members with execution rights for this command.

mdns-sd apply-profile tx

```
mdns-sd apply-profile <PROFILE-NAME> tx
no mdns-sd apply-profile <PROFILE-NAME> tx
```

Description

Configures mDNS gateway profile on the VLAN interface. When a profile is applied in the transmit direction, all the mDNS traffic transmitted on the VLAN interface will be filtered based on the rules specified in the transmit profile.

The no form of this command deletes the profile configuration from the VLAN interface in the transmit direction.

This command is applicable only to VLAN interfaces.
When no profile is configured on an interface then the default action is permit.

Parameters

<PROFILE-NAME>

Specifies the profile name. Maximum 32 characters.

Examples

Configuring mDNS gateway profile on VLAN 10:

```
switch(config)# interface vlan 10
switch(config-if-vlan)# mdns-sd
switch(config-if-vlan)# mdns-sd apply-profile student tx
```

Deleting mDNS gateway profile on VLAN 10:

```
switch(config)# interface vlan 10
switch(config-if-vlan)# no mdns-sd apply-profile student tx
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config-if-vlan	Administrators or local user group members with execution rights for this command.

mdns-sd enable

```
mdns-sd enable
no mdns-sd enable
```

Description

Enables mDNS gateway.

The no form of this command disables mDNS gateway. Once the no form of this command is executed, all the SVI VLANs, even though enabled with mDNS gateway, will stop reflecting mDNS packets to the enabled VLANs.

Examples

Enable mDNS gateway:

```
switch(config)# mdns-sd enable
```

Disable mDNS gateway:

```
switch(config)# no mdns-sd enable
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	`config`	Administrators or local user group members with execution rights for this command.

mdns-sd profile

`mdns-sd profile <PROFILE-NAME>`

Description

Creates a profile that can be applied on one or more L3 VLAN interfaces.

The profile contains a set of rules that define various match parameters such as service-name and service-instance-name.

Parameters

<PROFILE-NAME>

Specifies the name of the profile. Maximum 32 characters.

Examples

Creating a profile:

```
switch(config)# mdns-sd profile student
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	`config`	Administrators or local user group members with execution rights for this command.

mdns-sd service

```
mdns-sd service <SERVICE-NAME>
no mdns-sd service
```

Description

Configures a service for mDNS gateway. You can group multiple service IDs into a single user-defined service name.

The `no` form of this command deletes a service.

A service cannot be deleted if it is being used as a match parameter in a filter rule in any profile.

Parameters

<SERVICE-NAME>

Specifies the name of the service. Maximum 32 characters.

Examples

Configure a service for mDNS gateway:

```
switch(config)# mdns-sd service students
```

Delete a service:

```
switch(config)# no mdns-sd service students
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	`config`	Administrators or local user group members with execution rights for this command.

clear mdns-sd statistics

```
clear mdns-sd statistics
```

Description

Clears all mDNS gateway statistics.

Examples

Clear mDNS gateway statistics:

```
switch(config)# clear mdns-sd statistics
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	config	Administrators or local user group members with execution rights for this command.

sequence-number

```
<SEQUENCE_NUMBER> {permit | deny}
 {service-name <SERVICE-NAME> | service-instance-name <SERVICE-INSTANCE-NAME>}
no <SEQUENCE-NUMBER> {permit | deny}
 {service-name <SERVICE-NAME> | service-instance-name <SERVICE-INSTANCE-NAME>}
```

Description

Adds a filter rule to the service profile. The sequence number configured determines the priority with which the rule is matched. Lower the sequence number, higher is the priority.

Following are the filter match parameters:

- **Service-name:** mDNS packets are matched against the service IDs configured under the service name.
- **Service-instance-name:** mDNS packets are matched against the service instance name present in the mDNS packets.

When no match criteria is specified in the rule, then the rule can be matched against any mDNS packet. Once the match is found then either the packet can be permitted or denied based on the action specified in the rule.

The `no` form of this command deletes the filter configured in the service profile.

When an mDNS packet does not match any of the filters configured in the profile, then the packet is denied.

Parameters

<SERVICE-NAME>

Specifies the service name. Maximum 32 characters.

<SERVICE-INSTANCE-NAME>

Specifies the service instance name. Maximum 128 characters.

Examples

Adding filter rules to a service profile:

```
switch(config)# mdns-sd profile student
switch(config-mdns-sd-profile)# 10 permit service-name default-appletv
switch(config-mdns-sd-profile)# 20 deny service-name default-appletv service-
instance-name office._pdl-datastream._tcp.local
switch(config-mdns-sd-profile)# 30 permit service-instance-name library._pdl-
datastream._tcp.local
switch(config-mdns-sd-profile)# 40 deny
```

Deleting filter rules to a service profile:

```
switch(config)# mdns-sd profile student
switch(config-mdns-sd-profile)# 10 permit service-name default-appletv
switch(config-mdns-sd-profile)# 20 deny service-name default-appletv service-
instance-name office._pdl-datastream._tcp.local
switch(config-mdns-sd-profile)# 30 permit service-instance-name library._pdl-
datastream._tcp.local
switch(config-mdns-sd-profile)# no 30 permit service-instance-name library._pdl-
datastream._tcp.local
switch(config-mdns-sd-profile)# 40 deny
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	`config-mdns-sd-profile`	Administrators or local user group members with execution rights for this command.

show mdns-sd service-entries

`show mdns-sd service-entries {service-id <SERVICE-ID> | record-type <RECORD-TYPE>}`

Description

Shows all the services exchanged in the mDNS gateway enabled VLANs.

Parameters

<SERVICE-ID>

Specifies the service ID. Maximum 128 characters.

<RECORD-TYPE>

Specifies the type of record. Record can be one of the following values:

- PTR
- SRV

- TXT
- A

Examples

Displaying service entries learnt from mDNS gateway enabled VLANS:

```
switch# show mdns-sd service-entries
MAC-Address : 01:00:00:0e:21:23
VLAN Id     : 10
Record Name : _touch-able._tcp.local
Record Type : PTR
TTL         : 4500

MAC-Address : 01:00:00:0e:21:23
VLAN Id     : 10
Record Name : 523899E219D4C562._touch-able._tcp.local
Record Type : SRV
TTL         : 4500

MAC-Address : 01:00:00:0e:21:23
VLAN Id     : 10
Record Name : 523899E219D4C562._touch-able._tcp.local
Record Type : TXT
TTL         : 4500
```

Displaying service entries for a service and record type:

```
switch# show mdns-sd service-entries service-id _touch-able._tcp record-type ptr
MAC-Address : 01:00:00:0e:21:23
VLAN Id     : 10
Record Name : _touch-able._tcp.local
Record Type : PTR
TTL         : 4500
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show mdns-sd statistics

`show mdns-sd statistics [vlan [<VLAN-ID>]]`

Description

Shows the mDNS packets received and sent globally, and per VLAN.

Parameters

<VLAN-ID>

Specifies the VLAN ID. Required. Range 1 to 4094.

Examples

Displays total packets:

```
switch# show mdns-sd statistics
Packets Recieved    : 100
Packets Sent        : 150
Packets Dropped     :  50
```

Displays total packets for all VLANs:

```
switch# show mdns-sd statistics vlan
VLAN 10
Packets Recieved    : 100
Packets Sent        : 100
Packets Dropped     :   0

VLAN 20
Packets Recieved    :   0
Packets Sent        :  50
Packets Dropped     :  50
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show mdns-sd statistics profile

`show mdns-sd statistics profile <PROFILE-NAME>`

Description

Displays the number of packets permitted or denied by various filter rules in a profile.

Parameters

<PROFILE-NAME>

Specifies the profile name. Maximum 32 characters.

Examples

Displaying statistics for a profile:

```
switch# show mdns-sd statistics profile student
--------------------------
Sequence-Number Hit-Count
--------------------------
10              100
20               25
30              150

Total number of packets permitted by the profile : 250
Total number of packets denied by the profile    :  50
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show mdns-sd summary

```
show mdns-sd summary
```

Description

Shows whether mDNS gateway is enabled globally and at the VLAN interface level. It also shows the profile applied on various VLAN interfaces.

Examples

Displaying mDNS gateway summary:

```
switch# show mdns-sd summary
global mdns-sd status: enabled
----------------------------
VLAN-Id Status   Tx-Profile
----------------------------
1       enabled  student
2       enabled  employee
3       disabled teacher
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show running-config interface

`show running-config interface <INTERFACE-NAME>`

Description

Shows the configuration of profiles for an interface.

Parameters

<INTERFACE-NAME>

Specifies the interface name.

Examples

Displaying configuration of profile at VLAN 10:

```
switch# show running-config interface vlan10
interface vlan10
    mdns-sd
    mdns-sd apply-profile teacher tx
    ip address 10.1.1.1/24
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

Platforms	Command context	Authority
8360 8400		

show running-config mdns-sd profile

`show running-config mdns-sd profile <PROFILE-NAME>`

Description

Shows the configuration of all or a specific profile.

Parameters

<PROFILE-NAME>

Specifies the profile name. Maximum 32 characters.

Examples

Displaying configuration of all profiles:

```
switch# show running-config mdns-sd profile
mdns-sd profile student
  10 deny service-type default-print service-instance-name office._pdl-datastream._
tcp.local
  50 permit service-type default-airplay
  51 permit service-type default-print

mdns-sd profile teacher
  10 deny service-type default-print service-instance-name office._pdl-datastream._
tcp.local
  50 permit service-type default-airplay
  51 permit service-type default-print
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show running-config mdns-sd service

`show running-config mdns-sd service <SERVICE-NAME>`

Description

Shows the running configuration of all or a specific mDNS service.

Parameters

<SERVICE-NAME>

Specifies the service name. Maximum 32 characters.

Examples

Displaying running configuration of all mDNS services:

```
switch# show running-config mdns-sd service
mdns-sd service default-airplay
  id _airplay._tcp
  id _appletv-v2._tcp
  id _roap._tcp

mdns-sd service itunes
  id _home-sharing._tcp
  id _apple-mobdev._dev
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

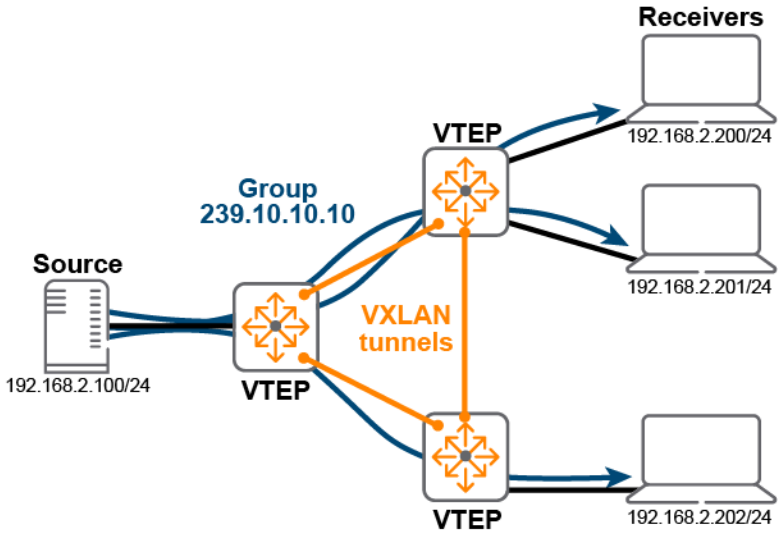
Platforms	Command context	Authority
6300 6400 8320 8325 8360 8400	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

The Aruba 6200 and 8320 Switch Series do not support VXLAN.

IPv4 multicast forwarding for both L2 and L3 are supported with AOS-CX VXLAN/EVPN deployments. Refer to the *VXLAN Guide* for more info on VXLAN/EVPN and overlays/underlays.

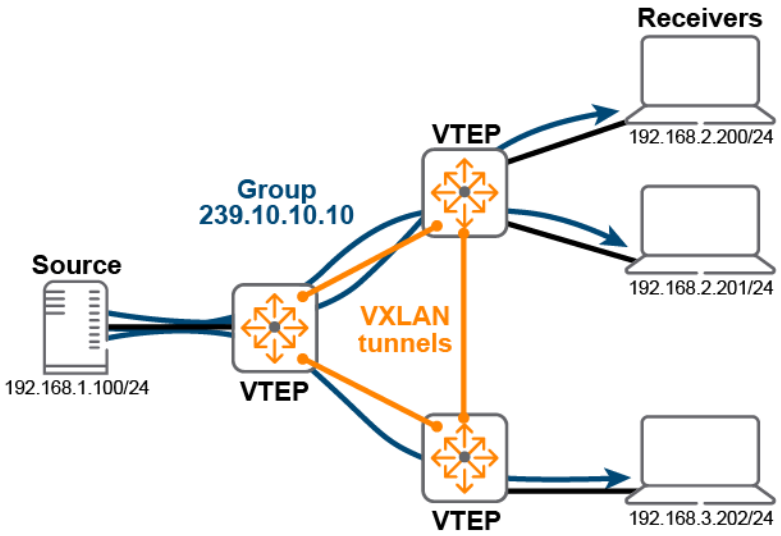
L2 multicast over VXLAN refers to deployments where the multicast sources/receivers are on the same L2 subnet/VLAN and bridging is required between switches that function as VXLAN Tunnel End Points (VTEPs), as seen in Figure 1, L2 multicast over VXLAN:

Figure 1 *L2 multicast over VXLAN*



L3 multicast over VXLAN refers to deployments where the multicast sources/receivers are on different subnets/VLANs and routing is required between VTEPs as seen in Figure 2, L3 multicast over VXLAN.

Figure 2 *L3 multicast over VXLAN*



Protocol and feature details

Broadcast, unknown unicast, multicast (BUM) traffic replication

The AOS-CX implementation uses head end replication where BUM packets are replicated from the source connected VTEP towards all destination VTEPs interested in the same VXLAN Network Identifier (VNI). The underlay network between VTEPs should only be configured for unicast routing, multicast PIM should not be configured in the underlay network.

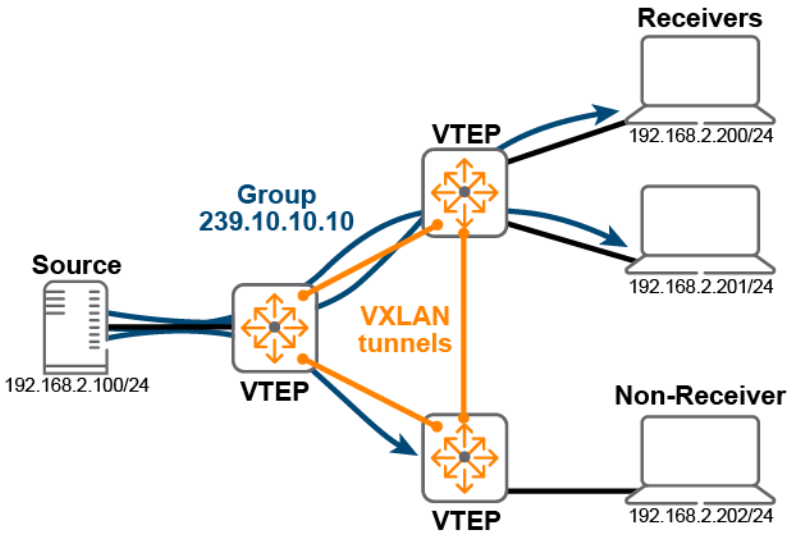
Overlay multicast support

The AOS-CX implementation runs native L2 and L3 multicast protocols over VXLAN tunnels, this is done to make the configuration and debugging of overlay and underlay multicast simpler. With this implementation, multicast traffic will not be part of regular BUM flows and will only be forwarded based on PIM and IGMP forwarding needs. IGMP and PIM-SM (v4) support are added to VXLAN to route and bridge traffic across the tunnels.

L2 multicast over VXLAN

By default, L2 multicast data streams are sent by the source connected VTEP to all other remote VTEPs interested in the same VNI, even if there are devices that are non-receivers (devices that are not interested in that multicast stream).

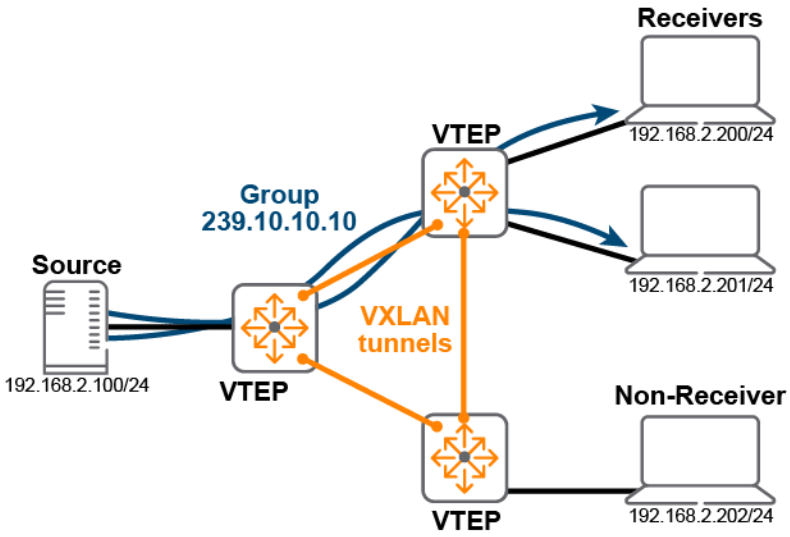
Figure 1 *L2 multicast over VXLAN with non-receiver*



L2 multicast over VXLAN enabled with IGMP snooping

IGMP snooping can be configured at the VLAN level with L2 multicast over VXLAN tunnels, this will prevent the source connected VTEP from sending the multicast stream to VTEPs without any interested receivers (non-receivers).

Figure 2 *L2 multicast over VXLAN enabled with IGMP snooping*



L2 multicast over VXLAN enabled with IGMP snooping has the following characteristics:

- IGMP snooping, once enabled prevents flooding over the L2 VNI; multicast data will only be forwarded to ports where IGMP joins are received.
- VTEPs have full meshed VXLAN tunnels between them.
- IGMP snooping is enabled per VLAN; the VLAN is mapped with L2 VNIs.
- Joins and leaves are learned over VTEPs.
- Packets (data and control) are sent over VXLAN tunnels and regular physical ports.
- All versions of IGMP snooping (v1/v2/v3) are supported over VXLAN.

- The querier can be inside or outside the VXLAN network.
- VSX is supported and can be L2 extended.
- When IGMP snooping is enabled on a VLAN (L2 VNI), all the tunnels are added as forwarded ports (forwarded tunnels) for control packets; the control packets are flooded to all VTEPs.
- As the network is meshed, joins from a non-querier VTEP will be sent to the source VTEP, even if is not the querier.
- Multicast data packets are sent from source VTEP to remote VTEPs.
- Split horizon is implemented at the L2 level such that packets that ingress a VXLAN tunnel will not get re-forwarded to other VTEPs.

Split horizon and L2 multicast

AOS-CX implements split horizon in VXLAN networks to prevent loops; ingressing traffic on a VXLAN tunnel will not be sent to another VXLAN tunnel. This can cause traffic loss to both unknown multicast and L2 multicast as IGMP joins are sent to querier. The querier typically is the middle device that will transmit packets from one port to another. In case of IGMP over an L2 VXLAN tunnel, this will be blocked by split horizon. To prevent this, the receiver-connected VTEP will forward IGMP joins to all VTEPs irrespective of whether they are queriers or not. This will prevent tunnel hop as every source VTEP will only be a single tunnel hop away from every receiver and source data will be sent to the receiver VTEP directly without the involvement of the IGMP querier.

VSX and L2 multicast

In the AOS-CX implementation, two switches/VTEPs configured with Virtual Switching Extension (VSX) are configured as a single logical VTEP. AOS-CX does not use EVPN route type 1 and 4 for load balancing and multihoming; regular VSX-based syncing is used for those purposes. The VSX switches can be access or distribution/core VTEPs in a campus network, and are typically VSX leaf switches in a data center.

There are two scenarios that need to be considered for an L2 VNI that is stretched across VTEPs where one (or more) of the VTEPs have a VSX Link Aggregation Group (LAG).

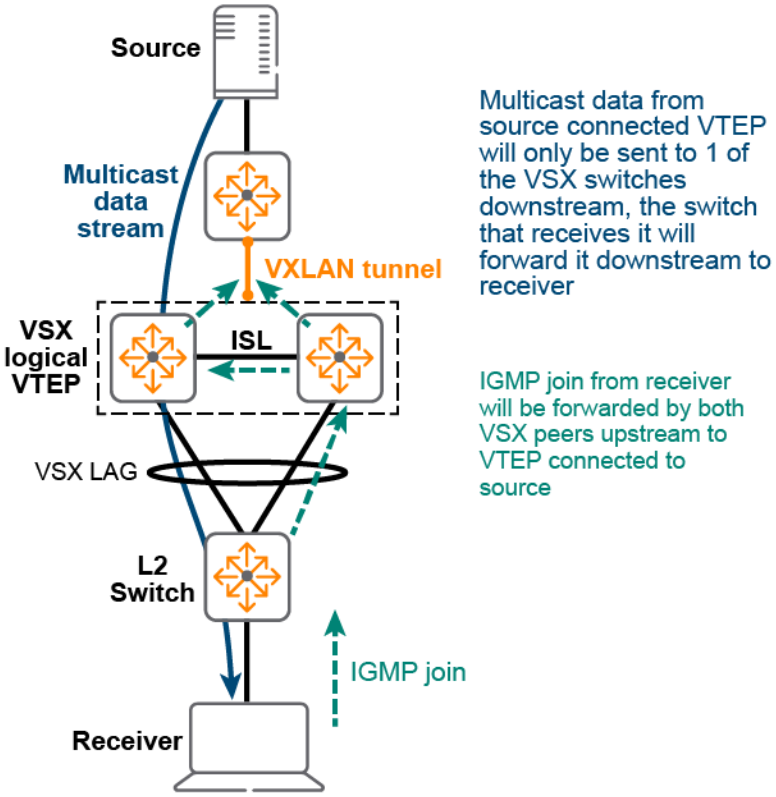
- Scenario 1: Receivers connected to VSX LAG and source on the VXLAN overlay network.
- Scenario 2: Source connected to VSX LAG and receivers on the VXLAN overlay network.

Scenario 1: Receivers connected to VSX LAG and source on the VXLAN overlay network

There are two cases to consider: dual homed VSX LAG and single homed VSX LAG.

Dual-homed VSX LAG with receivers

Figure 3 *Dual-homed VSX LAG with receivers*

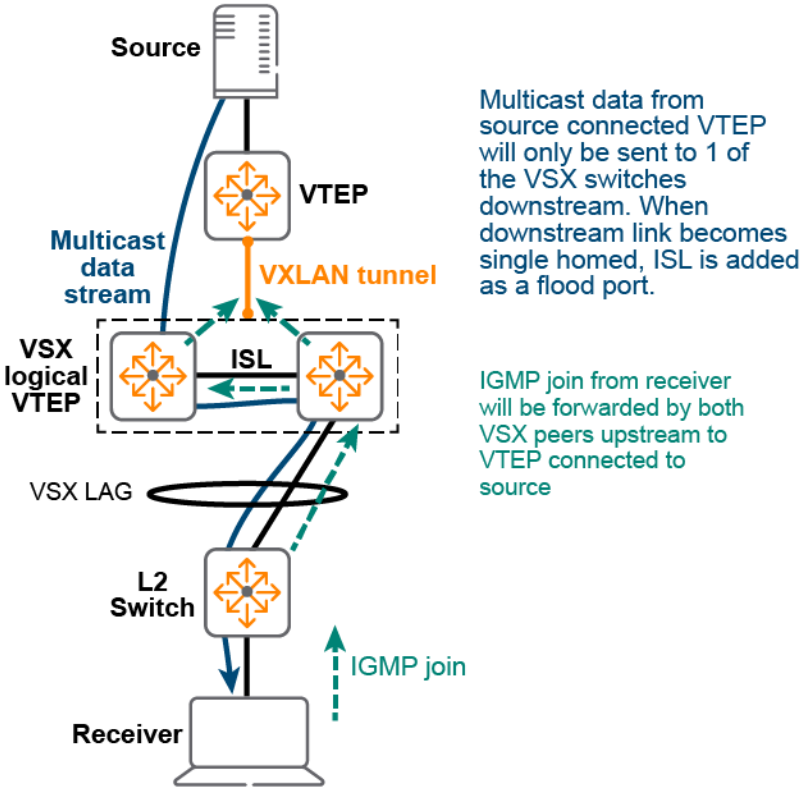


The following operation is done in no particular order:

- IGMP joins from receiver or an access switch are synced between the VSX switches over the ISL link, as a result both VSX switches will learn the join from the VSX LAG link.
- Data traffic from the multicast source through the VXLAN tunnel reaches one of the VSX switches.
- Whichever VSX VTEP receives the traffic, will forward it downstream.
- When one of the VSX switches is the querier, the traffic will be forwarded to the querier as well via Inter Switch Link (ISL); otherwise there will be no traffic on the ISL link.
- Egress filtering rule prevents ingress data on an ISL port from going down the VSX LAG if it is multi-homed.

Single-homed VSX LAG with receivers

Figure 4 *Single-homed VSX LAG with receivers*



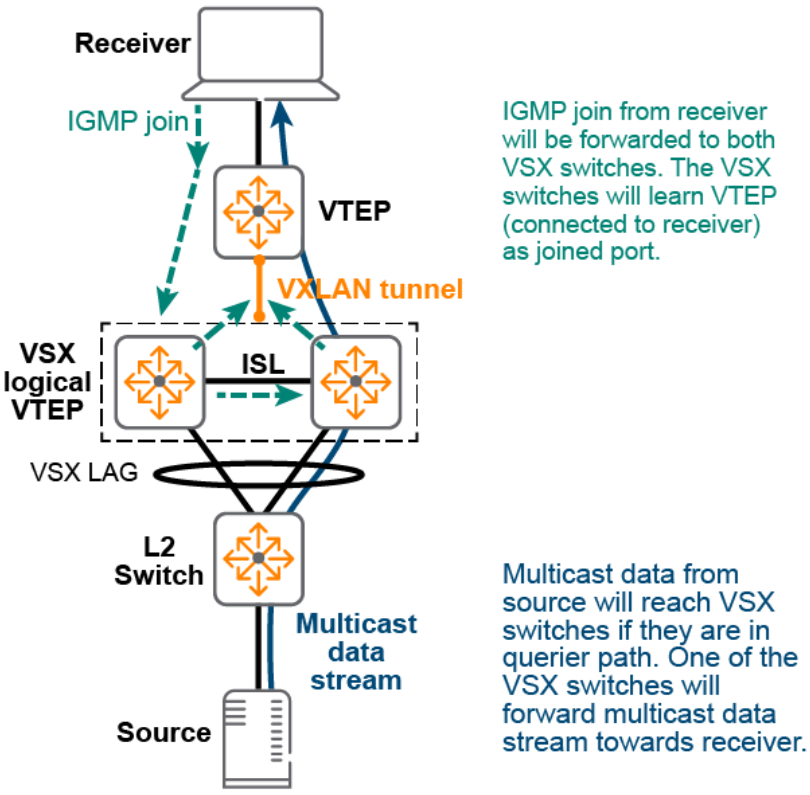
The following operation is done in no particular order:

- The IGMP joins from a receiver or an access switch are synced between the VSX switches over the ISL link, as a result both the VSX switches will learn the join over the VSX LAG link.
- The moment the VSX LAG becomes single homed, the ISL port is added as a flood port. This ensures any data received by one of VSX VTEP, will always be forwarded to the peer
- Data traffic from the multicast source through the VXLAN tunnel reaches one of VSX switches, and is forwarded via ISL to its peer.
- Whichever VSX VTEP has its link up will forward the data downstream, either received directly or via ISL.
- As the VSX LAG is single-homed, there is no egress filtering that prevents data going from ISL to VSX LAG.

Scenario 2: Source connected to VSX LAG and receivers on the VXLAN overlay network

As shown below, the source can be directly connected to the VSX VTEPs or it could be connected via an L2 switch. In both the cases, data will reach one of the VSX VTEPs because of VSX hash.

Figure 5 *Source connected to VSX LAG*



The following sequence can happen in no particular order:

- One of the switches in the L2 network will be elected as querier, unknown multicast are always sent to the querier port. IGMP joins are always forwarded to VXLAN tunnels as well as to the querier port.
- Data traffic from the multicast source reaches the VSX switches either because they are in the querier path, or because of the VSX LAG hash (in case directly connected),
- IGMP joins from receiver reaches one of the VSX switches. The joins are sent over ISL port to the peer switch. The peer VSX switch does a MAC lookup to figure out whether the join is to be learned on the ISL port or over the VXLAN tunnel.
- Once the join is learned on the VXLAN tunnel, multicast data is sent over the VXLAN tunnel when received from the VSX LAG. The path is the same for both a single-homed and a dual-homed VSX LAG.

Recommended configuration on the VSX VTEPs

As shown in Figure 5, Source connected to VSX LAG, the receiver-connected VTEP has a VXLAN tunnel to the VSX logical VTEP. The joins from receiver-connected VTEP are received by one of the VSX switches over the VXLAN tunnel and by the other switch via ISL. The VTEP that receives over ISL is a de-capsulated packet and does not have the VXLAN header. That switch needs to perform a MAC lookup and that MAC sometimes might not be available to the VSX VTEP.

To avoid this condition, the following two commands are recommended on L2 connected VSX VTEPs:

- `redistribute local-mac`

  This command is used to enable Type-2 route advertisement for local MAC address of all EVPN enabled VLANs.

- `redistribute local-svi`

This command is used to enable Type-2 route advertisement for local IP address and MAC address of the SVI interfaces corresponding to the EVPN enabled VLANs (only required if SVI is configured).

IGMP querier positioning

An IGMP querier is one of the routers in the network whose responsibility is to send periodic IGMP queries. In regular IGMP operation, IGMP joins are forwarded to the IGMP querier. In addition, unknown multicast data are also sent to the querier. That is the way that the querier connects source and destination routers. Sending joins towards the querier is a must for the IGMP snooping operation; however in a VXLAN network, because of split-horizon rules, data packets are not sent across VTEPs. The querier does not need to be a centralized router in a VXLAN network as every IGMP join from the receiver connected VTEP is always forwarded to all remote VTEPs with the same VNI. In the AOS-CX implementation, there is no particular recommendation on where to place the querier in a VXLAN network.

L3 multicast over VXLAN

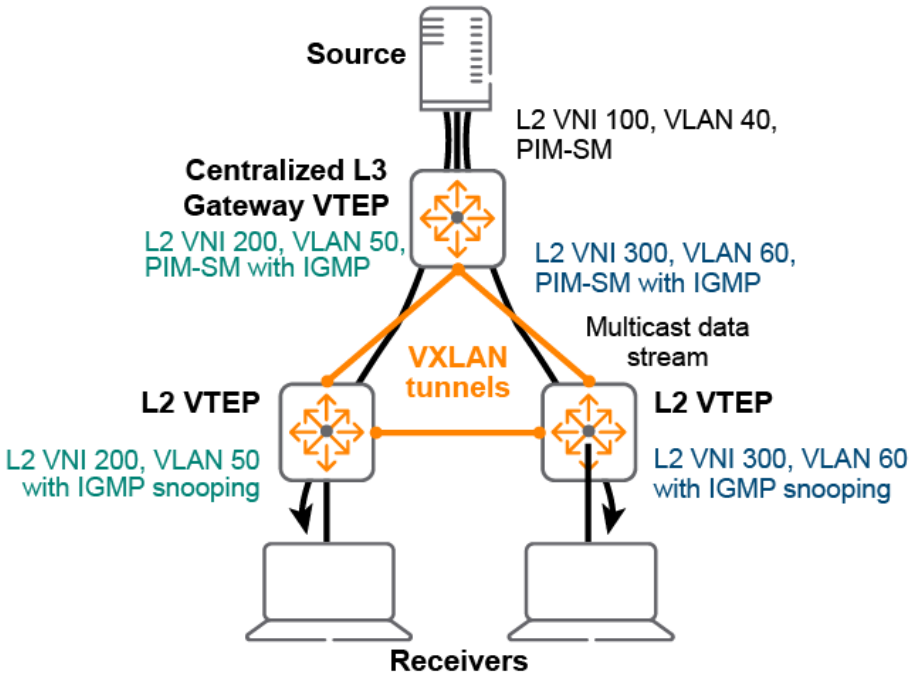
For L3 Multicast over VXLAN, both centralized L3 gateway and distributed L3 gateway use cases are supported.

Centralized L3 gateway

As shown in Figure 6, Centralized L3 gateway, PIM-SM is only enabled at the centralized L3 gateway VTEP which has VLAN mapped to VNIs. The remaining switches function as L2 VTEPs. The L2 VTEPs may or may not have IGMP snooping enabled.

- This use case is simple to implement as PIM-SM is enabled only at the centralized L3 gateway VTEP.
- Mroute entries are simple as routing is between Switch Virtual Interfaces (SVI)/Routed Only Ports (ROP) to L2 VNIs.
- The only difference is that the downstream VLANs are mapped to L2 VNIs; multicast data stream packets are tunneled via L2 VNI from the centralized L3 gateway VTEP towards the L2 VTEPs.

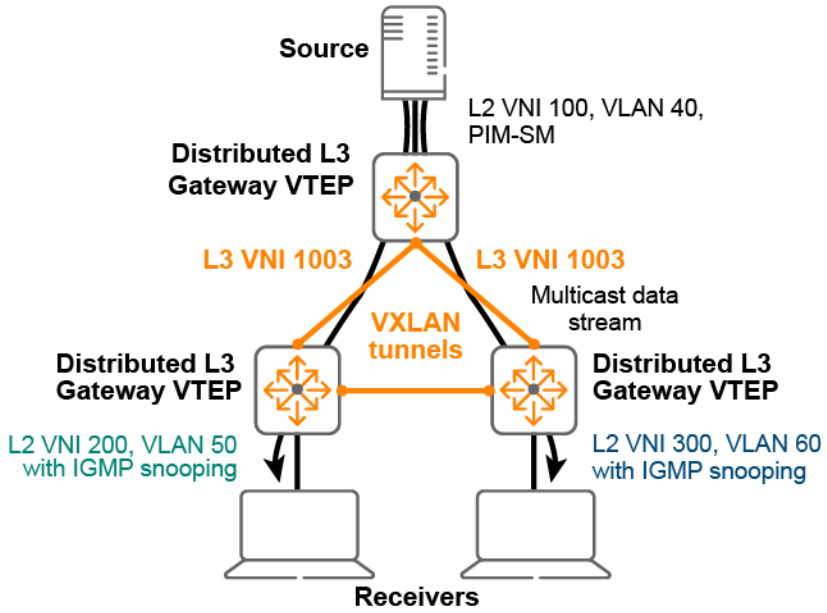
Figure 6 *Centralized L3 gateway*



Distributed L3 gateways

- For distributed L3 gateways (See Figure 7, Distributed L3 Gateways), AOS-CX only supports Symmetric IRB and multicast routing by extension of the PIM-SM protocol in the VXLAN tunnel. Only PIM-SM protocol is supported with L3 multicast over VXLAN tunnels.
- An L3 VNI is used to route traffic from one VLAN to another as the same VLAN/L2 VNI is not present across all VTEPs. PIM creates a logical interface on L3 VNI when `router pim` is enabled on the overlay VRF. This interface is created once the VXLAN EVPN tunnels are formed.
- All VTEPs create their per-tenant VRF L3 VNI interface and exchange PIM messages (e.g. hellos and joins) to other VTEPs through it. They form PIM neighbors via this interface; when the remote VTEP requests traffic via PIM joins on this interface on the source-connected VTEP, a multicast route entry will be installed with the incoming interface as SVI interface (source-connected SVI) and Outgoing Interface List (OIL) with an L3 VNI<#> interface.
- On the receiver connected VTEP, a multicast route entry will be created to route traffic coming from L3 VNI to the SVI where the receivers are present. Incoming interface will be L3 VNI#, with OIL as the receiver SVI.

Figure 7 *Distributed L3 Gateways*

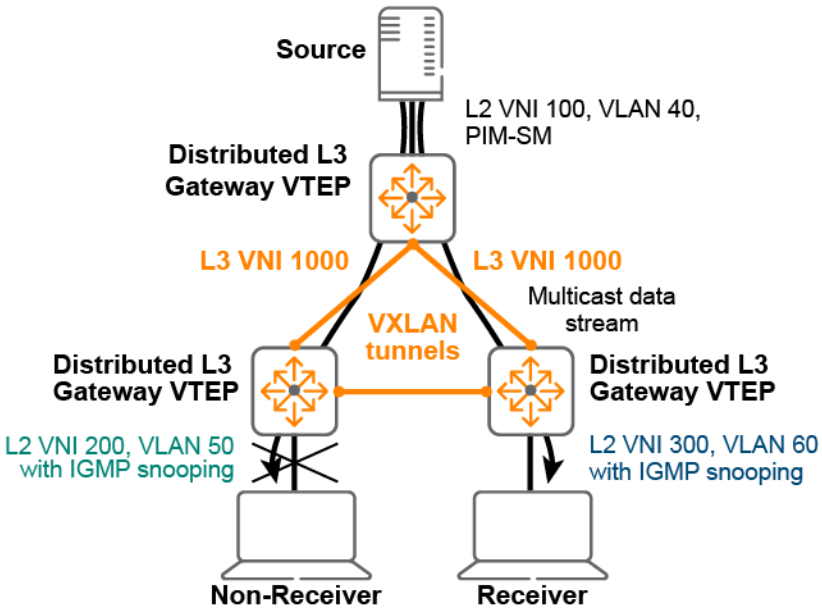


Additional details include the following:

- Symmetric IRB with full meshed L3 VNIs.
- L2 VNIs can extended across switches.
- IGMP joins may be present in some/all the VTEPs for a particular flow.
- IGMP snooping will be enabled in VTEPs.
- PIM-SM is enabled on all the VRFs on the different VTEPs.
- PIM neighbors are formed across L3 VNIs.
- RPs can be present on any of the VTEPs.
- PIM control (join and prune) packets are sent on the other side of the L3 VNIs (where source is present) for every IGMP join.
- When the source connected VTEP sees a PIM join from an L3 VNI, it adds the L3 VNI as OIL.

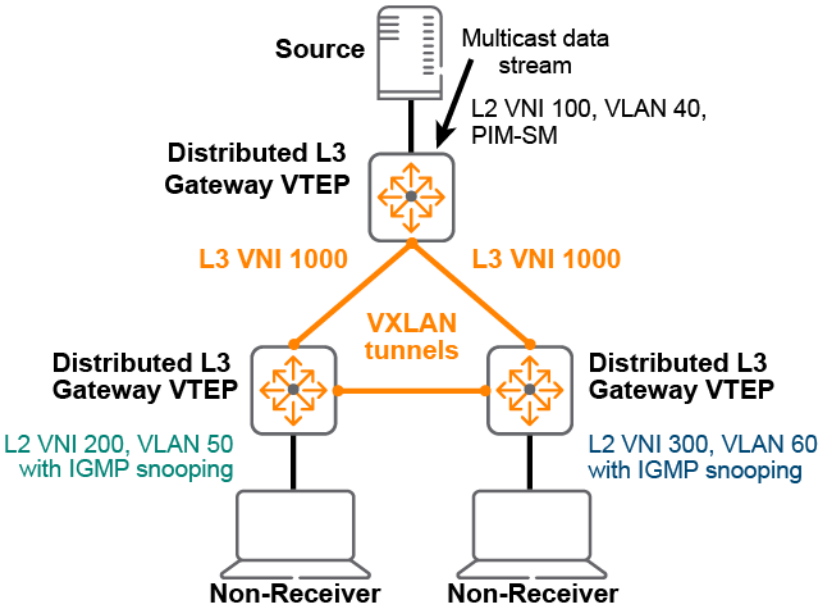
- Data traffic from the multicast source is flooded across L3VNIs, split horizon rules will prevent data from flooding across VTEPs (see Figure 8, Distributed L3 Gateways with non-receiver, multicast data stream sent and pruned at remote VTEP).
- Non-interested VTEPs will drop/prune the multicast data (see Figure 8, Distributed L3 Gateways with non-receiver, multicast data stream sent and pruned at remote VTEP).
- In mixed mode there could be some L2VNIs that will be extended over VTEPS whereas L3 VNIs are enabled in all the VTEPs (per VRF).
- Mix of IGMP snooping and PIM-SM for intra VLAN and inter VLAN routing.

Figure 8 *Distributed L3 Gateways with non-receiver, multicast data stream sent and pruned at remote VTEP*



In case there are no interested receivers at remote VTEPs, L3 VNI will not be added as an outgoing interface and data will be pruned at the source-connected VTEP (See Figure 9, Distributed L3 Gateways with non-receivers, multicast data stream pruned at source VTEP).

Figure 9 *Distributed L3 Gateways with non-receivers, multicast data stream pruned at source VTEP*

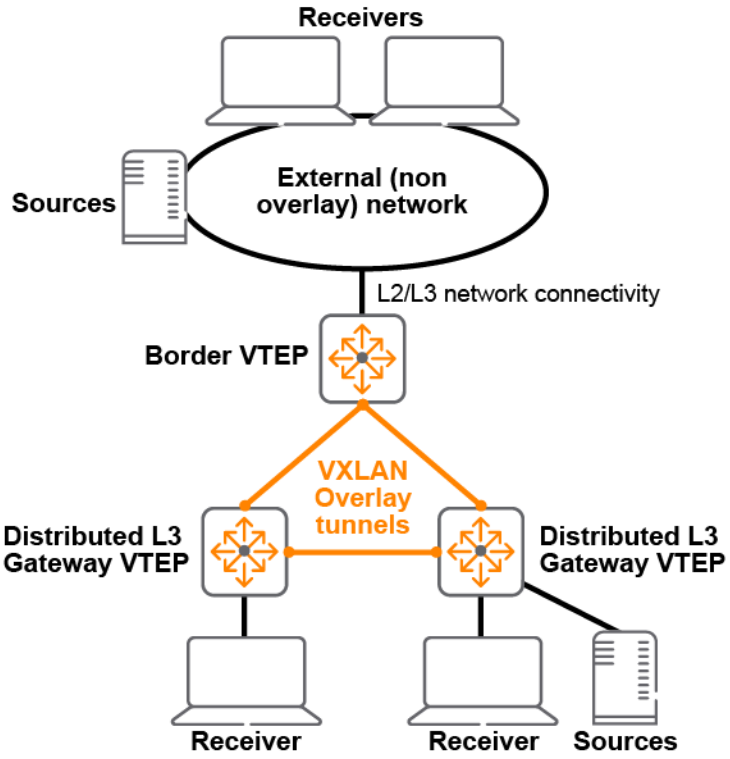


Border VTEP to external (non overlay) network

A border VTEP can be used to connect the VXLAN overlay network to external (non overlay) networks via either L2 or L3, sources and receivers in both networks will be able to send and receive multicast streams.

L3 multicast routing using PIM-SM between the VXLAN and external (non overlay) network is recommended for most deployments as this provides clear demarcation between the two networks.

Figure 10 *Border VTEP to external (non overlay) network*



VSX and L3 Multicast

The following actions are done for all VSX VTEPs with PIM-SM and/or IGMP enabled:

The control packets (PIM packets) are synced between the VSX switches

Unknown multicast packets are also synced between the VSX switches

One of the VSX switches will forward the packets to prevent duplicates

There are different combinations with VSX, with source inside the VXLAN overlay network and receivers on external (non overlay) network and vice versa. The different ways a receiver or a source is connected to a VSX border VTEP are:

L2 VSX LAG

L2 VSX LAG with SVIs

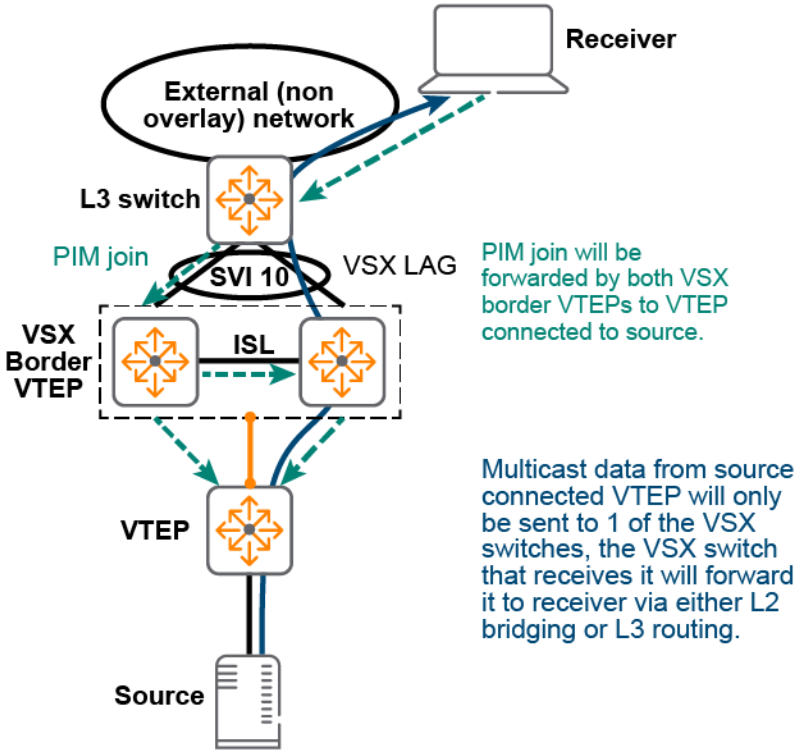
ROP

Point-to-Point (P2P) SVIs

VSX Border VTEP with L3 connectivity to external (non overlay) network

Figure 11, VSX Border VTEP with VSX LAG to receiver on external (non overlay) network shows a border VTEP with VSX LAG and SVI connected to an L3 switch with receivers on the external (non overlay) network.

Figure 11 *VSX Border VTEP with VSX LAG to receiver on external (non overlay) network*



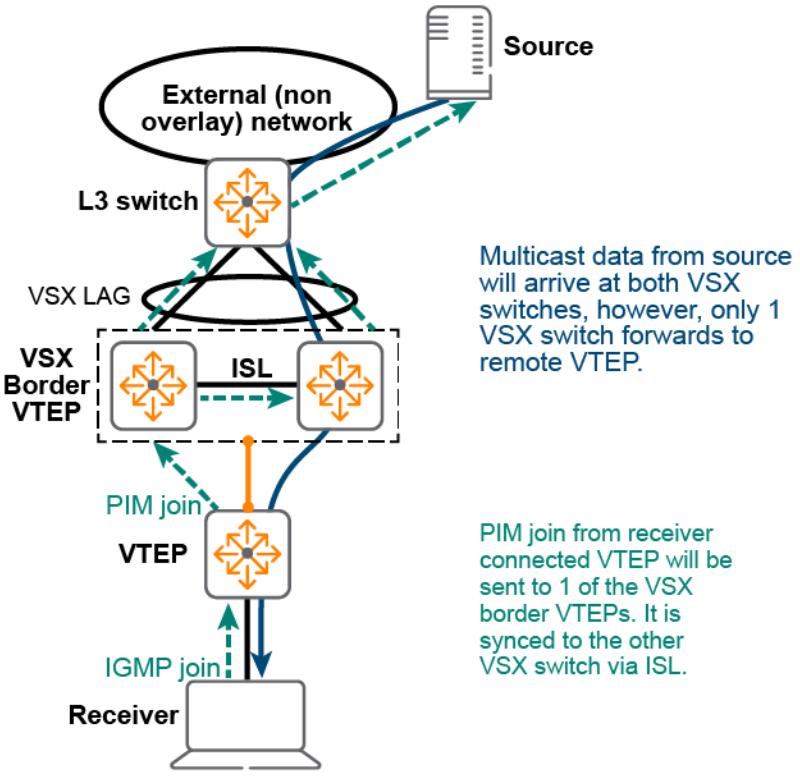
The following actions are taken:

1. PIM hello packets are synced between the VSX border VTEPs via L3 over ISL.
2. PIM joins are received by both VSX switches from the VSX LAG with SVI, both switches send PIM joins to the source-connected VTEP via L3 VNI.
3. The source-connected VTEP adds L3 VNI as the OIL even if it gets two PIM joins.
4. Data traffic from the multicast source is hashed from the source-connected VTEP to only one of the VSX switches as a unicast packet over the VXLAN tunnel.
5. The VSX switch that receives the multicast data stream forms the Mroute entry with the SVI connected to VSX LAG as egress.

6. The data stream packet goes to the other switch via ISL.
7. The egress filtering rule will prevent duplicates as the second switch will have a bridge entry for the egress SVI.
8. The external L3 Switch will route to the receiver.
9. A similar action will occur for a single-homed border VTEP with VSX LAG.

VSX Border VTEP with VSX LAG to receiver on external (non overlay) network shows a border VTEP with VSX LAG and SVI connected to an L3 switch with source on the external (non overlay) network.

Figure 12 *VSX Border VTEP with VSX LAG to source on external (non overlay) network*

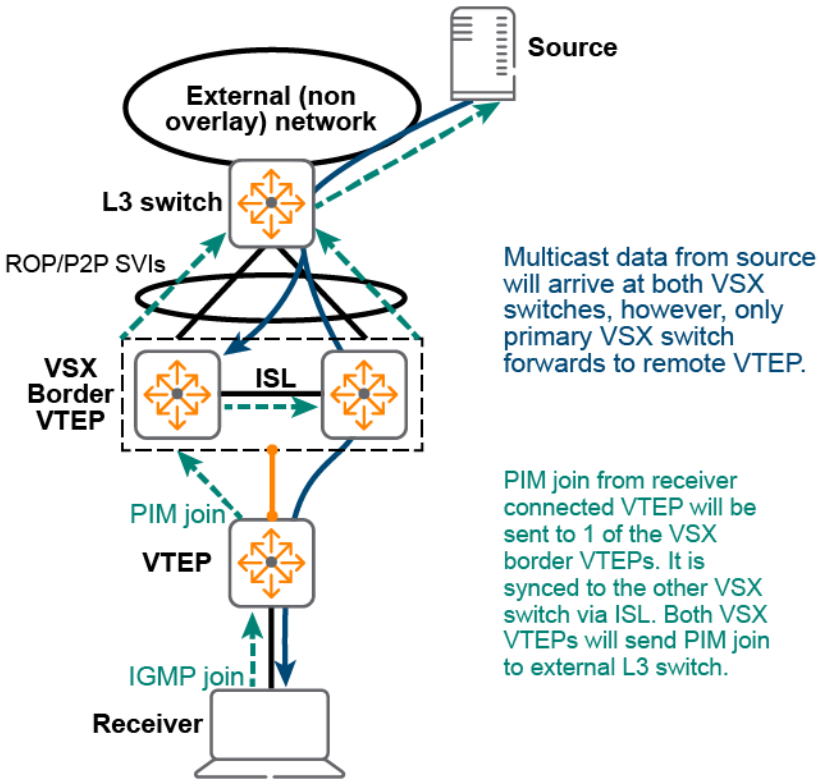


The following actions are taken:

1. PIM joins from the receiver-connected VTEP will only be sent to one of the VSX border VTEP, this will be synced to the other VSX peer.
2. PIM hello packets are synced between the VSX switches via L3 over ISL.
3. Both VSX border VTEPs that receive the PIM join will add L3 VNI as OIL.
4. Multicast data stream from the external network will reach both VSX border VTEPs via VSX LAG with SVI followed by ISL.
5. The primary VSX switch will forward the data to receiver-connected remote VTEP (applies to the Aruba 8325 and 8400 Switch Series).
6. When 1 of the VSX border VTEP gets data directly and not via ISL, it will forward to the receiver-connected remote VTEP (applies to the Aruba 6400 and 8360 Switch Series).

VSX Border VTEP with ROP/P2P SVIs to source on external (non overlay) network shows a border VTEP with ROP/P2P SVIs connected to an L3 switch with source on the external (non overlay) network.

Figure 13 *VSX Border VTEP with ROP/P2P SVIs to source on external (non overlay) network*



The following actions are taken:

1. PIM hello packets are synced between the VSX VTEPs via L3 over ISL.
2. Both VTEPs send PIM joins to the external L3 switch via ROPs; the assumption is that the source has Equal Cost Multi Pathing (ECMP) to both VTEPs.
3. The external L3 switch will add two ROPs/P2P SVIs as OIL in its Mroute entry.
4. Multicast data will be sent to both border VTEPs.
5. 8325/8400—only VSX primary VTEP forwards.
6. 6400/8360—only the VTEP that has pending joins will forward.
7. If the link from primary VTEP to the source goes down and primary becomes unreachable, then there can be traffic loss. In such a scenario, it is recommended to connect an additional L3 link per tenant VRF and enable PIM over them. This link will typically be a P2P SVI between the VSX peers. Each tenant VRF will require its own P2P SVI. The `ip pim-sparse vsx virtual-neighbor` command should not be configured on this P2P SVI.

A. VSX Border VTEP with ROP/P2P SVIs to receivers on external (non-overlay) network and B. VSX Border VTEP with ROP/P2P SVIs to receivers on external (non-overlay) network show a border VTEP with ROP/P2P SVIs connected to an L3 switch with receivers on the external (non overlay) network. The example in Figure 16 shows multicast data and joins sent to different VSX switches, and the example in B. VSX Border VTEP with ROP/P2P SVIs to receivers on external (non-overlay) network shows multicast data and joins sent to the same VSX switch.

Figure 14 *A. VSX Border VTEP with ROP/P2P SVIs to receivers on external (non-overlay) network*

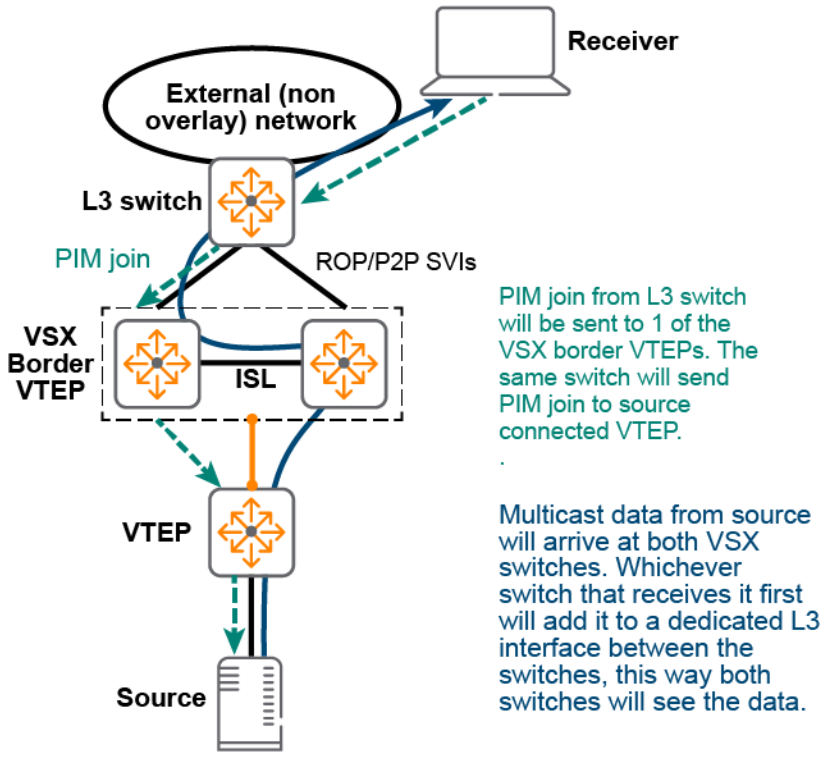
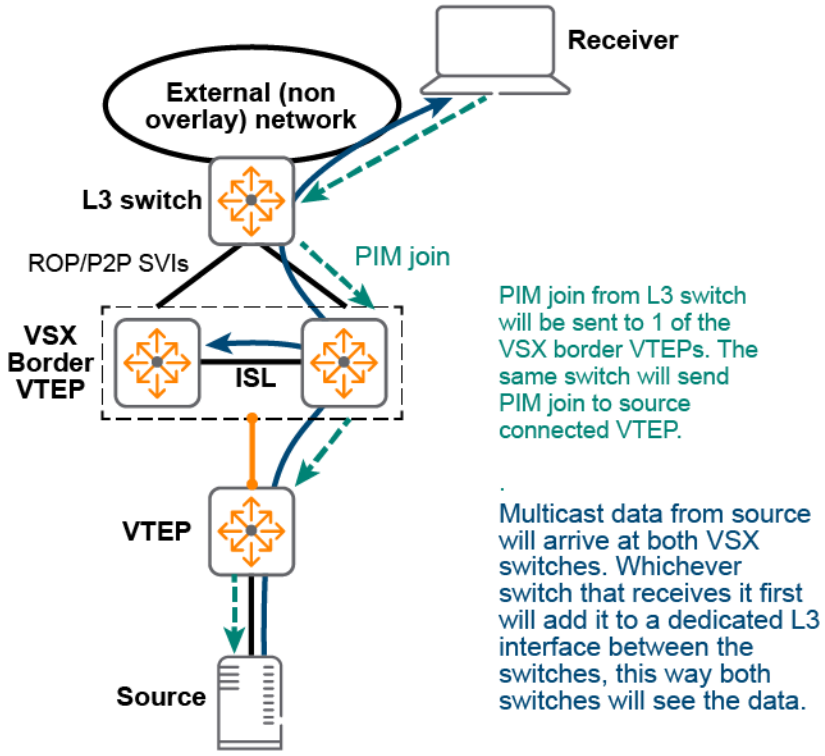


Figure 15 *B. VSX Border VTEP with ROP/P2P SVIs to receivers on external (non-overlay) network*



The following actions are taken:

1. PIM hello packets are synced between VSX switches via L3 over ISL.
2. PIM joins from ROP/P2P will reach one of the VSX switches.
3. Only one VSX switch will send the PIM join towards the source-connected VTEP.

4. The source-connected VTEP will only add the L3 VNI as an OIL and forward multicast data to the L3 VNI.
5. Any VSX switch that receives data from the L3 VNI will add the dedicated L3 Interface (as an OIL for all data coming from L3 VNI) and pending joined port as egress interface.
6. The other VSX switch receives data over the dedicated L3 Interface. That VSX switch adds any pending ROP/P2P joins as egress interface. No SVI is added as OIL as the VSX switch which received the data from the L3VNI would have already added the SVI to OIL.

Dedicated interface details for the default forwarder

- One interface will be created per VRF, this will function as a default interface for forwarding packets if the incoming interface is L3 VNI.
- Note that packets will be forwarded to this interface irrespective whether the OIL is ROP/P2P SVI or not.
- The receiver side VSX device will also add the OIL on every interface that has pending joins.
- Note that when the source is extended via ROP/P2P SVI, it is recommended to create an alternate L3 P2P interface between the VSX peers. This solution uses those interfaces only.

RP placement and election

Rendezvous Point (RP) placement is very important in a multicast network. The RP should to be located close to the multicast source.

The recommendations for RP are:

- If there is an existing multicast network with sources and receivers, the new VXLAN network VTEPs should learn about the existing RPs (on non VXLAN network) via BSR or point to the existing RPs statically.
- If the new VXLAN network does not require multicast connectivity with the external network, redundant VTEPs as new BSR/RPs should be deployed (this could be 2 x standalone VTEPs or 1 x VSX logical VTEP that utilizes unique loopback IPs as BSR/RP with the primary VSX switch typically set to preferred. If the primary VSX switch fails, all VTEPs will utilize the secondary VSX switch unique loopback IP as the remaining BSR/RP (refer to Use case 1: Campus network with centralized L3 gateway sample configs for a better understanding).

Supported platforms and standards

IPv4 multicast VXLAN is supported by the Aruba 6300, 6400, 8325, 8360, and 8400 Switch Series.

Scale

Table 1: *Scale*

	6300	6400	8325	8360	8400
VLANs/L2 VNIs (Multicast support)	128	128	128	128	128
L3 VNI/VRF (Each VRF requires 1 x L3 VNI)	16	16	32	32	32
PIM interfaces (SVIs)	64	64	64	64	64
IGMP groups	2000	2000	2000	2000	8000
Mroutes	2000	2000	3500	3500	8000
VTEPs	32	32	32	32	32

Supported RFCs and standards

The AOS-CX IPv4 multicast VXLAN implementation is currently proprietary and is not able to inter-operate with other vendors. However, the border VTEP that connects to the external non-VXLAN network uses standards-based protocols such as PIM-SM (RFC 4601) + IGMP (RFC 3376 and RFC 2236).

Configuration task list

Multicast VXLAN and EVPN

Table 1: *Configuration task list for Multicast VXLAN and EVPN*

Step	Command	Comments
1. Enter evpn	`evpn`	
2. Enable redistribute local-mac and local-svi	`redistribute local-mac` `redistribute local-svi`	This should be enabled on all VTEPs at the evpn level

VSX VTEP

Table 2: *Configuration task list for VSX VTEPs*

Step	Command	Comments
1. Enter desired SVI	`int vlan number`	
2. Enable PIM VSX virtual neighbor	`ip pim-sparse vsx-virtual-neighbor`	Only required on VSX VTEPs to allow the interface to be in the same multicast data path state on both VSX VTEPs. This allows a VTEP to process IGMP and PIM joins received on this interface regardless of its DR or prime neighbor role.

IGMP snooping

Table 3: *Configuration task list for IGMP snooping*

Step	Command	Comments
1. Enter desired VLAN	`vlan number`	
2. Enable IGMP snooping	`ip igmp snooping enable`	This should be enabled on all VTEPs at the VLAN level

PIM and IGMP on SVI with source and receivers

Table 4: *Configuration task list for PIM and IGMP to be enabled on an SVI with source and receivers attached to the VXLAN overlay network.*

Step	Command	Comments
1. Enter desired SVI	`int vlan number`	This should be enabled on all VTEPs at the SVI level
2. Attach VRF to loopback	`vrf attach name`	Loopback should be part of overlay VRF
3. Enable PIM on SVI	`ip pim-sparse enable`	Required if source or receivers are expected
4. Enable PIM VSX virtual neighbor	`ip pim-sparse vsx-virtual-neighbor`	Only required on VSX VTEPs
5. Enable IGMP on SVI	`ip igmp enable`	Only required if receivers are expected

6. Add desired IPs and Active Gateway info to SVIs	`ip address IP-address`
	`active-gateway ip mac MAC-address`
	`active-gateway ip IP-address`
		The SVI and Active Gateway IPs need to be different

Static RP on VTEP

Table 5: *Configuration task list for PIM VTEPs that utilize remote static RPs*

Step	Command	Comments
1. Enter desired PIM VRF	`router pim vrf name`	
2. Enable PIM at the VRF level	`enable`	This should be enabled on all VTEPs at the PIM VRF level
3. Point to remote static RP	`rp-address IP-address`	RPs could be in the VXLAN overlay or on the external non-VXLAN network

Overlay BSR/RP on VTEP

Table 6: *Configuration task list to enable redundant BSRs/RPs in the VXLAN overlay (if static RPs are not used and BSR/RP is preferred)*

Step	Command	Comments
1. Enter desired SVI	`int lo number`	This should only be enabled on the 2 VTEPs identified as BSR/RP
2. Attach VRF to loopback	`vrf attach name`	Loopback should be part of overlay VRF
3. Enable PIM on Loopback	`ip pim-sparse enable`	
4. Add desired IPs	`ip address IP-address`	The redundant BSRs/RPs should have different /32 IPs
5. Enter desired PIM VRF	`router pim vrf name`	This should only be enabled on the 2 VTEPs identified as BSR/RP
6. Enable RP functionality	`rp-candidate source-ip-interface loopback-number` `rp-candidate group-prefix 224.0.0.0/4`	Specify previously identified loopback as RP Specify prefix for RP
7. Enable BSR functionality	`bsr-candidate source-ip-interface loopback-number`	Specify previously identified loopback as BSR

Considerations and best practices

The following considerations and best practices are recommended for IPv4 Multicast VXLAN:

- IGMP snooping should be enabled on all VTEPs; multicast traffic flooding will happen without IGMP snooping.
- `redistribute local-svi` or `redistribute local-mac` are required on all VTEPs for proper querier information propagation.
- `ip pim-sparse vsx-virtual-neighbor` in SVIs is required on VSX VTEPs.
- A unique virtual-mac should be configured on all VTEPs for a distributed L3 gateway use case; a VSX VTEP pair should be configured with the same virtual-mac.
- It is recommended for RPs to be placed near multicast sources.
- Underlay links, which is used to establish overlay connectivity, should not be enabled with multicast (PIM/IGMP) configuration.
- Overlay RPs/BSRs on VSX VTEPs are only supported on the Aruba 6400 and 8360 Switch Series.

These are the supported VSX VTEP use cases:

- VSX switches (logical VTEPs) for IGMP snooping and PIM-SM
- VSX border VTEP with VSX LAG, L2 extension to sources/receivers in external/non overlay network
- VSX border VTEP with VSX LAG, SVI + PIM-SM L3 extension to sources/receivers in external/non overlay network
- VSX border VTEP with ROP/P2P SVIs + PIM-SM L3 extension to sources in external/non overlay network

Consider the following when deploying ROP and P2P SVI as uplinks on VSX border VTEPs to non-VXLAN networks:

- An additional L3 link per tenant VRF between VSX primary and secondary on overlay is required to handle failover scenarios, this link will normally be P2P SVIs over ISL.
- In the Aruba 6400 and 8360 Switch Series, L3 peering between VSX nodes should be made over an additional dedicated link (this can be another 802.1Q trunk similar to VSX ISL); the VSX ISL cannot be used.
- When using a P2P SVI link extension, do not allow upstream VLANs in ISL; it will make the link non P2P.
- `ip pim-sparse vsx-virtual-neighbor` is not recommended to be enabled on the additional L3 link/P2P SVI link per tenant VRF between VSX peers.

The following restrictions are applicable for IPv4 Multicast VXLAN:

- MSDP, mDNS, mtrace, Inter VRF Route Leaking (IVRL), and PIM-DM over VXLAN are not supported.
- Multicast over static VXLAN tunnels are not supported.
- GShut is not supported on VXLAN based overlay networks.

Use cases

The use cases provide examples of networks using multicast VXLAN configuration.

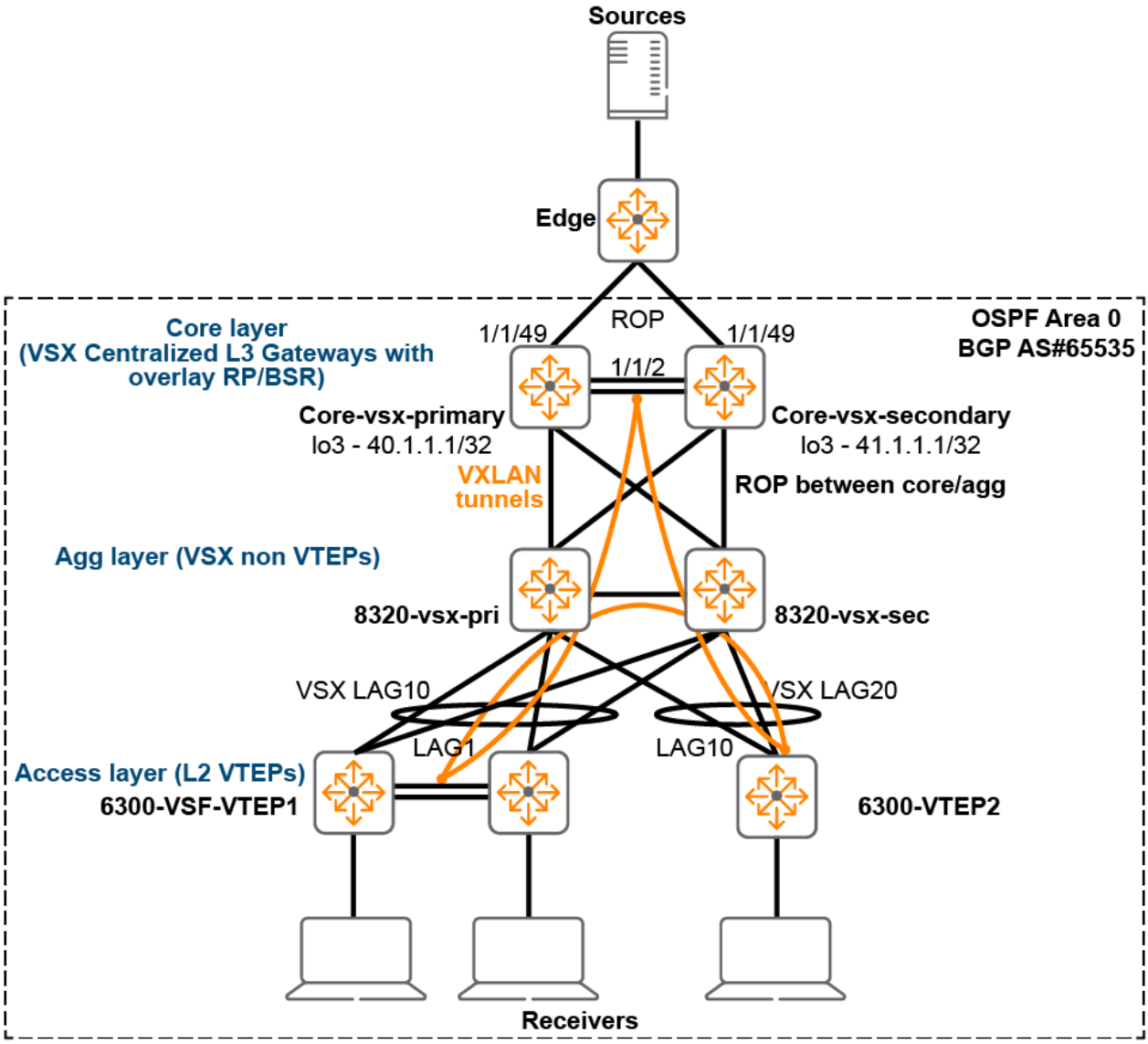
Use case 1: Campus network with centralized L3 gateway

This use case provides the following details:

- Sample configurations
- Relevant verification commands for a campus network with centralized L3 gateway
- Overlay BSRs/RPs on VSX switches
- Receivers in overlay
- Sources in external non-VXLAN network and external network that learn about overlay BSRs/RPs

On the Aruba 8360 VSX centralized L3 gateway, the additional 802.1Q link is required as ROP is used towards the non-VXLAN network (as mentioned in the Considerations and best practices section).

Figure 1 *Use case 1 – Campus network with centralized L3 gateway topology*



Configuration and verification details for the devices in this use case are provided in the following sections:

- Edge
- Core-vsx-primary
- Core-vsx-secondary
- 8320-vsx-pri
- 8320-vsx-sec
- 6300-VSF-VTEP1
- 6300-VTEP2

Edge

Configuration

```
!export-password: default
hostname Edge
```

```
profile Leaf
!
!
!
!
!
ssh server vrf mgmt
vlan 1
interface mgmt
    no shutdown
    ip dhcp
system interface-group 1 speed 10g
    !interface group 1 contains ports 1/1/1-1/1/12
system interface-group 2 speed 10g
    !interface group 2 contains ports 1/1/13-1/1/24
system interface-group 3 speed 10g
    !interface group 3 contains ports 1/1/25-1/1/36
interface 1/1/1
    no shutdown
interface 1/1/2
    no shutdown
interface 1/1/25
    no shutdown
    description Connnection to Ixia Sources
    ip address 60.1.1.1/24
    ip ospf 1 area 0.0.0.0
    ip ospf passive
    ip pim-sparse enable
interface 1/1/26
    no shutdown
interface 1/1/53
    no shutdown
    description Conneciton to Core-vsx-primary
    ip address 80.2.1.2/30
    ip ospf 1 area 0.0.0.0
    ip ospf network point-to-point
    ip pim-sparse enable
interface 1/1/54
    no shutdown
    description Conneciton to Core-vsx-secondary
    ip address 80.3.1.2/30
    ip ospf 1 area 0.0.0.0
    ip ospf network point-to-point
    ip pim-sparse enable
interface loopback 0
    ip address 20.20.20.20/32
    ip ospf 1 area 0.0.0.0
interface loopback 1
    ip address 20.20.20.1/32
    ip ospf 1 area 0.0.0.0
    ip pim-sparse enable
!
!
!
!
!
router ospf 1
    router-id 20.20.20.20
    area 0.0.0.0
router pim
    enable
https-server vrf mgmt
```

Verification

Verify OSPF neighbors

```
Edge# show ip ospf neighbors
VRF : default                              Process : 1
================================================

Total Number of Neighbors : 2

Neighbor ID      Priority  State              Nbr Address       Interface
-------------------------------------------------------------------------
30.1.1.6         n/a       FULL               80.2.1.1           1/1/53

30.2.1.6         n/a       FULL               80.3.1.1           1/1/54
```

Verify PIM neighbors

```
Edge# show ip pim neighbor all-vrfs

PIM Neighbor


VRF                         : default
Total number of neighbors : 2

IP Address                  : 80.2.1.1
Interface                   : 1/1/53
Up Time (HH:MM:SS)          : 00:39:17
Expire Time (HH:MM:SS)      : 00:01:31
DR Priority                 : 1
Hold Time (HH:MM:SS)        : 00:01:45

IP Address                  : 80.3.1.1
Interface                   : 1/1/54
Up Time (HH:MM:SS)          : 00:40:05
Expire Time (HH:MM:SS)      : 00:01:41
DR Priority                 : 1
Hold Time (HH:MM:SS)        : 00:01:45
```

Verify PIM interfaces

```
Edge# show ip pim interface

PIM Interfaces

VRF: default
Total Number of interfaces : 4

Interface  : 1/1/53
Neighbor count : 1
IP Address : 80.2.1.2/30
Mode       : sparse
Designated Router : 80.2.1.2
Proxy DR              : false
Hello Interval (sec)  : 30
Hello Delay (sec)     : 5
Override Interval (msec)  : 2500              Lan Prune Delay     : Yes
Propagation Delay (msec)  : 500               Configured DR Priority    : 1
Operational DR Priority   : 1
Neighbor Timeout          : 92
```

```
Interface  : 1/1/25
Neighbor count : 0
IP Address : 60.1.1.1/24
Mode       : sparse
Designated Router : 60.1.1.1
Proxy DR              : false
Hello Interval (sec)  : 30
Hello Delay (sec)     : 5
Override Interval (msec)  : 2500              Lan Prune Delay     : Yes
Propagation Delay (msec)  : 500               Configured DR Priority    : 1
Operational DR Priority   : 1
Neighbor Timeout          : 0

Interface  : 1/1/54
Neighbor count : 1
IP Address : 80.3.1.2/30
Mode       : sparse
Designated Router : 80.3.1.2
Proxy DR              : false
Hello Interval (sec)  : 30
Hello Delay (sec)     : 5
Override Interval (msec)  : 2500              Lan Prune Delay     : Yes
Propagation Delay (msec)  : 500               Configured DR Priority    : 1
Operational DR Priority   : 1
Neighbor Timeout          : 102

Interface  : loopback1
Neighbor count : 0
IP Address : 20.20.20.1/32
Mode       : sparse
```

Verify mroutes

```
Edge# show ip mroute all-vrfs
IP Multicast Route Entries

VRF : default
Total number of entries : 10

Group Address           : 225.1.1.1
Source Address          : 60.1.1.10
Neighbor                :
Incoming interface      : 1/1/25
Outgoing Interface List :
Interface       State
-----------     ----------
1/1/53          forwarding
1/1/54          forwarding

Group Address           : 225.2.1.1
Source Address          : 60.1.1.10
Neighbor                :
Incoming interface      : 1/1/25
Outgoing Interface List :
Interface       State
-----------     ----------
1/1/54          forwarding
1/1/53          forwarding
!snip
```

```
Group Address           : 225.9.1.1
Source Address          : 60.1.1.10
Neighbor                :
Incoming interface      : 1/1/25
Outgoing Interface List :
Interface       State
-----------     ----------
1/1/54          forwarding
1/1/53          forwarding

Group Address           : 225.10.1.1
Source Address          : 60.1.1.10
Neighbor                :
Incoming interface      : 1/1/25
Outgoing Interface List :
Interface       State
-----------     ----------
1/1/53          forwarding
1/1/54          forwarding
```

Verify BSR information

```
Edge# show ip pim bsr all-vrfs
Status and Counters- PIM-SM Bootstrap Router Information

VRF                       : default
E-BSR Address             : 40.1.1.1
E-BSR Priority            : 100
E-BSR Hash Mask Length    : 30
E-BSR Up Time             : 1 hour 11 mins 18 secs
Next Bootstrap Message    : 1 mins 52 secs

C-BSR Admin Status        : This system is not a Candidate-BSR

C-RP Admin Status         : This system is not a Candidate-RP
```

Verify RP information

```
Edge# show ip pim rp-set all-vrfs

VRF: default

Status and Counters - PIM-SM Learned RP-Set Information
Group Address    Group Mask       RP Address       Hold Time  Expire Time
---------------  ---------------  ---------------  ---------  -----------
224.0.0.0        240.0.0.0        40.1.1.1         150        119
224.0.0.0        240.0.0.0        41.1.1.1         150        119
```

Core-vsx-primary

Configuration

```
!export-password: default
hostname Core-vsx-primary
user admin group administrators password ciphertext
```

```
AQBapY6cG7OGjeUOSUjD8JmBYxBiqulUS3CpBAJhXwz2c6sgYgAAANSAd/CskaIkHsCsIYti0XwXMICwnxbU
dzxWRYTg9XM4uyZuVaRCX37T2FpbesioloyEeCYquFNcD82AWH3oGzm8oZVla8yEV52tqYYPJZAxpZRw1giy
p+7Yl9z3CSk/32Ct
clock timezone us/pacific
no ip icmp redirect
profile Aggregation-Leaf
!
!
!
!
!
ssh server vrf mgmt
vlan 1,10,101
vlan 1001
    ip igmp snooping enable
vlan 1002
    ip igmp snooping enable
vlan 1003
    ip igmp snooping enable
vlan 1004
    ip igmp snooping enable
vlan 1005
    ip igmp snooping enable
vlan 1006
    ip igmp snooping enable
vlan 1007
    ip igmp snooping enable
vlan 1008
    ip igmp snooping enable
vlan 1009
    ip igmp snooping enable
vlan 1010
    ip igmp snooping enable
evpn
    redistribute local-svi
    vlan 1001
        rd 172.1.1.5:1001
        route-target export 1001:1001
        route-target import 1001:1001
        redistribute host-route
    vlan 1002
        rd 172.1.1.5:1002
        route-target export 1002:1002
        route-target import 1002:1002
        redistribute host-route
    vlan 1003
        rd 172.1.1.5:1003
        route-target export 1003:1003
        route-target import 1003:1003
        redistribute host-route
    vlan 1004
        rd 172.1.1.5:1004
        route-target export 1004:1004
        route-target import 1004:1004
        redistribute host-route
    vlan 1005
        rd 172.1.1.5:1005
        route-target export 1005:1005
        route-target import 1005:1005
        redistribute host-route
    vlan 1006
        rd 172.1.1.5:1006
```

```
        route-target export 1006:1006
        route-target import 1006:1006
        redistribute host-route
    vlan 1007
        rd 172.1.1.5:1007
        route-target export 1007:1007
        route-target import 1007:1007
        redistribute host-route
    vlan 1008
        rd 172.1.1.5:1008
        route-target export 1008:1008
        route-target import 1008:1008
        redistribute host-route
    vlan 1009
        rd 172.1.1.5:1009
        route-target export 1009:1009
        route-target import 1009:1009
        redistribute host-route
    vlan 1010
        rd 172.1.1.5:1010
        route-target export 1010:1010
        route-target import 1010:1010
        redistribute host-route
interface mgmt
    no shutdown
    ip dhcp
interface lag 10 multi-chassis
    no shutdown
    no routing
    vlan trunk native 1
    vlan trunk allowed all
    lacp mode active
interface lag 100
    no shutdown
    description ISL
    no routing
    vlan trunk native 1 tag
    vlan trunk allowed all
    lacp mode active
interface 1/1/1
    no shutdown
    lag 100
interface 1/1/2
    description additional L3 link
    no shutdown
    ip address 80.1.1.1/30
    ip ospf 1 area 0.0.0.0
    ip ospf network point-to-point
    ip pim-sparse enable
interface 1/1/3
    no shutdown
interface 1/1/4
    no shutdown
interface 1/1/5
    no shutdown
    description KA
    ip address 192.168.100.1/30
interface 1/1/7
    no shutdown
interface 1/1/28
    no shutdown
interface 1/1/47
```

```
    no shutdown
    description Orphan port to Ixia
    no routing
    vlan trunk native 1
    vlan trunk allowed 1001-1010
interface 1/1/49
    no shutdown
    description Connection to Edge
    ip address 80.2.1.1/30
    ip ospf 1 area 0.0.0.0
    ip ospf network point-to-point
    ip pim-sparse enable
interface 1/1/50
    no shutdown
interface 1/1/51
    no shutdown
    description Connection to Distro_primary
    ip address 30.1.1.2/30
    ip ospf 1 area 0.0.0.0
    ip ospf cost 10
interface 1/1/52
    no shutdown
    description Connection to Distro_secondary
    ip address 30.1.1.6/30
    ip ospf 1 area 0.0.0.0
    ip ospf cost 10
interface loopback 1
    ip address 172.16.1.5/32
    ip ospf 1 area 0.0.0.0
interface loopback 2
    ip address 172.1.1.5/32
    ip ospf 1 area 0.0.0.0
interface loopback 3
    ip address 40.1.1.1/32
    ip ospf 1 area 0.0.0.0
    ip pim-sparse enable
interface loopback 12
interface vlan 1001
    vsx-sync active-gateways
    ip address 101.1.1.252/24
    active-gateway ip mac 00:00:20:00:10:01
    active-gateway ip 101.1.1.254
    ip igmp enable
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 1002
    vsx-sync active-gateways
    ip address 101.2.1.252/24
    active-gateway ip mac 00:00:20:00:10:01
    active-gateway ip 101.2.1.254
    ip igmp enable
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 1003
    vsx-sync active-gateways
    ip address 101.3.1.252/24
    active-gateway ip mac 00:00:20:00:10:01
    active-gateway ip 101.3.1.254
    ip igmp enable
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 1004
```

```
    vsx-sync active-gateways
    ip address 101.4.1.252/24
    active-gateway ip mac 00:00:20:00:10:01
    active-gateway ip 101.4.1.254
    ip igmp enable
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 1005
    vsx-sync active-gateways
    ip address 101.5.1.252/24
    active-gateway ip mac 00:00:20:00:10:01
    active-gateway ip 101.5.1.254
    ip igmp enable
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 1006
    vsx-sync active-gateways
    ip address 101.6.1.252/24
    active-gateway ip mac 00:00:20:00:10:01
    active-gateway ip 101.6.1.254
    ip igmp enable
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 1007
    vsx-sync active-gateways
    ip address 101.7.1.252/24
    active-gateway ip mac 00:00:20:00:10:01
    active-gateway ip 101.7.1.254
    ip igmp enable
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 1008
    vsx-sync active-gateways
    ip address 101.8.1.252/24
    active-gateway ip mac 00:00:20:00:10:01
    active-gateway ip 101.8.1.254
    ip igmp enable
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 1009
    vsx-sync active-gateways
    ip address 101.9.1.252/24
    active-gateway ip mac 00:00:20:00:10:01
    active-gateway ip 101.9.1.254
    ip igmp enable
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 1010
    vsx-sync active-gateways
    ip address 101.10.1.252/24
    active-gateway ip mac 00:00:20:00:10:01
    active-gateway ip 101.10.1.254
    ip igmp enable
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vxlan 1
    source ip 172.1.1.5
    vxlan-counters aggregate
    no shutdown
    vni 1001
        vlan 1001
    vni 1002
```

```
        vlan 1002
    vni 1003
        vlan 1003
    vni 1004
        vlan 1004
    vni 1005
        vlan 1005
    vni 1006
        vlan 1006
    vni 1007
        vlan 1007
    vni 1008
        vlan 1008
    vni 1009
        vlan 1009
    vni 1010
        vlan 1010
vsx
    inter-switch-link lag 100
    role primary
    keepalive peer 192.168.100.2 source 192.168.100.1
    no split-recovery
    vsx-sync evpn
!
!
!
!
!
router ospf 1
    router-id 30.1.1.6
    distance 210
    redistribute connected
    area 0.0.0.0
router bgp 65535
    bgp router-id 172.16.1.5
    no bgp fast-external-fallover
    neighbor 172.16.1.1 remote-as 65535
    neighbor 172.16.1.1 update-source loopback 1
    neighbor 172.16.1.2 remote-as 65535
    neighbor 172.16.1.2 update-source loopback 1
    address-family ipv4 unicast
        network 40.1.1.1/32
    exit-address-family
    address-family l2vpn evpn
        neighbor 172.16.1.1 activate
        neighbor 172.16.1.1 send-community extended
        neighbor 172.16.1.2 activate
        neighbor 172.16.1.2 send-community extended
    exit-address-family
!
router pim
    enable
    rp-candidate source-ip-interface loopback3 group-prefix 224.0.0.0/4
    rp-candidate priority 200
    bsr-candidate source-ip-interface loopback3
    bsr-candidate priority 100
https-server vrf mgmt
```

Verification

Verify OSPF neighbors

```
Core-vsx-primary(config)# show ip ospf neighbors all-vrfs
VRF : default                          Process : 1
================================================

Total Number of Neighbors : 3

Neighbor ID      Priority  State             Nbr Address       Interface
-------------------------------------------------------------------------
20.20.20.20      n/a       FULL              80.2.1.2           1/1/49

30.1.1.1         1         FULL/BDR          30.1.1.1           1/1/51

30.2.1.1         1         FULL/DR           30.1.1.5           1/1/52
```

Verify BGP neighbors

```
Core-vsx-primary(config)# show bgp all summary
VRF : default
BGP Summary
-----------
 Local AS               : 65535        BGP Router Identifier  : 172.16.1.5
 Peers                  : 2            Log Neighbor Changes   : No
 Cfg. Hold Time         : 180          Cfg. Keep Alive        : 60
 Confederation Id       : 0

Address-family : IPv4 Unicast
------------------------------

Address-family : IPv6 Unicast
------------------------------

Address-family : L2VPN EVPN
------------------------------
 Neighbor        Remote-AS MsgRcvd MsgSent   Up/Down Time State        AdminStatus
 172.16.1.1      65535       217     180     02h:03m:15s  Established   Up
 172.16.1.2      65535       171     181     02h:03m:22s  Established   Up
```

Verify VXLAN tunnel, VTEP peers, and VNIs

```
Leaf01-primary# show interface vxlan
Core-vsx-primary(config)# show interface vxlan vteps
Source           Destination      Origin       Status               VNI       Routing   VLAN  VRF
---------------- ---------------- ------------ -------------------- --------- --------- ----- ---
172.1.1.5        172.1.1.1        evpn         operational          1001      disabled  1001   --
172.1.1.5        172.1.1.1        evpn         operational          1002      disabled  1002   --
172.1.1.5        172.1.1.1        evpn         operational          1003      disabled  1003   --
172.1.1.5        172.1.1.1        evpn         operational          1004      disabled  1004   --
172.1.1.5        172.1.1.1        evpn         operational          1005      disabled  1005   --
172.1.1.5        172.1.1.1        evpn         operational          1006      disabled  1006   --
172.1.1.5        172.1.1.1        evpn         operational          1007      disabled  1007   --
172.1.1.5        172.1.1.1        evpn         operational          1008      disabled  1008   --
172.1.1.5        172.1.1.1        evpn         operational          1009      disabled  1009   --
172.1.1.5        172.1.1.1        evpn         operational          1010      disabled  1010   --
172.1.1.5        172.1.1.2        evpn         operational          1001      disabled  1001   --
172.1.1.5        172.1.1.2        evpn         operational          1002      disabled  1002   --
172.1.1.5        172.1.1.2        evpn         operational          1003      disabled  1003   --
172.1.1.5        172.1.1.2        evpn         operational          1004      disabled  1004   --
172.1.1.5        172.1.1.2        evpn         operational          1005      disabled  1005   --
172.1.1.5        172.1.1.2        evpn         operational          1006      disabled  1006   --
```

```
172.1.1.5        172.1.1.2        evpn         operational          1007      disabled  1007   --
172.1.1.5        172.1.1.2        evpn         operational          1008      disabled  1008   --
172.1.1.5        172.1.1.2        evpn         operational          1009      disabled  1009   --
172.1.1.5        172.1.1.2        evpn         operational          1010      disabled  1010   --
```

Verify BGP EVPN table

```
Core-vsx-primary(config)# show bgp l2vpn evpn
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
              i internal, e external S Stale, R Removed, a additional-paths
Origin codes: i - IGP, e - EGP, ? - incomplete

EVPN Route-Type 2 prefix: [2]:[ESI]:[EthTag]:[MAC]:[OrigIP]
EVPN Route-Type 3 prefix: [3]:[EthTag]:[OrigIP]
EVPN Route-Type 5 prefix: [5]:[ESI]:[EthTag]:[IPAddrLen]:[IPAddr]
VRF : default
Local Router-ID 172.16.1.5

     Network                                          Nexthop         Metric     LocPrf    Weight   Path
-----------------------------------------------------------------------------------------------------------
Route Distinguisher: 172.1.1.1:1001       (L2VNI 1001)
*>i [2]:[0]:[0]:[00:11:01:00:00:01]:[]                172.1.1.1       0          100        0       ?
*>i [3]:[0]:[172.1.1.1]                               172.1.1.1       0          100        0       ?

Route Distinguisher: 172.1.1.2:1001       (L2VNI 1001)
*>i [2]:[0]:[0]:[00:13:01:00:00:01]:[]                172.1.1.2       0          100        0       ?
*>i [3]:[0]:[172.1.1.2]                               172.1.1.2       0          100        0       ?

Route Distinguisher: 172.1.1.5:1001       (L2VNI 1001)
*>  [2]:[0]:[0]:[00:00:20:00:10:01]:[101.1.1.254]    172.1.1.5       0          100        0       ?
*>  [2]:[0]:[0]:[b8:d4:e7:5d:8a:00]:[101.1.1.252]    172.1.1.5       0          100        0       ?
*>  [3]:[0]:[172.1.1.5]                               172.1.1.5       0          100        0       ?

Route Distinguisher: 172.1.1.1:1002       (L2VNI 1002)
*>i [2]:[0]:[0]:[00:11:01:00:00:02]:[]                172.1.1.1       0          100        0       ?
*>i [3]:[0]:[172.1.1.1]                               172.1.1.1       0          100        0       ?

Route Distinguisher: 172.1.1.2:1002       (L2VNI 1002)
*>i [2]:[0]:[0]:[00:13:01:00:00:02]:[]                172.1.1.2       0          100        0       ?
*>i [3]:[0]:[172.1.1.2]                               172.1.1.2       0          100        0       ?

Route Distinguisher: 172.1.1.5:1002       (L2VNI 1002)
*>  [2]:[0]:[0]:[00:00:20:00:10:01]:[101.2.1.254]    172.1.1.5       0          100        0       ?
*>  [2]:[0]:[0]:[b8:d4:e7:5d:8a:00]:[101.2.1.252]    172.1.1.5       0          100        0       ?
*>  [3]:[0]:[172.1.1.5]                               172.1.1.5       0          100        0       ?

Route Distinguisher: 172.1.1.1:1003       (L2VNI 1003)
*>i [2]:[0]:[0]:[00:11:01:00:00:03]:[]                172.1.1.1       0          100        0       ?
*>i [3]:[0]:[172.1.1.1]                               172.1.1.1       0          100        0       ?

Route Distinguisher: 172.1.1.2:1003       (L2VNI 1003)
*>i [2]:[0]:[0]:[00:13:01:00:00:03]:[]                172.1.1.2       0          100        0       ?
*>i [3]:[0]:[172.1.1.2]                               172.1.1.2       0          100        0       ?
!snip

Route Distinguisher: 172.1.1.2:1009       (L2VNI 1009)
*>i [2]:[0]:[0]:[00:13:01:00:00:09]:[]                172.1.1.2       0          100        0       ?
*>i [3]:[0]:[172.1.1.2]                               172.1.1.2       0          100        0       ?

Route Distinguisher: 172.1.1.5:1009       (L2VNI 1009)
*>  [2]:[0]:[0]:[00:00:20:00:10:01]:[101.9.1.254]    172.1.1.5       0          100        0       ?
```

```
*>  [2]:[0]:[0]:[b8:d4:e7:5d:8a:00]:[101.9.1.252]          172.1.1.5       0          100        0       ?
*>  [3]:[0]:[172.1.1.5]                                    172.1.1.5       0          100        0       ?

Route Distinguisher: 172.1.1.1:1010       (L2VNI 1010)
*>i [2]:[0]:[0]:[00:11:01:00:00:0a]:[]                     172.1.1.1       0          100        0       ?
*>i [3]:[0]:[172.1.1.1]                                    172.1.1.1       0          100        0       ?

Route Distinguisher: 172.1.1.2:1010       (L2VNI 1010)
*>i [2]:[0]:[0]:[00:13:01:00:00:0a]:[]                     172.1.1.2       0          100        0       ?
*>i [3]:[0]:[172.1.1.2]                                    172.1.1.2       0          100        0       ?

Route Distinguisher: 172.1.1.5:1010       (L2VNI 1010)
*>  [2]:[0]:[0]:[00:00:20:00:10:01]:[101.10.1.254]        172.1.1.5       0          100        0       ?
*>  [2]:[0]:[0]:[b8:d4:e7:5d:8a:00]:[101.10.1.252]        172.1.1.5       0          100        0       ?
*>  [3]:[0]:[172.1.1.5]                                    172.1.1.5       0          100        0       ?
Total number of entries 70
```

Verify PIM neighbors

```
Core-vsx-primary(config)# do show ip pim neighbor all-vrfs

PIM Neighbor


VRF                         : default
Total number of neighbors   : 11

IP Address                  : 80.2.1.2
Interface                   : 1/1/49
Up Time (HH:MM:SS)          : 01:15:56
Expire Time (HH:MM:SS)      : 00:01:25
DR Priority                 : 1
Hold Time (HH:MM:SS)        : 00:01:45

IP Address                  : 101.1.1.253
Interface                   : vlan1001
Up Time (HH:MM:SS)          : 02:03:48
Expire Time (HH:MM:SS)      : 00:01:33
DR Priority                 : 83952044
Hold Time (HH:MM:SS)        : 00:01:45

IP Address                  : 101.2.1.253
Interface                   : vlan1002
Up Time (HH:MM:SS)          : 02:03:48
Expire Time (HH:MM:SS)      : 00:01:32
DR Priority                 : 83952044
Hold Time (HH:MM:SS)        : 00:01:45

IP Address                  : 101.3.1.253
Interface                   : vlan1003
Up Time (HH:MM:SS)          : 02:03:47
Expire Time (HH:MM:SS)      : 00:01:32
DR Priority                 : 83952044
Hold Time (HH:MM:SS)        : 00:01:45
!snip

IP Address                  : 101.8.1.253
Interface                   : vlan1008
Up Time (HH:MM:SS)          : 02:03:47
Expire Time (HH:MM:SS)      : 00:01:30
DR Priority                 : 83952044
```

```
Hold Time (HH:MM:SS)      : 00:01:45

IP Address                : 101.9.1.253
Interface                 : vlan1009
Up Time (HH:MM:SS)        : 02:03:48
Expire Time (HH:MM:SS)    : 00:01:29
DR Priority               : 83952044
Hold Time (HH:MM:SS)      : 00:01:45

IP Address                : 101.10.1.253
Interface                 : vlan1010
Up Time (HH:MM:SS)        : 02:03:48
Expire Time (HH:MM:SS)    : 00:01:33
DR Priority               : 83952044
Hold Time (HH:MM:SS)      : 00:01:45
```

Verify PIM interfaces

```
Core-vsx-primary(config)# show ip pim interface

PIM Interfaces

VRF: default
Total Number of interfaces : 13

Interface  : vlan1003
Neighbor count : 1
IP Address : 101.3.1.252/24
Mode       : sparse
Designated Router : 101.3.1.252
Proxy DR              : false
Hello Interval (sec)  : 30
Hello Delay (sec)     : 5
Override Interval (msec)  : 2500              Lan Prune Delay     : Yes
Propagation Delay (msec)  : 500               Configured DR Priority    : 1
Operational DR Priority   : 83952044
Neighbor Timeout          : 87

Interface  : loopback3
Neighbor count : 0
IP Address : 40.1.1.1/32
Mode       : sparse

Interface  : 1/1/2
Neighbor count : 0
IP Address : 80.1.1.1/30
Mode       : sparse
Designated Router : 80.1.1.1
Proxy DR              : false
Hello Interval (sec)  : 30
Hello Delay (sec)     : 5
Override Interval (msec)  : 2500              Lan Prune Delay     : Yes
Propagation Delay (msec)  : 500               Configured DR Priority    : 1
Operational DR Priority   : 1
Neighbor Timeout          : 0

Interface  : vlan1001
Neighbor count : 1
IP Address : 101.1.1.252/24
Mode       : sparse
Designated Router : 101.1.1.252
```

```
Proxy DR              : false
Hello Interval (sec)  : 30
Hello Delay (sec)     : 5
Override Interval (msec)  : 2500              Lan Prune Delay     : Yes
Propagation Delay (msec)  : 500               Configured DR Priority    : 1
Operational DR Priority   : 83952044
Neighbor Timeout          : 88
!snip

Interface  : vlan1002
Neighbor count : 1
IP Address : 101.2.1.252/24
Mode       : sparse
Designated Router : 101.2.1.252
Proxy DR              : false
Hello Interval (sec)  : 30
Hello Delay (sec)     : 5
Override Interval (msec)  : 2500              Lan Prune Delay     : Yes
Propagation Delay (msec)  : 500               Configured DR Priority    : 1
Operational DR Priority   : 83952044
Neighbor Timeout          : 87
```

Verify mroutes

```
Core-vsx-primary(config)# show ip mroute all-vrfs
IP Multicast Route Entries

VRF : default
Total number of entries : 10

Group Address           : 225.1.1.1
Source Address          : 60.1.1.10
Neighbor                : 80.2.1.2
Incoming interface      : 1/1/49
Outgoing Interface List :
Interface       State
-----------     ----------
vlan1001        forwarding

Group Address           : 225.2.1.1
Source Address          : 60.1.1.10
Neighbor                : 80.2.1.2
Incoming interface      : 1/1/49
Outgoing Interface List :
Interface       State
-----------     ----------
vlan1002        forwarding

Group Address           : 225.3.1.1
Source Address          : 60.1.1.10
Neighbor                : 80.2.1.2
Incoming interface      : 1/1/49
Outgoing Interface List :
Interface       State
-----------     ----------
vlan1003        forwarding

Group Address           : 225.4.1.1
Source Address          : 60.1.1.10
Neighbor                : 80.2.1.2
Incoming interface      : 1/1/49
```

```
Outgoing Interface List :
Interface       State
-----------     ----------
vlan1004        forwarding
!snip

Group Address           : 225.9.1.1
Source Address          : 60.1.1.10
Neighbor                : 80.2.1.2
Incoming interface      : 1/1/49
Outgoing Interface List :
Interface       State
-----------     ----------
vlan1009        forwarding

Group Address           : 225.10.1.1
Source Address          : 60.1.1.10
Neighbor                : 80.2.1.2
Incoming interface      : 1/1/49
Outgoing Interface List :
Interface       State
-----------     ----------
vlan1010        forwarding
```

Verify BSR information

```
Core-vsx-primary(config)# show ip pim bsr all-vrfs
Status and Counters- PIM-SM Bootstrap Router Information

VRF                       : default
E-BSR Address             : 40.1.1.1
E-BSR Priority            : 100
E-BSR Hash Mask Length    : 30
E-BSR Up Time             : 2 hour 7 mins 49 secs
Next Bootstrap Message    : 14 secs

C-BSR Admin Status        : This system is a Candidate-BSR
C-BSR Address             : 40.1.1.1
C-BSR Priority            : 100
C-BSR Hash Mask Length    : 30
C-BSR Message Interval    : 60
C-BSR Source IP Interface : loopback3

C-RP Admin Status         : This system is a Candidate-RP
C-RP Address              : 40.1.1.1
C-RP Hold Time            : 150
C-RP Advertise Period     : 60
C-RP Priority             : 200
C-RP Source IP Interface  : loopback3

Group Address    Group Mask
---------------  ---------------
224.0.0.0        240.0.0.0
```

Verify RP information

```
Core-vsx-primary(config)# show ip pim rp-set all-vrfs

VRF: default
```

```
Status and Counters - PIM-SM Learned RP-Set Information
Group Address    Group Mask       RP Address       Hold Time  Expire Time
---------------  ---------------  ---------------  ---------  -----------
224.0.0.0        240.0.0.0        40.1.1.1         150        97
224.0.0.0        240.0.0.0        41.1.1.1         150        97
```

Verify IGMP snooping

```
Core-vsx-primary(config)# show ip igmp snooping

IGMP Snooping Protocol Info

Total VLANs with IGMP enabled             : 10
Current count of multicast groups joined  : 10

IGMP Drop Unknown Multicast               : Global
VLAN ID : 1001
VLAN Name : VLAN1001
IGMP Configured Version : 3
IGMP Operating Version : 3
Querier Address [this switch] : 101.1.1.252
Querier Port :
Querier UpTime :2h 9m
Querier Expiration Time :1m 37s

Active Group Address   Tracking  Vers Mode Uptime    Expires
---------------------- ---------- ---- ---- --------- ----------
225.1.1.1              Filter    2         1h 40m    3m 56s

VLAN ID : 1002
VLAN Name : VLAN1002
IGMP Configured Version : 3
IGMP Operating Version : 3
Querier Address [this switch] : 101.2.1.252
Querier Port :
Querier UpTime :2h 9m
Querier Expiration Time :1m 37s

Active Group Address   Tracking  Vers Mode Uptime    Expires
---------------------- ---------- ---- ---- --------- ----------
225.2.1.1              Filter    2         1h 40m    4m 1s

VLAN ID : 1003
VLAN Name : VLAN1003
IGMP Configured Version : 3
IGMP Operating Version : 3
Querier Address [this switch] : 101.3.1.252
Querier Port :
Querier UpTime :2h 9m
Querier Expiration Time :1m 37s

Active Group Address   Tracking  Vers Mode Uptime    Expires
---------------------- ---------- ---- ---- --------- ----------
225.3.1.1              Filter    2         1h 40m    4m 0s

VLAN ID : 1004
VLAN Name : VLAN1004
IGMP Configured Version : 3
IGMP Operating Version : 3
Querier Address [this switch] : 101.4.1.252
```

```
Querier Port :
Querier UpTime :2h 9m
Querier Expiration Time :1m 37s

Active Group Address   Tracking  Vers Mode Uptime    Expires
---------------------- ---------- ---- ---- --------- ----------
225.4.1.1              Filter    2         1h 40m    4m 2s
!snip

VLAN ID : 1009
VLAN Name : VLAN1009
IGMP Configured Version : 3
IGMP Operating Version : 3
Querier Address [this switch] : 101.9.1.252
Querier Port :
Querier UpTime :2h 9m
Querier Expiration Time :1m 37s

Active Group Address   Tracking  Vers Mode Uptime    Expires
---------------------- ---------- ---- ---- --------- ----------
225.9.1.1              Filter    2         1h 40m    3m 58s

VLAN ID : 1010
VLAN Name : VLAN1010
IGMP Configured Version : 3
IGMP Operating Version : 3
Querier Address [this switch] : 101.10.1.252
Querier Port :
Querier UpTime :2h 9m
Querier Expiration Time :1m 37s

Active Group Address   Tracking  Vers Mode Uptime    Expires
---------------------- ---------- ---- ---- --------- ----------
225.10.1.1             Filter    2         1h 40m    4m 0s
```

Verify IGMP

```
Core-vsx-primary(config)# show ip igmp

VRF Name   : default
Interface  : vlan1001
IGMP Configured Version  : 3
IGMP Operating Version   : 3
Querier State              : Querier
Querier IP [this switch]   : 101.1.1.252
Querier Uptime             : 2h 9m
Querier Expiration Time    : 1m 30s
IGMP Snoop Enabled on VLAN : True

Active Group Address   Vers Mode Uptime    Expires
---------------------- ---- ---- --------- ---------
225.1.1.1              2         1h 40m    3m 49s

VRF Name   : default
Interface  : vlan1002
IGMP Configured Version  : 3
IGMP Operating Version   : 3
Querier State              : Querier
Querier IP [this switch]   : 101.2.1.252
Querier Uptime             : 2h 9m
Querier Expiration Time    : 1m 30s
```

```
IGMP Snoop Enabled on VLAN : True

Active Group Address   Vers Mode Uptime    Expires
---------------------- ---- ---- --------- ---------
225.2.1.1              2         1h 40m    3m 54s

VRF Name   : default
Interface  : vlan1003
IGMP Configured Version  : 3
IGMP Operating Version   : 3
Querier State              : Querier
Querier IP [this switch]   : 101.3.1.252
Querier Uptime             : 2h 9m
Querier Expiration Time    : 1m 30s
IGMP Snoop Enabled on VLAN : True

Active Group Address   Vers Mode Uptime    Expires
---------------------- ---- ---- --------- ---------
225.3.1.1              2         1h 43m    3m 53s
!snip

VRF Name   : default
Interface  : vlan1010
IGMP Configured Version  : 3
IGMP Operating Version   : 3
Querier State              : Querier
Querier IP [this switch]   : 101.10.1.252
Querier Uptime             : 2h 9m
Querier Expiration Time    : 1m 30s
IGMP Snoop Enabled on VLAN : True

Active Group Address   Vers Mode Uptime    Expires
---------------------- ---- ---- --------- ---------
225.10.1.1             2         1h 43m    3m 53s
```

Core-vsx-secondary

Configuration

```
!export-password: default
hostname Core-vsx-secondary
clock timezone us/pacific
no ip icmp redirect
profile Aggregation-Leaf
!
!
!
!
!
ssh server vrf mgmt
vlan 1,101
vlan 1001
    ip igmp snooping enable
vlan 1002
    ip igmp snooping enable
vlan 1003
    ip igmp snooping enable
vlan 1004
    ip igmp snooping enable
vlan 1005
    ip igmp snooping enable
```

```
vlan 1006
    ip igmp snooping enable
vlan 1007
    ip igmp snooping enable
vlan 1008
    ip igmp snooping enable
vlan 1009
    ip igmp snooping enable
vlan 1010
    ip igmp snooping enable
evpn
    redistribute local-svi
    vlan 1001
        rd 172.1.1.5:1001
        route-target export 1001:1001
        route-target import 1001:1001
        redistribute host-route
    vlan 1002
        rd 172.1.1.5:1002
        route-target export 1002:1002
        route-target import 1002:1002
        redistribute host-route
    vlan 1003
        rd 172.1.1.5:1003
        route-target export 1003:1003
        route-target import 1003:1003
        redistribute host-route
    vlan 1004
        rd 172.1.1.5:1004
        route-target export 1004:1004
        route-target import 1004:1004
        redistribute host-route
    vlan 1005
        rd 172.1.1.5:1005
        route-target export 1005:1005
        route-target import 1005:1005
        redistribute host-route
    vlan 1006
        rd 172.1.1.5:1006
        route-target export 1006:1006
        route-target import 1006:1006
        redistribute host-route
    vlan 1007
        rd 172.1.1.5:1007
        route-target export 1007:1007
        route-target import 1007:1007
        redistribute host-route
    vlan 1008
        rd 172.1.1.5:1008
        route-target export 1008:1008
        route-target import 1008:1008
        redistribute host-route
    vlan 1009
        rd 172.1.1.5:1009
        route-target export 1009:1009
        route-target import 1009:1009
        redistribute host-route
    vlan 1010
        rd 172.1.1.5:1010
        route-target export 1010:1010
        route-target import 1010:1010
        redistribute host-route
```

```
interface mgmt
    no shutdown
    ip dhcp
interface lag 100
    no shutdown
    description ISL
    no routing
    vlan trunk native 1 tag
    vlan trunk allowed all
    lacp mode active
interface 1/1/1
    no shutdown
    lag 100
interface 1/1/2
    no shutdown
    description Additional L3 link
    ip address 80.1.1.1/30
    ip ospf 1 area 0.0.0.0
    ip ospf network point-to-point
interface 1/1/3
    no shutdown
interface 1/1/4
    no shutdown
interface 1/1/5
    no shutdown
    description KA
    ip address 192.168.100.2/30
interface 1/1/7
    no shutdown
interface 1/1/28
    no shutdown
interface 1/1/47
    no shutdown
    description Orphan port to Ixia
    no routing
    vlan trunk native 1
    vlan trunk allowed 1001-1010
interface 1/1/49
    no shutdown
    description Connection to Edge
    ip address 80.3.1.1/30
    ip ospf 1 area 0.0.0.0
    ip ospf network point-to-point
    ip pim-sparse enable
interface 1/1/50
    no shutdown
interface 1/1/51
    no shutdown
    description Connection to Distro_primary
    ip address 30.2.1.2/30
    ip ospf 1 area 0.0.0.0
    ip ospf cost 10
interface 1/1/52
    no shutdown
    description Connection to Distro_secondary
    ip address 30.2.1.6/30
    ip ospf 1 area 0.0.0.0
    ip ospf cost 10
interface loopback 1
    ip address 172.16.1.4/32
    ip ospf 1 area 0.0.0.0
interface loopback 2
```

```
    ip address 172.1.1.5/32
    ip ospf 1 area 0.0.0.0
interface loopback 3
    ip address 41.1.1.1/32
    ip ospf 1 area 0.0.0.0
    ip pim-sparse enable
interface vlan 1001
    vsx-sync active-gateways
    ip address 101.1.1.253/24
    active-gateway ip mac 00:00:20:00:10:01
    active-gateway ip 101.1.1.254
    ip igmp enable
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 1002
    vsx-sync active-gateways
    ip address 101.2.1.253/24
    active-gateway ip mac 00:00:20:00:10:01
    active-gateway ip 101.2.1.254
    ip igmp enable
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 1003
    vsx-sync active-gateways
    ip address 101.3.1.253/24
    active-gateway ip mac 00:00:20:00:10:01
    active-gateway ip 101.3.1.254
    ip igmp enable
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 1004
    vsx-sync active-gateways
    ip address 101.4.1.253/24
    active-gateway ip mac 00:00:20:00:10:01
    active-gateway ip 101.4.1.254
    ip igmp enable
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 1005
    vsx-sync active-gateways
    ip address 101.5.1.253/24
    active-gateway ip mac 00:00:20:00:10:01
    active-gateway ip 101.5.1.254
    ip igmp enable
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 1006
    vsx-sync active-gateways
    ip address 101.6.1.253/24
    active-gateway ip mac 00:00:20:00:10:01
    active-gateway ip 101.6.1.254
    ip igmp enable
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 1007
    vsx-sync active-gateways
    ip address 101.7.1.253/24
    active-gateway ip mac 00:00:20:00:10:01
    active-gateway ip 101.7.1.254
    ip igmp enable
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
```

```
interface vlan 1008
    vsx-sync active-gateways
    ip address 101.8.1.253/24
    active-gateway ip mac 00:00:20:00:10:01
    active-gateway ip 101.8.1.254
    ip igmp enable
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 1009
    vsx-sync active-gateways
    ip address 101.9.1.253/24
    active-gateway ip mac 00:00:20:00:10:01
    active-gateway ip 101.9.1.254
    ip igmp enable
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 1010
    vsx-sync active-gateways
    ip address 101.10.1.253/24
    active-gateway ip mac 00:00:20:00:10:01
    active-gateway ip 101.10.1.254
    ip igmp enable
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vxlan 1
    source ip 172.1.1.5
    vxlan-counters aggregate
    no shutdown
    vni 1001
        vlan 1001
    vni 1002
        vlan 1002
    vni 1003
        vlan 1003
    vni 1004
        vlan 1004
    vni 1005
        vlan 1005
    vni 1006
        vlan 1006
    vni 1007
        vlan 1007
    vni 1008
        vlan 1008
    vni 1009
        vlan 1009
    vni 1010
        vlan 1010
vsx
    inter-switch-link lag 100
    role secondary
    keepalive peer 192.168.100.1 source 192.168.100.2
    vsx-sync evpn
!
!
!
!
!
router ospf 1
    router-id 30.2.1.6
    distance 210
    redistribute connected
```

```
    area 0.0.0.0
router bgp 65535
    bgp router-id 172.16.1.4
    no bgp fast-external-fallover
    neighbor 172.16.1.1 remote-as 65535
    neighbor 172.16.1.1 update-source loopback 1
    neighbor 172.16.1.2 remote-as 65535
    neighbor 172.16.1.2 update-source loopback 1
    address-family ipv4 unicast
        network 41.1.1.1/32
    exit-address-family
    address-family l2vpn evpn
        neighbor 172.16.1.1 activate
        neighbor 172.16.1.1 send-community extended
        neighbor 172.16.1.2 activate
        neighbor 172.16.1.2 send-community extended
    exit-address-family
!
router pim
    enable
    rp-candidate source-ip-interface loopback3 group-prefix 224.0.0.0/4
    bsr-candidate source-ip-interface loopback3
https-server vrf mgmt
```

Verification

Verify OSPF neighbors

```
Core-vsx-secondary(config)# show ip ospf neighbors
VRF : default                           Process : 1
================================================

Total Number of Neighbors : 3

Neighbor ID      Priority  State             Nbr Address       Interface
-------------------------------------------------------------------------
20.20.20.20      n/a       FULL              80.3.1.2           1/1/49

30.1.1.1         1         FULL/BDR          30.2.1.1           1/1/51

30.2.1.1         1         FULL/BDR          30.2.1.5           1/1/52
```

Verify BGP neighbors

```
Core-vsx-secondary(config)# show bgp all summary
VRF : default
BGP Summary
-----------
 Local AS               : 65535        BGP Router Identifier  : 172.16.1.4
 Peers                  : 2            Log Neighbor Changes   : No
 Cfg. Hold Time         : 180          Cfg. Keep Alive        : 60
 Confederation Id       : 0

Address-family : IPv4 Unicast
-----------------------------

Address-family : IPv6 Unicast
-----------------------------
```

```
Address-family : L2VPN EVPN
------------------------------
 Neighbor        Remote-AS MsgRcvd MsgSent   Up/Down Time State        AdminStatus
 172.16.1.1      65535       199     189     02h:12m:11s  Established   Up
 172.16.1.2      65535       182     187     02h:12m:12s  Established   Up
```

Verify VXLAN tunnel, VTEP peers, and VNIs

```
Core-vsx-secondary(config)# show interface vxlan vteps
Source            Destination       Origin       Status                VNI       Routing   VLAN  VRF
----------------- ----------------- ------------ --------------------- --------- --------- ----- ---
-
172.1.1.5         172.1.1.1         evpn         operational           1001      disabled  1001   --
172.1.1.5         172.1.1.1         evpn         operational           1002      disabled  1002   --
172.1.1.5         172.1.1.1         evpn         operational           1003      disabled  1003   --
172.1.1.5         172.1.1.1         evpn         operational           1004      disabled  1004   --
172.1.1.5         172.1.1.1         evpn         operational           1005      disabled  1005   --
172.1.1.5         172.1.1.1         evpn         operational           1006      disabled  1006   --
172.1.1.5         172.1.1.1         evpn         operational           1007      disabled  1007   --
172.1.1.5         172.1.1.1         evpn         operational           1008      disabled  1008   --
172.1.1.5         172.1.1.1         evpn         operational           1009      disabled  1009   --
172.1.1.5         172.1.1.1         evpn         operational           1010      disabled  1010   --
172.1.1.5         172.1.1.2         evpn         operational           1001      disabled  1001   --
172.1.1.5         172.1.1.2         evpn         operational           1002      disabled  1002   --
172.1.1.5         172.1.1.2         evpn         operational           1003      disabled  1003   --
172.1.1.5         172.1.1.2         evpn         operational           1004      disabled  1004   --
172.1.1.5         172.1.1.2         evpn         operational           1005      disabled  1005   --
172.1.1.5         172.1.1.2         evpn         operational           1006      disabled  1006   --
172.1.1.5         172.1.1.2         evpn         operational           1007      disabled  1007   --
172.1.1.5         172.1.1.2         evpn         operational           1008      disabled  1008   --
172.1.1.5         172.1.1.2         evpn         operational           1009      disabled  1009   --
172.1.1.5         172.1.1.2         evpn         operational           1010      disabled  1010   --
```

Verify BGP EVPN table

```
Core-vsx-secondary(config)# show bgp l2vpn evpn
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
              i internal, e external S Stale, R Removed, a additional-paths
Origin codes: i - IGP, e - EGP, ? - incomplete

EVPN Route-Type 2 prefix: [2]:[ESI]:[EthTag]:[MAC]:[OrigIP]
EVPN Route-Type 3 prefix: [3]:[EthTag]:[OrigIP]
EVPN Route-Type 5 prefix: [5]:[ESI]:[EthTag]:[IPAddrLen]:[IPAddr]
VRF : default
Local Router-ID 172.16.1.4

     Network                                          Nexthop         Metric     LocPrf    Weight   Path
-------------------------------------------------------------------------------------------------------
Route Distinguisher: 172.1.1.1:1001       (L2VNI 1001)
*>i [2]:[0]:[0]:[00:11:01:00:00:01]:[]                172.1.1.1       0          100        0       ?
*>i [3]:[0]:[172.1.1.1]                               172.1.1.1       0          100        0       ?

Route Distinguisher: 172.1.1.2:1001       (L2VNI 1001)
*>i [2]:[0]:[0]:[00:13:01:00:00:01]:[]                172.1.1.2       0          100        0       ?
*>i [3]:[0]:[172.1.1.2]                               172.1.1.2       0          100        0       ?

Route Distinguisher: 172.1.1.5:1001       (L2VNI 1001)
*>  [2]:[0]:[0]:[00:00:20:00:10:01]:[101.1.1.254]    172.1.1.5       0          100        0       ?
*>  [2]:[0]:[0]:[b8:d4:e7:5b:2c:00]:[101.1.1.253]    172.1.1.5       0          100        0       ?
```

```
*>  [3]:[0]:[172.1.1.5]                                  172.1.1.5       0          100        0       ?

Route Distinguisher: 172.1.1.1:1002       (L2VNI 1002)
*>i [2]:[0]:[0]:[00:11:01:00:00:02]:[]                   172.1.1.1       0          100        0       ?
*>i [3]:[0]:[172.1.1.1]                                  172.1.1.1       0          100        0       ?

Route Distinguisher: 172.1.1.2:1002       (L2VNI 1002)
*>i [2]:[0]:[0]:[00:13:01:00:00:02]:[]                   172.1.1.2       0          100        0       ?
*>i [3]:[0]:[172.1.1.2]                                  172.1.1.2       0          100        0       ?

Route Distinguisher: 172.1.1.5:1002       (L2VNI 1002)
*>  [2]:[0]:[0]:[00:00:20:00:10:01]:[101.2.1.254]        172.1.1.5       0          100        0       ?
*>  [2]:[0]:[0]:[b8:d4:e7:5b:2c:00]:[101.2.1.253]        172.1.1.5       0          100        0       ?
*>  [3]:[0]:[172.1.1.5]                                  172.1.1.5       0          100        0       ?
!snip

Route Distinguisher: 172.1.1.1:1010       (L2VNI 1010)
*>i [2]:[0]:[0]:[00:11:01:00:00:0a]:[]                   172.1.1.1       0          100        0       ?
*>i [3]:[0]:[172.1.1.1]                                  172.1.1.1       0          100        0       ?

Route Distinguisher: 172.1.1.2:1010       (L2VNI 1010)
*>i [2]:[0]:[0]:[00:13:01:00:00:0a]:[]                   172.1.1.2       0          100        0       ?
*>i [3]:[0]:[172.1.1.2]                                  172.1.1.2       0          100        0       ?

Route Distinguisher: 172.1.1.5:1010       (L2VNI 1010)
*>  [2]:[0]:[0]:[00:00:20:00:10:01]:[101.10.1.254]       172.1.1.5       0          100        0       ?
*>  [2]:[0]:[0]:[b8:d4:e7:5b:2c:00]:[101.10.1.253]       172.1.1.5       0          100        0       ?
*>  [3]:[0]:[172.1.1.5]                                  172.1.1.5       0          100        0       ?
Total number of entries 70
```

Verify PIM neighbors

```
Core-vsx-secondary(config)# show ip pim neighbor

PIM Neighbor

VRF                         : default
Total number of neighbors : 11

IP Address                  : 80.3.1.2
Interface                   : 1/1/49
Up Time (HH:MM:SS)          : 01:27:10
Expire Time (HH:MM:SS)      : 00:01:37
DR Priority                 : 1
Hold Time (HH:MM:SS)        : 00:01:45

IP Address                  : 101.1.1.252
Interface                   : vlan1001
Up Time (HH:MM:SS)          : 02:14:14
Expire Time (HH:MM:SS)      : 00:01:36
DR Priority                 : 83952044
Hold Time (HH:MM:SS)        : 00:01:45
Secondary IP Addresses :
 101.1.1.254
!snip

IP Address                  : 101.9.1.252
Interface                   : vlan1009
Up Time (HH:MM:SS)          : 02:14:14
Expire Time (HH:MM:SS)      : 00:01:35
DR Priority                 : 83952044
```

```
Hold Time (HH:MM:SS)      : 00:01:45
Secondary IP Addresses :
 101.9.1.254

IP Address                : 101.10.1.252
Interface                 : vlan1010
Up Time (HH:MM:SS)        : 02:14:14
Expire Time (HH:MM:SS)    : 00:01:35
DR Priority               : 83952044
Hold Time (HH:MM:SS)      : 00:01:45
Secondary IP Addresses :
 101.10.1.254
```

Verify mroutes

```
Core-vsx-secondary(config)# show ip mroute
IP Multicast Route Entries

VRF : default
Total number of entries : 20

Group Address           : 225.1.1.1
Source Address          : 60.1.1.10
Neighbor                : 80.3.1.2
Incoming interface      : 1/1/49
Outgoing Interface List :
Interface       State
-----------     ----------
vlan1001        forwarding

Group Address           : 225.1.1.1
Source Address          : 60.1.1.10
Neighbor                :
Incoming interface      : vlan1001

Group Address           : 225.2.1.1
Source Address          : 60.1.1.10
Neighbor                :
Incoming interface      : vlan1002

Group Address           : 225.2.1.1
Source Address          : 60.1.1.10
Neighbor                : 80.3.1.2
Incoming interface      : 1/1/49
Outgoing Interface List :
Interface       State
-----------     ----------
vlan1002        forwarding
!snip

Group Address           : 225.9.1.1
Source Address          : 60.1.1.10
Neighbor                : 80.3.1.2
Incoming interface      : 1/1/49
Outgoing Interface List :
Interface       State
-----------     ----------
vlan1009        forwarding

Group Address           : 225.10.1.1
Source Address          : 60.1.1.10
```

```
Neighbor                : 80.3.1.2
Incoming interface      : 1/1/49
Outgoing Interface List :
Interface       State
-----------     ----------
vlan1010        forwarding

Group Address           : 225.10.1.1
Source Address          : 60.1.1.10
Neighbor                :
Incoming interface      : vlan1010
```

Verify PIM interfaces

```
Core-vsx-secondary(config)# show ip pim interface

PIM Interfaces

VRF: default
Total Number of interfaces : 12

Interface  : vlan1001
Neighbor count : 1
IP Address : 101.1.1.253/24
Mode       : sparse
Designated Router : 101.1.1.253
Proxy DR              : false
Hello Interval (sec)  : 30
Hello Delay (sec)     : 5
Override Interval (msec)  : 2500              Lan Prune Delay     : Yes
Propagation Delay (msec)  : 500               Configured DR Priority    : 1
Operational DR Priority   : 83952044
Neighbor Timeout          : 84

Interface  : vlan1005
Neighbor count : 1
IP Address : 101.5.1.253/24
Mode       : sparse
Designated Router : 101.5.1.253
Proxy DR              : false
Hello Interval (sec)  : 30
Hello Delay (sec)     : 5
Override Interval (msec)  : 2500              Lan Prune Delay     : Yes
Propagation Delay (msec)  : 500               Configured DR Priority    : 1
Operational DR Priority   : 83952044
Neighbor Timeout          : 83
!snip

Interface  : loopback3
Neighbor count : 0
IP Address : 41.1.1.1/32
Mode       : sparse

Interface  : vlan1002
Neighbor count : 1
IP Address : 101.2.1.253/24
Mode       : sparse
Designated Router : 101.2.1.253
Proxy DR              : false
Hello Interval (sec)  : 30
Hello Delay (sec)     : 5
```

```
Override Interval (msec)  : 2500              Lan Prune Delay     : Yes
Propagation Delay (msec)  : 500               Configured DR Priority    : 1
Operational DR Priority   : 83952044
Neighbor Timeout          : 81

Interface  : 1/1/49
Neighbor count : 1
IP Address : 80.3.1.1/30
Mode       : sparse
Designated Router : 80.3.1.2
Proxy DR              : false
Hello Interval (sec)  : 30
Hello Delay (sec)     : 5
Override Interval (msec)  : 2500              Lan Prune Delay     : Yes
Propagation Delay (msec)  : 500               Configured DR Priority    : 1
Operational DR Priority   : 1
Neighbor Timeout          : 85
```

Verify BSR information

```
Core-vsx-secondary(config)# show ip pim bsr
Status and Counters- PIM-SM Bootstrap Router Information

VRF                       : default
E-BSR Address             : 40.1.1.1
E-BSR Priority            : 100
E-BSR Hash Mask Length    : 30
E-BSR Up Time             : 2 hour 13 mins 17 secs
Next Bootstrap Message    : 2 mins 4 secs

C-BSR Admin Status        : This system is a Candidate-BSR
C-BSR Address             : 41.1.1.1
C-BSR Priority            : 0
C-BSR Hash Mask Length    : 30
C-BSR Message Interval    : 60
C-BSR Source IP Interface : loopback3

C-RP Admin Status         : This system is a Candidate-RP
C-RP Address              : 41.1.1.1
C-RP Hold Time            : 150
C-RP Advertise Period     : 60
C-RP Priority             : 192
C-RP Source IP Interface  : loopback3

Group Address    Group Mask
---------------  ---------------
224.0.0.0        240.0.0.0
```

Verify RP information

```
Core-vsx-secondary(config)# show ip pim rp-set

VRF: default

Status and Counters - PIM-SM Learned RP-Set Information
Group Address    Group Mask       RP Address       Hold Time  Expire Time
---------------  ---------------  ---------------  ---------  -----------
224.0.0.0        240.0.0.0        40.1.1.1         150        132
224.0.0.0        240.0.0.0        41.1.1.1         150        132
```

```
Verify IGMP snooping
Core-vsx-secondary(config)# show ip igmp snooping

IGMP Snooping Protocol Info

Total VLANs with IGMP enabled             : 10
Current count of multicast groups joined  : 10

IGMP Drop Unknown Multicast               : Global
VLAN ID : 1001
VLAN Name : VLAN1001
IGMP Configured Version : 3
IGMP Operating Version : 3
Querier Address : 101.1.1.252
Querier Port : lag100
Querier UpTime :2h 16m
Querier Expiration Time :2m 14s

Active Group Address   Tracking  Vers Mode Uptime    Expires
---------------------- ---------- ---- ---- --------- ----------
225.1.1.1              Filter    2         1h 50m    2m 28s

VLAN ID : 1002
VLAN Name : VLAN1002
IGMP Configured Version : 3
IGMP Operating Version : 3
Querier Address : 101.2.1.252
Querier Port : lag100
Querier UpTime :2h 16m
Querier Expiration Time :2m 14s

Active Group Address   Tracking  Vers Mode Uptime    Expires
---------------------- ---------- ---- ---- --------- ----------
225.2.1.1              Filter    2         1h 50m    2m 30s
!snip

VLAN ID : 1009
VLAN Name : VLAN1009
IGMP Configured Version : 3
IGMP Operating Version : 3
Querier Address : 101.9.1.252
Querier Port : lag100
Querier UpTime :2h 17m
Querier Expiration Time :2m 14s

Active Group Address   Tracking  Vers Mode Uptime    Expires
---------------------- ---------- ---- ---- --------- ----------
225.9.1.1              Filter    2         1h 50m    2m 27s

VLAN ID : 1010
VLAN Name : VLAN1010
IGMP Configured Version : 3
IGMP Operating Version : 3
Querier Address : 101.10.1.252
Querier Port : lag100
Querier UpTime :2h 17m
Querier Expiration Time :2m 14s

Active Group Address   Tracking  Vers Mode Uptime    Expires
---------------------- ---------- ---- ---- --------- ----------
```

```
225.10.1.1              Filter    2         1h 50m    2m 28s
```

8320-vsx-pri

Configuration

```
!export-password: default
hostname 8320-vsx-pri
no ip icmp redirect
profile L3-core
ntp server 16.110.135.123 minpoll 4 maxpoll 4 iburst
cli-session
    timeout 0
!
!
!
!
!
ssh server vrf mgmt
vlan 1,10-11,20,22
interface mgmt
    no shutdown
    ip dhcp
interface lag 2 multi-chassis
    no routing
    vlan access 1
    lacp mode active
interface lag 10 multi-chassis
    no shutdown
    description MC_LAG to VTEP1
    no routing
    vlan trunk native 1
    vlan trunk allowed 11
    lacp mode active
interface lag 20 multi-chassis
    no shutdown
    description MC_LAG to VTEP2
    no routing
    vlan trunk native 1
    vlan trunk allowed 20
    lacp mode active
interface lag 100
    no shutdown
    description ISL
    no routing
    vlan trunk native 1 tag
    vlan trunk allowed all
interface 1/1/1
    no shutdown
interface 1/1/9
    no shutdown
interface 1/1/15
    no shutdown
    lag 20
interface 1/1/17
    no shutdown
interface 1/1/18
    no shutdown
interface 1/1/19
    no shutdown
interface 1/1/20
```

```
    no shutdown
interface 1/1/33
    no shutdown
    lag 10
interface 1/1/34
    no shutdown
    lag 10
interface 1/1/39
    no shutdown
interface 1/1/40
    no shutdown
interface 1/1/41
    no shutdown
interface 1/1/42
    no shutdown
interface 1/1/46
    no shutdown
    lag 100
interface 1/1/47
    no shutdown
    lag 100
interface 1/1/48
    no shutdown
    description KA
    ip address 2.1.1.1/30
interface 1/1/51
    no shutdown
    description ROP to Core-VSX-primary
    ip address 30.1.1.1/30
    ip ospf 1 area 0.0.0.0
interface 1/1/52
    no shutdown
    description ROP to Core-VSX-secondary
    ip address 30.2.1.1/30
    ip ospf 1 area 0.0.0.0
interface vlan 11
    vsx active-forwarding
    ip address 11.10.1.3/29
    ip ospf 1 area 0.0.0.1
interface vlan 20
    vsx active-forwarding
    ip address 11.20.2.3/29
    ip ospf 1 area 0.0.0.2
vsx
    inter-switch-link lag 100
    role primary
    keepalive peer 2.1.1.2 source 2.1.1.1
!
!
!
!
!
router ospf 1
    router-id 30.1.1.1
    area 0.0.0.0
    area 0.0.0.1
    area 0.0.0.2
https-server vrf mgmt
```

8320-vsx-sec

Configuration

```
!export-password: default
hostname 8320-vsx-sec
no ip icmp redirect
profile L3-core
cli-session
    timeout 0
!
!
!
!
!
ssh server vrf mgmt
vlan 1,10-11,20-21
interface mgmt
    no shutdown
    ip dhcp
interface lag 1
    no shutdown
    no routing
    vlan trunk native 1
    vlan trunk allowed 21
    lacp mode active
interface lag 10 multi-chassis
    no shutdown
    description MC-LAG to VTEP1
    no routing
    vlan trunk native 1
    vlan trunk allowed 11
    lacp mode active
interface lag 20 multi-chassis
    no shutdown
    description MC-LAG to VTEP2
    no routing
    vlan trunk native 1
    vlan trunk allowed 20
    lacp mode active
interface lag 100
    no shutdown
    description ISL
    no routing
    vlan trunk native 1 tag
    vlan trunk allowed all
interface 1/1/1
    no shutdown
interface 1/1/7
    no shutdown
    ip address 30.2.1.1/30
    ip ospf 1 area 0.0.0.0
interface 1/1/9
    no shutdown
interface 1/1/15
    no shutdown
    lag 20
interface 1/1/33
    no shutdown
    lag 10
interface 1/1/34
    no shutdown
    lag 10
interface 1/1/46
    no shutdown
    lag 100
```

```
interface 1/1/47
    no shutdown
    lag 100
interface 1/1/48
    no shutdown
    description KA
    ip address 2.1.1.2/30
interface 1/1/49
    no shutdown
interface 1/1/50
    no shutdown
interface 1/1/51
    no shutdown
    description ROP to Core-VSX-primary
    ip address 30.1.1.5/30
    ip ospf 1 area 0.0.0.0
interface 1/1/52
    no shutdown
    description ROP to Core-VSX-secondary
    ip address 30.2.1.5/30
    ip ospf 1 area 0.0.0.0
interface vlan 11
    vsx active-forwarding
    ip address 11.10.1.2/29
    ip ospf 1 area 0.0.0.1
interface vlan 20
    vsx active-forwarding
    ip address 11.20.2.2/29
    ip ospf 1 area 0.0.0.2
interface vlan 21
    ip address 11.20.1.2/30
    ip ospf 1 area 0.0.0.1
    ip ospf network point-to-point
vsx
    inter-switch-link lag 100
    role secondary
    keepalive peer 2.1.1.1 source 2.1.1.2
mirror session 1
    destination cpu
    source interface 1/1/51 rx
!
!
!
!
!
router ospf 1
    router-id 30.2.1.1
    area 0.0.0.0
    area 0.0.0.1
    area 0.0.0.2
https-server vrf mgmt
```

6300-VSF-VTEP1

```
!export-password: default
hostname 6300-VSF-VTEP1
!
!
!
!
!
```

```
!
ssh server vrf default
ssh server vrf mgmt
vsf secondary-member 2
vsf member 1
    type jl668a
    link 1 1/1/28
    link 2 1/1/26
vsf member 2
    type jl668a
    link 1 2/1/28
    link 2 2/1/27
vsf member 3
    type jl668a
    link 1 3/1/27
    link 2 3/1/26
vlan 1,11,21
vlan 1001
    ip igmp snooping enable
vlan 1002
    ip igmp snooping enable
vlan 1003
    ip igmp snooping enable
vlan 1004
    ip igmp snooping enable
vlan 1005
    ip igmp snooping enable
vlan 1006
    ip igmp snooping enable
vlan 1007
    ip igmp snooping enable
vlan 1008
    ip igmp snooping enable
vlan 1009
    ip igmp snooping enable
vlan 1010
    ip igmp snooping enable
evpn
    vlan 1001
        rd 172.1.1.1:1001
        route-target export 1001:1001
        route-target import 1001:1001
        redistribute host-route
    vlan 1002
        rd 172.1.1.1:1002
        route-target export 1002:1002
        route-target import 1002:1002
        redistribute host-route
    vlan 1003
        rd 172.1.1.1:1003
        route-target export 1003:1003
        route-target import 1003:1003
        redistribute host-route
    vlan 1004
        rd 172.1.1.1:1004
        route-target export 1004:1004
        route-target import 1004:1004
        redistribute host-route
    vlan 1005
        rd 172.1.1.1:1005
        route-target export 1005:1005
        route-target import 1005:1005
```

```
        redistribute host-route
    vlan 1006
        rd 172.1.1.1:1006
        route-target export 1006:1006
        route-target import 1006:1006
        redistribute host-route
    vlan 1007
        rd 172.1.1.1:1007
        route-target export 1007:1007
        route-target import 1007:1007
        redistribute host-route
    vlan 1008
        rd 172.1.1.1:1008
        route-target export 1008:1008
        route-target import 1008:1008
        redistribute host-route
    vlan 1009
        rd 172.1.1.1:1009
        route-target export 1009:1009
        route-target import 1009:1009
        redistribute host-route
    vlan 1010
        rd 172.1.1.1:1010
        route-target export 1010:1010
        route-target import 1010:1010
        redistribute host-route
spanning-tree
interface mgmt
    no shutdown
    ip dhcp
interface lag 1
    no shutdown
    description MC-LAG to Distro-VSX
    no routing
    vlan trunk native 1
    vlan trunk allowed 11
    lacp mode active
interface 1/1/1
    no shutdown
    no routing
    vlan access 1
interface 1/1/2
    no shutdown
    no routing
    vlan access 1
interface 1/1/3
    no shutdown
    no routing
    vlan access 1
interface 1/1/4
    no shutdown
    no routing
    vlan access 1
interface 1/1/5
    no shutdown
    no routing
    vlan access 1
interface 1/1/6
    no shutdown
    no routing
    vlan access 1
interface 1/1/7
```

```
    no shutdown
    no routing
    vlan access 1
interface 1/1/8
    no shutdown
    no routing
    vlan access 1
interface 1/1/9
    no shutdown
    no routing
    vlan access 1
interface 1/1/10
    no shutdown
    no routing
    vlan access 1
interface 1/1/11
    no shutdown
    no routing
    vlan access 1
interface 1/1/12
    no shutdown
    no routing
    vlan access 1
interface 1/1/13
    no shutdown
    no routing
    vlan access 1
interface 1/1/14
    no shutdown
    no routing
    vlan access 1
interface 1/1/15
    no shutdown
    no routing
    vlan access 1
interface 1/1/16
    no shutdown
    no routing
    vlan access 1
interface 1/1/17
    no shutdown
    no routing
    vlan access 1
interface 1/1/18
    no shutdown
    no routing
    vlan access 1
interface 1/1/19
    no shutdown
    no routing
    vlan access 1
interface 1/1/20
    no shutdown
    no routing
    vlan access 1
interface 1/1/21
    no shutdown
    no routing
    vlan access 1
interface 1/1/22
    no shutdown
    no routing
```

```
    vlan access 1
interface 1/1/23
    no shutdown
    no routing
    vlan access 1
interface 1/1/24
    no shutdown
    no routing
    vlan access 1
interface 1/1/25
    no shutdown
    lag 1
interface 1/1/26
    no shutdown
interface 1/1/27
    no shutdown
    no routing
    vlan trunk native 1
    vlan trunk allowed 1001-1010
interface 1/1/28
    no shutdown
interface 2/1/1
    no shutdown
    no routing
    vlan access 1
interface 2/1/2
    no shutdown
    no routing
    vlan access 1
interface 2/1/3
    no shutdown
    no routing
    vlan access 1
interface 2/1/4
    no shutdown
    no routing
    vlan access 1
interface 2/1/5
    no shutdown
    no routing
    vlan access 1
interface 2/1/6
    no shutdown
    no routing
    vlan access 1
interface 2/1/7
    no shutdown
    no routing
    vlan access 1
interface 2/1/8
    no shutdown
    no routing
    vlan access 1
interface 2/1/9
    no shutdown
    no routing
    vlan access 1
interface 2/1/10
    no shutdown
    no routing
    vlan access 1
interface 2/1/11
```

```
    no shutdown
    no routing
    vlan access 1
interface 2/1/12
    no shutdown
    no routing
    vlan access 1
interface 2/1/13
    no shutdown
    no routing
    vlan access 1
interface 2/1/14
    no shutdown
    no routing
    vlan access 1
interface 2/1/15
    no shutdown
    no routing
    vlan access 1
interface 2/1/16
    no shutdown
    no routing
    vlan access 1
interface 2/1/17
    no shutdown
    no routing
    vlan access 1
interface 2/1/18
    no shutdown
    no routing
    vlan access 1
interface 2/1/19
    no shutdown
    no routing
    vlan access 1
interface 2/1/20
    no shutdown
    no routing
    vlan access 1
interface 2/1/21
    no shutdown
    no routing
    vlan access 1
interface 2/1/22
    no shutdown
    no routing
    vlan access 1
interface 2/1/23
    no shutdown
    no routing
    vlan access 1
interface 2/1/24
    no shutdown
    no routing
    vlan access 1
interface 2/1/25
    no shutdown
    lag 1
interface 2/1/26
    no shutdown
    lag 1
interface 2/1/27
```

```
    no shutdown
interface 2/1/28
    no shutdown
interface 3/1/1
    no shutdown
    no routing
    vlan access 1
interface 3/1/2
    no shutdown
    no routing
    vlan access 1
interface 3/1/3
    no shutdown
    no routing
    vlan access 1
interface 3/1/4
    no shutdown
    no routing
    vlan access 1
interface 3/1/5
    no shutdown
    no routing
    vlan access 1
interface 3/1/6
    no shutdown
    no routing
    vlan access 1
interface 3/1/7
    no shutdown
    no routing
    vlan access 1
interface 3/1/8
    no shutdown
    no routing
    vlan access 1
interface 3/1/9
    no shutdown
    no routing
    vlan access 1
interface 3/1/10
    no shutdown
    no routing
    vlan access 1
interface 3/1/11
    no shutdown
    no routing
    vlan access 1
interface 3/1/12
    no shutdown
    no routing
    vlan access 1
interface 3/1/13
    no shutdown
    no routing
    vlan access 1
interface 3/1/14
    no shutdown
    no routing
    vlan access 1
interface 3/1/15
    no shutdown
    no routing
```

```
    vlan access 1
interface 3/1/16
    no shutdown
    no routing
    vlan access 1
interface 3/1/17
    no shutdown
    no routing
    vlan access 1
interface 3/1/18
    no shutdown
    no routing
    vlan access 1
interface 3/1/19
    no shutdown
    no routing
    vlan access 1
interface 3/1/20
    no shutdown
    no routing
    vlan access 1
interface 3/1/21
    no shutdown
    no routing
    vlan access 1
interface 3/1/22
    no shutdown
    no routing
    vlan access 1
interface 3/1/23
    no shutdown
    no routing
    vlan access 1
interface 3/1/24
    no shutdown
    no routing
    vlan access 1
interface 3/1/25
    no shutdown
    lag 1
interface 3/1/26
    no shutdown
interface 3/1/27
    no shutdown
interface 3/1/28
    no shutdown
    no routing
    vlan trunk native 1
    vlan trunk allowed 1001-1010
interface loopback 1
    ip address 172.16.1.1/32
    ip ospf 1 area 0.0.0.1
interface loopback 2
    ip address 172.1.1.1/32
    ip ospf 1 area 0.0.0.1
interface vlan 1
    ip dhcp
interface vlan 11
    ip address 11.10.1.1/29
    ip ospf 1 area 0.0.0.1
interface vlan 21
    ip address 11.20.1.1/30
```

```
    ip ospf 1 area 0.0.0.1
    ip ospf network point-to-point
interface vxlan 1
    source ip 172.1.1.1
    no shutdown
    vni 1001
        vlan 1001
    vni 1002
        vlan 1002
    vni 1003
        vlan 1003
    vni 1004
        vlan 1004
    vni 1005
        vlan 1005
    vni 1006
        vlan 1006
    vni 1007
        vlan 1007
    vni 1008
        vlan 1008
    vni 1009
        vlan 1009
    vni 1010
        vlan 1010
!
!
!
!
!
router ospf 1
    router-id 11.20.1.1
    area 0.0.0.1
router bgp 65535
    bgp router-id 172.16.1.1
    no bgp fast-external-fallover
    neighbor 172.16.1.2 remote-as 65535
    neighbor 172.16.1.2 update-source 172.16.1.1
    neighbor 172.16.1.4 remote-as 65535
    neighbor 172.16.1.4 update-source 172.16.1.1
    neighbor 172.16.1.5 remote-as 65535
    neighbor 172.16.1.5 update-source 172.16.1.1
    address-family l2vpn evpn
        neighbor 172.16.1.2 activate
        neighbor 172.16.1.2 send-community extended
        neighbor 172.16.1.4 activate
        neighbor 172.16.1.4 send-community extended
        neighbor 172.16.1.5 activate
        neighbor 172.16.1.5 send-community extended
    exit-address-family
!
https-server vrf default
https-server vrf mgmt
```

Verification

Verify OSPF neighbors

```
6300-VSF-VTEP1(config)# show ip ospf neighbors
VRF : default                           Process : 1
==================================================
```

```
Total Number of Neighbors : 2

Neighbor ID      Priority  State             Nbr Address       Interface
-------------------------------------------------------------------------
30.1.1.1         1         FULL/DR           11.10.1.3          vlan11

30.2.1.1         1         FULL/BDR          11.10.1.2          vlan11
```

Verify BGP neighbors

```
6300-VSF-VTEP1(config)# show bgp all summary
VRF : default
BGP Summary
-----------
 Local AS               : 65535        BGP Router Identifier  : 172.16.1.1
 Peers                  : 3            Log Neighbor Changes   : No
 Cfg. Hold Time         : 180          Cfg. Keep Alive        : 60
 Confederation Id       : 0

Address-family : IPv4 Unicast
------------------------------

Address-family : IPv6 Unicast
------------------------------

Address-family : L2VPN EVPN
------------------------------
 Neighbor        Remote-AS MsgRcvd MsgSent   Up/Down Time State        AdminStatus
 172.16.1.2      65535       15521   13377   01d:08h:25m  Established   Up
 172.16.1.4      65535       30068   13611   23h:52m:29s  Established   Up
 172.16.1.5      65535       27204   14966   02h:28m:51s  Established   Up
```

Verify BGP EVPN able

```
6300-VSF-VTEP1(config)# show bgp l2vpn evpn
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
              i internal, e external S Stale, R Removed, a additional-paths
Origin codes: i - IGP, e - EGP, ? - incomplete

EVPN Route-Type 2 prefix: [2]:[ESI]:[EthTag]:[MAC]:[OrigIP]
EVPN Route-Type 3 prefix: [3]:[EthTag]:[OrigIP]
EVPN Route-Type 5 prefix: [5]:[ESI]:[EthTag]:[IPAddrLen]:[IPAddr]
VRF : default
Local Router-ID 172.16.1.1

     Network                                          Nexthop         Metric     LocPrf    Weight   Path
-------------------------------------------------------------------------------------------------------
Route Distinguisher: 172.1.1.1:1001       (L2VNI 1001)
*>  [2]:[0]:[0]:[00:11:01:00:00:01]:[]                172.1.1.1       0          100        0       ?
*>  [3]:[0]:[172.1.1.1]                               172.1.1.1       0          100        0       ?

Route Distinguisher: 172.1.1.2:1001       (L2VNI 1001)
*>i [2]:[0]:[0]:[00:13:01:00:00:01]:[]                172.1.1.2       0          100        0       ?
*>i [3]:[0]:[172.1.1.2]                               172.1.1.2       0          100        0       ?

Route Distinguisher: 172.1.1.5:1001       (L2VNI 1001)
*>i [2]:[0]:[0]:[00:00:20:00:10:01]:[101.1.1.254]     172.1.1.5       0          100        0       ?
* i [2]:[0]:[0]:[00:00:20:00:10:01]:[101.1.1.254]     172.1.1.5       0          100        0       ?
```

```
*>i [2]:[0]:[0]:[b8:d4:e7:5b:2c:00]:[101.1.1.253]          172.1.1.5       0          100        0       ?
*>i [2]:[0]:[0]:[b8:d4:e7:5d:8a:00]:[101.1.1.252]          172.1.1.5       0          100        0       ?
*>i [3]:[0]:[172.1.1.5]                                    172.1.1.5       0          100        0       ?
* i [3]:[0]:[172.1.1.5]                                     172.1.1.5       0          100        0       ?

Route Distinguisher: 172.1.1.1:1002       (L2VNI 1002)
*>  [2]:[0]:[0]:[00:11:01:00:00:02]:[]                     172.1.1.1       0          100        0       ?
*>  [3]:[0]:[172.1.1.1]                                    172.1.1.1       0          100        0       ?

Route Distinguisher: 172.1.1.2:1002       (L2VNI 1002)
*>i [2]:[0]:[0]:[00:13:01:00:00:02]:[]                     172.1.1.2       0          100        0       ?
*>i [3]:[0]:[172.1.1.2]                                    172.1.1.2       0          100        0       ?

Route Distinguisher: 172.1.1.5:1002       (L2VNI 1002)
*>i [2]:[0]:[0]:[00:00:20:00:10:01]:[101.2.1.254]          172.1.1.5       0          100        0       ?
* i [2]:[0]:[0]:[00:00:20:00:10:01]:[101.2.1.254]          172.1.1.5       0          100        0       ?
*>i [2]:[0]:[0]:[b8:d4:e7:5b:2c:00]:[101.2.1.253]          172.1.1.5       0          100        0       ?
*>i [2]:[0]:[0]:[b8:d4:e7:5d:8a:00]:[101.2.1.252]          172.1.1.5       0          100        0       ?
*>i [3]:[0]:[172.1.1.5]                                    172.1.1.5       0          100        0       ?
* i [3]:[0]:[172.1.1.5]                                     172.1.1.5       0          100        0       ?
!snip

Route Distinguisher: 172.1.1.1:1009       (L2VNI 1009)
*>  [2]:[0]:[0]:[00:11:01:00:00:09]:[]                     172.1.1.1       0          100        0       ?
*>  [3]:[0]:[172.1.1.1]                                    172.1.1.1       0          100        0       ?

Route Distinguisher: 172.1.1.2:1009       (L2VNI 1009)
*>i [2]:[0]:[0]:[00:13:01:00:00:09]:[]                     172.1.1.2       0          100        0       ?
*>i [3]:[0]:[172.1.1.2]                                    172.1.1.2       0          100        0       ?

Route Distinguisher: 172.1.1.5:1009       (L2VNI 1009)
*>i [2]:[0]:[0]:[00:00:20:00:10:01]:[101.9.1.254]          172.1.1.5       0          100        0       ?
* i [2]:[0]:[0]:[00:00:20:00:10:01]:[101.9.1.254]          172.1.1.5       0          100        0       ?
*>i [2]:[0]:[0]:[b8:d4:e7:5b:2c:00]:[101.9.1.253]          172.1.1.5       0          100        0       ?
*>i [2]:[0]:[0]:[b8:d4:e7:5d:8a:00]:[101.9.1.252]          172.1.1.5       0          100        0       ?
*>i [3]:[0]:[172.1.1.5]                                    172.1.1.5       0          100        0       ?
* i [3]:[0]:[172.1.1.5]                                     172.1.1.5       0          100        0       ?

Route Distinguisher: 172.1.1.1:1010       (L2VNI 1010)
*>  [2]:[0]:[0]:[00:11:01:00:00:0a]:[]                     172.1.1.1       0          100        0       ?
*>  [3]:[0]:[172.1.1.1]                                    172.1.1.1       0          100        0       ?

Route Distinguisher: 172.1.1.2:1010       (L2VNI 1010)
*>i [2]:[0]:[0]:[00:13:01:00:00:0a]:[]                     172.1.1.2       0          100        0       ?
*>i [3]:[0]:[172.1.1.2]                                    172.1.1.2       0          100        0       ?

Route Distinguisher: 172.1.1.5:1010       (L2VNI 1010)
*>i [2]:[0]:[0]:[00:00:20:00:10:01]:[101.10.1.254]         172.1.1.5       0          100        0       ?
* i [2]:[0]:[0]:[00:00:20:00:10:01]:[101.10.1.254]         172.1.1.5       0          100        0       ?
*>i [2]:[0]:[0]:[b8:d4:e7:5b:2c:00]:[101.10.1.253]         172.1.1.5       0          100        0       ?
*>i [2]:[0]:[0]:[b8:d4:e7:5d:8a:00]:[101.10.1.252]         172.1.1.5       0          100        0       ?
*>i [3]:[0]:[172.1.1.5]                                    172.1.1.5       0          100        0       ?
* i [3]:[0]:[172.1.1.5]                                     172.1.1.5       0          100        0       ?
Total number of entries 100
```

Verify VXLAN tunnel, VTEP peers, and VNIs

```
6300-VSF-VTEP1(config)# show interface vxlan vteps
Source           Destination      Origin       Status                VNI       Routing   VLAN  VRF
---------------- ---------------- ------------ --------------------- --------- --------- ----- ---
-
```

```
172.1.1.1       172.1.1.2       evpn        operational          1001     disabled  1001   --
172.1.1.1       172.1.1.2       evpn        operational          1002     disabled  1002   --
172.1.1.1       172.1.1.2       evpn        operational          1003     disabled  1003   --
172.1.1.1       172.1.1.2       evpn        operational          1004     disabled  1004   --
172.1.1.1       172.1.1.2       evpn        operational          1005     disabled  1005   --
172.1.1.1       172.1.1.2       evpn        operational          1006     disabled  1006   --
172.1.1.1       172.1.1.2       evpn        operational          1007     disabled  1007   --
172.1.1.1       172.1.1.2       evpn        operational          1008     disabled  1008   --
172.1.1.1       172.1.1.2       evpn        operational          1009     disabled  1009   --
172.1.1.1       172.1.1.2       evpn        operational          1010     disabled  1010   --
172.1.1.1       172.1.1.5       evpn        operational          1001     disabled  1001   --
172.1.1.1       172.1.1.5       evpn        operational          1002     disabled  1002   --
172.1.1.1       172.1.1.5       evpn        operational          1003     disabled  1003   --
172.1.1.1       172.1.1.5       evpn        operational          1004     disabled  1004   --
172.1.1.1       172.1.1.5       evpn        operational          1005     disabled  1005   --
172.1.1.1       172.1.1.5       evpn        operational          1006     disabled  1006   --
172.1.1.1       172.1.1.5       evpn        operational          1007     disabled  1007   --
172.1.1.1       172.1.1.5       evpn        operational          1008     disabled  1008   --
172.1.1.1       172.1.1.5       evpn        operational          1009     disabled  1009   --
172.1.1.1       172.1.1.5       evpn        operational          1010     disabled  1010   --
```

Verify IGMP snooping

```
6300-VSF-VTEP1(config)# show ip igmp snooping

IGMP Snooping Protocol Info

Total VLANs with IGMP enabled             : 10
Current count of multicast groups joined  : 11

IGMP Drop Unknown Multicast               : Global
VLAN ID : 1001
VLAN Name : VLAN1001
IGMP Configured Version : 3
IGMP Operating Version : 3
Querier Address : 101.1.1.252
Querier Port : vxlan1(172.1.1.5)
Querier UpTime :2h 30m
Querier Expiration Time :2m 23s

Active Group Address   Tracking  Vers Mode Uptime    Expires
---------------------- ---------- ---- ---- --------- ----------
225.1.1.1              Filter    2         5m 57s    2m 40s

VLAN ID : 1002
VLAN Name : VLAN1002
IGMP Configured Version : 3
IGMP Operating Version : 3
Querier Address : 101.2.1.252
Querier Port : vxlan1(172.1.1.5)
Querier UpTime :2h 30m
Querier Expiration Time :2m 23s

Active Group Address   Tracking  Vers Mode Uptime    Expires
---------------------- ---------- ---- ---- --------- ----------
225.2.1.1              Filter    2         5m 55s    2m 35s
!snip

VLAN ID : 1009
VLAN Name : VLAN1009
IGMP Configured Version : 3
```

```
IGMP Operating Version : 3
Querier Address : 101.9.1.252
Querier Port : vxlan1(172.1.1.5)
Querier UpTime :2h 30m
Querier Expiration Time :2m 18s

Active Group Address   Tracking  Vers Mode Uptime    Expires
---------------------- ---------- ---- ---- --------- ----------
225.9.1.1              Filter    2         6m 0s     2m 24s

VLAN ID : 1010
VLAN Name : VLAN1010
IGMP Configured Version : 3
IGMP Operating Version : 3
Querier Address : 101.10.1.252
Querier Port : vxlan1(172.1.1.5)
Querier UpTime :2h 30m
Querier Expiration Time :2m 18s

Active Group Address   Tracking  Vers Mode Uptime    Expires
---------------------- ---------- ---- ---- --------- ----------
225.10.1.1             Filter    2         5m 55s    2m 21s
```

6300-VTEP2

Configuration

```
!export-password: default
hostname 6300-VTEP2
user admin group administrators password ciphertext
AQBapSlnp7JaPOWttid6/sPULR9294P5Y1I4pcw7Uwm5cXc5YgAAADUrPl5vyqQcFNfTJPou6XByU9MNfYyH
enV88cNMkqrOJ68oAmFuxr5STGHWu409uXdKOkXQACuJTpnYsdNeIvjOT0eRHAonCFHKLlgGVdd72RIk73gt
lO8ED0qCrosc2Nqn
!
!
!
!
!
!
ssh server vrf default
ssh server vrf mgmt
vsf member 1
    type jl668a
vlan 1,10,20-21
vlan 1001
    ip igmp snooping enable
vlan 1002
    ip igmp snooping enable
vlan 1003
    ip igmp snooping enable
vlan 1004
    ip igmp snooping enable
vlan 1005
    ip igmp snooping enable
vlan 1006
    ip igmp snooping enable
vlan 1007
    ip igmp snooping enable
vlan 1008
    ip igmp snooping enable
vlan 1009
```

```
    ip igmp snooping enable
vlan 1010
    ip igmp snooping enable
evpn
    redistribute local-mac
    vlan 1001
        rd 172.1.1.2:1001
        route-target export 1001:1001
        route-target import 1001:1001
        redistribute host-route
    vlan 1002
        rd 172.1.1.2:1002
        route-target export 1002:1002
        route-target import 1002:1002
        redistribute host-route
    vlan 1003
        rd 172.1.1.2:1003
        route-target export 1003:1003
        route-target import 1003:1003
        redistribute host-route
    vlan 1004
        rd 172.1.1.2:1004
        route-target export 1004:1004
        route-target import 1004:1004
        redistribute host-route
    vlan 1005
        rd 172.1.1.2:1005
        route-target export 1005:1005
        route-target import 1005:1005
        redistribute host-route
    vlan 1006
        rd 172.1.1.2:1006
        route-target export 1006:1006
        route-target import 1006:1006
        redistribute host-route
    vlan 1007
        rd 172.1.1.2:1007
        route-target export 1007:1007
        route-target import 1007:1007
        redistribute host-route
    vlan 1008
        rd 172.1.1.2:1008
        route-target export 1008:1008
        route-target import 1008:1008
        redistribute host-route
    vlan 1009
        rd 172.1.1.2:1009
        route-target export 1009:1009
        route-target import 1009:1009
        redistribute host-route
    vlan 1010
        rd 172.1.1.2:1010
        route-target export 1010:1010
        route-target import 1010:1010
        redistribute host-route
spanning-tree
interface mgmt
    no shutdown
    ip dhcp
interface lag 10
    no shutdown
    description MC-LAG to Distro VSX
```

```
    no routing
    vlan trunk native 1
    vlan trunk allowed 20
    lacp mode active
interface 1/1/1
    no shutdown
    no routing
    vlan access 1
interface 1/1/2
    no shutdown
    no routing
    vlan access 1
interface 1/1/3
    no shutdown
    no routing
    vlan access 1
interface 1/1/4
    no shutdown
    no routing
    vlan access 1
interface 1/1/5
    no shutdown
    no routing
    vlan trunk native 1
    vlan trunk allowed 1001-1010
interface 1/1/6
    no shutdown
    no routing
    vlan trunk native 1
    vlan trunk allowed 1001-1010
interface 1/1/7
    no shutdown
    no routing
    vlan access 1
interface 1/1/8
    no shutdown
    no routing
    vlan access 1
interface 1/1/9
    no shutdown
    no routing
    vlan access 1
interface 1/1/10
    no shutdown
    no routing
    vlan access 1
interface 1/1/11
    no shutdown
    no routing
    vlan access 1
interface 1/1/12
    no shutdown
    no routing
    vlan access 1
interface 1/1/13
    no shutdown
    no routing
    vlan access 1
interface 1/1/14
    no shutdown
    no routing
    vlan access 1
```

```
interface 1/1/15
    no shutdown
    no routing
    vlan access 1
interface 1/1/16
    no shutdown
    no routing
    vlan access 1
interface 1/1/17
    no shutdown
    no routing
    vlan access 1
interface 1/1/18
    no shutdown
    no routing
    vlan access 1
interface 1/1/19
    no shutdown
    no routing
    vlan access 1
interface 1/1/20
    no shutdown
    no routing
    vlan access 1
interface 1/1/21
    no shutdown
    no routing
    vlan access 1
interface 1/1/22
    no shutdown
    no routing
    vlan access 1
interface 1/1/23
    no shutdown
    no routing
    vlan access 1
interface 1/1/24
    no shutdown
    no routing
    vlan access 1
interface 1/1/25
    shutdown
    no routing
    vlan access 1
interface 1/1/26
    shutdown
    no routing
    vlan access 1
interface 1/1/27
    no shutdown
    lag 10
interface 1/1/28
    no shutdown
    lag 10
interface loopback 1
    ip address 172.16.1.2/32
    ip ospf 1 area 0.0.0.2
interface loopback 2
    ip address 172.1.1.2/32
    ip ospf 1 area 0.0.0.2
interface vlan 1
    ip dhcp
```

```
interface vlan 20
    ip address 11.20.2.1/29
    ip ospf 1 area 0.0.0.2
interface vxlan 1
    source ip 172.1.1.2
    no shutdown
    vni 1001
        vlan 1001
    vni 1002
        vlan 1002
    vni 1003
        vlan 1003
    vni 1004
        vlan 1004
    vni 1005
        vlan 1005
    vni 1006
        vlan 1006
    vni 1007
        vlan 1007
    vni 1008
        vlan 1008
    vni 1009
        vlan 1009
    vni 1010
        vlan 1010
!
!
!
!
!
router ospf 1
    router-id 11.20.2.1
    area 0.0.0.2
router bgp 65535
    bgp router-id 172.16.1.2
    no bgp fast-external-fallover
    neighbor 172.16.1.1 remote-as 65535
    neighbor 172.16.1.1 update-source 172.16.1.2
    neighbor 172.16.1.4 remote-as 65535
    neighbor 172.16.1.4 update-source 172.16.1.2
    neighbor 172.16.1.5 remote-as 65535
    neighbor 172.16.1.5 update-source 172.16.1.2
    address-family l2vpn evpn
        neighbor 172.16.1.1 activate
        neighbor 172.16.1.1 send-community extended
        neighbor 172.16.1.4 activate
        neighbor 172.16.1.4 send-community extended
        neighbor 172.16.1.5 activate
        neighbor 172.16.1.5 send-community extended
    exit-address-family
!
https-server vrf default
https-server vrf mgmt
```

Verify OSPF neighbors

```
6300-VTEP2(config)# show ip ospf neighbors
VRF : default                          Process : 1
==================================================
```

```
Total Number of Neighbors : 2

Neighbor ID      Priority  State             Nbr Address       Interface
-------------------------------------------------------------------------
30.1.1.1         1         FULL/DR           11.20.2.3          vlan20

30.2.1.1         1         FULL/BDR          11.20.2.2          vlan20
```

Verify BGP neighbors

```
6300-VTEP2(config)# show bgp all summary
VRF : default
BGP Summary
-----------
 Local AS               : 65535        BGP Router Identifier  : 172.16.1.2
 Peers                  : 3            Log Neighbor Changes   : No
 Cfg. Hold Time         : 180          Cfg. Keep Alive        : 60
 Confederation Id       : 0

Address-family : IPv4 Unicast
------------------------------

Address-family : IPv6 Unicast
------------------------------

Address-family : L2VPN EVPN
------------------------------
 Neighbor        Remote-AS MsgRcvd MsgSent   Up/Down Time State        AdminStatus
 172.16.1.1      65535       13423   15570   01d:08h:30m  Established   Up
 172.16.1.4      65535       30063   15780   23h:56m:42s  Established   Up
 172.16.1.5      65535       27210   17141   02h:33m:21s  Established   Up
```

Verify VXLAN tunnel, VTEP peers, and VNIs

```
6300-VTEP2(config)# show interface vxlan vteps
Source           Destination      Origin       Status               VNI       Routing   VLAN  VRF
---------------- ---------------- ------------ -------------------- --------- --------- ----- ---
-
172.1.1.2        172.1.1.1        evpn         operational          1001      disabled  1001   --
172.1.1.2        172.1.1.1        evpn         operational          1002      disabled  1002   --
172.1.1.2        172.1.1.1        evpn         operational          1003      disabled  1003   --
172.1.1.2        172.1.1.1        evpn         operational          1004      disabled  1004   --
172.1.1.2        172.1.1.1        evpn         operational          1005      disabled  1005   --
172.1.1.2        172.1.1.1        evpn         operational          1006      disabled  1006   --
172.1.1.2        172.1.1.1        evpn         operational          1007      disabled  1007   --
172.1.1.2        172.1.1.1        evpn         operational          1008      disabled  1008   --
172.1.1.2        172.1.1.1        evpn         operational          1009      disabled  1009   --
172.1.1.2        172.1.1.1        evpn         operational          1010      disabled  1010   --
172.1.1.2        172.1.1.5        evpn         operational          1001      disabled  1001   --
172.1.1.2        172.1.1.5        evpn         operational          1002      disabled  1002   --
172.1.1.2        172.1.1.5        evpn         operational          1003      disabled  1003   --
172.1.1.2        172.1.1.5        evpn         operational          1004      disabled  1004   --
172.1.1.2        172.1.1.5        evpn         operational          1005      disabled  1005   --
172.1.1.2        172.1.1.5        evpn         operational          1006      disabled  1006   --
172.1.1.2        172.1.1.5        evpn         operational          1007      disabled  1007   --
172.1.1.2        172.1.1.5        evpn         operational          1008      disabled  1008   --
172.1.1.2        172.1.1.5        evpn         operational          1009      disabled  1009   --
172.1.1.2        172.1.1.5        evpn         operational          1010      disabled  1010   --
```

Verify BGP EVPN table

```
6300-VTEP2(config)# show bgp l2vpn evpn
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
              i internal, e external S Stale, R Removed, a additional-paths
Origin codes: i - IGP, e - EGP, ? - incomplete

EVPN Route-Type 2 prefix: [2]:[ESI]:[EthTag]:[MAC]:[OrigIP]
EVPN Route-Type 3 prefix: [3]:[EthTag]:[OrigIP]
EVPN Route-Type 5 prefix: [5]:[ESI]:[EthTag]:[IPAddrLen]:[IPAddr]
VRF : default
Local Router-ID 172.16.1.2

     Network                                                Nexthop         Metric     LocPrf    Weight   Path
-------------------------------------------------------------------------------------------------------------------
Route Distinguisher: 172.1.1.1:1001       (L2VNI 1001)
*>i [2]:[0]:[0]:[00:11:01:00:00:01]:[]                     172.1.1.1       0          100       0       ?
*>i [3]:[0]:[172.1.1.1]                                    172.1.1.1       0          100       0       ?

Route Distinguisher: 172.1.1.2:1001       (L2VNI 1001)
*>  [2]:[0]:[0]:[00:13:01:00:00:01]:[]                     172.1.1.2       0          100       0       ?
*>  [3]:[0]:[172.1.1.2]                                    172.1.1.2       0          100       0       ?

Route Distinguisher: 172.1.1.5:1001       (L2VNI 1001)
*>i [2]:[0]:[0]:[00:00:20:00:10:01]:[101.1.1.254]          172.1.1.5       0          100       0       ?
* i [2]:[0]:[0]:[00:00:20:00:10:01]:[101.1.1.254]          172.1.1.5       0          100       0       ?
*>i [2]:[0]:[0]:[b8:d4:e7:5b:2c:00]:[101.1.1.253]          172.1.1.5       0          100       0       ?
*>i [2]:[0]:[0]:[b8:d4:e7:5d:8a:00]:[101.1.1.252]          172.1.1.5       0          100       0       ?
*>i [3]:[0]:[172.1.1.5]                                    172.1.1.5       0          100       0       ?
* i [3]:[0]:[172.1.1.5]                                    172.1.1.5       0          100       0       ?

Route Distinguisher: 172.1.1.1:1002       (L2VNI 1002)
*>i [2]:[0]:[0]:[00:11:01:00:00:02]:[]                     172.1.1.1       0          100       0       ?
*>i [3]:[0]:[172.1.1.1]                                    172.1.1.1       0          100       0       ?

Route Distinguisher: 172.1.1.2:1002       (L2VNI 1002)
*>  [2]:[0]:[0]:[00:13:01:00:00:02]:[]                     172.1.1.2       0          100       0       ?
*>  [3]:[0]:[172.1.1.2]                                    172.1.1.2       0          100       0       ?

Route Distinguisher: 172.1.1.5:1002       (L2VNI 1002)
*>i [2]:[0]:[0]:[00:00:20:00:10:01]:[101.2.1.254]          172.1.1.5       0          100       0       ?
* i [2]:[0]:[0]:[00:00:20:00:10:01]:[101.2.1.254]          172.1.1.5       0          100       0       ?
*>i [2]:[0]:[0]:[b8:d4:e7:5b:2c:00]:[101.2.1.253]          172.1.1.5       0          100       0       ?
*>i [2]:[0]:[0]:[b8:d4:e7:5d:8a:00]:[101.2.1.252]          172.1.1.5       0          100       0       ?
*>i [3]:[0]:[172.1.1.5]                                    172.1.1.5       0          100       0       ?
* i [3]:[0]:[172.1.1.5]                                    172.1.1.5       0          100       0       ?

!snip

Route Distinguisher: 172.1.1.2:1010       (L2VNI 1010)
*>  [2]:[0]:[0]:[00:13:01:00:00:0a]:[]                     172.1.1.2       0          100       0       ?
*>  [3]:[0]:[172.1.1.2]                                    172.1.1.2       0          100       0       ?

Route Distinguisher: 172.1.1.5:1010       (L2VNI 1010)
*>i [2]:[0]:[0]:[00:00:20:00:10:01]:[101.10.1.254]         172.1.1.5       0          100       0       ?
* i [2]:[0]:[0]:[00:00:20:00:10:01]:[101.10.1.254]         172.1.1.5       0          100       0       ?
*>i [2]:[0]:[0]:[b8:d4:e7:5b:2c:00]:[101.10.1.253]         172.1.1.5       0          100       0       ?
*>i [2]:[0]:[0]:[b8:d4:e7:5d:8a:00]:[101.10.1.252]         172.1.1.5       0          100       0       ?
*>i [3]:[0]:[172.1.1.5]                                    172.1.1.5       0          100       0       ?
* i [3]:[0]:[172.1.1.5]                                    172.1.1.5       0          100       0       ?
Total number of entries 100
```

Verify IGMP snooping

```
6300-VTEP2(config)# show ip igmp snooping

IGMP Snooping Protocol Info

Total VLANs with IGMP enabled             : 10
Current count of multicast groups joined  : 10

IGMP Drop Unknown Multicast               : Global
VLAN ID : 1001
VLAN Name : VLAN1001
IGMP Configured Version : 3
IGMP Operating Version : 3
Querier Address : 101.1.1.252
Querier Port : vxlan1(172.1.1.5)
Querier UpTime :10m 19s
Querier Expiration Time :2m 20s

Active Group Address   Tracking  Vers Mode Uptime    Expires
---------------------- ---------- ---- ---- --------- ----------
225.1.1.1              Filter    2         10m 10s   2m 29s

VLAN ID : 1002
VLAN Name : VLAN1002
IGMP Configured Version : 3
IGMP Operating Version : 3
Querier Address : 101.2.1.252
Querier Port : vxlan1(172.1.1.5)
Querier UpTime :10m 19s
Querier Expiration Time :2m 20s

Active Group Address   Tracking  Vers Mode Uptime    Expires
---------------------- ---------- ---- ---- --------- ----------
225.2.1.1              Filter    2         10m 14s   2m 34s

VLAN ID : 1003
VLAN Name : VLAN1003
IGMP Configured Version : 3
IGMP Operating Version : 3
Querier Address : 101.3.1.252
Querier Port : vxlan1(172.1.1.5)
Querier UpTime :10m 19s
Querier Expiration Time :2m 15s

Active Group Address   Tracking  Vers Mode Uptime    Expires
---------------------- ---------- ---- ---- --------- ----------
225.3.1.1              Filter    2         10m 15s   2m 19s

VLAN ID : 1004
VLAN Name : VLAN1004
IGMP Configured Version : 3
IGMP Operating Version : 3
Querier Address : 101.4.1.252
Querier Port : vxlan1(172.1.1.5)
Querier UpTime :10m 19s
Querier Expiration Time :2m 15s

Active Group Address   Tracking  Vers Mode Uptime    Expires
---------------------- ---------- ---- ---- --------- ----------
225.4.1.1              Filter    2         10m 11s   2m 19s

VLAN ID : 1005
VLAN Name : VLAN1005
```

```
IGMP Configured Version : 3
IGMP Operating Version : 3
Querier Address : 101.5.1.252
Querier Port : vxlan1(172.1.1.5)
Querier UpTime :10m 19s
Querier Expiration Time :2m 15s

Active Group Address   Tracking  Vers Mode Uptime    Expires
---------------------- ---------- ---- ---- --------- ----------
225.5.1.1              Filter    2         10m 16s   2m 24s

VLAN ID : 1006
VLAN Name : VLAN1006
IGMP Configured Version : 3
IGMP Operating Version : 3
Querier Address : 101.6.1.252
Querier Port : vxlan1(172.1.1.5)
Querier UpTime :10m 19s
Querier Expiration Time :2m 15s

Active Group Address   Tracking  Vers Mode Uptime    Expires
---------------------- ---------- ---- ---- --------- ----------
225.6.1.1              Filter    2         10m 13s   2m 18s

VLAN ID : 1007
VLAN Name : VLAN1007
IGMP Configured Version : 3
IGMP Operating Version : 3
Querier Address : 101.7.1.252
Querier Port : vxlan1(172.1.1.5)
Querier UpTime :10m 19s
Querier Expiration Time :2m 15s

Active Group Address   Tracking  Vers Mode Uptime    Expires
---------------------- ---------- ---- ---- --------- ----------
225.7.1.1              Filter    2         10m 12s   2m 25s

VLAN ID : 1008
VLAN Name : VLAN1008
IGMP Configured Version : 3
IGMP Operating Version : 3
Querier Address : 101.8.1.252
Querier Port : vxlan1(172.1.1.5)
Querier UpTime :10m 19s
Querier Expiration Time :2m 15s

Active Group Address   Tracking  Vers Mode Uptime    Expires
---------------------- ---------- ---- ---- --------- ----------
225.8.1.1              Filter    2         10m 17s   2m 24s

VLAN ID : 1009
VLAN Name : VLAN1009
IGMP Configured Version : 3
IGMP Operating Version : 3
Querier Address : 101.9.1.252
Querier Port : vxlan1(172.1.1.5)
Querier UpTime :10m 19s
Querier Expiration Time :2m 15s

Active Group Address   Tracking  Vers Mode Uptime    Expires
---------------------- ---------- ---- ---- --------- ----------
225.9.1.1              Filter    2         10m 12s   2m 19s
```

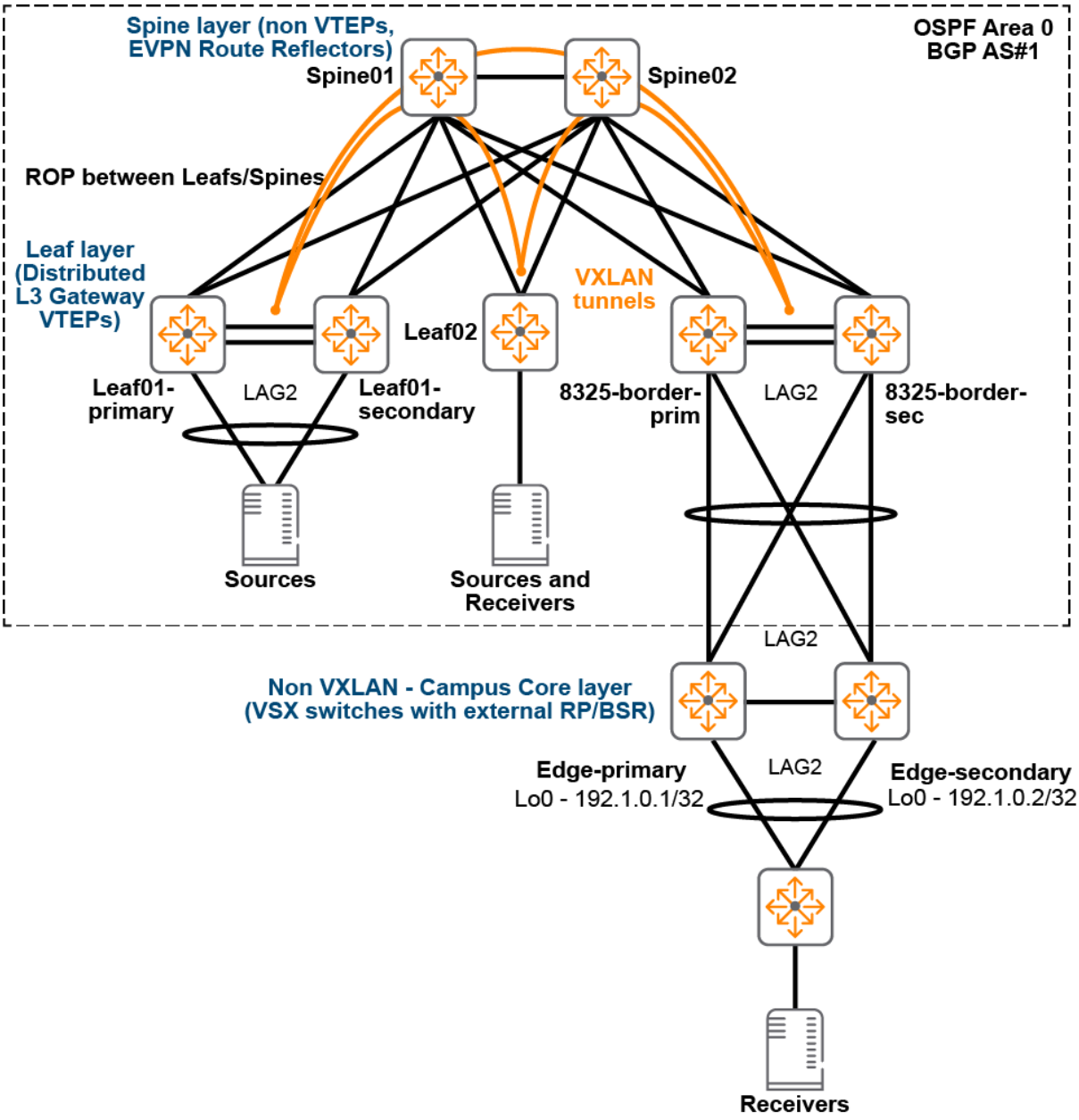
```
VLAN ID : 1010
VLAN Name : VLAN1010
IGMP Configured Version : 3
IGMP Operating Version : 3
Querier Address : 101.10.1.252
Querier Port : vxlan1(172.1.1.5)
Querier UpTime :10m 19s
Querier Expiration Time :2m 15s

Active Group Address   Tracking  Vers Mode Uptime    Expires
---------------------- ---------- ---- ---- --------- ----------
225.10.1.1             Filter    2         10m 11s   2m 22s
```

Use case 2: DC network with distributed L3 gateway

This use case shows sample configurations and relevant verification commands for a DC network with distributed L3 gateway, external BSR/RPs on a non-VXLAN network, sources in DC VXLAN network, and receivers in a non-VXLAN network.

Figure 1 *DC network with distributed L3 gateway topology*



Configuration and verification details for the devices in this use case are provided in the following sections:

- Spine01
- Spine02
- Leaf01-primary
- Leaf01-secondary
- Leaf02
- 8325-border-prim
- 8325-border-sec
- Edge-primary
- Edge-secondary

Spine01

Configuration

```
!export-password: default
hostname Spine01
module 1/1 product-number jl363a
cli-session
    timeout 0
!
!
!
ssh server vrf mgmt
vlan 1
interface mgmt
    no shutdown
    ip dhcp
interface 1/1/4
    no shutdown
    mtu 9198
    ip mtu 9198
    ip address 20.0.0.2/30
    ip ospf 1 area 0.0.0.0
interface 1/1/5
    no shutdown
    mtu 9198
    ip mtu 9198
    ip address 21.0.0.2/30
    ip ospf 1 area 0.0.0.0
interface 1/1/6
    no shutdown
    mtu 9198
    ip mtu 9198
    ip address 22.0.0.2/30
    ip ospf 1 area 0.0.0.0
interface 1/1/28
    no shutdown
    mtu 9198
    ip mtu 9198
    ip address 24.0.0.2/30
    ip ospf 1 area 0.0.0.0
interface 1/1/29
    no shutdown
    mtu 9198
    ip mtu 9198
    ip address 25.0.0.2/30
    ip ospf 1 area 0.0.0.0
interface loopback 0
    ip address 4.4.4.4/32
    ip ospf 1 area 0.0.0.0
!
!
!
!
!
router ospf 1
    router-id 44.44.44.44
    area 0.0.0.0
router bgp 1
    bgp router-id 4.4.4.4
    neighbor 1.1.1.1 remote-as 1
    neighbor 1.1.1.1 update-source loopback 0
    neighbor 1.1.2.1 remote-as 1
    neighbor 1.1.2.1 update-source loopback 0
    neighbor 6.6.6.6 remote-as 1
    neighbor 6.6.6.6 update-source loopback 0
```

```
    neighbor 109.0.0.1 remote-as 1
    neighbor 109.0.0.1 update-source loopback 0
    neighbor 110.0.0.1 remote-as 1
    neighbor 110.0.0.1 update-source loopback 0
    address-family ipv4 unicast
        redistribute connected
    exit-address-family
    address-family l2vpn evpn
        neighbor 1.1.1.1 activate
        neighbor 1.1.1.1 route-reflector-client
        neighbor 1.1.1.1 send-community extended
        neighbor 1.1.2.1 activate
        neighbor 1.1.2.1 route-reflector-client
        neighbor 1.1.2.1 send-community extended
        neighbor 6.6.6.6 activate
        neighbor 6.6.6.6 route-reflector-client
        neighbor 6.6.6.6 send-community extended
        neighbor 109.0.0.1 activate
        neighbor 109.0.0.1 route-reflector-client
        neighbor 109.0.0.1 send-community extended
        neighbor 110.0.0.1 activate
        neighbor 110.0.0.1 route-reflector-client
        neighbor 110.0.0.1 send-community extended
    exit-address-family
!
https-server vrf mgmt
```

Spine02

Configuration

```
!export-password: default
hostname Spine02
profile Spine
cli-session
    timeout 0
!
!
!
ssh server vrf mgmt
vlan 1
interface mgmt
    no shutdown
    ip dhcp
system interface-group 1 speed 10g
    !interface group 1 contains ports 1/1/1-1/1/12
system interface-group 3 speed 10g
    !interface group 3 contains ports 1/1/25-1/1/36
system interface-group 4 speed 10g
    !interface group 4 contains ports 1/1/37-1/1/48
interface 1/1/1
    no shutdown
    mtu 9198
    ip mtu 9198
    ip address 20.0.0.6/30
    ip ospf 1 area 0.0.0.0
interface 1/1/2
    no shutdown
    mtu 9198
    ip mtu 9198
    ip address 21.0.0.6/30
```

```
    ip ospf 1 area 0.0.0.0
interface 1/1/5
    no shutdown
    mtu 9198
    ip mtu 9198
    ip address 22.0.0.6/30
    ip ospf 1 area 0.0.0.0
interface 1/1/41
    no shutdown
    mtu 9198
    ip mtu 9198
    ip address 24.0.0.6/30
    ip ospf 1 area 0.0.0.0
interface 1/1/42
    no shutdown
    mtu 9198
    ip mtu 9198
    ip address 25.0.0.6/30
    ip ospf 1 area 0.0.0.0
interface loopback 0
    ip address 5.5.5.5/32
    ip ospf 1 area 0.0.0.0
!
!
!
!
!
router ospf 1
    router-id 45.45.45.45
    area 0.0.0.0
router bgp 1
    bgp router-id 5.5.5.5
    neighbor 1.1.1.1 remote-as 1
    neighbor 1.1.1.1 update-source loopback 0
    neighbor 1.1.2.1 remote-as 1
    neighbor 1.1.2.1 update-source loopback 0
    neighbor 6.6.6.6 remote-as 1
    neighbor 6.6.6.6 update-source loopback 0
    neighbor 109.0.0.1 remote-as 1
    neighbor 109.0.0.1 update-source loopback 0
    neighbor 110.0.0.1 remote-as 1
    neighbor 110.0.0.1 update-source loopback 0
    address-family ipv4 unicast
        redistribute connected
    exit-address-family
    address-family l2vpn evpn
        neighbor 1.1.1.1 activate
        neighbor 1.1.1.1 route-reflector-client
        neighbor 1.1.1.1 send-community extended
        neighbor 1.1.2.1 activate
        neighbor 1.1.2.1 route-reflector-client
        neighbor 1.1.2.1 send-community extended
        neighbor 6.6.6.6 activate
        neighbor 6.6.6.6 route-reflector-client
        neighbor 6.6.6.6 send-community extended
        neighbor 109.0.0.1 activate
        neighbor 109.0.0.1 route-reflector-client
        neighbor 109.0.0.1 send-community extended
        neighbor 110.0.0.1 activate
        neighbor 110.0.0.1 route-reflector-client
        neighbor 110.0.0.1 send-community extended
    exit-address-family
```

```
!
https-server vrf mgmt
```

Leaf01-primary

Configuration

```
!export-password: default
hostname Leaf01-primary
profile Leaf
vrf DC
    rd 192.1.0.10:1
    route-target export 65501:1 evpn
    route-target import 65501:1 evpn
cli-session
    timeout 0
!
!
!
!
!
ssh server vrf mgmt
vlan 1
vlan 101
    ip igmp snooping enable
vlan 102
    ip igmp snooping enable
vlan 103
    ip igmp snooping enable
vlan 104
    ip igmp snooping enable
vlan 105
    ip igmp snooping enable
vlan 106
    ip igmp snooping enable
vlan 107
    ip igmp snooping enable
vlan 108
    ip igmp snooping enable
vlan 109
    ip igmp snooping enable
vlan 110
    ip igmp snooping enable
vlan 111
    ip igmp snooping enable
vlan 900
    description DC_Leaf_L3
vlan 1111
virtual-mac 00:00:00:0a:0a:0a
evpn
    redistribute local-svi
    vlan 101
        rd auto
        route-target export auto
        route-target import auto
        redistribute host-route
    vlan 102
        rd auto
        route-target export auto
        route-target import auto
        redistribute host-route
```

```
    vlan 103
        rd auto
        route-target export auto
        route-target import auto
        redistribute host-route
    vlan 104
        rd auto
        route-target export auto
        route-target import auto
        redistribute host-route
    vlan 105
        rd auto
        route-target export auto
        route-target import auto
        redistribute host-route
    vlan 106
        rd auto
        route-target export auto
        route-target import auto
        redistribute host-route
    vlan 107
        rd auto
        route-target export auto
        route-target import auto
        redistribute host-route
    vlan 108
        rd auto
        route-target export auto
        route-target import auto
        redistribute host-route
    vlan 109
        rd auto
        route-target export auto
        route-target import auto
        redistribute host-route
    vlan 110
        rd auto
        route-target export auto
        route-target import auto
        redistribute host-route
    vlan 111
        rd auto
        route-target export auto
        route-target import auto
        redistribute host-route
interface mgmt
    no shutdown
    ip dhcp
system interface-group 1 speed 10g
    !interface group 1 contains ports 1/1/1-1/1/12
system interface-group 2 speed 10g
    !interface group 2 contains ports 1/1/13-1/1/24
system interface-group 3 speed 10g
    !interface group 3 contains ports 1/1/25-1/1/36
system interface-group 4 speed 10g
    !interface group 4 contains ports 1/1/37-1/1/48
interface lag 1
    no shutdown
    no routing
    vlan trunk native 1 tag
    vlan trunk allowed all
    lacp mode active
```

```
interface lag 2 multi-chassis
    no shutdown
    no routing
    vlan trunk native 1
    vlan trunk allowed 101-111
    lacp mode active
interface 1/1/5
    no shutdown
    mtu 9198
    ip mtu 9198
    ip address 20.0.0.1/30
    ip ospf 1 area 0.0.0.0
interface 1/1/6
    no shutdown
    mtu 9198
    ip mtu 9198
    ip address 20.0.0.5/30
    ip ospf 1 area 0.0.0.0
interface 1/1/7
    no shutdown
    mtu 9198
    lag 2
interface 1/1/32
    no shutdown
    mtu 9198
    lag 1
interface 1/1/33
    no shutdown
    mtu 9198
    ip mtu 9198
    ip address 192.168.1.1/30
interface loopback 0
    ip address 1.1.1.1/32
    ip ospf 1 area 0.0.0.0
interface loopback 1
    ip address 192.1.0.10/32
    ip ospf 1 area 0.0.0.0
interface vlan 101
    vrf attach DC
    ip address 192.1.1.2/24
    active-gateway ip mac 02:aa:bb:cc:00:01
    active-gateway ip 192.1.1.1
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 102
    vrf attach DC
    ip address 192.1.2.2/24
    active-gateway ip mac 02:aa:bb:cc:00:01
    active-gateway ip 192.1.2.1
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 103
    vrf attach DC
    ip address 192.1.3.2/24
    active-gateway ip mac 02:aa:bb:cc:00:01
    active-gateway ip 192.1.3.1
    ip igmp enable
    ip igmp version 2
```

```
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 104
    vrf attach DC
    ip address 192.1.4.2/24
    active-gateway ip mac 02:aa:bb:cc:00:01
    active-gateway ip 192.1.4.1
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 105
    vrf attach DC
    ip address 192.1.5.2/24
    active-gateway ip mac 02:aa:bb:cc:00:01
    active-gateway ip 192.1.5.1
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 106
    vrf attach DC
    ip address 192.1.6.2/24
    active-gateway ip mac 02:aa:bb:cc:00:01
    active-gateway ip 192.1.6.1
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 107
    vrf attach DC
    ip address 192.1.7.2/24
    active-gateway ip mac 02:aa:bb:cc:00:01
    active-gateway ip 192.1.7.1
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 108
    vrf attach DC
    ip address 192.1.8.2/24
    active-gateway ip mac 02:aa:bb:cc:00:01
    active-gateway ip 192.1.8.1
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 109
    vrf attach DC
    ip address 192.1.9.2/24
    active-gateway ip mac 02:aa:bb:cc:00:01
    active-gateway ip 192.1.9.1
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 110
    vrf attach DC
    ip address 192.1.10.2/24
    active-gateway ip mac 02:aa:bb:cc:00:01
    active-gateway ip 192.1.10.1
    ip igmp enable
```

```
    ip igmp version 2
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 111
    vrf attach DC
    ip address 192.1.11.2/24
    active-gateway ip mac 02:aa:bb:cc:00:01
    active-gateway ip 192.1.11.1
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 900
    description DC_Leaf_L3
    ip mtu 9198
    ip address 192.1.240.2/31
    ip ospf 1 area 0.0.0.0
    ip ospf cost 50
    ip ospf network point-to-point
interface vxlan 1
    source ip 192.1.0.10
    no shutdown
    vni 100
    vni 101
        vlan 101
    vni 102
        vlan 102
    vni 103
        vlan 103
    vni 104
        vlan 104
    vni 105
        vlan 105
    vni 106
        vlan 106
    vni 107
        vlan 107
    vni 108
        vlan 108
    vni 109
        vlan 109
    vni 110
        vlan 110
    vni 111
        vlan 111
    vni 100001
        vrf DC
        routing
vsx
    system-mac 00:00:00:0a:0a:0a
    inter-switch-link lag 1
    role primary
    keepalive peer 192.168.1.2 source 192.168.1.1
    no split-recovery
    vsx-sync evpn
!
!
!
!
!
router ospf 1
    router-id 11.11.11.11
```

```
    area 0.0.0.0
router bgp 1
    bgp router-id 1.1.1.1
    no bgp fast-external-fallover
    neighbor 4.4.4.4 remote-as 1
    neighbor 4.4.4.4 update-source loopback 0
    neighbor 5.5.5.5 remote-as 1
    neighbor 5.5.5.5 update-source loopback 0
    address-family ipv4 unicast
        redistribute connected
    exit-address-family
    address-family l2vpn evpn
        neighbor 4.4.4.4 activate
        neighbor 4.4.4.4 send-community extended
        neighbor 5.5.5.5 activate
        neighbor 5.5.5.5 send-community extended
    exit-address-family
!
    vrf DC
        no bgp fast-external-fallover
        address-family ipv4 unicast
            redistribute connected
            redistribute static
        exit-address-family
!
router pim vrf DC
    enable
https-server vrf mgmt
```

Verification

Verify OSPF neighbors

```
Leaf01-primary# show ip ospf neighbors all-vrfs
VRF : default                           Process : 1
================================================
Total Number of Neighbors : 2
Neighbor ID      Priority  State             Nbr Address       Interface
-------------------------------------------------------------------------
44.44.44.44      1         FULL/DR           20.0.0.2           1/1/5
45.45.45.45      1         FULL/DR           20.0.0.6           1/1/6
```

Verify BGP EVPN neighbors

```
Leaf01-primary# show bgp l2vpn evpn summary
VRF : default
BGP Summary
-----------
Local AS               : 1           BGP Router Identifier  : 1.1.1.1
Peers                  : 2           Log Neighbor Changes   : No
Cfg. Hold Time         : 180         Cfg. Keep Alive        : 60
Confederation Id       : 0
Neighbor        Remote-AS MsgRcvd MsgSent   Up/Down Time State        AdminStatus
4.4.4.4         1           167     93      00h:11m:41s  Established   Up
5.5.5.5         1           168     93      00h:11m:41s  Established   Up
```

Verify VXLAN tunnel, VTEP peers, and VNIs

```
Leaf01-primary# show interface vxlan vteps
Source           Destination      Origin       Status               VNI       Routing   VLAN  VRF
---------------- ---------------- ------------ -------------------- --------- --------- ----- ---
-
192.1.0.10       192.1.0.7        evpn         operational          101       disabled  101    --
192.1.0.10       192.1.0.7        evpn         operational          102       disabled  102    --
192.1.0.10       192.1.0.7        evpn         operational          103       disabled  103    --
192.1.0.10       192.1.0.7        evpn         operational          104       disabled  104    --
192.1.0.10       192.1.0.7        evpn         operational          105       disabled  105    --
192.1.0.10       192.1.0.7        evpn         operational          106       disabled  106    --
192.1.0.10       192.1.0.7        evpn         operational          107       disabled  107    --
192.1.0.10       192.1.0.7        evpn         operational          108       disabled  108    --
192.1.0.10       192.1.0.7        evpn         operational          109       disabled  109    --
192.1.0.10       192.1.0.7        evpn         operational          110       disabled  110    --
192.1.0.10       192.1.0.7        evpn         operational          100001    enabled   --     DC
192.1.0.10       192.1.0.17       evpn         operational          101       disabled  101    --
192.1.0.10       192.1.0.17       evpn         operational          102       disabled  102    --
192.1.0.10       192.1.0.17       evpn         operational          103       disabled  103    --
192.1.0.10       192.1.0.17       evpn         operational          104       disabled  104    --
192.1.0.10       192.1.0.17       evpn         operational          105       disabled  105    --
192.1.0.10       192.1.0.17       evpn         operational          106       disabled  106    --
192.1.0.10       192.1.0.17       evpn         operational          107       disabled  107    --
192.1.0.10       192.1.0.17       evpn         operational          108       disabled  108    --
192.1.0.10       192.1.0.17       evpn         operational          109       disabled  109    --
192.1.0.10       192.1.0.17       evpn         operational          110       disabled  110    --
192.1.0.10       192.1.0.17       evpn         operational          100001    enabled   --     DC
```

Verify PIM neighbors

```
Leaf01-primary# show ip pim neighbor all-vrfs

PIM Neighbor


VRF                         : DC
Total number of neighbors : 43

IP Address                  : 192.1.0.7
Interface                   : vni100001
Up Time (HH:MM:SS)          : 00:12:01
Expire Time (HH:MM:SS)      : 00:03:05
DR Priority                 : 1
Hold Time (HH:MM:SS)        : 00:03:30

IP Address                  : 192.1.0.17
Interface                   : vni100001
Up Time (HH:MM:SS)          : 00:11:25
Expire Time (HH:MM:SS)      : 00:03:05
DR Priority                 : 1
Hold Time (HH:MM:SS)        : 00:03:30

IP Address                  : 192.1.1.3
Interface                   : vlan101
Up Time (HH:MM:SS)          : 00:12:53
Expire Time (HH:MM:SS)      : 00:01:23
DR Priority                 : 167772608
Hold Time (HH:MM:SS)        : 00:01:45
Secondary IP Addresses :
 192.1.1.1

! snip
```

```
IP Address                : 192.1.11.3
Interface                 : vlan111
Up Time (HH:MM:SS)        : 00:12:58
Expire Time (HH:MM:SS)    : 00:01:17
DR Priority               : 167772608
Hold Time (HH:MM:SS)      : 00:01:45
Secondary IP Addresses :
 192.1.11.1
```

Verify RP information

```
Leaf01-primary# show ip pim rp-set all-vrfs

VRF: DC

Status and Counters - PIM-SM Learned RP-Set Information
Group Address    Group Mask       RP Address       Hold Time  Expire Time
---------------  ---------------  ---------------  ---------  -----------
224.0.0.0        240.0.0.0        192.1.0.1        150        124
224.0.0.0        240.0.0.0        192.1.0.2        150        124
```

Verify BSR information

```
Leaf01-primary# show ip pim bsr elected all-vrfs

Status and Counters - PIM-SM Elected Bootstrap Router Information

VRF                       : DC
E-BSR Address             : 192.1.0.2
E-BSR Priority            : 0
E-BSR Hash Mask Length    : 30
E-BSR Up Time             : 10 mins 30 secs
Next Bootstrap Message    : 1 mins 40 secs
```

Verify mroutes

```
Leaf01-primary# show ip mroute all-vrfs
IP Multicast Route Entries

VRF : DC
Total number of entries : 39

Group Address           : 225.1.1.1
Source Address          : 192.1.1.11
Neighbor                :
Incoming interface      : vlan101

Group Address           : 225.1.2.1
Source Address          : 192.1.1.11
Neighbor                :
Incoming interface      : vlan101

Group Address           : 225.1.2.1
Source Address          : 192.1.1.11
Neighbor                :
Incoming interface      : vlan102
```

```
Group Address           : 225.1.3.1
Source Address          : 192.1.1.11
Neighbor                :
Incoming interface      : vlan103
! snip

Group Address           : 230.1.1.1
Source Address          : 192.1.11.12
Neighbor                :
Incoming interface      : vlan111
Outgoing Interface List :
Interface       State
-----------     ----------
vni100001       forwarding

Group Address           : 230.1.2.1
Source Address          : 192.1.11.12
Neighbor                :
Incoming interface      : vlan111
Outgoing Interface List :
Interface       State
-----------     ----------
vni100001       forwarding

Group Address           : 230.1.3.1
Source Address          : 192.1.11.12
Neighbor                :
Incoming interface      : vlan111
Outgoing Interface List :
Interface       State
-----------     ----------
vni100001       forwarding

Group Address           : 230.1.4.1
Source Address          : 192.1.11.12
Neighbor                :
Incoming interface      : vlan111
Outgoing Interface List :
Interface       State
-----------     ----------
vni100001       forwarding
```

Verify PIM interfaces

```
Leaf01-primary# show ip pim interface vlan 101

PIM Interfaces

VRF: DC

Interface  : vlan101
Neighbor count : 4
IP Address : 192.1.1.2/24
Mode       : sparse
Designated Router : 192.1.1.4
Proxy DR              : false
Hello Interval (sec)  : 30
Hello Delay (sec)     : 5
Override Interval (msec)  : 2500             Lan Prune Delay     : Yes

Propagation Delay (msec)  : 500              Configured DR Priority    : 1
```

```
Operational DR Priority   : 167772608
Neighbor Timeout          : 91


Leaf01-primary# show ip pim interface vlan 110

PIM Interfaces

VRF: DC

Interface  : vlan110
Neighbor count : 4
IP Address : 192.1.10.2/24
Mode       : sparse
Designated Router : 192.1.10.4
Proxy DR              : false
Hello Interval (sec)  : 30
Hello Delay (sec)     : 5
Override Interval (msec)  : 2500              Lan Prune Delay     : Yes

Propagation Delay (msec)  : 500               Configured DR Priority    : 1

Operational DR Priority   : 167772608
Neighbor Timeout          : 93


Leaf01-primary# show ip pim interface vlan 111

PIM Interfaces

VRF: DC

Interface  : vlan111
Neighbor count : 1
IP Address : 192.1.11.2/24
Mode       : sparse
Designated Router : 192.1.11.2
Proxy DR              : false
Hello Interval (sec)  : 30
Hello Delay (sec)     : 5
Override Interval (msec)  : 2500              Lan Prune Delay     : Yes

Propagation Delay (msec)  : 500               Configured DR Priority    : 1

Operational DR Priority   : 167772608
Neighbor Timeout          : 83
```

Verify BGP EVPN table

```
Leaf01-primary# show bgp l2vpn evpn
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
              i internal, e external S Stale, R Removed, a additional-paths
Origin codes: i - IGP, e - EGP, ? - incomplete

EVPN Route-Type 2 prefix: [2]:[ESI]:[EthTag]:[MAC]:[OrigIP]
EVPN Route-Type 3 prefix: [3]:[EthTag]:[OrigIP]
EVPN Route-Type 5 prefix: [5]:[ESI]:[EthTag]:[IPAddrLen]:[IPAddr]
VRF : default
Local Router-ID 1.1.1.1
```

```
     Network                                          Nexthop         Metric     LocPrf    Weight   Path
-------------------------------------------------------------------------------------------------------------
Route Distinguisher: 192.1.0.10:101       (L2VNI 101)
*>  [2]:[0]:[0]:[00:11:01:00:00:01]:[192.1.1.11]          192.1.0.10      0          100        0       ?
*>  [2]:[0]:[0]:[00:11:01:00:00:01]:[]                    192.1.0.10      0          100        0       ?
*>  [2]:[0]:[0]:[00:12:01:00:00:01]:[192.1.1.12]          192.1.0.10      0          100        0       ?
*>  [2]:[0]:[0]:[00:12:01:00:00:01]:[]                    192.1.0.10      0          100        0       ?
*>  [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.1.1]           192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[b8:6a:97:21:e4:42]:[192.1.1.3]          192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[b8:6a:97:21:e4:42]:[192.1.1.3]          192.1.0.10      0          100        0       ?
*>  [2]:[0]:[0]:[b8:6a:97:21:e9:42]:[192.1.1.2]          192.1.0.10      0          100        0       ?
*>  [3]:[0]:[192.1.0.10]                                 192.1.0.10      0          100        0       ?

Route Distinguisher: 192.1.0.17:101       (L2VNI 101)
*>i [2]:[0]:[0]:[00:13:01:00:00:01]:[192.1.1.13]          192.1.0.17      0          100        0       ?
* i [2]:[0]:[0]:[00:13:01:00:00:01]:[192.1.1.13]          192.1.0.17      0          100        0       ?
*>i [2]:[0]:[0]:[00:13:01:00:00:01]:[]                    192.1.0.17      0          100        0       ?
* i [2]:[0]:[0]:[00:13:01:00:00:01]:[]                    192.1.0.17      0          100        0       ?
*>i [2]:[0]:[0]:[00:14:01:00:00:01]:[192.1.1.23]          192.1.0.17      0          100        0       ?
* i [2]:[0]:[0]:[00:14:01:00:00:01]:[192.1.1.23]          192.1.0.17      0          100        0       ?
*>i [2]:[0]:[0]:[00:14:01:00:00:01]:[]                    192.1.0.17      0          100        0       ?
* i [2]:[0]:[0]:[00:14:01:00:00:01]:[]                    192.1.0.17      0          100        0       ?
*>i [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.1.1]           192.1.0.17      0          100        0       ?
* i [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.1.1]           192.1.0.17      0          100        0       ?
*>i [2]:[0]:[0]:[54:80:28:3c:00:00]:[192.1.1.4]          192.1.0.17      0          100        0       ?
* i [2]:[0]:[0]:[54:80:28:3c:00:00]:[192.1.1.4]          192.1.0.17      0          100        0       ?
*>i [3]:[0]:[192.1.0.17]                                 192.1.0.17      0          100        0       ?
* i [3]:[0]:[192.1.0.17]                                 192.1.0.17      0          100        0       ?

Route Distinguisher: 192.1.0.7:101        (L2VNI 101)
*>i [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.1.1]           192.1.0.7       0          100        0       ?
* i [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.1.1]           192.1.0.7       0          100        0       ?
*>i [2]:[0]:[0]:[3c:2c:99:ff:da:a5]:[192.1.1.6]          192.1.0.7       0          100        0       ?
* i [2]:[0]:[0]:[3c:2c:99:ff:da:a5]:[192.1.1.6]          192.1.0.7       0          100        0       ?
*>i [2]:[0]:[0]:[b8:6a:97:21:f5:42]:[192.1.1.7]          192.1.0.7       0          100        0       ?
* i [2]:[0]:[0]:[b8:6a:97:21:f5:42]:[192.1.1.7]          192.1.0.7       0          100        0       ?
*>i [3]:[0]:[192.1.0.7]                                  192.1.0.7       0          100        0       ?
* i [3]:[0]:[192.1.0.7]                                  192.1.0.7       0          100        0       ?

Route Distinguisher: 192.1.0.10:102       (L2VNI 102)
*>  [2]:[0]:[0]:[00:11:01:00:00:02]:[192.1.2.11]          192.1.0.10      0          100        0       ?
*>  [2]:[0]:[0]:[00:11:01:00:00:02]:[]                    192.1.0.10      0          100        0       ?
*>  [2]:[0]:[0]:[00:12:01:00:00:02]:[192.1.2.12]          192.1.0.10      0          100        0       ?
*>  [2]:[0]:[0]:[00:12:01:00:00:02]:[]                    192.1.0.10      0          100        0       ?
*>  [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.2.1]           192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[b8:6a:97:21:e4:42]:[192.1.2.3]          192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[b8:6a:97:21:e4:42]:[192.1.2.3]          192.1.0.10      0          100        0       ?
*>  [2]:[0]:[0]:[b8:6a:97:21:e9:42]:[192.1.2.2]          192.1.0.10      0          100        0       ?
*>  [3]:[0]:[192.1.0.10]                                 192.1.0.10      0          100        0       ?

!snip

Route Distinguisher: 192.1.0.10:1         (L3VNI 100001)
*>  [5]:[0]:[0]:[24]:[192.1.1.0]                         192.1.0.10      0          100        0       ?
*>  [5]:[0]:[0]:[24]:[192.1.10.0]                        192.1.0.10      0          100        0       ?
*>  [5]:[0]:[0]:[24]:[192.1.11.0]                        192.1.0.10      0          100        0       ?
*>  [5]:[0]:[0]:[24]:[192.1.2.0]                         192.1.0.10      0          100        0       ?
*>  [5]:[0]:[0]:[24]:[192.1.3.0]                         192.1.0.10      0          100        0       ?
*>  [5]:[0]:[0]:[24]:[192.1.4.0]                         192.1.0.10      0          100        0       ?
*>  [5]:[0]:[0]:[24]:[192.1.5.0]                         192.1.0.10      0          100        0       ?
*>  [5]:[0]:[0]:[24]:[192.1.6.0]                         192.1.0.10      0          100        0       ?
*>  [5]:[0]:[0]:[24]:[192.1.7.0]                         192.1.0.10      0          100        0       ?
```

```
*>  [5]:[0]:[0]:[24]:[192.1.8.0]                          192.1.0.10      0          100        0       ?
*>  [5]:[0]:[0]:[24]:[192.1.9.0]                          192.1.0.10      0          100        0       ?

Route Distinguisher: 192.1.0.10:101       (L3VNI 100001)
*>  [2]:[0]:[0]:[00:11:01:00:00:01]:[192.1.1.11]          192.1.0.10      0          100        0       ?
*>  [2]:[0]:[0]:[00:11:01:00:00:01]:[]                    192.1.0.10      0          100        0       ?
*>  [2]:[0]:[0]:[00:12:01:00:00:01]:[192.1.1.12]          192.1.0.10      0          100        0       ?
*>  [2]:[0]:[0]:[00:12:01:00:00:01]:[]                    192.1.0.10      0          100        0       ?
*>  [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.1.1]           192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[b8:6a:97:21:e4:42]:[192.1.1.3]          192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[b8:6a:97:21:e4:42]:[192.1.1.3]          192.1.0.10      0          100        0       ?
*>  [2]:[0]:[0]:[b8:6a:97:21:e9:42]:[192.1.1.2]          192.1.0.10      0          100        0       ?

Route Distinguisher: 192.1.0.10:102       (L3VNI 100001)
*>  [2]:[0]:[0]:[00:11:01:00:00:02]:[192.1.2.11]          192.1.0.10      0          100        0       ?
*>  [2]:[0]:[0]:[00:11:01:00:00:02]:[]                    192.1.0.10      0          100        0       ?
*>  [2]:[0]:[0]:[00:12:01:00:00:02]:[192.1.2.12]          192.1.0.10      0          100        0       ?
*>  [2]:[0]:[0]:[00:12:01:00:00:02]:[]                    192.1.0.10      0          100        0       ?
*>  [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.2.1]           192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[b8:6a:97:21:e4:42]:[192.1.2.3]          192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[b8:6a:97:21:e4:42]:[192.1.2.3]          192.1.0.10      0          100        0       ?
*>  [2]:[0]:[0]:[b8:6a:97:21:e9:42]:[192.1.2.2]          192.1.0.10      0          100        0       ?
Total number of entries 844
```

Leaf01-secondary

Configuration

```
hostname Leaf01-secondary
profile Leaf
vrf DC
    rd 192.1.0.10:1
    route-target export 65501:1 evpn
    route-target import 65501:1 evpn
ntp server 10.100.0.12 minpoll 4 maxpoll 4 iburst
cli-session
    timeout 0
!
!
!
!
!
ssh server vrf mgmt
vlan 1
vlan 101
    ip igmp snooping enable
vlan 102
    ip igmp snooping enable
vlan 103
    ip igmp snooping enable
vlan 104
    ip igmp snooping enable
vlan 105
    ip igmp snooping enable
vlan 106
    ip igmp snooping enable
vlan 107
    ip igmp snooping enable
vlan 108
    ip igmp snooping enable
vlan 109
```

```
    ip igmp snooping enable
vlan 110
    ip igmp snooping enable
vlan 111
    ip igmp snooping enable
vlan 900
virtual-mac 00:00:00:0a:0a:0a
evpn
    redistribute local-svi
    vlan 101
        rd auto
        route-target export auto
        route-target import auto
        redistribute host-route
    vlan 102
        rd auto
        route-target export auto
        route-target import auto
        redistribute host-route
    vlan 103
        rd auto
        route-target export auto
        route-target import auto
        redistribute host-route
    vlan 104
        rd auto
        route-target export auto
        route-target import auto
        redistribute host-route
    vlan 105
        rd auto
        route-target export auto
        route-target import auto
        redistribute host-route
    vlan 106
        rd auto
        route-target export auto
        route-target import auto
        redistribute host-route
    vlan 107
        rd auto
        route-target export auto
        route-target import auto
        redistribute host-route
    vlan 108
        rd auto
        route-target export auto
        route-target import auto
        redistribute host-route
    vlan 109
        rd auto
        route-target export auto
        route-target import auto
        redistribute host-route
    vlan 110
        rd auto
        route-target export auto
        route-target import auto
        redistribute host-route
    vlan 111
        rd auto
        route-target export auto
```

```
        route-target import auto
        redistribute host-route
interface mgmt
    no shutdown
    ip dhcp
system interface-group 1 speed 10g
    !interface group 1 contains ports 1/1/1-1/1/12
system interface-group 2 speed 10g
    !interface group 2 contains ports 1/1/13-1/1/24
system interface-group 3 speed 10g
    !interface group 3 contains ports 1/1/25-1/1/36
system interface-group 4 speed 10g
    !interface group 4 contains ports 1/1/37-1/1/48
interface lag 1
    no shutdown
    no routing
    vlan trunk native 1 tag
    vlan trunk allowed all
    lacp mode active
interface lag 2 multi-chassis
    no shutdown
    no routing
    vlan trunk native 1
    vlan trunk allowed 101-111
    lacp mode active
interface 1/1/5
    no shutdown
    mtu 9198
    ip mtu 9198
    ip address 21.0.0.1/30
    ip ospf 1 area 0.0.0.0
interface 1/1/6
    no shutdown
    mtu 9198
    ip mtu 9198
    ip address 21.0.0.5/30
    ip ospf 1 area 0.0.0.0
interface 1/1/7
    no shutdown
    mtu 9198
    lag 2
interface 1/1/32
    no shutdown
    mtu 9198
    lag 1
interface 1/1/33
    no shutdown
    mtu 9198
    ip mtu 9198
    ip address 192.168.1.2/30
interface loopback 0
    ip address 1.1.2.1/32
    ip ospf 1 area 0.0.0.0
interface loopback 1
    ip address 192.1.0.10/32
    ip ospf 1 area 0.0.0.0
interface vlan 101
    vrf attach DC
    ip address 192.1.1.3/24
    active-gateway ip mac 02:aa:bb:cc:00:01
    active-gateway ip 192.1.1.1
    ip igmp enable
```

```
    ip igmp version 2
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 102
    vrf attach DC
    ip address 192.1.2.3/24
    active-gateway ip mac 02:aa:bb:cc:00:01
    active-gateway ip 192.1.2.1
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 103
    vrf attach DC
    ip address 192.1.3.3/24
    active-gateway ip mac 02:aa:bb:cc:00:01
    active-gateway ip 192.1.3.1
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 104
    vrf attach DC
    ip address 192.1.4.3/24
    active-gateway ip mac 02:aa:bb:cc:00:01
    active-gateway ip 192.1.4.1
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 105
    vrf attach DC
    ip address 192.1.5.3/24
    active-gateway ip mac 02:aa:bb:cc:00:01
    active-gateway ip 192.1.5.1
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 106
    vrf attach DC
    ip address 192.1.6.3/24
    active-gateway ip mac 02:aa:bb:cc:00:01
    active-gateway ip 192.1.6.1
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 107
    vrf attach DC
    ip address 192.1.7.3/24
    active-gateway ip mac 02:aa:bb:cc:00:01
    active-gateway ip 192.1.7.1
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 108
    vrf attach DC
    ip address 192.1.8.3/24
    active-gateway ip mac 02:aa:bb:cc:00:01
    active-gateway ip 192.1.8.1
```

```
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 109
    vrf attach DC
    ip address 192.1.9.3/24
    active-gateway ip mac 02:aa:bb:cc:00:01
    active-gateway ip 192.1.9.1
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 110
    vrf attach DC
    ip address 192.1.10.3/24
    active-gateway ip mac 02:aa:bb:cc:00:01
    active-gateway ip 192.1.10.1
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 111
    vrf attach DC
    ip address 192.1.11.3/24
    active-gateway ip mac 02:aa:bb:cc:00:01
    active-gateway ip 192.1.11.1
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vxlan 1
    source ip 192.1.0.10
    no shutdown
    vni 100
    vni 101
        vlan 101
    vni 102
        vlan 102
    vni 103
        vlan 103
    vni 104
        vlan 104
    vni 105
        vlan 105
    vni 106
        vlan 106
    vni 107
        vlan 107
    vni 108
        vlan 108
    vni 109
        vlan 109
    vni 110
        vlan 110
    vni 111
        vlan 111
    vni 100001
        vrf DC
        routing
vsx
    system-mac 00:00:00:0a:0a:0a
```

```
    inter-switch-link lag 1
    role secondary
    keepalive peer 192.168.1.1 source 192.168.1.2
    no split-recovery
    vsx-sync evpn
!
!
!
!
!
router ospf 1
    router-id 1.1.2.1
    area 0.0.0.0
router bgp 1
    bgp router-id 1.1.2.1
    neighbor 4.4.4.4 remote-as 1
    neighbor 4.4.4.4 update-source loopback 0
    neighbor 5.5.5.5 remote-as 1
    neighbor 5.5.5.5 update-source loopback 0
    address-family ipv4 unicast
        redistribute connected
    exit-address-family
    address-family l2vpn evpn
        neighbor 4.4.4.4 activate
        neighbor 4.4.4.4 send-community extended
        neighbor 5.5.5.5 activate
        neighbor 5.5.5.5 send-community extended
    exit-address-family
!
    vrf DC
        address-family ipv4 unicast
            redistribute connected
            redistribute static
        exit-address-family
!
router pim vrf DC
    enable
https-server vrf mgmt
```

Verification

Verify OSPF neighbors

```
Leaf01-secondary# show ip ospf neighbors all-vrfs
VRF : default                           Process : 1
================================================

Total Number of Neighbors : 2

Neighbor ID      Priority  State             Nbr Address       Interface
-------------------------------------------------------------------------
44.44.44.44      1         FULL/DR           21.0.0.2           1/1/5

45.45.45.45      1         FULL/DR           21.0.0.6           1/1/6
```

Verify BGP EVPN neighbors

```
Leaf01-secondary# show bgp l2vpn evpn summary
VRF : default
```

```
BGP Summary
-----------
 Local AS               : 1           BGP Router Identifier  : 1.1.2.1
 Peers                  : 2           Log Neighbor Changes   : No
 Cfg. Hold Time         : 180         Cfg. Keep Alive        : 60
 Confederation Id       : 0

 Neighbor        Remote-AS MsgRcvd MsgSent   Up/Down Time State        AdminStatus
 4.4.4.4         1           258     93      00h:12m:51s  Established   Up
 5.5.5.5         1           259     93      00h:12m:51s  Established   Up
```

Verify VXLAN tunnel, VTEP peers, and VNIs

```
Leaf01-secondary# show interface vxlan vteps
Source           Destination      Origin       Status               VNI       Routing   VLAN  VRF

---------------- ---------------- ------------ -------------------- --------- --------- ----- ---
-
192.1.0.10       192.1.0.7        evpn         operational          101       disabled  101    --

192.1.0.10       192.1.0.7        evpn         operational          102       disabled  102    --

192.1.0.10       192.1.0.7        evpn         operational          103       disabled  103    --

192.1.0.10       192.1.0.7        evpn         operational          104       disabled  104    --

192.1.0.10       192.1.0.7        evpn         operational          105       disabled  105    --

192.1.0.10       192.1.0.7        evpn         operational          106       disabled  106    --

192.1.0.10       192.1.0.7        evpn         operational          107       disabled  107    --

192.1.0.10       192.1.0.7        evpn         operational          108       disabled  108    --

192.1.0.10       192.1.0.7        evpn         operational          109       disabled  109    --

192.1.0.10       192.1.0.7        evpn         operational          110       disabled  110    --

192.1.0.10       192.1.0.7        evpn         operational          100001    enabled   --     DC

192.1.0.10       192.1.0.17       evpn         operational          101       disabled  101    --

192.1.0.10       192.1.0.17       evpn         operational          102       disabled  102    --

192.1.0.10       192.1.0.17       evpn         operational          103       disabled  103    --

192.1.0.10       192.1.0.17       evpn         operational          104       disabled  104    --

192.1.0.10       192.1.0.17       evpn         operational          105       disabled  105    --

192.1.0.10       192.1.0.17       evpn         operational          106       disabled  106    --

192.1.0.10       192.1.0.17       evpn         operational          107       disabled  107    --

192.1.0.10       192.1.0.17       evpn         operational          108       disabled  108    --

192.1.0.10       192.1.0.17       evpn         operational          109       disabled  109    --

192.1.0.10       192.1.0.17       evpn         operational          110       disabled  110    --

192.1.0.10       192.1.0.17       evpn         operational          100001    enabled   --     DC
```

Verify PIM neighbors

```
Leaf01-secondary# show ip pim neighbor all-vrfs

PIM Neighbor


VRF                         : DC
Total number of neighbors : 43

IP Address                  : 192.1.0.7
Interface                   : vni100001
Up Time (HH:MM:SS)          : 00:12:52
Expire Time (HH:MM:SS)      : 00:03:15
DR Priority                 : 1
Hold Time (HH:MM:SS)        : 00:03:30

IP Address                  : 192.1.0.17
Interface                   : vni100001
Up Time (HH:MM:SS)          : 00:12:15
Expire Time (HH:MM:SS)      : 00:03:15
DR Priority                 : 1
Hold Time (HH:MM:SS)        : 00:03:30

IP Address                  : 192.1.1.2
Interface                   : vlan101
Up Time (HH:MM:SS)          : 00:13:42
Expire Time (HH:MM:SS)      : 00:01:32
DR Priority                 : 167772608
Hold Time (HH:MM:SS)        : 00:01:45
Secondary IP Addresses :
 192.1.1.1

! snip
IP Address                  : 192.1.11.2
Interface                   : vlan111
Up Time (HH:MM:SS)          : 00:13:49
Expire Time (HH:MM:SS)      : 00:01:29
DR Priority                 : 167772608
Hold Time (HH:MM:SS)        : 00:01:45
Secondary IP Addresses :
 192.1.11.1
```

Verify PIM interfaces

```
Leaf01-secondary# show ip pim interface vlan 101

PIM Interfaces

VRF: DC

Interface  : vlan101
Neighbor count : 4
IP Address : 192.1.1.3/24
Mode       : sparse
Designated Router : 192.1.1.4
Proxy DR              : false
```

```
Hello Interval (sec)  : 30
Hello Delay (sec)     : 5
Override Interval (msec)  : 2500              Lan Prune Delay     : Yes

Propagation Delay (msec)  : 500               Configured DR Priority    : 1

Operational DR Priority   : 167772608
Neighbor Timeout          : 81


Leaf01-secondary# show ip pim interface vlan 101

PIM Interfaces

VRF: DC

Interface  : vlan101
Neighbor count : 4
IP Address : 192.1.1.3/24
Mode       : sparse
Designated Router : 192.1.1.4
Proxy DR              : false
Hello Interval (sec)  : 30
Hello Delay (sec)     : 5
Override Interval (msec)  : 2500              Lan Prune Delay     : Yes

Propagation Delay (msec)  : 500               Configured DR Priority    : 1

Operational DR Priority   : 167772608
Neighbor Timeout          : 79


Leaf01-secondary# show ip pim interface vlan 110

PIM Interfaces

VRF: DC

Interface  : vlan110
Neighbor count : 4
IP Address : 192.1.10.3/24
Mode       : sparse
Designated Router : 192.1.10.4
Proxy DR              : false
Hello Interval (sec)  : 30
Hello Delay (sec)     : 5
Override Interval (msec)  : 2500              Lan Prune Delay     : Yes

Propagation Delay (msec)  : 500               Configured DR Priority    : 1

Operational DR Priority   : 167772608
Neighbor Timeout          : 76


Leaf01-secondary# show ip pim interface vlan 111

PIM Interfaces

VRF: DC

Interface  : vlan111
Neighbor count : 1
```

```
IP Address : 192.1.11.3/24
Mode       : sparse
Designated Router : 192.1.11.3
Proxy DR              : false
Hello Interval (sec)  : 30
Hello Delay (sec)     : 5
Override Interval (msec)  : 2500              Lan Prune Delay     : Yes

Propagation Delay (msec)  : 500               Configured DR Priority    : 1

Operational DR Priority   : 167772608
Neighbor Timeout          : 104
```

Verify mroutes

```
Leaf01-secondary# show ip mroute all-vrfs
IP Multicast Route Entries

VRF : DC
Total number of entries : 39

Group Address           : 225.1.1.1
Source Address          : 192.1.1.11
Neighbor                :
Incoming interface      : vlan101

Group Address           : 225.1.2.1
Source Address          : 192.1.1.11
Neighbor                :
Incoming interface      : vlan102

Group Address           : 225.1.2.1
Source Address          : 192.1.1.11
Neighbor                :
Incoming interface      : vlan101

Group Address           : 225.1.3.1
Source Address          : 192.1.1.11
Neighbor                :
Incoming interface      : vlan101

Group Address           : 225.1.3.1
Source Address          : 192.1.1.11
Neighbor                :
Incoming interface      : vlan103
! snip

Group Address           : 239.1.1.1
Source Address          : 192.1.151.101
Neighbor                :
Incoming interface      : vlan101

Group Address           : 239.1.2.1
Source Address          : 192.1.151.101
Neighbor                :
Incoming interface      : vlan102

Group Address           : 239.1.3.1
Source Address          : 192.1.151.101
Neighbor                :
Incoming interface      : vlan103
```

```
Group Address           : 239.1.4.1
Source Address          : 192.1.151.101
Neighbor                :
Incoming interface      : vlan104

Group Address           : 239.1.5.1
Source Address          : 192.1.151.101
Neighbor                :
Incoming interface      : vlan105

Group Address           : 239.1.6.1
Source Address          : 192.1.151.101
Neighbor                :
Incoming interface      : vlan106

Group Address           : 239.1.7.1
Source Address          : 192.1.151.101
Neighbor                :
Incoming interface      : vlan107

Group Address           : 239.1.8.1
Source Address          : 192.1.151.101
Neighbor                :
Incoming interface      : vlan108

Group Address           : 239.1.9.1
Source Address          : 192.1.151.101
Neighbor                :
Incoming interface      : vlan109

Group Address           : 239.1.10.1
Source Address          : 192.1.151.101
Neighbor                :
Incoming interface      : vlan110
```

Verify BGP EVPN table

```
Leaf01-secondary# show bgp l2vpn evpn
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
              i internal, e external S Stale, R Removed, a additional-paths
Origin codes: i - IGP, e - EGP, ? - incomplete

EVPN Route-Type 2 prefix: [2]:[ESI]:[EthTag]:[MAC]:[OrigIP]
EVPN Route-Type 3 prefix: [3]:[EthTag]:[OrigIP]
EVPN Route-Type 5 prefix: [5]:[ESI]:[EthTag]:[IPAddrLen]:[IPAddr]
VRF : default
Local Router-ID 1.1.2.1

     Network                                          Nexthop         Metric     LocPrf    Weight   Path
-------------------------------------------------------------------------------------------------------------
Route Distinguisher: 192.1.0.10:101       (L2VNI 101)
*>  [2]:[0]:[0]:[00:11:01:00:00:01]:[192.1.1.11]          192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[00:11:01:00:00:01]:[192.1.1.11]          192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[00:11:01:00:00:01]:[192.1.1.11]          192.1.0.10      0          100        0       ?
*>  [2]:[0]:[0]:[00:11:01:00:00:01]:[]                    192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[00:11:01:00:00:01]:[]                    192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[00:11:01:00:00:01]:[]                    192.1.0.10      0          100        0       ?
*>  [2]:[0]:[0]:[00:12:01:00:00:01]:[192.1.1.12]          192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[00:12:01:00:00:01]:[192.1.1.12]          192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[00:12:01:00:00:01]:[192.1.1.12]          192.1.0.10      0          100        0       ?
```

```
*>  [2]:[0]:[0]:[00:12:01:00:00:01]:[]                    192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[00:12:01:00:00:01]:[]                    192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[00:12:01:00:00:01]:[]                    192.1.0.10      0          100        0       ?
*>  [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.1.1]          192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.1.1]          192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.1.1]          192.1.0.10      0          100        0       ?
*>  [2]:[0]:[0]:[b8:6a:97:21:e4:42]:[192.1.1.3]          192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[b8:6a:97:21:e9:42]:[192.1.1.2]          192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[b8:6a:97:21:e9:42]:[192.1.1.2]          192.1.0.10      0          100        0       ?
*>  [3]:[0]:[192.1.0.10]                                 192.1.0.10      0          100        0       ?
* i [3]:[0]:[192.1.0.10]                                 192.1.0.10      0          100        0       ?
* i [3]:[0]:[192.1.0.10]                                 192.1.0.10      0          100        0       ?

Route Distinguisher: 192.1.0.17:101       (L2VNI 101)
*>i [2]:[0]:[0]:[00:13:01:00:00:01]:[192.1.1.13]        192.1.0.17      0          100        0       ?
* i [2]:[0]:[0]:[00:13:01:00:00:01]:[192.1.1.13]        192.1.0.17      0          100        0       ?
*>i [2]:[0]:[0]:[00:13:01:00:00:01]:[]                  192.1.0.17      0          100        0       ?
* i [2]:[0]:[0]:[00:13:01:00:00:01]:[]                  192.1.0.17      0          100        0       ?
*>i [2]:[0]:[0]:[00:14:01:00:00:01]:[192.1.1.23]        192.1.0.17      0          100        0       ?
* i [2]:[0]:[0]:[00:14:01:00:00:01]:[192.1.1.23]        192.1.0.17      0          100        0       ?
*>i [2]:[0]:[0]:[00:14:01:00:00:01]:[]                  192.1.0.17      0          100        0       ?
* i [2]:[0]:[0]:[00:14:01:00:00:01]:[]                  192.1.0.17      0          100        0       ?
*>i [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.1.1]        192.1.0.17      0          100        0       ?
* i [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.1.1]        192.1.0.17      0          100        0       ?
*>i [2]:[0]:[0]:[54:80:28:3c:00:00]:[192.1.1.4]        192.1.0.17      0          100        0       ?
* i [2]:[0]:[0]:[54:80:28:3c:00:00]:[192.1.1.4]        192.1.0.17      0          100        0       ?
*>i [3]:[0]:[192.1.0.17]                               192.1.0.17      0          100        0       ?
* i [3]:[0]:[192.1.0.17]                               192.1.0.17      0          100        0       ?

Route Distinguisher: 192.1.0.7:101        (L2VNI 101)
*>i [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.1.1]        192.1.0.7       0          100        0       ?
* i [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.1.1]        192.1.0.7       0          100        0       ?
*>i [2]:[0]:[0]:[3c:2c:99:ff:da:a5]:[192.1.1.6]        192.1.0.7       0          100        0       ?
* i [2]:[0]:[0]:[3c:2c:99:ff:da:a5]:[192.1.1.6]        192.1.0.7       0          100        0       ?
*>i [2]:[0]:[0]:[b8:6a:97:21:f5:42]:[192.1.1.7]        192.1.0.7       0          100        0       ?
* i [2]:[0]:[0]:[b8:6a:97:21:f5:42]:[192.1.1.7]        192.1.0.7       0          100        0       ?
*>i [3]:[0]:[192.1.0.7]                                192.1.0.7       0          100        0       ?
* i [3]:[0]:[192.1.0.7]                                192.1.0.7       0          100        0       ?

Route Distinguisher: 192.1.0.10:102       (L2VNI 102)
*>  [2]:[0]:[0]:[00:11:01:00:00:02]:[192.1.2.11]       192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[00:11:01:00:00:02]:[192.1.2.11]       192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[00:11:01:00:00:02]:[192.1.2.11]       192.1.0.10      0          100        0       ?
*>  [2]:[0]:[0]:[00:11:01:00:00:02]:[]                 192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[00:11:01:00:00:02]:[]                 192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[00:11:01:00:00:02]:[]                 192.1.0.10      0          100        0       ?
*>  [2]:[0]:[0]:[00:12:01:00:00:02]:[192.1.2.12]       192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[00:12:01:00:00:02]:[192.1.2.12]       192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[00:12:01:00:00:02]:[192.1.2.12]       192.1.0.10      0          100        0       ?
*>  [2]:[0]:[0]:[00:12:01:00:00:02]:[]                 192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[00:12:01:00:00:02]:[]                 192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[00:12:01:00:00:02]:[]                 192.1.0.10      0          100        0       ?
*>  [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.2.1]        192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.2.1]        192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.2.1]        192.1.0.10      0          100        0       ?
*>  [2]:[0]:[0]:[b8:6a:97:21:e4:42]:[192.1.2.3]        192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[b8:6a:97:21:e9:42]:[192.1.2.2]        192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[b8:6a:97:21:e9:42]:[192.1.2.2]        192.1.0.10      0          100        0       ?
*>  [3]:[0]:[192.1.0.10]                               192.1.0.10      0          100        0       ?
* i [3]:[0]:[192.1.0.10]                               192.1.0.10      0          100        0       ?
* i [3]:[0]:[192.1.0.10]                               192.1.0.10      0          100        0       ?
```

```
!snip

Route Distinguisher: 192.1.0.7:109       (L3VNI 100001)
*>i [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.9.1]           192.1.0.7       0          100        0       ?
* i [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.9.1]           192.1.0.7       0          100        0       ?
*>i [2]:[0]:[0]:[3c:2c:99:ff:da:a5]:[192.1.9.6]           192.1.0.7       0          100        0       ?
* i [2]:[0]:[0]:[3c:2c:99:ff:da:a5]:[192.1.9.6]           192.1.0.7       0          100        0       ?
*>i [2]:[0]:[0]:[b8:6a:97:21:f5:42]:[192.1.9.7]           192.1.0.7       0          100        0       ?
* i [2]:[0]:[0]:[b8:6a:97:21:f5:42]:[192.1.9.7]           192.1.0.7       0          100        0       ?

Route Distinguisher: 192.1.0.7:110       (L3VNI 100001)
*>i [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.10.1]          192.1.0.7       0          100        0       ?
* i [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.10.1]          192.1.0.7       0          100        0       ?
*>i [2]:[0]:[0]:[3c:2c:99:ff:da:a5]:[192.1.10.6]          192.1.0.7       0          100        0       ?
* i [2]:[0]:[0]:[3c:2c:99:ff:da:a5]:[192.1.10.6]          192.1.0.7       0          100        0       ?
*>i [2]:[0]:[0]:[b8:6a:97:21:f5:42]:[192.1.10.7]          192.1.0.7       0          100        0       ?
* i [2]:[0]:[0]:[b8:6a:97:21:f5:42]:[192.1.10.7]          192.1.0.7       0          100        0       ?
Total number of entries 1084
```

Leaf02

Configuration

```
hostname Leaf02
profile Leaf
vrf DC
    rd 192.1.0.17:1
    route-target export 65501:1 evpn
    route-target import 65501:1 evpn
cli-session
    timeout 0
!
!
!
!
!
ssh server vrf mgmt
vlan 1
vlan 101
    ip igmp snooping enable
vlan 102
    ip igmp snooping enable
vlan 103
    ip igmp snooping enable
vlan 104
    ip igmp snooping enable
vlan 105
    ip igmp snooping enable
vlan 106
    ip igmp snooping enable
vlan 107
    ip igmp snooping enable
vlan 108
    ip igmp snooping enable
vlan 109
    ip igmp snooping enable
vlan 110
    ip igmp snooping enable
virtual-mac 00:00:00:0b:0b:0b
evpn
    redistribute local-svi
```

```
    vlan 101
        rd auto
        route-target export auto
        route-target import auto
        redistribute host-route
    vlan 102
        rd auto
        route-target export auto
        route-target import auto
        redistribute host-route
    vlan 103
        rd auto
        route-target export auto
        route-target import auto
        redistribute host-route
    vlan 104
        rd auto
        route-target export auto
        route-target import auto
        redistribute host-route
    vlan 105
        rd auto
        route-target export auto
        route-target import auto
        redistribute host-route
    vlan 106
        rd auto
        route-target export auto
        route-target import auto
        redistribute host-route
    vlan 107
        rd auto
        route-target export auto
        route-target import auto
        redistribute host-route
    vlan 108
        rd auto
        route-target export auto
        route-target import auto
        redistribute host-route
    vlan 109
        rd auto
        route-target export auto
        route-target import auto
        redistribute host-route
    vlan 110
        rd auto
        route-target export auto
        route-target import auto
        redistribute host-route
interface mgmt
    no shutdown
    ip dhcp
system interface-group 1 speed 10g
    !interface group 1 contains ports 1/1/1-1/1/12
system interface-group 2 speed 10g
    !interface group 2 contains ports 1/1/13-1/1/24
system interface-group 3 speed 10g
    !interface group 3 contains ports 1/1/25-1/1/36
system interface-group 4 speed 10g
    !interface group 4 contains ports 1/1/37-1/1/48
interface lag 1
```

```
    no shutdown
    no routing
    vlan access 1
    lacp mode active
interface 1/1/1
    no shutdown
    mtu 9198
    ip mtu 9198
    ip address 22.0.0.1/30
    ip ospf 1 area 0.0.0.0
interface 1/1/2
    no shutdown
    mtu 9198
    ip mtu 9198
    ip address 22.0.0.5/30
    ip ospf 1 area 0.0.0.0
interface 1/1/7
    no shutdown
    mtu 9198
    no routing
    vlan trunk native 1
    vlan trunk allowed 101-110
interface 1/1/9
    no shutdown
    no routing
    vlan trunk native 1
    vlan trunk allowed 101-110
interface loopback 0
    ip address 6.6.6.6/32
    ip ospf 1 area 0.0.0.0
interface loopback 1
    ip address 192.1.0.17/32
    ip ospf 1 area 0.0.0.0
interface vlan 101
    vrf attach DC
    ip address 192.1.1.4/24
    active-gateway ip mac 02:aa:bb:cc:00:01
    active-gateway ip 192.1.1.1
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 102
    vrf attach DC
    ip address 192.1.2.4/24
    active-gateway ip mac 02:aa:bb:cc:00:01
    active-gateway ip 192.1.2.1
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 103
    vrf attach DC
    ip address 192.1.3.4/24
    active-gateway ip mac 02:aa:bb:cc:00:01
    active-gateway ip 192.1.3.1
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 104
    vrf attach DC
```

```
    ip address 192.1.4.4/24
    active-gateway ip mac 02:aa:bb:cc:00:01
    active-gateway ip 192.1.4.1
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 105
    vrf attach DC
    ip address 192.1.5.4/24
    active-gateway ip mac 02:aa:bb:cc:00:01
    active-gateway ip 192.1.5.1
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 106
    vrf attach DC
    ip address 192.1.6.4/24
    active-gateway ip mac 02:aa:bb:cc:00:01
    active-gateway ip 192.1.6.1
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 107
    vrf attach DC
    ip address 192.1.7.4/24
    active-gateway ip mac 02:aa:bb:cc:00:01
    active-gateway ip 192.1.7.1
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 108
    vrf attach DC
    ip address 192.1.8.4/24
    active-gateway ip mac 02:aa:bb:cc:00:01
    active-gateway ip 192.1.8.1
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 109
    vrf attach DC
    ip address 192.1.9.4/24
    active-gateway ip mac 02:aa:bb:cc:00:01
    active-gateway ip 192.1.9.1
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 110
    vrf attach DC
    ip address 192.1.10.4/24
    active-gateway ip mac 02:aa:bb:cc:00:01
    active-gateway ip 192.1.10.1
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vxlan 1
```

```
    source ip 192.1.0.17
    no shutdown
    vni 101
        vlan 101
    vni 102
        vlan 102
    vni 103
        vlan 103
    vni 104
        vlan 104
    vni 105
        vlan 105
    vni 106
        vlan 106
    vni 107
        vlan 107
    vni 108
        vlan 108
    vni 109
        vlan 109
    vni 110
        vlan 110
    vni 100001
        vrf DC
        routing
!
!
!
!
!
router ospf 1
    router-id 6.6.6.6
    area 0.0.0.0
router bgp 1
    bgp router-id 6.6.6.6
    neighbor 4.4.4.4 remote-as 1
    neighbor 4.4.4.4 update-source loopback 0
    neighbor 5.5.5.5 remote-as 1
    neighbor 5.5.5.5 update-source loopback 0
    address-family l2vpn evpn
        neighbor 4.4.4.4 activate
        neighbor 4.4.4.4 send-community extended
        neighbor 5.5.5.5 activate
        neighbor 5.5.5.5 send-community extended
    exit-address-family
!
    vrf DC
        address-family ipv4 unicast
            redistribute connected
            redistribute static
        exit-address-family
!
router pim vrf DC
    enable
https-server vrf mgmt
```

Verification

Verify OSPF neighbors

```
Leaf02# show ip ospf neighbors all-vrfs
```

```
VRF : default                              Process : 1
================================================

Total Number of Neighbors : 2

Neighbor ID      Priority  State             Nbr Address       Interface
-------------------------------------------------------------------------
44.44.44.44      1         FULL/DR           22.0.0.2           1/1/1

45.45.45.45      1         FULL/DR           22.0.0.6           1/1/2
```

Verify BGP EVPN neighbors

```
Leaf02# show bgp l2vpn evpn summary
VRF : default
BGP Summary
-----------
 Local AS               : 1           BGP Router Identifier  : 6.6.6.6
 Peers                  : 2           Log Neighbor Changes   : No
 Cfg. Hold Time         : 180         Cfg. Keep Alive        : 60
 Confederation Id       : 0

 Neighbor        Remote-AS MsgRcvd MsgSent   Up/Down Time State        AdminStatus
 4.4.4.4         1           196     73      00h:13m:44s  Established   Up
 5.5.5.5         1           190     71      00h:13m:37s  Established   Up
```

Verify VXLAN tunnel, VTEP peers, and VNIs

```
Leaf02# show interface vxlan vteps
Source           Destination      Origin       Status               VNI       Routing   VLAN  VRF
---------------- ---------------- ------------ -------------------- --------- --------- ----- ---
--
192.1.0.17       192.1.0.7        evpn         operational          101       disabled  101    --

192.1.0.17       192.1.0.7        evpn         operational          102       disabled  102    --

192.1.0.17       192.1.0.7        evpn         operational          103       disabled  103    --

192.1.0.17       192.1.0.7        evpn         operational          104       disabled  104    --

192.1.0.17       192.1.0.7        evpn         operational          105       disabled  105    --

192.1.0.17       192.1.0.7        evpn         operational          106       disabled  106    --

192.1.0.17       192.1.0.7        evpn         operational          107       disabled  107    --

192.1.0.17       192.1.0.7        evpn         operational          108       disabled  108    --

192.1.0.17       192.1.0.7        evpn         operational          109       disabled  109    --

192.1.0.17       192.1.0.7        evpn         operational          110       disabled  110    --

192.1.0.17       192.1.0.7        evpn         operational          100001    enabled   --     DC

192.1.0.17       192.1.0.10       evpn         operational          101       disabled  101    --

192.1.0.17       192.1.0.10       evpn         operational          102       disabled  102    --
```

```
192.1.0.17      192.1.0.10      evpn        operational          103      disabled  103    --

192.1.0.17      192.1.0.10      evpn        operational          104      disabled  104    --

192.1.0.17      192.1.0.10      evpn        operational          105      disabled  105    --

192.1.0.17      192.1.0.10      evpn        operational          106      disabled  106    --

192.1.0.17      192.1.0.10      evpn        operational          107      disabled  107    --

192.1.0.17      192.1.0.10      evpn        operational          108      disabled  108    --

192.1.0.17      192.1.0.10      evpn        operational          109      disabled  109    --

192.1.0.17      192.1.0.10      evpn        operational          110      disabled  110    --

192.1.0.17      192.1.0.10      evpn        operational          100001   enabled   --     DC
```

Verify mroutes

```
Leaf02# show ip mroute all-vrfs
IP Multicast Route Entries

VRF : DC
Total number of entries : 20

Group Address           : 225.1.1.1
Source Address          : 192.1.1.11
Neighbor                :
Incoming interface      : vlan101

Group Address           : 225.1.2.1
Source Address          : 192.1.1.11
Neighbor                :
Incoming interface      : vlan101
Outgoing Interface List :
Interface       State
-----------     ----------
vlan102         forwarding

Group Address           : 225.1.3.1
Source Address          : 192.1.1.11
Neighbor                :
Incoming interface      : vlan101
Outgoing Interface List :
Interface       State
-----------     ----------
vlan103         forwarding

Group Address           : 225.1.4.1
Source Address          : 192.1.1.11
Neighbor                :
Incoming interface      : vlan101
Outgoing Interface List :
Interface       State
-----------     ----------
vlan104         forwarding

Group Address           : 225.1.5.1
Source Address          : 192.1.1.11
```

```
Neighbor                :
Incoming interface      : vlan101
Outgoing Interface List :
Interface       State
-----------     ----------
vlan105         forwarding
!snip

Group Address           : 239.1.8.1
Source Address          : 192.1.151.101
Neighbor                : 192.1.0.7
Incoming interface      : vni100001
Outgoing Interface List :
Interface       State
-----------     ----------
vlan108         forwarding

Group Address           : 239.1.9.1
Source Address          : 192.1.151.101
Neighbor                : 192.1.0.7
Incoming interface      : vni100001
Outgoing Interface List :
Interface       State
-----------     ----------
vlan109         forwarding

Group Address           : 239.1.10.1
Source Address          : 192.1.151.101
Neighbor                : 192.1.0.7
Incoming interface      : vni100001
Outgoing Interface List :
Interface       State
-----------     ----------
vlan110         forwarding
```

Verify PIM interfaces

```
Leaf02# show ip pim interface vlan 101

PIM Interfaces

VRF: DC

Interface  : vlan101
Neighbor count : 4
IP Address : 192.1.1.4/24
Mode       : sparse
Designated Router : 192.1.1.4
Proxy DR              : false
Hello Interval (sec)  : 30
Hello Delay (sec)     : 5
Override Interval (msec)  : 2500              Lan Prune Delay     : Yes

Propagation Delay (msec)  : 500               Configured DR Priority    : 1

Operational DR Priority   : 285213120
Neighbor Timeout          : 102



Leaf02# show ip pim interface vlan 102
```

```
PIM Interfaces

VRF: DC

Interface  : vlan102
Neighbor count : 4
IP Address : 192.1.2.4/24
Mode       : sparse
Designated Router : 192.1.2.4
Proxy DR              : false
Hello Interval (sec)  : 30
Hello Delay (sec)     : 5
Override Interval (msec)  : 2500              Lan Prune Delay     : Yes

Propagation Delay (msec)  : 500               Configured DR Priority    : 1

Operational DR Priority   : 285213120
Neighbor Timeout          : 102



Leaf02# show ip pim interface vlan 110

PIM Interfaces

VRF: DC

Interface  : vlan110
Neighbor count : 4
IP Address : 192.1.10.4/24
Mode       : sparse
Designated Router : 192.1.10.4
Proxy DR              : false
Hello Interval (sec)  : 30
Hello Delay (sec)     : 5
Override Interval (msec)  : 2500              Lan Prune Delay     : Yes

Propagation Delay (msec)  : 500               Configured DR Priority    : 1

Operational DR Priority   : 285213120
Neighbor Timeout          : 97
```

Verify BGP EVPN table

```
Leaf02# show bgp l2vpn evpn
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
              i internal, e external S Stale, R Removed, a additional-paths
Origin codes: i - IGP, e - EGP, ? - incomplete

EVPN Route-Type 2 prefix: [2]:[ESI]:[EthTag]:[MAC]:[OrigIP]
EVPN Route-Type 3 prefix: [3]:[EthTag]:[OrigIP]
EVPN Route-Type 5 prefix: [5]:[ESI]:[EthTag]:[IPAddrLen]:[IPAddr]
VRF : default
Local Router-ID 6.6.6.6

     Network                                          Nexthop         Metric     LocPrf    Weight   Path
-------------------------------------------------------------------------------------------------------------
Route Distinguisher: 192.1.0.10:101       (L2VNI 101)
*>i [2]:[0]:[0]:[00:11:01:00:00:01]:[192.1.1.11]          192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[00:11:01:00:00:01]:[192.1.1.11]          192.1.0.10      0          100        0       ?
```

```
*>i [2]:[0]:[0]:[00:11:01:00:00:01]:[]                    192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[00:11:01:00:00:01]:[]                    192.1.0.10      0          100        0       ?
*>i [2]:[0]:[0]:[00:12:01:00:00:01]:[192.1.1.12]          192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[00:12:01:00:00:01]:[192.1.1.12]          192.1.0.10      0          100        0       ?
*>i [2]:[0]:[0]:[00:12:01:00:00:01]:[]                    192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[00:12:01:00:00:01]:[]                    192.1.0.10      0          100        0       ?
*>i [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.1.1]           192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.1.1]           192.1.0.10      0          100        0       ?
*>i [2]:[0]:[0]:[b8:6a:97:21:e4:42]:[192.1.1.3]          192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[b8:6a:97:21:e4:42]:[192.1.1.3]          192.1.0.10      0          100        0       ?
*>i [2]:[0]:[0]:[b8:6a:97:21:e9:42]:[192.1.1.2]          192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[b8:6a:97:21:e9:42]:[192.1.1.2]          192.1.0.10      0          100        0       ?
*>i [3]:[0]:[192.1.0.10]                                 192.1.0.10      0          100        0       ?
* i [3]:[0]:[192.1.0.10]                                 192.1.0.10      0          100        0       ?

Route Distinguisher: 192.1.0.17:101       (L2VNI 101)
*>  [2]:[0]:[0]:[00:13:01:00:00:01]:[192.1.1.13]         192.1.0.17      0          100        0       ?
*>  [2]:[0]:[0]:[00:13:01:00:00:01]:[]                   192.1.0.17      0          100        0       ?
*>  [2]:[0]:[0]:[00:14:01:00:00:01]:[192.1.1.23]         192.1.0.17      0          100        0       ?
*>  [2]:[0]:[0]:[00:14:01:00:00:01]:[]                   192.1.0.17      0          100        0       ?
*>  [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.1.1]          192.1.0.17      0          100        0       ?
*>  [2]:[0]:[0]:[54:80:28:3c:00:00]:[192.1.1.4]          192.1.0.17      0          100        0       ?
*>  [3]:[0]:[192.1.0.17]                                 192.1.0.17      0          100        0       ?

Route Distinguisher: 192.1.0.7:101        (L2VNI 101)
*>i [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.1.1]          192.1.0.7       0          100        0       ?
* i [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.1.1]          192.1.0.7       0          100        0       ?
*>i [2]:[0]:[0]:[3c:2c:99:ff:da:a5]:[192.1.1.6]          192.1.0.7       0          100        0       ?
* i [2]:[0]:[0]:[3c:2c:99:ff:da:a5]:[192.1.1.6]          192.1.0.7       0          100        0       ?
*>i [2]:[0]:[0]:[b8:6a:97:21:f5:42]:[192.1.1.7]          192.1.0.7       0          100        0       ?
* i [2]:[0]:[0]:[b8:6a:97:21:f5:42]:[192.1.1.7]          192.1.0.7       0          100        0       ?
*>i [3]:[0]:[192.1.0.7]                                  192.1.0.7       0          100        0       ?
* i [3]:[0]:[192.1.0.7]                                  192.1.0.7       0          100        0       ?

Route Distinguisher: 192.1.0.10:102       (L2VNI 102)
*>i [2]:[0]:[0]:[00:11:01:00:00:02]:[]                   192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[00:11:01:00:00:02]:[]                   192.1.0.10      0          100        0       ?
*>i [2]:[0]:[0]:[00:12:01:00:00:02]:[192.1.2.12]         192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[00:12:01:00:00:02]:[192.1.2.12]         192.1.0.10      0          100        0       ?
*>i [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.2.1]          192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.2.1]          192.1.0.10      0          100        0       ?
*>i [2]:[0]:[0]:[b8:6a:97:21:e4:42]:[192.1.2.3]          192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[b8:6a:97:21:e4:42]:[192.1.2.3]          192.1.0.10      0          100        0       ?
*>i [2]:[0]:[0]:[b8:6a:97:21:e9:42]:[192.1.2.2]          192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[b8:6a:97:21:e9:42]:[192.1.2.2]          192.1.0.10      0          100        0       ?
*>i [3]:[0]:[192.1.0.10]                                 192.1.0.10      0          100        0       ?
* i [3]:[0]:[192.1.0.10]                                 192.1.0.10      0          100        0       ?

Route Distinguisher: 192.1.0.17:102       (L2VNI 102)
*>  [2]:[0]:[0]:[00:13:01:00:00:02]:[192.1.2.13]         192.1.0.17      0          100        0       ?
*>  [2]:[0]:[0]:[00:13:01:00:00:02]:[]                   192.1.0.17      0          100        0       ?
*>  [2]:[0]:[0]:[00:14:01:00:00:02]:[192.1.2.23]         192.1.0.17      0          100        0       ?
*>  [2]:[0]:[0]:[00:14:01:00:00:02]:[]                   192.1.0.17      0          100        0       ?
*>  [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.2.1]          192.1.0.17      0          100        0       ?
*>  [2]:[0]:[0]:[54:80:28:3c:00:00]:[192.1.2.4]          192.1.0.17      0          100        0       ?
*>  [3]:[0]:[192.1.0.17]                                 192.1.0.17      0          100        0       ?
!snip

Route Distinguisher: 192.1.0.7:107        (L3VNI 100001)
*>i [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.7.1]          192.1.0.7       0          100        0       ?
* i [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.7.1]          192.1.0.7       0          100        0       ?
*>i [2]:[0]:[0]:[3c:2c:99:ff:da:a5]:[192.1.7.6]          192.1.0.7       0          100        0       ?
```

```
* i [2]:[0]:[0]:[3c:2c:99:ff:da:a5]:[192.1.7.6]            192.1.0.7       0          100        0       ?
*>i [2]:[0]:[0]:[b8:6a:97:21:f5:42]:[192.1.7.7]           192.1.0.7       0          100        0       ?
* i [2]:[0]:[0]:[b8:6a:97:21:f5:42]:[192.1.7.7]           192.1.0.7       0          100        0       ?

Route Distinguisher: 192.1.0.7:108        (L3VNI 100001)
*>i [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.8.1]           192.1.0.7       0          100        0       ?
* i [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.8.1]           192.1.0.7       0          100        0       ?
*>i [2]:[0]:[0]:[3c:2c:99:ff:da:a5]:[192.1.8.6]           192.1.0.7       0          100        0       ?
* i [2]:[0]:[0]:[3c:2c:99:ff:da:a5]:[192.1.8.6]           192.1.0.7       0          100        0       ?
*>i [2]:[0]:[0]:[b8:6a:97:21:f5:42]:[192.1.8.7]           192.1.0.7       0          100        0       ?
* i [2]:[0]:[0]:[b8:6a:97:21:f5:42]:[192.1.8.7]           192.1.0.7       0          100        0       ?

Route Distinguisher: 192.1.0.7:109        (L3VNI 100001)
*>i [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.9.1]           192.1.0.7       0          100        0       ?
* i [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.9.1]           192.1.0.7       0          100        0       ?
*>i [2]:[0]:[0]:[3c:2c:99:ff:da:a5]:[192.1.9.6]           192.1.0.7       0          100        0       ?
* i [2]:[0]:[0]:[3c:2c:99:ff:da:a5]:[192.1.9.6]           192.1.0.7       0          100        0       ?
*>i [2]:[0]:[0]:[b8:6a:97:21:f5:42]:[192.1.9.7]           192.1.0.7       0          100        0       ?
* i [2]:[0]:[0]:[b8:6a:97:21:f5:42]:[192.1.9.7]           192.1.0.7       0          100        0       ?

Route Distinguisher: 192.1.0.7:110        (L3VNI 100001)
*>i [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.10.1]          192.1.0.7       0          100        0       ?
* i [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.10.1]          192.1.0.7       0          100        0       ?
*>i [2]:[0]:[0]:[3c:2c:99:ff:da:a5]:[192.1.10.6]          192.1.0.7       0          100        0       ?
* i [2]:[0]:[0]:[3c:2c:99:ff:da:a5]:[192.1.10.6]          192.1.0.7       0          100        0       ?
*>i [2]:[0]:[0]:[b8:6a:97:21:f5:42]:[192.1.10.7]          192.1.0.7       0          100        0       ?
* i [2]:[0]:[0]:[b8:6a:97:21:f5:42]:[192.1.10.7]          192.1.0.7       0          100        0       ?
Total number of entries 782
```

8325-border-prim

Configuration

```
!export-password: default
hostname 8325-border-prim
no ip icmp redirect
profile Leaf
vrf DC
    rd 192.1.0.7:1
    route-target export 65501:1 evpn
    route-target import 65501:1 evpn
cli-session
    timeout 0
!
!
!
!
!
ssh server vrf mgmt
vlan 1
vlan 101
    ip igmp snooping enable
vlan 102
    ip igmp snooping enable
vlan 103
    ip igmp snooping enable
vlan 104
    ip igmp snooping enable
vlan 105
    ip igmp snooping enable
vlan 106
```

```
    ip igmp snooping enable
vlan 107
    ip igmp snooping enable
vlan 108
    ip igmp snooping enable
vlan 109
    ip igmp snooping enable
vlan 110
    ip igmp snooping enable
vlan 500
virtual-mac 00:00:00:0c:0c:0c
evpn
    redistribute local-svi
    vlan 101
        rd auto
        route-target export auto
        route-target import auto
        redistribute host-route
    vlan 102
        rd auto
        route-target export auto
        route-target import auto
        redistribute host-route
    vlan 103
        rd auto
        route-target export auto
        route-target import auto
        redistribute host-route
    vlan 104
        rd auto
        route-target export auto
        route-target import auto
        redistribute host-route
    vlan 105
        rd auto
        route-target export auto
        route-target import auto
        redistribute host-route
    vlan 106
        rd auto
        route-target export auto
        route-target import auto
        redistribute host-route
    vlan 107
        rd auto
        route-target export auto
        route-target import auto
        redistribute host-route
    vlan 108
        rd auto
        route-target export auto
        route-target import auto
        redistribute host-route
    vlan 109
        rd auto
        route-target export auto
        route-target import auto
        redistribute host-route
    vlan 110
        rd auto
        route-target export auto
        route-target import auto
```

```
        redistribute host-route
interface mgmt
    no shutdown
    ip dhcp
system interface-group 1 speed 10g
    !interface group 1 contains ports 1/1/1-1/1/12
system interface-group 2 speed 10g
    !interface group 2 contains ports 1/1/13-1/1/24
system interface-group 3 speed 10g
    !interface group 3 contains ports 1/1/25-1/1/36
system interface-group 4 speed 10g
    !interface group 4 contains ports 1/1/37-1/1/48
interface lag 1
    no shutdown
    no routing
    vlan trunk native 1 tag
    vlan trunk allowed all
    lacp mode active
interface lag 2 multi-chassis
    no shutdown
    no routing
    vlan trunk native 1
    vlan trunk allowed 500
    lacp mode active
interface 1/1/1
    no shutdown
    mtu 9198
    ip mtu 9198
    ip address 24.0.0.1/30
    ip ospf 1 area 0.0.0.0
interface 1/1/2
    no shutdown
    mtu 9198
    ip mtu 9198
    ip address 24.0.0.5/30
    ip ospf 1 area 0.0.0.0
interface 1/1/4
    no shutdown
    mtu 9198
    lag 2
interface 1/1/6
    no shutdown
    mtu 9198
    lag 2
interface 1/1/14
    no shutdown
interface 1/1/49
    no shutdown
    mtu 9198
    lag 1
interface 1/1/55
    no shutdown
    mtu 9198
    ip mtu 9198
    ip address 192.168.3.1/30
interface loopback 0
    ip address 109.0.0.1/32
    ip ospf 1 area 0.0.0.0
interface loopback 1
    ip address 192.1.0.7/32
    ip ospf 1 area 0.0.0.0
interface loopback 2
```

```
    vrf attach DC
    ip address 192.1.0.18/32
    ip ospf 2 area 0.0.0.0
interface vlan 101
    vrf attach DC
    ip address 192.1.1.6/24
    active-gateway ip mac 02:aa:bb:cc:00:01
    active-gateway ip 192.1.1.1
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 102
    vrf attach DC
    ip address 192.1.2.6/24
    active-gateway ip mac 02:aa:bb:cc:00:01
    active-gateway ip 192.1.2.1
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 103
    vrf attach DC
    ip address 192.1.3.6/24
    active-gateway ip mac 02:aa:bb:cc:00:01
    active-gateway ip 192.1.3.1
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 104
    vrf attach DC
    ip address 192.1.4.6/24
    active-gateway ip mac 02:aa:bb:cc:00:01
    active-gateway ip 192.1.4.1
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 105
    vrf attach DC
    ip address 192.1.5.6/24
    active-gateway ip mac 02:aa:bb:cc:00:01
    active-gateway ip 192.1.5.1
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 106
    vrf attach DC
    ip address 192.1.6.6/24
    active-gateway ip mac 02:aa:bb:cc:00:01
    active-gateway ip 192.1.6.1
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 107
    vrf attach DC
    ip address 192.1.7.6/24
    active-gateway ip mac 02:aa:bb:cc:00:01
    active-gateway ip 192.1.7.1
```

```
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 108
    vrf attach DC
    ip address 192.1.8.6/24
    active-gateway ip mac 02:aa:bb:cc:00:01
    active-gateway ip 192.1.8.1
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 109
    vrf attach DC
    ip address 192.1.9.6/24
    active-gateway ip mac 02:aa:bb:cc:00:01
    active-gateway ip 192.1.9.1
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 110
    vrf attach DC
    ip address 192.1.10.6/24
    active-gateway ip mac 02:aa:bb:cc:00:01
    active-gateway ip 192.1.10.1
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 500
    vrf attach DC
    vsx active-forwarding
    ip address 192.1.0.53/29
    ip ospf 2 area 0.0.0.0
    ip ospf priority 100
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vxlan 1
    source ip 192.1.0.7
    no shutdown
    vni 101
        vlan 101
    vni 102
        vlan 102
    vni 103
        vlan 103
    vni 104
        vlan 104
    vni 105
        vlan 105
    vni 106
        vlan 106
    vni 107
        vlan 107
    vni 108
        vlan 108
    vni 109
        vlan 109
    vni 110
        vlan 110
```

```
    vni 100001
        vrf DC
        routing
vsx
    system-mac 00:00:00:0c:0c:0c
    inter-switch-link lag 1
    role primary
    keepalive peer 192.168.3.2 source 192.168.3.1
    no split-recovery
    vsx-sync evpn
!
!
!
!
!
router ospf 2 vrf DC
    router-id 192.1.0.18
    distance 210
    redistribute bgp
    redistribute connected
    area 0.0.0.0
router ospf 1
    router-id 9.9.9.9
    area 0.0.0.0
router bgp 1
    bgp router-id 109.0.0.1
    neighbor 4.4.4.4 remote-as 1
    neighbor 4.4.4.4 update-source loopback 0
    neighbor 5.5.5.5 remote-as 1
    neighbor 5.5.5.5 update-source loopback 0
    address-family l2vpn evpn
        neighbor 4.4.4.4 activate
        neighbor 4.4.4.4 send-community extended
        neighbor 5.5.5.5 activate
        neighbor 5.5.5.5 send-community extended
    exit-address-family
!
    vrf DC
        address-family ipv4 unicast
            redistribute connected
            redistribute ospf
        exit-address-family
!
router pim vrf DC
    enable
https-server vrf mgmt
```

Verification

Verify OSPF neighbors

```
8325-border-prim# show ip ospf neighbors all-vrfs
VRF : DC                                Process : 2
================================================

Total Number of Neighbors : 3

Neighbor ID      Priority  State             Nbr Address       Interface
-------------------------------------------------------------------------
192.1.0.1        1         FULL/DROther      192.1.0.49         vlan500
```

```
192.1.0.2        1         FULL/DROther      192.1.0.50         vlan500

192.1.10.7       200       FULL/DR           192.1.0.54         vlan500

VRF : default                            Process : 1
================================================

Total Number of Neighbors : 2

Neighbor ID      Priority  State             Nbr Address       Interface
-------------------------------------------------------------------------
44.44.44.44      1         FULL/DR           24.0.0.2           1/1/1

45.45.45.45      1         FULL/DR           24.0.0.6           1/1/2
```

Verify BGP EVPN neighbors

```
8325-border-prim# show bgp l2vpn evpn summary
VRF : default
BGP Summary
-----------
 Local AS               : 1            BGP Router Identifier  : 109.0.0.1
 Peers                  : 2            Log Neighbor Changes   : No
 Cfg. Hold Time         : 180          Cfg. Keep Alive        : 60
 Confederation Id       : 0

 Neighbor        Remote-AS MsgRcvd MsgSent   Up/Down Time State        AdminStatus
 4.4.4.4         1           303     62      00h:15m:22s  Established   Up
 5.5.5.5         1           300     62      00h:15m:22s  Established   Up
```

Verify VXLAN tunnel, VTEP peers, and VNIs

```
8325-border-prim# show interface vxlan vteps
Source           Destination      Origin       Status               VNI       Routing   VLAN  VRF
---------------- ---------------- ------------ -------------------- --------- --------- ----- ---
-
192.1.0.7        192.1.0.10       evpn         operational          101       disabled  101    --

192.1.0.7        192.1.0.10       evpn         operational          102       disabled  102    --

192.1.0.7        192.1.0.10       evpn         operational          103       disabled  103    --

192.1.0.7        192.1.0.10       evpn         operational          104       disabled  104    --

192.1.0.7        192.1.0.10       evpn         operational          105       disabled  105    --

192.1.0.7        192.1.0.10       evpn         operational          106       disabled  106    --

192.1.0.7        192.1.0.10       evpn         operational          107       disabled  107    --

192.1.0.7        192.1.0.10       evpn         operational          108       disabled  108    --

192.1.0.7        192.1.0.10       evpn         operational          109       disabled  109    --

192.1.0.7        192.1.0.10       evpn         operational          110       disabled  110    --

192.1.0.7        192.1.0.10       evpn         operational          100001    enabled   --     DC
```

```
192.1.0.7       192.1.0.17      evpn        operational         101       disabled  101    --

192.1.0.7       192.1.0.17      evpn        operational         102       disabled  102    --

192.1.0.7       192.1.0.17      evpn        operational         103       disabled  103    --

192.1.0.7       192.1.0.17      evpn        operational         104       disabled  104    --

192.1.0.7       192.1.0.17      evpn        operational         105       disabled  105    --

192.1.0.7       192.1.0.17      evpn        operational         106       disabled  106    --

192.1.0.7       192.1.0.17      evpn        operational         107       disabled  107    --

192.1.0.7       192.1.0.17      evpn        operational         108       disabled  108    --

192.1.0.7       192.1.0.17      evpn        operational         109       disabled  109    --

192.1.0.7       192.1.0.17      evpn        operational         110       disabled  110    --

192.1.0.7       192.1.0.17      evpn        operational         100001    enabled   --     DC
```

Verify PIM neighbors

```
8325-border-prim# show ip pim neighbor all-vrfs

PIM Neighbor


VRF                         : DC
Total number of neighbors : 45

IP Address                  : 192.1.0.10
Interface                   : vni100001
Up Time (HH:MM:SS)          : 00:14:44
Expire Time (HH:MM:SS)      : 00:03:24
DR Priority                 : 1
Hold Time (HH:MM:SS)        : 00:03:30

IP Address                  : 192.1.0.17
Interface                   : vni100001
Up Time (HH:MM:SS)          : 00:14:47
Expire Time (HH:MM:SS)      : 00:03:19
DR Priority                 : 1
Hold Time (HH:MM:SS)        : 00:03:30

IP Address                  : 192.1.0.49
Interface                   : vlan500
Up Time (HH:MM:SS)          : 00:14:38
Expire Time (HH:MM:SS)      : 00:01:37
DR Priority                 : 1
Hold Time (HH:MM:SS)        : 00:01:45

IP Address                  : 192.1.0.50
Interface                   : vlan500
Up Time (HH:MM:SS)          : 00:14:39
Expire Time (HH:MM:SS)      : 00:01:40
DR Priority                 : 1
Hold Time (HH:MM:SS)        : 00:01:45
```

```
IP Address                : 192.1.0.54
Interface                 : vlan500
Up Time (HH:MM:SS)        : 00:16:12
Expire Time (HH:MM:SS)    : 00:01:40
DR Priority               : 117440960
Hold Time (HH:MM:SS)      : 00:01:45
!snip

IP Address                : 192.1.10.7
Interface                 : vlan110
Up Time (HH:MM:SS)        : 00:16:13
Expire Time (HH:MM:SS)    : 00:01:37
DR Priority               : 117440960
Hold Time (HH:MM:SS)      : 00:01:45
Secondary IP Addresses :
 192.1.10.1
```

Verify PIM interfaces

```
8325-border-prim# show ip pim interface vlan 101

PIM Interfaces

VRF: DC

Interface  : vlan101
Neighbor count : 4
IP Address : 192.1.1.6/24
Mode       : sparse
Designated Router : 192.1.1.4
Proxy DR              : false
Hello Interval (sec)  : 30
Hello Delay (sec)     : 5
Override Interval (msec)  : 2500              Lan Prune Delay     : Yes

Propagation Delay (msec)  : 500               Configured DR Priority    : 1

Operational DR Priority   : 117440960
Neighbor Timeout          : 88


8325-border-prim# show ip pim interface vlan 102

PIM Interfaces

VRF: DC

Interface  : vlan102
Neighbor count : 4
IP Address : 192.1.2.6/24
Mode       : sparse
Designated Router : 192.1.2.4
Proxy DR              : false
Hello Interval (sec)  : 30
Hello Delay (sec)     : 5
Override Interval (msec)  : 2500              Lan Prune Delay     : Yes

Propagation Delay (msec)  : 500               Configured DR Priority    : 1

Operational DR Priority   : 117440960
Neighbor Timeout          : 88
```

```
8325-border-prim# show ip pim interface vlan 500

PIM Interfaces

VRF: DC

Interface  : vlan500
Neighbor count : 3
IP Address : 192.1.0.53/29
Mode       : sparse
Designated Router : 192.1.0.53
Proxy DR              : false
Hello Interval (sec)  : 30
Hello Delay (sec)     : 5
Override Interval (msec)  : 2500              Lan Prune Delay     : Yes

Propagation Delay (msec)  : 500               Configured DR Priority    : 1

Operational DR Priority   : 117440960
Neighbor Timeout          : 84



8325-border-prim# show ip pim interface vlan 110

PIM Interfaces

VRF: DC

Interface  : vlan110
Neighbor count : 4
IP Address : 192.1.10.6/24
Mode       : sparse
Designated Router : 192.1.10.4
Proxy DR              : false
Hello Interval (sec)  : 30
Hello Delay (sec)     : 5
Override Interval (msec)  : 2500              Lan Prune Delay     : Yes

Propagation Delay (msec)  : 500               Configured DR Priority    : 1

Operational DR Priority   : 117440960
Neighbor Timeout          : 80
```

Verify mroutes

```
8325-border-prim# show ip mroute all-vrfs
IP Multicast Route Entries

VRF : DC
Total number of entries : 54

Group Address           : 225.1.1.1
Source Address          : 192.1.1.11
Neighbor                :
Incoming interface      : vlan101
Outgoing Interface List :
Interface       State
-----------     ----------
```

```
vlan500         forwarding

Group Address           : 225.1.2.1
Source Address          : 192.1.1.11
Neighbor                :
Incoming interface      : vlan101
Outgoing Interface List :
Interface       State
-----------     ----------
vlan500         forwarding

Group Address           : 225.1.2.1
Source Address          : 192.1.1.11
Neighbor                :
Incoming interface      : vlan102

Group Address           : 225.1.3.1
Source Address          : 192.1.1.11
Neighbor                :
Incoming interface      : vlan101
Outgoing Interface List :
Interface       State
-----------     ----------
vlan500         forwarding
!snip

Group Address           : 239.1.6.1
Source Address          : 192.1.151.101
Neighbor                : 192.1.0.50
Incoming interface      : vlan106

Group Address           : 239.1.7.1
Source Address          : 192.1.151.101
Neighbor                : 192.1.0.50
Incoming interface      : vlan500
Outgoing Interface List :
Interface       State
-----------     ----------
vni100001       forwarding

Group Address           : 239.1.7.1
Source Address          : 192.1.151.101
Neighbor                :
Incoming interface      : vlan107

Group Address           : 239.1.8.1
Source Address          : 192.1.151.101
Neighbor                : 192.1.0.50
Incoming interface      : vlan500
Outgoing Interface List :
Interface       State
-----------     ----------
vni100001       forwarding

Group Address           : 239.1.8.1
Source Address          : 192.1.151.101
Neighbor                :
Incoming interface      : vlan108

Group Address           : 239.1.9.1
Source Address          : 192.1.151.101
Neighbor                :
```

```
Incoming interface      : vlan109

Group Address           : 239.1.9.1
Source Address          : 192.1.151.101
Neighbor                : 192.1.0.50
Incoming interface      : vlan500
Outgoing Interface List :
Interface       State
-----------     ----------
vni100001       forwarding

Group Address           : 239.1.10.1
Source Address          : 192.1.151.101
Neighbor                :
Incoming interface      : vlan110

Group Address           : 239.1.10.1
Source Address          : 192.1.151.101
Neighbor                : 192.1.0.50
Incoming interface      : vlan500
Outgoing Interface List :
Interface       State
-----------     ----------
vni100001       forwarding
```

Verify BGP EVPN table

```
8325-border-prim# show bgp l2vpn evpn
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
              i internal, e external S Stale, R Removed, a additional-paths
Origin codes: i - IGP, e - EGP, ? - incomplete

EVPN Route-Type 2 prefix: [2]:[ESI]:[EthTag]:[MAC]:[OrigIP]
EVPN Route-Type 3 prefix: [3]:[EthTag]:[OrigIP]
EVPN Route-Type 5 prefix: [5]:[ESI]:[EthTag]:[IPAddrLen]:[IPAddr]
VRF : default
Local Router-ID 109.0.0.1

     Network                                          Nexthop         Metric     LocPrf    Weight   Path
-------------------------------------------------------------------------------------------------------------
Route Distinguisher: 192.1.0.10:101       (L2VNI 101)
*>i [2]:[0]:[0]:[00:11:01:00:00:01]:[192.1.1.11]          192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[00:11:01:00:00:01]:[192.1.1.11]          192.1.0.10      0          100        0       ?
*>i [2]:[0]:[0]:[00:11:01:00:00:01]:[]                    192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[00:11:01:00:00:01]:[]                    192.1.0.10      0          100        0       ?
*>i [2]:[0]:[0]:[00:12:01:00:00:01]:[192.1.1.12]          192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[00:12:01:00:00:01]:[192.1.1.12]          192.1.0.10      0          100        0       ?
*>i [2]:[0]:[0]:[00:12:01:00:00:01]:[]                    192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[00:12:01:00:00:01]:[]                    192.1.0.10      0          100        0       ?
*>i [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.1.1]           192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.1.1]           192.1.0.10      0          100        0       ?
*>i [2]:[0]:[0]:[b8:6a:97:21:e4:42]:[192.1.1.3]           192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[b8:6a:97:21:e4:42]:[192.1.1.3]           192.1.0.10      0          100        0       ?
*>i [2]:[0]:[0]:[b8:6a:97:21:e9:42]:[192.1.1.2]           192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[b8:6a:97:21:e9:42]:[192.1.1.2]           192.1.0.10      0          100        0       ?
*>i [3]:[0]:[192.1.0.10]                                  192.1.0.10      0          100        0       ?
* i [3]:[0]:[192.1.0.10]                                  192.1.0.10      0          100        0       ?

Route Distinguisher: 192.1.0.17:101       (L2VNI 101)
*>i [2]:[0]:[0]:[00:13:01:00:00:01]:[192.1.1.13]          192.1.0.17      0          100        0       ?
* i [2]:[0]:[0]:[00:13:01:00:00:01]:[192.1.1.13]          192.1.0.17      0          100        0       ?
```

```
*>i [2]:[0]:[0]:[00:13:01:00:00:01]:[]                    192.1.0.17      0          100        0       ?
* i [2]:[0]:[0]:[00:13:01:00:00:01]:[]                    192.1.0.17      0          100        0       ?
*>i [2]:[0]:[0]:[00:14:01:00:00:01]:[192.1.1.23]         192.1.0.17      0          100        0       ?
* i [2]:[0]:[0]:[00:14:01:00:00:01]:[192.1.1.23]         192.1.0.17      0          100        0       ?
*>i [2]:[0]:[0]:[00:14:01:00:00:01]:[]                    192.1.0.17      0          100        0       ?
* i [2]:[0]:[0]:[00:14:01:00:00:01]:[]                    192.1.0.17      0          100        0       ?
*>i [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.1.1]          192.1.0.17      0          100        0       ?
* i [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.1.1]          192.1.0.17      0          100        0       ?
*>i [2]:[0]:[0]:[54:80:28:3c:00:00]:[192.1.1.4]          192.1.0.17      0          100        0       ?
* i [2]:[0]:[0]:[54:80:28:3c:00:00]:[192.1.1.4]          192.1.0.17      0          100        0       ?
*>i [3]:[0]:[192.1.0.17]                                 192.1.0.17      0          100        0       ?
* i [3]:[0]:[192.1.0.17]                                 192.1.0.17      0          100        0       ?

Route Distinguisher: 192.1.0.7:101        (L2VNI 101)
*>  [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.1.1]          192.1.0.7       0          100        0       ?
*>  [2]:[0]:[0]:[3c:2c:99:ff:da:a5]:[192.1.1.6]          192.1.0.7       0          100        0       ?
* i [2]:[0]:[0]:[b8:6a:97:21:f5:42]:[192.1.1.7]          192.1.0.7       0          100        0       ?
* i [2]:[0]:[0]:[b8:6a:97:21:f5:42]:[192.1.1.7]          192.1.0.7       0          100        0       ?
*>  [3]:[0]:[192.1.0.7]                                  192.1.0.7       0          100        0       ?

Route Distinguisher: 192.1.0.10:102       (L2VNI 102)
*>i [2]:[0]:[0]:[00:11:01:00:00:02]:[192.1.2.11]         192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[00:11:01:00:00:02]:[192.1.2.11]         192.1.0.10      0          100        0       ?
*>i [2]:[0]:[0]:[00:11:01:00:00:02]:[]                    192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[00:11:01:00:00:02]:[]                    192.1.0.10      0          100        0       ?
*>i [2]:[0]:[0]:[00:12:01:00:00:02]:[192.1.2.12]         192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[00:12:01:00:00:02]:[192.1.2.12]         192.1.0.10      0          100        0       ?
*>i [2]:[0]:[0]:[00:12:01:00:00:02]:[]                    192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[00:12:01:00:00:02]:[]                    192.1.0.10      0          100        0       ?
*>i [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.2.1]          192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.2.1]          192.1.0.10      0          100        0       ?
*>i [2]:[0]:[0]:[b8:6a:97:21:e4:42]:[192.1.2.3]          192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[b8:6a:97:21:e4:42]:[192.1.2.3]          192.1.0.10      0          100        0       ?
*>i [2]:[0]:[0]:[b8:6a:97:21:e9:42]:[192.1.2.2]          192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[b8:6a:97:21:e9:42]:[192.1.2.2]          192.1.0.10      0          100        0       ?
*>i [3]:[0]:[192.1.0.10]                                 192.1.0.10      0          100        0       ?
* i [3]:[0]:[192.1.0.10]                                 192.1.0.10      0          100        0       ?
!snip

Route Distinguisher: 192.1.0.7:106        (L3VNI 100001)
*>  [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.6.1]          192.1.0.7       0          100        0       ?
*>  [2]:[0]:[0]:[3c:2c:99:ff:da:a5]:[192.1.6.6]          192.1.0.7       0          100        0       ?
* i [2]:[0]:[0]:[b8:6a:97:21:f5:42]:[192.1.6.7]          192.1.0.7       0          100        0       ?
* i [2]:[0]:[0]:[b8:6a:97:21:f5:42]:[192.1.6.7]          192.1.0.7       0          100        0       ?

Route Distinguisher: 192.1.0.7:107        (L3VNI 100001)
*>  [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.7.1]          192.1.0.7       0          100        0       ?
*>  [2]:[0]:[0]:[3c:2c:99:ff:da:a5]:[192.1.7.6]          192.1.0.7       0          100        0       ?
* i [2]:[0]:[0]:[b8:6a:97:21:f5:42]:[192.1.7.7]          192.1.0.7       0          100        0       ?
* i [2]:[0]:[0]:[b8:6a:97:21:f5:42]:[192.1.7.7]          192.1.0.7       0          100        0       ?

Route Distinguisher: 192.1.0.7:108        (L3VNI 100001)
*>  [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.8.1]          192.1.0.7       0          100        0       ?
*>  [2]:[0]:[0]:[3c:2c:99:ff:da:a5]:[192.1.8.6]          192.1.0.7       0          100        0       ?
* i [2]:[0]:[0]:[b8:6a:97:21:f5:42]:[192.1.8.7]          192.1.0.7       0          100        0       ?
* i [2]:[0]:[0]:[b8:6a:97:21:f5:42]:[192.1.8.7]          192.1.0.7       0          100        0       ?

Route Distinguisher: 192.1.0.7:109        (L3VNI 100001)
*>  [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.9.1]          192.1.0.7       0          100        0       ?
*>  [2]:[0]:[0]:[3c:2c:99:ff:da:a5]:[192.1.9.6]          192.1.0.7       0          100        0       ?
* i [2]:[0]:[0]:[b8:6a:97:21:f5:42]:[192.1.9.7]          192.1.0.7       0          100        0       ?
* i [2]:[0]:[0]:[b8:6a:97:21:f5:42]:[192.1.9.7]          192.1.0.7       0          100        0       ?
```

```
Route Distinguisher: 192.1.0.7:110        (L3VNI 100001)
*>  [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.10.1]           192.1.0.7       0          100        0       ?
*>  [2]:[0]:[0]:[3c:2c:99:ff:da:a5]:[192.1.10.6]           192.1.0.7       0          100        0       ?
* i [2]:[0]:[0]:[b8:6a:97:21:f5:42]:[192.1.10.7]           192.1.0.7       0          100        0       ?
* i [2]:[0]:[0]:[b8:6a:97:21:f5:42]:[192.1.10.7]           192.1.0.7       0          100        0       ?
Total number of entries 825
```

8325-border-sec

Configuration

```
!export-password: default
hostname 8325-border-sec
no ip icmp redirect
profile Leaf
vrf DC
    rd 192.1.0.7:1
    route-target export 65501:1 evpn
    route-target import 65501:1 evpn
ntp server 10.100.0.12 minpoll 4 maxpoll 4 iburst
cli-session
    timeout 0
!
!
!
!
!
ssh server vrf mgmt
vlan 1
vlan 101
    ip igmp snooping enable
vlan 102
    ip igmp snooping enable
vlan 103
    ip igmp snooping enable
vlan 104
    ip igmp snooping enable
vlan 105
    ip igmp snooping enable
vlan 106
    ip igmp snooping enable
vlan 107
    ip igmp snooping enable
vlan 108
    ip igmp snooping enable
vlan 109
    ip igmp snooping enable
vlan 110
    ip igmp snooping enable
vlan 500
virtual-mac 00:00:00:0c:0c:0c
evpn
    redistribute local-svi
    vlan 101
        rd auto
        route-target export auto
        route-target import auto
        redistribute host-route
    vlan 102
        rd auto
```

```
        route-target export auto
        route-target import auto
        redistribute host-route
    vlan 103
        rd auto
        route-target export auto
        route-target import auto
        redistribute host-route
    vlan 104
        rd auto
        route-target export auto
        route-target import auto
        redistribute host-route
    vlan 105
        rd auto
        route-target export auto
        route-target import auto
        redistribute host-route
    vlan 106
        rd auto
        route-target export auto
        route-target import auto
        redistribute host-route
    vlan 107
        rd auto
        route-target export auto
        route-target import auto
        redistribute host-route
    vlan 108
        rd auto
        route-target export auto
        route-target import auto
        redistribute host-route
    vlan 109
        rd auto
        route-target export auto
        route-target import auto
        redistribute host-route
    vlan 110
        rd auto
        route-target export auto
        route-target import auto
        redistribute host-route
interface mgmt
    no shutdown
    ip dhcp
system interface-group 1 speed 10g
    !interface group 1 contains ports 1/1/1-1/1/12
system interface-group 2 speed 10g
    !interface group 2 contains ports 1/1/13-1/1/24
system interface-group 3 speed 10g
    !interface group 3 contains ports 1/1/25-1/1/36
system interface-group 4 speed 10g
    !interface group 4 contains ports 1/1/37-1/1/48
interface lag 1
    no shutdown
    no routing
    vlan trunk native 1 tag
    vlan trunk allowed all
    lacp mode active
interface lag 2 multi-chassis
    no shutdown
```

```
    no routing
    vlan trunk native 1
    vlan trunk allowed 500
    lacp mode active
interface 1/1/1
    no shutdown
    mtu 9198
    ip mtu 9198
    ip address 25.0.0.1/30
    ip ospf 1 area 0.0.0.0
interface 1/1/2
    no shutdown
    mtu 9198
    ip mtu 9198
    ip address 25.0.0.5/30
    ip ospf 1 area 0.0.0.0
interface 1/1/13
    no shutdown
    mtu 9198
    lag 2
interface 1/1/25
    no shutdown
    lag 2
interface 1/1/49
    no shutdown
    mtu 9198
    lag 1
interface 1/1/56
    no shutdown
    mtu 9198
    ip mtu 9198
    ip address 192.168.3.2/30
interface loopback 0
    ip address 110.0.0.1/32
    ip ospf 1 area 0.0.0.0
interface loopback 1
    ip address 192.1.0.7/32
    ip ospf 1 area 0.0.0.0
interface vlan 101
    vrf attach DC
    ip address 192.1.1.7/24
    active-gateway ip mac 02:aa:bb:cc:00:01
    active-gateway ip 192.1.1.1
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 102
    vrf attach DC
    ip address 192.1.2.7/24
    active-gateway ip mac 02:aa:bb:cc:00:01
    active-gateway ip 192.1.2.1
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 103
    vrf attach DC
    ip address 192.1.3.7/24
    active-gateway ip mac 02:aa:bb:cc:00:01
    active-gateway ip 192.1.3.1
    ip igmp enable
```

```
    ip igmp version 2
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 104
    vrf attach DC
    ip address 192.1.4.7/24
    active-gateway ip mac 02:aa:bb:cc:00:01
    active-gateway ip 192.1.4.1
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 105
    vrf attach DC
    ip address 192.1.5.7/24
    active-gateway ip mac 02:aa:bb:cc:00:01
    active-gateway ip 192.1.5.1
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 106
    vrf attach DC
    ip address 192.1.6.7/24
    active-gateway ip mac 02:aa:bb:cc:00:01
    active-gateway ip 192.1.6.1
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 107
    vrf attach DC
    ip address 192.1.7.7/24
    active-gateway ip mac 02:aa:bb:cc:00:01
    active-gateway ip 192.1.7.1
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 108
    vrf attach DC
    ip address 192.1.8.7/24
    active-gateway ip mac 02:aa:bb:cc:00:01
    active-gateway ip 192.1.8.1
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 109
    vrf attach DC
    ip address 192.1.9.7/24
    active-gateway ip mac 02:aa:bb:cc:00:01
    active-gateway ip 192.1.9.1
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 110
    vrf attach DC
    ip address 192.1.10.7/24
    active-gateway ip mac 02:aa:bb:cc:00:01
    active-gateway ip 192.1.10.1
```

```
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vlan 500
    vrf attach DC
    vsx active-forwarding
    ip address 192.1.0.54/29
    ip ospf 2 area 0.0.0.0
    ip ospf priority 200
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor
interface vxlan 1
    source ip 192.1.0.7
    no shutdown
    vni 101
        vlan 101
    vni 102
        vlan 102
    vni 103
        vlan 103
    vni 104
        vlan 104
    vni 105
        vlan 105
    vni 106
        vlan 106
    vni 107
        vlan 107
    vni 108
        vlan 108
    vni 109
        vlan 109
    vni 110
        vlan 110
    vni 100001
        vrf DC
        routing
vsx
    system-mac 00:00:00:0c:0c:0c
    inter-switch-link lag 1
    role secondary
    keepalive peer 192.168.3.1 source 192.168.3.2
    no split-recovery
    vsx-sync evpn
!
!
!
!
!
router ospf 2 vrf DC
    distance 210
    redistribute bgp
    redistribute connected
    area 0.0.0.0
router ospf 1
    router-id 99.99.99.99
    area 0.0.0.0
router bgp 1
    bgp router-id 110.0.0.1
    neighbor 4.4.4.4 remote-as 1
    neighbor 4.4.4.4 update-source loopback 0
```

```
    neighbor 5.5.5.5 remote-as 1
    neighbor 5.5.5.5 update-source loopback 0
    address-family l2vpn evpn
        neighbor 4.4.4.4 activate
        neighbor 4.4.4.4 send-community extended
        neighbor 5.5.5.5 activate
        neighbor 5.5.5.5 send-community extended
    exit-address-family
!
    vrf DC
        address-family ipv4 unicast
            redistribute connected
            redistribute ospf
        exit-address-family
!
router pim vrf DC
    enable
https-server vrf mgmt.
```

Verification

Verify OSPF neighbors

```
8325-border-sec# show ip ospf neighbors all-vrfs
VRF : DC                                  Process : 2
================================================

Total Number of Neighbors : 3

Neighbor ID      Priority  State             Nbr Address       Interface
-------------------------------------------------------------------------
192.1.0.1        1         FULL/DROther      192.1.0.49         vlan500

192.1.0.2        1         FULL/DROther      192.1.0.50         vlan500

192.1.0.18       100       FULL/BDR          192.1.0.53         vlan500

VRF : default                             Process : 1
================================================

Total Number of Neighbors : 2

Neighbor ID      Priority  State             Nbr Address       Interface
-------------------------------------------------------------------------
44.44.44.44      1         FULL/BDR          25.0.0.2           1/1/1

45.45.45.45      1         FULL/BDR          25.0.0.6           1/1/2
```

Verify BGP EVPN neighbors

```
8325-border-sec#  show bgp l2vpn evpn summary
VRF : default
BGP Summary
-----------
 Local AS               : 1           BGP Router Identifier  : 110.0.0.1
 Peers                  : 2           Log Neighbor Changes   : No
 Cfg. Hold Time         : 180         Cfg. Keep Alive        : 60
 Confederation Id       : 0
```

```
 Neighbor        Remote-AS MsgRcvd MsgSent   Up/Down Time State        AdminStatus
 4.4.4.4         1         310     64        00h:16m:33s  Established   Up
 5.5.5.5         1         308     63        00h:16m:30s  Established   Up
```

Verify VXLAN tunnel, VTEP peers, and VNIs

```
8325-border-sec# show interface vxlan vteps
Source           Destination      Origin       Status               VNI       Routing   VLAN  VRF
---------------- ---------------- ------------ -------------------- --------- --------- ----- ---
-
192.1.0.7        192.1.0.10       evpn         operational          101       disabled  101    --
192.1.0.7        192.1.0.10       evpn         operational          102       disabled  102    --
192.1.0.7        192.1.0.10       evpn         operational          103       disabled  103    --
192.1.0.7        192.1.0.10       evpn         operational          104       disabled  104    --
192.1.0.7        192.1.0.10       evpn         operational          105       disabled  105    --
192.1.0.7        192.1.0.10       evpn         operational          106       disabled  106    --
192.1.0.7        192.1.0.10       evpn         operational          107       disabled  107    --
192.1.0.7        192.1.0.10       evpn         operational          108       disabled  108    --
192.1.0.7        192.1.0.10       evpn         operational          109       disabled  109    --
192.1.0.7        192.1.0.10       evpn         operational          110       disabled  110    --
192.1.0.7        192.1.0.10       evpn         operational          100001    enabled   --     DC
192.1.0.7        192.1.0.17       evpn         operational          101       disabled  101    --
192.1.0.7        192.1.0.17       evpn         operational          102       disabled  102    --
192.1.0.7        192.1.0.17       evpn         operational          103       disabled  103    --
192.1.0.7        192.1.0.17       evpn         operational          104       disabled  104    --
192.1.0.7        192.1.0.17       evpn         operational          105       disabled  105    --
192.1.0.7        192.1.0.17       evpn         operational          106       disabled  106    --
192.1.0.7        192.1.0.17       evpn         operational          107       disabled  107    --
192.1.0.7        192.1.0.17       evpn         operational          108       disabled  108    --
192.1.0.7        192.1.0.17       evpn         operational          109       disabled  109    --
192.1.0.7        192.1.0.17       evpn         operational          110       disabled  110    --
192.1.0.7        192.1.0.17       evpn         operational          100001    enabled   --     DC
```

Verify PIM neighbors

```
8325-border-sec# show ip pim neighbor all-vrfs
```

```
PIM Neighbor


VRF                         : DC
Total number of neighbors : 45

IP Address                  : 192.1.0.10
Interface                   : vni100001
Up Time (HH:MM:SS)          : 00:15:58
Expire Time (HH:MM:SS)      : 00:03:10
DR Priority                 : 1
Hold Time (HH:MM:SS)        : 00:03:30

IP Address                  : 192.1.0.17
Interface                   : vni100001
Up Time (HH:MM:SS)          : 00:16:01
Expire Time (HH:MM:SS)      : 00:03:05
DR Priority                 : 1
Hold Time (HH:MM:SS)        : 00:03:30

IP Address                  : 192.1.0.49
Interface                   : vlan500
Up Time (HH:MM:SS)          : 00:15:52
Expire Time (HH:MM:SS)      : 00:01:23
DR Priority                 : 1
Hold Time (HH:MM:SS)        : 00:01:45

IP Address                  : 192.1.0.50
Interface                   : vlan500
Up Time (HH:MM:SS)          : 00:15:54
Expire Time (HH:MM:SS)      : 00:01:26
DR Priority                 : 1
Hold Time (HH:MM:SS)        : 00:01:45
!snip

IP Address                  : 192.1.10.3
Interface                   : vlan110
Up Time (HH:MM:SS)          : 00:15:56
Expire Time (HH:MM:SS)      : 00:01:25
DR Priority                 : 167772608
Hold Time (HH:MM:SS)        : 00:01:45

IP Address                  : 192.1.10.4
Interface                   : vlan110
Up Time (HH:MM:SS)          : 00:15:58
Expire Time (HH:MM:SS)      : 00:01:21
DR Priority                 : 285213120
Hold Time (HH:MM:SS)        : 00:01:45

IP Address                  : 192.1.10.6
Interface                   : vlan110
Up Time (HH:MM:SS)          : 00:17:30
Expire Time (HH:MM:SS)      : 00:01:24
DR Priority                 : 117440960
Hold Time (HH:MM:SS)        : 00:01:45
Secondary IP Addresses :
 192.1.10.1
```

Verify mroutes

```
8325-border-sec# show ip mroute all-vrfs
IP Multicast Route Entries

VRF : DC
Total number of entries : 64

Group Address           : 225.1.1.1
Source Address          : 192.1.1.11
Neighbor                :
Incoming interface      : vlan500

Group Address           : 225.1.1.1
Source Address          : 192.1.1.11
Neighbor                :
Incoming interface      : vlan101
Outgoing Interface List :
Interface       State
-----------     ----------
vlan500         forwarding

Group Address           : 225.1.2.1
Source Address          : 192.1.1.11
Neighbor                :
Incoming interface      : vlan500

Group Address           : 225.1.2.1
Source Address          : 192.1.1.11
Neighbor                :
Incoming interface      : vlan101
Outgoing Interface List :
Interface       State
-----------     ----------
vlan500         forwarding

Group Address           : 225.1.2.1
Source Address          : 192.1.1.11
Neighbor                :
Incoming interface      : vlan102

Group Address           : 225.1.3.1
Source Address          : 192.1.1.11
Neighbor                :
Incoming interface      : vlan500

Group Address           : 225.1.3.1
Source Address          : 192.1.1.11
Neighbor                :
Incoming interface      : vlan101
Outgoing Interface List :
Interface       State
-----------     ----------
vlan500         forwarding

Group Address           : 225.1.3.1
Source Address          : 192.1.1.11
Neighbor                :
Incoming interface      : vlan103

Group Address           : 225.1.4.1
Source Address          : 192.1.1.11
Neighbor                :
Incoming interface      : vlan101
```

```
Outgoing Interface List :
Interface       State
-----------     ----------
vlan500         forwarding
!snip

Group Address           : 239.1.8.1
Source Address          : 192.1.151.101
Neighbor                : 192.1.0.50
Incoming interface      : vlan108

Group Address           : 239.1.9.1
Source Address          : 192.1.151.101
Neighbor                : 192.1.0.50
Incoming interface      : vlan500
Outgoing Interface List :
Interface       State
-----------     ----------
vni100001       forwarding

Group Address           : 239.1.9.1
Source Address          : 192.1.151.101
Neighbor                : 192.1.0.50
Incoming interface      : vlan109

Group Address           : 239.1.10.1
Source Address          : 192.1.151.101
Neighbor                : 192.1.0.50
Incoming interface      : vlan500
Outgoing Interface List :
Interface       State
-----------     ----------
vni100001       forwarding

Group Address           : 239.1.10.1
Source Address          : 192.1.151.101
Neighbor                : 192.1.0.50
Incoming interface      : vlan110
```

Verify PIM interfaces

```
8325-border-sec# show ip pim interface vlan 101

PIM Interfaces

VRF: DC

Interface  : vlan101
Neighbor count : 4
IP Address : 192.1.1.7/24
Mode       : sparse
Designated Router : 192.1.1.4
Proxy DR              : false
Hello Interval (sec)  : 30
Hello Delay (sec)     : 5
Override Interval (msec)  : 2500             Lan Prune Delay     : Yes

Propagation Delay (msec)  : 500              Configured DR Priority    : 1

Operational DR Priority   : 117440960
Neighbor Timeout          : 97
```

```
8325-border-sec# show ip pim interface vlan 102

PIM Interfaces

VRF: DC

Interface  : vlan102
Neighbor count : 4
IP Address : 192.1.2.7/24
Mode       : sparse
Designated Router : 192.1.2.4
Proxy DR              : false
Hello Interval (sec)  : 30
Hello Delay (sec)     : 5
Override Interval (msec)  : 2500              Lan Prune Delay     : Yes

Propagation Delay (msec)  : 500               Configured DR Priority    : 1

Operational DR Priority   : 117440960
Neighbor Timeout          : 97



8325-border-sec# show ip pim interface vlan 110

PIM Interfaces

VRF: DC

Interface  : vlan110
Neighbor count : 4
IP Address : 192.1.10.7/24
Mode       : sparse
Designated Router : 192.1.10.4
Proxy DR              : false
Hello Interval (sec)  : 30
Hello Delay (sec)     : 5
Override Interval (msec)  : 2500              Lan Prune Delay     : Yes

Propagation Delay (msec)  : 500               Configured DR Priority    : 1

Operational DR Priority   : 117440960
Neighbor Timeout          : 95



8325-border-sec# show ip pim interface vlan 500

PIM Interfaces

VRF: DC

Interface  : vlan500
Neighbor count : 3
IP Address : 192.1.0.54/29
Mode       : sparse
Designated Router : 192.1.0.54
Proxy DR              : false
Hello Interval (sec)  : 30
```

```
Hello Delay (sec)      : 5
Override Interval (msec)  : 2500              Lan Prune Delay     : Yes

Propagation Delay (msec)  : 500               Configured DR Priority    : 1

Operational DR Priority   : 117440960
Neighbor Timeout          : 93
```

Verify BGP EVPN table

```
8325-border-sec# show bgp l2vpn evpn
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
              i internal, e external S Stale, R Removed, a additional-paths
Origin codes: i - IGP, e - EGP, ? - incomplete

EVPN Route-Type 2 prefix: [2]:[ESI]:[EthTag]:[MAC]:[OrigIP]
EVPN Route-Type 3 prefix: [3]:[EthTag]:[OrigIP]
EVPN Route-Type 5 prefix: [5]:[ESI]:[EthTag]:[IPAddrLen]:[IPAddr]
VRF : default
Local Router-ID 110.0.0.1

     Network                                          Nexthop         Metric     LocPrf    Weight   Path
-------------------------------------------------------------------------------------------------------------
Route Distinguisher: 192.1.0.10:101       (L2VNI 101)
*>i [2]:[0]:[0]:[00:11:01:00:00:01]:[192.1.1.11]          192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[00:11:01:00:00:01]:[192.1.1.11]          192.1.0.10      0          100        0       ?
*>i [2]:[0]:[0]:[00:11:01:00:00:01]:[]                    192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[00:11:01:00:00:01]:[]                    192.1.0.10      0          100        0       ?
*>i [2]:[0]:[0]:[00:12:01:00:00:01]:[192.1.1.12]          192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[00:12:01:00:00:01]:[192.1.1.12]          192.1.0.10      0          100        0       ?
*>i [2]:[0]:[0]:[00:12:01:00:00:01]:[]                    192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[00:12:01:00:00:01]:[]                    192.1.0.10      0          100        0       ?
*>i [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.1.1]           192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.1.1]           192.1.0.10      0          100        0       ?
*>i [2]:[0]:[0]:[b8:6a:97:21:e4:42]:[192.1.1.3]          192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[b8:6a:97:21:e4:42]:[192.1.1.3]          192.1.0.10      0          100        0       ?
*>i [2]:[0]:[0]:[b8:6a:97:21:e9:42]:[192.1.1.2]          192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[b8:6a:97:21:e9:42]:[192.1.1.2]          192.1.0.10      0          100        0       ?
*>i [3]:[0]:[192.1.0.10]                                 192.1.0.10      0          100        0       ?
* i [3]:[0]:[192.1.0.10]                                 192.1.0.10      0          100        0       ?

Route Distinguisher: 192.1.0.17:101       (L2VNI 101)
*>i [2]:[0]:[0]:[00:13:01:00:00:01]:[192.1.1.13]          192.1.0.17      0          100        0       ?
* i [2]:[0]:[0]:[00:13:01:00:00:01]:[192.1.1.13]          192.1.0.17      0          100        0       ?
*>i [2]:[0]:[0]:[00:13:01:00:00:01]:[]                    192.1.0.17      0          100        0       ?
* i [2]:[0]:[0]:[00:13:01:00:00:01]:[]                    192.1.0.17      0          100        0       ?
*>i [2]:[0]:[0]:[00:14:01:00:00:01]:[192.1.1.23]          192.1.0.17      0          100        0       ?
* i [2]:[0]:[0]:[00:14:01:00:00:01]:[192.1.1.23]          192.1.0.17      0          100        0       ?
*>i [2]:[0]:[0]:[00:14:01:00:00:01]:[]                    192.1.0.17      0          100        0       ?
* i [2]:[0]:[0]:[00:14:01:00:00:01]:[]                    192.1.0.17      0          100        0       ?
*>i [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.1.1]           192.1.0.17      0          100        0       ?
* i [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.1.1]           192.1.0.17      0          100        0       ?
*>i [2]:[0]:[0]:[54:80:28:3c:00:00]:[192.1.1.4]          192.1.0.17      0          100        0       ?
* i [2]:[0]:[0]:[54:80:28:3c:00:00]:[192.1.1.4]          192.1.0.17      0          100        0       ?
*>i [3]:[0]:[192.1.0.17]                                 192.1.0.17      0          100        0       ?
* i [3]:[0]:[192.1.0.17]                                 192.1.0.17      0          100        0       ?

Route Distinguisher: 192.1.0.7:101        (L2VNI 101)
*>  [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.1.1]          192.1.0.7       0          100        0       ?
* i [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.1.1]          192.1.0.7       0          100        0       ?
* i [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.1.1]          192.1.0.7       0          100        0       ?
```

```
* i [2]:[0]:[0]:[3c:2c:99:ff:da:a5]:[192.1.1.6]            192.1.0.7       0          100        0       ?
* i [2]:[0]:[0]:[3c:2c:99:ff:da:a5]:[192.1.1.6]            192.1.0.7       0          100        0       ?
*>  [2]:[0]:[0]:[b8:6a:97:21:f5:42]:[192.1.1.7]            192.1.0.7       0          100        0       ?
*>  [3]:[0]:[192.1.0.7]                                    192.1.0.7       0          100        0       ?
* i [3]:[0]:[192.1.0.7]                                    192.1.0.7       0          100        0       ?
* i [3]:[0]:[192.1.0.7]                                    192.1.0.7       0          100        0       ?

Route Distinguisher: 192.1.0.10:102       (L2VNI 102)
*>i [2]:[0]:[0]:[00:11:01:00:00:02]:[192.1.2.11]          192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[00:11:01:00:00:02]:[192.1.2.11]          192.1.0.10      0          100        0       ?
*>i [2]:[0]:[0]:[00:11:01:00:00:02]:[]                    192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[00:11:01:00:00:02]:[]                    192.1.0.10      0          100        0       ?
*>i [2]:[0]:[0]:[00:12:01:00:00:02]:[192.1.2.12]          192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[00:12:01:00:00:02]:[192.1.2.12]          192.1.0.10      0          100        0       ?
*>i [2]:[0]:[0]:[00:12:01:00:00:02]:[]                    192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[00:12:01:00:00:02]:[]                    192.1.0.10      0          100        0       ?
*>i [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.2.1]           192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.2.1]           192.1.0.10      0          100        0       ?
*>i [2]:[0]:[0]:[b8:6a:97:21:e4:42]:[192.1.2.3]          192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[b8:6a:97:21:e4:42]:[192.1.2.3]          192.1.0.10      0          100        0       ?
*>i [2]:[0]:[0]:[b8:6a:97:21:e9:42]:[192.1.2.2]          192.1.0.10      0          100        0       ?
* i [2]:[0]:[0]:[b8:6a:97:21:e9:42]:[192.1.2.2]          192.1.0.10      0          100        0       ?
*>i [3]:[0]:[192.1.0.10]                                 192.1.0.10      0          100        0       ?
* i [3]:[0]:[192.1.0.10]                                 192.1.0.10      0          100        0       ?
!snip       ?

Route Distinguisher: 192.1.0.7:108        (L3VNI 100001)
*>  [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.8.1]           192.1.0.7       0          100        0       ?
* i [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.8.1]           192.1.0.7       0          100        0       ?
* i [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.8.1]           192.1.0.7       0          100        0       ?
* i [2]:[0]:[0]:[3c:2c:99:ff:da:a5]:[192.1.8.6]           192.1.0.7       0          100        0       ?
* i [2]:[0]:[0]:[3c:2c:99:ff:da:a5]:[192.1.8.6]           192.1.0.7       0          100        0       ?
*>  [2]:[0]:[0]:[b8:6a:97:21:f5:42]:[192.1.8.7]           192.1.0.7       0          100        0       ?

Route Distinguisher: 192.1.0.7:109        (L3VNI 100001)
*>  [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.9.1]           192.1.0.7       0          100        0       ?
* i [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.9.1]           192.1.0.7       0          100        0       ?
* i [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.9.1]           192.1.0.7       0          100        0       ?
* i [2]:[0]:[0]:[3c:2c:99:ff:da:a5]:[192.1.9.6]           192.1.0.7       0          100        0       ?
* i [2]:[0]:[0]:[3c:2c:99:ff:da:a5]:[192.1.9.6]           192.1.0.7       0          100        0       ?
*>  [2]:[0]:[0]:[b8:6a:97:21:f5:42]:[192.1.9.7]           192.1.0.7       0          100        0       ?

Route Distinguisher: 192.1.0.7:110        (L3VNI 100001)
*>  [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.10.1]          192.1.0.7       0          100        0       ?
* i [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.10.1]          192.1.0.7       0          100        0       ?
* i [2]:[0]:[0]:[02:aa:bb:cc:00:01]:[192.1.10.1]          192.1.0.7       0          100        0       ?
* i [2]:[0]:[0]:[3c:2c:99:ff:da:a5]:[192.1.10.6]          192.1.0.7       0          100        0       ?
* i [2]:[0]:[0]:[3c:2c:99:ff:da:a5]:[192.1.10.6]          192.1.0.7       0          100        0       ?
*>  [2]:[0]:[0]:[b8:6a:97:21:f5:42]:[192.1.10.7]          192.1.0.7       0          100        0       ?
Total number of entries 1083
```

Edge-primary

Configuration

```
!export-password: default
hostname Edge-primary
no ip icmp redirect
profile Aggregation-Leaf
ntp server 10.100.0.12 minpoll 4 maxpoll 4 iburst
cli-session
```

```
    timeout 0
!
!
!
!
!
ssh server vrf mgmt
vlan 1
vlan 301
    ip igmp snooping enable
vlan 302
    ip igmp snooping enable
vlan 303
    ip igmp snooping enable
vlan 304
    ip igmp snooping enable
vlan 305
    ip igmp snooping enable
vlan 306
    ip igmp snooping enable
vlan 307
    ip igmp snooping enable
vlan 308
    ip igmp snooping enable
vlan 309
    ip igmp snooping enable
vlan 310
    ip igmp snooping enable
vlan 500
interface mgmt
    no shutdown
    ip dhcp
system interface-group 1 speed 10g
    !interface group 1 contains ports 1/1/1-1/1/4
interface lag 1
    no shutdown
    no routing
    vlan trunk native 1 tag
    vlan trunk allowed all
    lacp mode active
interface lag 2 multi-chassis
    no shutdown
    no routing
    vlan trunk native 1
    vlan trunk allowed 500
    lacp mode active
interface lag 3 multi-chassis
    no shutdown
    no routing
    vlan trunk native 1
    vlan trunk allowed 1,301-310
    lacp mode active
interface 1/1/1
    no shutdown
    lag 3
interface 1/1/20
    no shutdown
    ip address 192.168.4.1/30
    ip ospf 1 area 0.0.0.0
    ip pim-sparse enable
interface 1/1/31
    no shutdown
```

```
    lag 2
interface 1/1/32
    no shutdown
    lag 2
interface 1/1/33
    no shutdown
    lag 1
interface 1/1/34
    no shutdown
    lag 1
interface loopback 0
    ip address 192.1.0.1/32
    ip ospf 1 area 0.0.0.0
    ip pim-sparse enable
interface vlan 301
    ip address 192.1.151.3/24
    active-gateway ip mac 00:00:20:00:10:01
    active-gateway ip 192.1.151.1
    ip ospf 1 area 0.0.0.0
    ip ospf passive
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
interface vlan 302
    ip address 192.1.152.3/24
    active-gateway ip mac 00:00:20:00:10:01
    active-gateway ip 192.1.152.1
    ip ospf 1 area 0.0.0.0
    ip ospf passive
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
interface vlan 303
    ip address 192.1.153.3/24
    active-gateway ip mac 00:00:20:00:10:01
    active-gateway ip 192.1.153.1
    ip ospf 1 area 0.0.0.0
    ip ospf passive
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
interface vlan 304
    ip address 192.1.154.3/24
    active-gateway ip mac 00:00:20:00:10:01
    active-gateway ip 192.1.154.1
    ip ospf 1 area 0.0.0.0
    ip ospf passive
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
interface vlan 305
    ip address 192.1.155.3/24
    active-gateway ip mac 00:00:20:00:10:01
    active-gateway ip 192.1.155.1
    ip ospf 1 area 0.0.0.0
    ip ospf passive
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
interface vlan 306
    ip address 192.1.156.3/24
    active-gateway ip mac 00:00:20:00:10:01
```

```
    active-gateway ip 192.1.156.1
    ip ospf 1 area 0.0.0.0
    ip ospf passive
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
interface vlan 307
    ip address 192.1.157.3/24
    active-gateway ip mac 00:00:20:00:10:01
    active-gateway ip 192.1.157.1
    ip ospf 1 area 0.0.0.0
    ip ospf passive
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
interface vlan 308
    ip address 192.1.158.3/24
    active-gateway ip mac 00:00:20:00:10:01
    active-gateway ip 192.1.158.1
    ip ospf 1 area 0.0.0.0
    ip ospf passive
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
interface vlan 309
    ip address 192.1.159.3/24
    active-gateway ip mac 00:00:20:00:10:01
    active-gateway ip 192.1.159.1
    ip ospf 1 area 0.0.0.0
    ip ospf passive
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
interface vlan 310
    ip address 192.1.160.3/24
    active-gateway ip mac 00:00:20:00:10:01
    active-gateway ip 192.1.160.1
    ip ospf 1 area 0.0.0.0
    ip ospf passive
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
interface vlan 500
    vsx active-forwarding
    ip address 192.1.0.49/29
    ip ospf 1 area 0.0.0.0
    ip pim-sparse enable
vsx
    inter-switch-link lag 1
    role primary
    keepalive peer 192.168.4.2 source 192.168.4.1
!
!
!
!
!
router ospf 1
    router-id 192.1.0.1
    redistribute connected
    area 0.0.0.0
router pim
    enable
```

```
    rp-candidate source-ip-interface loopback0 group-prefix 224.0.0.0/4
    rp-candidate priority 180
    bsr-candidate source-ip-interface loopback0
    active-active
https-server vrf mgmt
```

Verification

Verify OSPF neighbors

```
Edge-primary# show ip ospf neighbors all-vrfs
VRF : default                          Process : 1
================================================

Total Number of Neighbors : 4

Neighbor ID      Priority  State             Nbr Address       Interface
-------------------------------------------------------------------------
192.1.0.2        1         FULL/DR           192.168.4.2        1/1/20

192.1.0.2        1         2-WAY/DROther     192.1.0.50         vlan500

192.1.0.18       100       FULL/BDR          192.1.0.53         vlan500

192.1.10.7       200       FULL/DR           192.1.0.54         vlan500
```

Verify PIM neighbors

```
Edge-primary# show ip pim neighbor all-vrfs

PIM Neighbor


VRF                        : default
Total number of neighbors  : 14

IP Address                 : 192.1.0.50
Interface                  : vlan500
Up Time (HH:MM:SS)         : 00:16:45
Expire Time (HH:MM:SS)     : 00:01:41
DR Priority                : 1
Hold Time (HH:MM:SS)       : 00:01:45

IP Address                 : 192.1.0.53
Interface                  : vlan500
Up Time (HH:MM:SS)         : 00:16:39
Expire Time (HH:MM:SS)     : 00:01:42
DR Priority                : 117440960
Hold Time (HH:MM:SS)       : 00:01:45

IP Address                 : 192.1.0.54
Interface                  : vlan500
Up Time (HH:MM:SS)         : 00:16:38
Expire Time (HH:MM:SS)     : 00:01:40
DR Priority                : 117440960
Hold Time (HH:MM:SS)       : 00:01:45

IP Address                 : 192.1.151.2
Interface                  : vlan301
```

```
Up Time (HH:MM:SS)        : 00:16:46
Expire Time (HH:MM:SS)    : 00:01:30
DR Priority               : 1
Hold Time (HH:MM:SS)      : 00:01:45
Secondary IP Addresses :
 192.1.151.1
!snip

IP Address                : 192.1.159.2
Interface                 : vlan309
Up Time (HH:MM:SS)        : 00:16:46
Expire Time (HH:MM:SS)    : 00:01:30
DR Priority               : 1
Hold Time (HH:MM:SS)      : 00:01:45
Secondary IP Addresses :
 192.1.159.1

IP Address                : 192.1.160.2
Interface                 : vlan310
Up Time (HH:MM:SS)        : 00:16:46
Expire Time (HH:MM:SS)    : 00:01:30
DR Priority               : 1
Hold Time (HH:MM:SS)      : 00:01:45
Secondary IP Addresses :
 192.1.160.1

IP Address                : 192.168.4.2
Interface                 : 1/1/20
Up Time (HH:MM:SS)        : 00:16:48
Expire Time (HH:MM:SS)    : 00:01:27
DR Priority               : 1
Hold Time (HH:MM:SS)      : 00:01:45
```

Verify PIM interfaces

```
Edge-primary# show ip pim interface vlan 301

PIM Interfaces

VRF: default

Interface  : vlan301
Neighbor count : 1
IP Address : 192.1.151.3/24
Mode       : sparse
Designated Router : 192.1.151.3
Proxy DR              : false
Hello Interval (sec)  : 30
Hello Delay (sec)     : 5
Override Interval (msec)  : 2500              Lan Prune Delay     : Yes

Propagation Delay (msec)  : 500               Configured DR Priority    : 1

Operational DR Priority   : 4294967295
Neighbor Timeout          : 85


Edge-primary# show ip pim interface vlan 310

PIM Interfaces
```

```
VRF: default

Interface  : vlan310
Neighbor count : 1
IP Address : 192.1.160.3/24
Mode       : sparse
Designated Router : 192.1.160.3
Proxy DR              : false
Hello Interval (sec)  : 30
Hello Delay (sec)     : 5
Override Interval (msec)  : 2500             Lan Prune Delay     : Yes

Propagation Delay (msec)  : 500              Configured DR Priority    : 1

Operational DR Priority   : 4294967295
Neighbor Timeout          : 83
```

Verify mroutes

```
Edge-primary# show ip mroute all-vrfs
IP Multicast Route Entries

VRF : default
Total number of entries : 40

Group Address           : 225.1.1.1
Source Address          : 192.1.1.11
Neighbor                : 192.1.0.54
Incoming interface      : vlan500
Outgoing Interface List :
Interface       State          VSX Role
-----------     -----------    --------
vlan301         forwarding     DR

Group Address           : 225.1.2.1
Source Address          : 192.1.1.11
Neighbor                : 192.1.0.54
Incoming interface      : vlan500
Outgoing Interface List :
Interface       State          VSX Role
-----------     -----------    --------
vlan302         forwarding     DR
!snip

Group Address           : 239.1.8.1
Source Address          : 192.1.151.101
Neighbor                :
Incoming interface      : vlan301

Group Address           : 239.1.9.1
Source Address          : 192.1.151.101
Neighbor                :
Incoming interface      : vlan301

Group Address           : 239.1.9.1
Source Address          : 192.1.151.101
Neighbor                :
Incoming interface      : vlan500

Group Address           : 239.1.10.1
Source Address          : 192.1.151.101
```

```
Neighbor                :
Incoming interface      : vlan500

Group Address           : 239.1.10.1
Source Address          : 192.1.151.101
Neighbor                :
Incoming interface      : vlan301
```

Edge-secondary

Configuration

```
!export-password: default
hostname Edge-secondary
no ip icmp redirect
profile Aggregation-Leaf
ntp server 10.100.0.12 minpoll 4 maxpoll 4 iburst
cli-session
    timeout 0
!
!
!
!
!
ssh server vrf mgmt
vlan 1
vlan 301
    ip igmp snooping enable
vlan 302
    ip igmp snooping enable
vlan 303
    ip igmp snooping enable
vlan 304
    ip igmp snooping enable
vlan 305
    ip igmp snooping enable
vlan 306
    ip igmp snooping enable
vlan 307
    ip igmp snooping enable
vlan 308
    ip igmp snooping enable
vlan 309
    ip igmp snooping enable
vlan 310
    ip igmp snooping enable
vlan 500
interface mgmt
    no shutdown
    ip dhcp
system interface-group 1 speed 10g
    !interface group 1 contains ports 1/1/1-1/1/4
interface lag 1
    no shutdown
    no routing
    vlan trunk native 1 tag
    vlan trunk allowed all
    lacp mode active
interface lag 2 multi-chassis
    no shutdown
    no routing
```

```
    vlan trunk native 1
    vlan trunk allowed 500
    lacp mode active
interface lag 3 multi-chassis
    no shutdown
    no routing
    vlan trunk native 1
    vlan trunk allowed 1,301-310
    lacp mode active
interface 1/1/1
    no shutdown
    lag 3
interface 1/1/3
    no shutdown
    ip address 192.168.4.2/30
    ip ospf 1 area 0.0.0.0
    ip pim-sparse enable
interface 1/1/31
    no shutdown
    lag 2
interface 1/1/32
    no shutdown
    lag 2
interface 1/1/35
    no shutdown
    lag 1
interface 1/1/36
    no shutdown
    lag 1
interface loopback 0
    ip address 192.1.0.2/32
    ip ospf 1 area 0.0.0.0
    ip pim-sparse enable
interface vlan 301
    ip address 192.1.151.2/24
    active-gateway ip mac 00:00:20:00:10:01
    active-gateway ip 192.1.151.1
    ip ospf 1 area 0.0.0.0
    ip ospf passive
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
interface vlan 302
    ip address 192.1.152.2/24
    active-gateway ip mac 00:00:20:00:10:01
    active-gateway ip 192.1.152.1
    ip ospf 1 area 0.0.0.0
    ip ospf passive
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
interface vlan 303
    ip address 192.1.153.2/24
    active-gateway ip mac 00:00:20:00:10:01
    active-gateway ip 192.1.153.1
    ip ospf 1 area 0.0.0.0
    ip ospf passive
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
interface vlan 304
    ip address 192.1.154.2/24
```

```
    active-gateway ip mac 00:00:20:00:10:01
    active-gateway ip 192.1.154.1
    ip ospf 1 area 0.0.0.0
    ip ospf passive
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
interface vlan 305
    ip address 192.1.155.2/24
    active-gateway ip mac 00:00:20:00:10:01
    active-gateway ip 192.1.155.1
    ip ospf 1 area 0.0.0.0
    ip ospf passive
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
interface vlan 306
    ip address 192.1.156.2/24
    active-gateway ip mac 00:00:20:00:10:01
    active-gateway ip 192.1.156.1
    ip ospf 1 area 0.0.0.0
    ip ospf passive
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
interface vlan 307
    ip address 192.1.157.2/24
    active-gateway ip mac 00:00:20:00:10:01
    active-gateway ip 192.1.157.1
    ip ospf 1 area 0.0.0.0
    ip ospf passive
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
interface vlan 308
    ip address 192.1.158.2/24
    active-gateway ip mac 00:00:20:00:10:01
    active-gateway ip 192.1.158.1
    ip ospf 1 area 0.0.0.0
    ip ospf passive
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
interface vlan 309
    ip address 192.1.159.2/24
    active-gateway ip mac 00:00:20:00:10:01
    active-gateway ip 192.1.159.1
    ip ospf 1 area 0.0.0.0
    ip ospf passive
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
interface vlan 310
    ip address 192.1.160.2/24
    active-gateway ip mac 00:00:20:00:10:01
    active-gateway ip 192.1.160.1
    ip ospf 1 area 0.0.0.0
    ip ospf passive
    ip igmp enable
    ip igmp version 2
    ip pim-sparse enable
interface vlan 500
```

```
    vsx active-forwarding
    ip address 192.1.0.50/29
    ip ospf 1 area 0.0.0.0
    ip pim-sparse enable
vsx
    inter-switch-link lag 1
    role secondary
    keepalive peer 192.168.4.1 source 192.168.4.2
!
!
!
!
!
router ospf 1
    router-id 192.1.0.2
    redistribute connected
    area 0.0.0.0
router pim
    enable
    rp-candidate source-ip-interface loopback0 group-prefix 224.0.0.0/4
    bsr-candidate source-ip-interface loopback0
    active-active
https-server vrf mgmt
```

Verification

Verify OSPF neighbors

```
Edge-secondary# show ip ospf neighbors all-vrfs
VRF : default                           Process : 1
================================================

Total Number of Neighbors : 4

Neighbor ID      Priority  State             Nbr Address       Interface
-------------------------------------------------------------------------
192.1.0.1        1         FULL/BDR          192.168.4.1        1/1/3

192.1.0.1        1         2-WAY/DROther     192.1.0.49         vlan500

192.1.0.18       100       FULL/BDR          192.1.0.53         vlan500

192.1.10.7       200       FULL/DR           192.1.0.54         vlan500
```

Verify PIM neighbors

```
Edge-secondary# show ip pim neighbor all-vrfs

PIM Neighbor


VRF                       : default
Total number of neighbors : 14

IP Address                : 192.1.0.49
Interface                 : vlan500
Up Time (HH:MM:SS)        : 00:17:05
Expire Time (HH:MM:SS)    : 00:01:45
DR Priority               : 1
```

```
Hold Time (HH:MM:SS)      : 00:01:45

IP Address                : 192.1.0.53
Interface                 : vlan500
Up Time (HH:MM:SS)        : 00:17:02
Expire Time (HH:MM:SS)    : 00:01:18
DR Priority               : 117440960
Hold Time (HH:MM:SS)      : 00:01:45

IP Address                : 192.1.0.54
Interface                 : vlan500
Up Time (HH:MM:SS)        : 00:17:01
Expire Time (HH:MM:SS)    : 00:01:17
DR Priority               : 117440960
Hold Time (HH:MM:SS)      : 00:01:45

IP Address                : 192.1.151.3
Interface                 : vlan301
Up Time (HH:MM:SS)        : 00:17:08
Expire Time (HH:MM:SS)    : 00:01:37
DR Priority               : 4294967295
Hold Time (HH:MM:SS)      : 00:01:45
Secondary IP Addresses :
 192.1.151.1

IP Address                : 192.1.152.3
Interface                 : vlan302
Up Time (HH:MM:SS)        : 00:17:08
Expire Time (HH:MM:SS)    : 00:01:37
DR Priority               : 4294967295
Hold Time (HH:MM:SS)      : 00:01:45
Secondary IP Addresses :
 192.1.152.1

IP Address                : 192.1.153.3
Interface                 : vlan303
Up Time (HH:MM:SS)        : 00:17:08
Expire Time (HH:MM:SS)    : 00:01:37
DR Priority               : 4294967295
Hold Time (HH:MM:SS)      : 00:01:45
Secondary IP Addresses :
 192.1.153.1

IP Address                : 192.1.154.3
Interface                 : vlan304
Up Time (HH:MM:SS)        : 00:17:08
Expire Time (HH:MM:SS)    : 00:01:37
DR Priority               : 4294967295
Hold Time (HH:MM:SS)      : 00:01:45
Secondary IP Addresses :
 192.1.154.1
!snip

IP Address                : 192.1.160.3
Interface                 : vlan310
Up Time (HH:MM:SS)        : 00:17:09
Expire Time (HH:MM:SS)    : 00:01:36
DR Priority               : 4294967295
Hold Time (HH:MM:SS)      : 00:01:45
Secondary IP Addresses :
 192.1.160.1
```

```
IP Address                : 192.168.4.1
Interface                 : 1/1/3
Up Time (HH:MM:SS)        : 00:17:11
Expire Time (HH:MM:SS)    : 00:01:39
DR Priority               : 1
Hold Time (HH:MM:SS)      : 00:01:45
```

Verify PIM interfaces

```
Edge-secondary# show ip pim interface vlan 301

PIM Interfaces

VRF: default

Interface  : vlan301
Neighbor count : 1
IP Address : 192.1.151.2/24
Mode       : sparse
Designated Router : 192.1.151.2
Proxy DR              : true
Hello Interval (sec)  : 30
Hello Delay (sec)     : 5
Override Interval (msec)  : 2500              Lan Prune Delay     : Yes

Propagation Delay (msec)  : 500               Configured DR Priority    : 1

Operational DR Priority   : 1
Neighbor Timeout          : 87


Edge-secondary# show ip pim interface vlan 310

PIM Interfaces

VRF: default

Interface  : vlan310
Neighbor count : 1
IP Address : 192.1.160.2/24
Mode       : sparse
Designated Router : 192.1.160.2
Proxy DR              : true
Hello Interval (sec)  : 30
Hello Delay (sec)     : 5
Override Interval (msec)  : 2500              Lan Prune Delay     : Yes

Propagation Delay (msec)  : 500               Configured DR Priority    : 1

Operational DR Priority   : 1
Neighbor Timeout          : 85
```

Verify mroutes

```
Edge-secondary# show ip mroute all-vrfs
IP Multicast Route Entries

VRF : default
Total number of entries : 50
```

```
Group Address           : 225.1.1.1
Source Address          : 192.1.1.11
Neighbor                : 192.1.0.54
Incoming interface      : vlan500
Outgoing Interface List :
Interface       State          VSX Role
-----------     ----------     --------
vlan301         forwarding     Proxy DR

Group Address           : 225.1.1.1
Source Address          : 192.1.1.11
Neighbor                :
Incoming interface      : vlan301

Group Address           : 225.1.2.1
Source Address          : 192.1.1.11
Neighbor                :
Incoming interface      : vlan500

Group Address           : 225.1.2.1
Source Address          : 192.1.1.11
Neighbor                :
Incoming interface      : vlan302

Group Address           : 225.1.3.1
Source Address          : 192.1.1.11
Neighbor                : 192.1.0.54
Incoming interface      : vlan303

Group Address           : 225.1.3.1
Source Address          : 192.1.1.11
Neighbor                : 192.1.0.54
Incoming interface      : vlan500
Outgoing Interface List :
Interface       State          VSX Role
-----------     ----------     --------
vlan303         forwarding     Proxy DR
!snip

Group Address           : 239.1.8.1
Source Address          : 192.1.151.101
Neighbor                :
Incoming interface      : vlan301
Outgoing Interface List :
Interface       State          VSX Role
-----------     ----------     --------
vlan500         forwarding     DR

Group Address           : 239.1.9.1
Source Address          : 192.1.151.101
Neighbor                :
Incoming interface      : vlan301
Outgoing Interface List :
Interface       State          VSX Role
-----------     ----------     --------
vlan500         forwarding     DR

Group Address           : 239.1.10.1
Source Address          : 192.1.151.101
Neighbor                :
Incoming interface      : vlan301
```

```
Outgoing Interface List :
Interface       State          VSX Role
-----------     -----------    --------
vlan500         forwarding     DR
```

Multicast VXLAN commands

ip pim-sparse vsx-virtual-neighbor

```
ip pim-sparse vsx-virtual-neighbor
no ip pim-sparse vsx-virtual-neighbor
```

Description

Once configured, the router processes IGMP/MLD and PIM joins received on this interface regardless of its DR or Prime Neighbor role. The command must be enabled for VSX VXLAN leaf switches for both L2 and L3 extensions. This allows for the interface to be in the same multicast data path state on both the VSX peers.

The `no` form of the command disables the vsx-virtual-neighbor on the interface.

This command is applicable for normal SVI interfaces and L2 VNI mapped SVI interfaces. It is valid for VXLAN-enabled VLANs only and has no effect on non-VXLAN-enabled VLANs.

Examples

```
switch(config)# interface vlan40
switch(config-if-vlan)# ip address 40.0.0.4/24
switch(config-if-vlan)# ip pim-sparse enable
switch(config-if-vlan)# ip pim-sparse vsx-virtual-neighbor
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	`config-if-vlan`	Administrators or local user group members with execution rights for this command.

show ip mroute

```
show ip mroute [all-vrfs | vrf <VRF-NAME>] [vsx-peer]
```

Description

Shows multicast routing information. Optionally, you can show specific information by VRF. If no options are specified, it shows information for the default VRF.

Parameters

`all-vrfs`

Shows all PIM neighbors information.

`vrf <VRF-NAME>`

Shows PIM neighbor information for a specific VRF.

`vsx-peer`

Shows the output from the VSX peer switch. If the switches do not have the VSX configuration or the ISL is down, the output from the VSX peer switch is not displayed. This parameter is available on switches that support VSX.

Examples

Multicast route with L3VNI in Incoming Interface List:

```
switch# show ip mroute all-vrfs
IP Multicast Route Entries

VRF : red
Total number of entries : 1

Group Address           : 225.1.1.1
Source Address          : 80.1.1.11
Neighbor                : 1.1.1.1
Incoming interface      : vni2
Outgoing Interface List :
Interface       State
-----------     ----------
vlan10          forwarding

switch# show ip mroute 225.1.1.1 80.1.1.11 all-vrfs

IP Multicast Route Entries

VRF : red

Group Address                 : 225.1.1.1
Source Address                : 80.1.1.11
Neighbor                      : 1.1.1.1
Incoming interface            : vni2
Multicast Routing Protocol    : PIM-SM
Unicast Routing Protocol      : BGP
Metric                        : 0
Metric  Pref                  : 200
Uptime (HH:MM:SS)             : 00:07:23
Downstream Interface
Interface       State
-----------     ----------
vlan10          forwarding
```

Multicast route with L3VNI in Outgoing Interface List:

```
switch# show ip mroute all-vrfs
IP Multicast Route Entries

VRF : red
Total number of entries : 1

Group Address           : 225.1.1.1
```

```
Source Address          : 80.1.1.11
Neighbor                :
Incoming interface      : vlan20
Outgoing Interface List :
Interface       State
-----------     ----------
vni2               forwarding

switch# show ip mroute 225.1.1.1 80.1.1.11 vrf red

IP Multicast Route Entries

VRF : red
Total number of entries : 1

Group Address                : 225.1.1.1
Source Address               : 80.1.1.11
Neighbor                     :
Incoming interface           : vlan20
Multicast Routing Protocol   : PIM-SM
Unicast Routing Protocol     : connected
Metric                       : 0
Metric  Pref                 : 0
Uptime (HH:MM:SS)            : 00:06:32
Downstream Interface
Interface       State
-----------     ----------
vni2               forwarding
```

Command History

Release	Modification
10.07 or earlier	--

Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

show ip pim neighbor

`show ip pim neighbor [<IP-ADDR>] [all-vrfs | vrf <VRF-NAME>]`

Description

Displays the information about PIM interfaces currently configured in the router for the given VRF. If VRF is not given, it displays for default VRF.

Parameters

<IP-ADDR>

Shows PIM neighbor information.

`all-vrfs`

Shows all PIM neighbors information.

`vrf <VRF-NAME>`

Shows PIM neighbor information for a specific VRF.

Examples

Show information for all VRFs:

```
switch# show ip pim neighbor all-vrfs

PIM Neighbor

VRF                         : Test_1
Total number of neighbors : 2

IP Address                  : 100.1.1.252
Interface                   : vlan100
Up Time (HH:MM:SS)          : 00:44:38
Expire Time (HH:MM:SS)      : 00:01:32
DR Priority                 : 1
Hold Time (HH:MM:SS)        : 00:01:45

IP Address                  : 172.1.1.1
Interface                   : vni1000
Up Time (HH:MM:SS)          : 00:44:35
Expire Time (HH:MM:SS)      : 00:03:25
DR Priority                 : 1
Hold Time (HH:MM:SS)        : 00:03:30
```

Command History

Release	Modification
10.07 or earlier	--

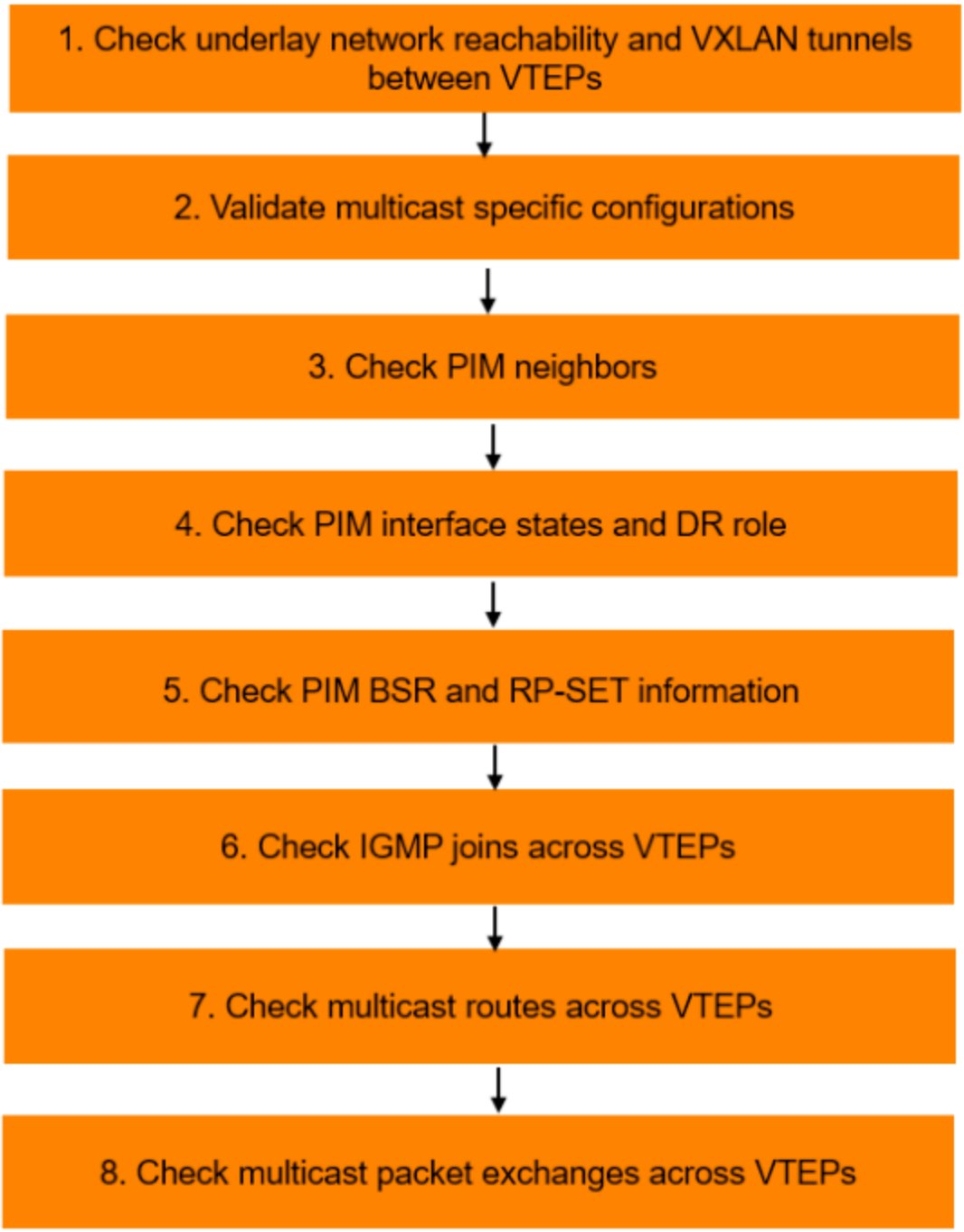
Command Information

Platforms	Command context	Authority
All platforms	Operator (>) or Manager (#)	Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

Debugging and troubleshooting

The recommended IPv4 multicast VXLAN troubleshooting flow is provided in Figure 1, Recommended IPv4 multicast VXLAN troubleshooting flow. Additional tips and guidance for each step are provided below.

Figure 1 *Recommended IPv4 multicast VXLAN troubleshooting flow*



The recommended IPv4 multicast VXLAN troubleshooting procedure includes the following sequence of steps:

Step 1: Check underlay network reachability and VXLAN tunnels between VTEPs.

a. Ensure tunnel source/destination loopback IPs are correctly advertised in the underlay network.
b. Use extended pings on VTEPs to confirm network connectivity between tunnel source/destination loopback IPs.
c. Fix underlay connectivity issues if discovered.
d. If there are no underlay network issues, validate VXLAN tunnels, ensure they are operational.

```
VTEP1# sh int vx vtep
Source        Destination      Origin   Status          VNI       Routing   VLAN  VRF
------------- ---------------- -------- --------------- --------- --------- ----- ---
192.168.2.6   192.168.2.5      evpn     operational     100001    enabled   --     VRF1
192.168.2.6   192.168.2.5      evpn     operational     100111    disabled  111    --
192.168.2.6   192.168.11.3     evpn     operational     100001    enabled   --     VRF1
192.168.2.6   192.168.11.3     evpn     operational     100002    enabled   --     VRF2
```

e. If EVPN tunnel is down, ensure correct EVPN configs are used.

Step 2: Validate multicast specific configurations.

a. In a distributed L3 gateway deployment, `virtual-mac` configuration is needed on all the VTEPs. Make sure `virtual-mac` is configured and it is unique per VTEP, a VSX VTEP peer would share 1 virtual-mac:

```
VTEP1# show run | i virtual-mac
virtual-mac 00:00:22:00:00:21
```

b. On VSX VTEPs, `ip pim-sparse vsx-virtual-neighbor` is required on all SVIs where PIM is enabled.

```
interface vlan40
 no shutdown
 vrf attach red
 ip address 40.40.40.1/24
 ip pim-sparse enable
 ip pim-sparse vsx-virtual-neighbor
```

c. If IGMP is enabled on any VLAN, the `redistribute local-svi` or `redistribute local-mac` command must be enabled under the evpn context. This is needed for proper querier information propagation.

d. Validate unicast reachability to the multicast sources/DR/RP/BSR addresses across all the VTEPs. Use `show ip route` command to validate the routes. For example:

```
VTEP1# show ip route 80.1.1.1 vrf red

VRF: red

   Prefix            : 80.1.1.0/24                VRF(egress)         : -
   Nexthop           : 11.1.1.1                   Interface           : -
   Origin            : bgp                        Type                : bgp_evpn
   Distance          : 200                        Metric              : 0
   Age               : 02h:08m:19s                Tag                 : 0
   Encap Type        : vxlan                      Encap Details       : l3vni 2
```

Step 3: Check PIM neighbors.

a. Ensure that PIM neighbors are formed between L3 VNI interfaces. For a L3 VNI neighbor, neighbor IP will be the underlay VTEP IP in the default VRF and this will be same for all the tenant VRFs.

b. If the same VLAN is extended across VTEPs, ensure that the PIM neighbors are formed on the extended VLANs across the VTEPs.

```
VTEP1# show ip pim neighbor all-vrfs
PIM Neighbor

VRF : red
Total number of neighbors : 2
IP Address : 1.1.1.1
Interface : vni2
Up Time (HH:MM:SS) : 00:33:30
Expire Time (HH:MM:SS) : 00:03:01
DR Priority : 1
Hold Time (HH:MM:SS) : 00:03:30

IP Address : 100.100.1.3
Interface : vlan10
Up Time (HH:MM:SS) : 00:33:29
Expire Time (HH:MM:SS) : 00:01:17
DR Priority : 16843009
Hold Time (HH:MM:SS) : 00:01:45
```

c. If PIM neighbors are not formed, validate the configurations and ensure `ip pim-sparse` is enabled on the interface and `router pim` is enabled on the corresponding VRF.
d. If the configurations are correct, validate PIM Hello packets are exchanged between the VTEPs. See Step 8: Check multicast packet exchanges between VTEPs for instructions.

Step 4: Check PIM interface states and DR role.

a. Validate PIM Interface configurations using the `show ip pim interface` command. Ensure that the DR election is successful and updated in the show command.
b. If the VLAN is extended across VTEPs. ensure only one VTEP is elected as DR on the VLAN. If the VTEP is a pair of VSX switches, both VSX peers will be elected as DR. Only one VSX peer will route the data.

```
VTEP1# show ip pim interface vlan 10
PIM Interfaces
VRF: red
Interface : vlan10
Neighbor count : 1
IP Address : 100.100.1.3/24
Mode : sparse
Designated Router : 100.100.1.4
Proxy DR : false
Hello Interval (sec) : 30
Hello Delay (sec) : 5
Override Interval (msec) : 2500 Lan Prune Delay : Yes
Propagation Delay (msec) : 500 Configured DR Priority : 1
Operational DR Priority : 16843009
Neighbor Timeout : 93
```

Step 5: Check PIM BSR and RP-SET information.

a. If BSR is configured, ensure that E-BSR is learnt on all the VTEPs.

```
VTEP1# show ip pim bsr
Status and Counters- PIM-SM Bootstrap Router Information

VRF                        : default
```

```
E-BSR Address              : 172.1.1.1
E-BSR Priority             : 0
E-BSR Hash Mask Length     : 30
E-BSR Up Time              : 49 secs
Next Bootstrap Message     : 21 secs

C-BSR Admin Status         : This system is a Candidate-BSR
C-BSR Address              : 172.1.1.1
C-BSR Priority             : 0
C-BSR Hash Mask Length     : 30
C-BSR Message Interval     : 60
C-BSR Source IP Interface  : loopback1

C-RP Admin Status          : This system is a Candidate-RP
C-RP Address               : 172.1.1.1
C-RP Hold Time             : 150
C-RP Advertise Period      : 60
C-RP Priority              : 192
C-RP Source IP Interface   : loopback1

Group Address    Group Mask
---------------  ---------------
224.0.0.0        240.0.0.0
```

b. Ensure RP-set is learned on all the VTEPs. If the RP is a static-RP, make sure all the VTEPs have the static RP configured.

```
VTEP1# show ip pim rp-set all-vrfs
VRF: red
Status and Counters - PIM-SM Learned RP-Set Information
Group Address    Group Mask       RP Address       Hold Time  Expire Time
---------------  ---------------  ---------------  ---------  -----------
224.0.0.0        240.0.0.0        172.1.1.1        150        94
```

c. If the BSR or RP-set is not learned, make sure of the unicast reachability to BSR/RP IP address. The `show ip route` command should display unicast routes to reach BSR/RP address.

d. Ensure that PIM is enabled on the next-hop pointed by the unicast route. If PIM is not enabled, E-BSR/RP-Set information will not be updated correctly.

e. If the unicast routes are present and PIM is enabled on the nexthop interface, check packet captures to validate that BSR bootstrap packets and candidate RP advertisement messages are exchanged across VTEPs.

Step 6: Check IGMP joins across VTEPs.

a. Ensure IGMP joins are present on the DR in the client VLAN.

```
VTEP1# show ip igmp interface vlan 10
VRF Name   : red
Interface  : vlan10
IGMP Configured Version  : 3
IGMP Operating Version   : 3
Querier State              : Querier
Querier IP [this switch]   : 100.100.1.2
Querier Uptime             : 2m 29s
Querier Expiration Time    : 0m 41s
```

```
IGMP Snoop Enabled on VLAN : False

Active Group Address   Vers Mode Uptime    Expires
---------------------- ---- ---- --------- ---------
239.1.1.1              2         0m 17s    4m 3s
```

b. If IGMP snooping is enabled, ensure that the joins are learned on the correct VTEP/port.

```
VTEP1# show ip igmp snooping vlan 10 group 239.1.1.1

IGMP ports and group information for group 239.1.1.1

VLAN ID   : 10
VLAN Name : VLAN10

Group Address : 239.1.1.1
Last Reporter : 200.200.1.1
Group Type    : Filter

                                                          V1        V2
Sources   Sources
Port                     Vers Mode Uptime    Expires   Timer     Timer
Forwarded Blocked
------------------------ ---- ---- --------- --------- --------- --------- ---
------ --------
vxlan1(1.1.1.1)          2    EXC  5h 24m    3m 38s              3m 38s    0
      0
```

c. If joins are not shown, make sure that the querier is elected successfully in the interface and the periodic AHQ packet reaches the clients.

d. Ensure joins are refreshed periodically and are not removed. Check uptime in `show ip igmp` and `show ip igmp snooping` outpus to ensure joins are stable.

e. On a VSX VTEP, IGMP joins are synchronized amongst the VSX switches. If IGMP snooping is enabled, make sure that the joined VTEP is the same in both VSX peers. Similarly querier port should be the same across both VSX peers. If they are different, ensure that the `redistribute local-svi` or `redistribute local-mac` command is configured on all VTEPS.

f. Make sure there are no COPP drops for IGMP class.

```
VTEP1# show copp-policy statistics class igmp
Statistics for CoPP policy 'default':
Class: igmp
Description: Internet Group Management Protocol.
priority : 4
rate (pps) : 1600
burst size (pkts) : 450
packets passed : 294267766 packets dropped : 0
```

Step 7: Check multicast routes across VTEPs.

a. Ensure multicast routes are formed correctly across VTEPS. Make sure L3 VNI interface is added correctly in the incoming/outgoing interface list in a distributed L3 gateway use case.

- Mroutes on Source DR (routing to L3 VNI Interface):

```
VTEP1# show ip mroute all-vrfs
IP Multicast Route Entries

VRF : red
Total number of entries : 1

Group Address           : 225.1.1.1
Source Address          : 73.1.1.11
Neighbor                : 100.100.1.3
Incoming interface      : vlan10
Outgoing Interface List :
Interface       State
-----------     ----------
vni2               forwarding
```

- Mroutes on last hop router (routing from L3 VNI interface to receiver SVI):

```
VTEP2# show ip mroute all-vrfs
IP Multicast Route Entries

VRF : red
Total number of entries : 1

Group Address           : 225.1.1.1
Source Address          : 73.1.1.11
Neighbor                : 5.5.5.5
Incoming interface      : vni2
Outgoing Interface List :
Interface       State
-----------     ----------
vlan20          forwarding
```

b. In the centralized L3 gateway use case, ensure multicast routes are formed correctly on the routers. In this case the multicast routes will have SVI/ROP/L3 LAG as incoming/outgoing interfaces.

c. If the outgoing interface is SVI and it contains VTEPs, multicast data traffic will be encapsulated and transmitted to the VTEP.

```
L3VTEP# show ip mroute all-vrfs
IP Multicast Route Entries

VRF : red
Total number of entries : 1

Group Address           : 239.1.1.1
Source Address          : 80.1.1.11
Neighbor                :
Incoming interface      : vlan20
Outgoing Interface List :
Interface       State
-----------     ----------
vlan30               forwarding
```

d. If the multicast routes are not formed as expected, there will be traffic loss. If the interface is missing in multicast routes or the mroute is in bridge state (no outgoing interfaces):

- On the client VLAN, ensure IGMP joins are present on the DR.
- Validate unicast reachability to RP and multicast source on the last hop router (LHR).
- Validate IGMP joins are processed by PIM using the `show ip pim pending` command. If the multicast data is seen by the router, there will not be any pending entries.
- If the joins are seen, check the packet captures between LHR to ensure PIM *,G joins are sent towards RP.
- If RP has received the *,G join, check the packet captures between RP and Source DR to ensure (S,G) joins are sent towards the source.
- Once LHR receives the data via RPT, ensure that the LHR is sending (S,G) joins towards source via packet captures.

e. If the multicast routes is not present in `show ip mroute` in the source DR:
- Ensure that the flow is active.
- If the flow is active, but mroutes are not shown, it indicates an issue in the PIM registration path.
- Make sure Source DR can reach RP and RP can reach back to the source DR.
- Check that the virtual-mac is configured correctly, this is needed for Register/Register-Stop packets to be processed correctly.

f. If the clients are seeing duplicate traffic:
- Ensure the `vsx-virtual-neighbor` command is enabled on all the VSX routers.
- In a VSX setup, only one of the routers is responsible for routing the traffic. Ensure this by monitoring interface statistics/packet captures.

Step 8: Check multicast packet exchanges between VTEPs.

- All the multicast packets (IGMP/PIM control packets, multicast data frames) exchanged across the VTEPS are encapsulated with VXLAN.
- The packets exchanged over VTEPs can be inspected by configuring a mirror session on non-VTEP core/spine switches. The mirror destination should be a port where a packet capture is running.

```
l2:/home/admin# tcpdump -i 1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on MirrorRxNet, link-type EN10MB (Ethernet), capture size 262144 bytes
08:58:51.562444 IP 1.1.1.1.35569 > 3.3.3.3.4789: VXLAN, flags [I] (0x08), vni 30 -->
Encapsulated PIM Hello packet
IP 1.1.1.1 > 224.0.0.13: PIMv2, Hello, length 34
```

FAQ

1. Can I enable multicast on both the overlay (leaf/access VTEP) and underlay (core/spine non-VTEP)?

No, it should not be done and is not recommended. The solution will not work if PIM or IGMP is enabled on the core/spine switches connected to VTEPs.

2. Does the solution require EVPN control plane?

Yes, the solution requires EVPN based control plane both for L2 and L3 multicast. Remote VTEPs are learned via EVPN type 3. In addition, remote hosts and routes are learned via EVPN type 2 and EVPN type 5. IGMP and PIM protocols rely on this information to forward packets.

3. Is PIM-SM used in underlay for BUM traffic replication?

No, the solution does not use PIM-SM at underlay to replicate BUM traffic. The solution uses Head End Replication to send multicast traffic to remote VTEPs, this means that each broadcast/multicast is encapsulated and replicated to all VTEPs from the source VTEP. The list of VTEPs to be replicated can be learned via EVPN type 3 or through multicast protocols running in the overlay.

4. Are there are any platform differences to be aware of?

- For the VSX VTEPs on the Aruba 8325 and 8400 Switch Series, when a packet is routed from a SVI/L3VNI to a L3VNI/L2VNI, only the primary VSX VTEP forwards. This prevents duplication of packets.
- For the VSX VTEPs on the Aruba 6400 and 8360 Switch Series , whichever device gets data directly (not via ISL) will forward. This is done because these platforms have a predicate rule programmed that any packet over ISL will not be sent over tunnel. This means there will never be a case when packets go over the VSX ISL and into a VXLAN tunnel.

5. Is the Active-Active command required on VSX VTEPs?

The Active-Active command is optional for VSX VTEPs. This is because VSX peers act as logical VTEPs and work in Active-Active mode by default. The command can be added without any side effect.

6. Why is the VSX virtual neighbor command required?

- The VSX virtual neighbor command needs to be enabled on all SVIs on VSX VTEPs, the command once enabled does multiple things.
- If the VLAN is the first hop connected router, then both the VSX VTEPs will become DR and will forward PIM joins for every IGMP join that received.
- If the VLAN is the not the first-hop connected router, then both the VSX VTEPs will ignore the prime neighbor check and will forward PIM joins upstream.

7. Does PIM need to be enabled on the L3 VNI?

No, PIM-SM does not need to be enabled on the L3 VNI. It will be automatically enabled when PIM-SM is enabled on the tenant VRF. A VTEP forms PIM neighbors with the other remote VTEPs over L3VNI. AOS-CX forms automatic PIM-SM neighbors with peer VTEPs over L3VNI as soon as PIM-SM is enabled on the tenant VRF.

8. Does the solution work for all types of underlay interfaces?

The solution work with all types of underlay interfaces that are currently supported in AOS-CX. The only restriction is IGMP or PIM cannot be enabled in the underlay.

9. If I change the DR priority of my DR on an SVI with multicast VXLAN, will it work?

In a logical VSX VTEP, DR priority is automatically derived from the VTEP address. This ensures that the VSX VTEPs have identical priorities with both of them functioning as DRs or as non DRs. In case DR priority is changed, one of the VSX peer will start behaving differently from the other. To conclude, do not change DR priority on SVIs of VSX VTEPs.

10. In a VSX VTEP, are VSX keepalive links mandatory for multicast VXLAN?

The VSX keepalive is not mandatory as private IP is used between VSX peers is used to sync joins received over L3 VNIs

11. Why do I require an additional L3 link between VSX border VTEPs when there is ROP/P2P SVI extension?

The additional connectivity is required from the VSX border VTEP to provide an additional link in case the main uplink connectivity from the primary VSX peer goes down. In general the rule that is programmed is that only VSX primary VTEP will forward. If uplink connectivity from the primary VTEP goes down then PIM joins from primary are sent to the secondary and the traffic is pulled from secondary towards the primary.

References

- *VXLAN Guide*
- AOS-CX VXLAN EVPN Symmetric IRB Distributed L3 Gateways
- AOS-CX Switch Simulator

Accessing Aruba Support

Aruba Support Services	https://www.arubanetworks.com/support-services/
Aruba Support Portal	https://asp.arubanetworks.com/
North America telephone	1-800-943-4526 (US & Canada Toll-Free Number) +1-408-754-1200 (Primary - Toll Number) +1-650-385-6582 (Backup - Toll Number - Use only when all other numbers are not working)
International telephone	https://www.arubanetworks.com/support-services/contact-support/

Be sure to collect the following information before contacting Support:

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Other useful sites

Other websites that can be used to find information:

Airheads social forums and Knowledge Base	https://community.arubanetworks.com/
Software licensing	https://lms.arubanetworks.com/
End-of-Life information	https://www.arubanetworks.com/support-services/end-of-life/
Aruba software and documentation	https://asp.arubanetworks.com/downloads

Accessing Updates

You can access updates from the Aruba Support Portal or the HPE My Networking Website.

Aruba Support Portal

https://asp.arubanetworks.com/downloads

If you are unable to find your product in the Aruba Support Portal, you may need to search My Networking, where older networking products can be found:

My Networking

https://www.hpe.com/networking/support

To view and update your entitlements, and to link your contracts and warranties with your profile, go to the Hewlett Packard Enterprise Support Center **More Information on Access to Support Materials** page:

https://support.hpe.com/portal/site/hpsc/aae/home/

Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HP Passport set up with relevant entitlements.

Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.

To subscribe to eNewsletters and alerts:

https://asp.arubanetworks.com/notifications/subscriptions (requires an active Aruba Support Portal (ASP) account to manage subscriptions). Security notices are viewable without an ASP account.

Warranty Information

To view warranty information for your product, go to https://www.arubanetworks.com/support-services/product-warranties/.

Regulatory Information

To view the regulatory information for your product, view the *Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products*, available at https://www.hpe.com/support/Safety-Compliance-EnterpriseProducts

Additional regulatory information

Aruba is committed to providing our customers with information about the chemical substances in our products as needed to comply with legal requirements, environmental data (company programs, product recycling, energy efficiency), and safety information and compliance data, (RoHS and WEEE). For more information, see https://www.arubanetworks.com/company/about-us/environmental-citizenship/.

Documentation Feedback

Aruba is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (docsfeedback-switching@hpe.com). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.