

AOS-CX 10.07 Multicast Guide

6300, 6400, 8320, 8325, 8360, 8400 Switch

Series



a Hewlett Packard
Enterprise company

Part Number: 5200-7876a
Published: June 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 | 13 |
| Multicast overview | 15 |
| Multicast protocols | 15 |
| Multicast addresses | 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 | 22 |
| ip igmp | 23 |
| ip igmp apply access-list | 23 |
| ip igmp last-member-query-interval | 24 |
| ip igmp querier | 25 |
| ip igmp querier interval | 25 |
| ip igmp querier query-max-response-time | 26 |
| ip igmp robustness | 27 |
| ip igmp static-group | 27 |
| ip igmp version | 28 |
| ip igmp version strict | 29 |
| no ip igmp | 29 |
| show ip igmp | 30 |
| show ip igmp counters | 32 |
| show ip igmp group | 34 |
| show ip igmp groups | 36 |
| show ip igmp interface | 38 |
| show ip igmp interface counters | 39 |
| show ip igmp interface group | 40 |
| show ip igmp interface groups | 41 |
| show ip igmp interface statistics | 42 |
| show ip igmp static-groups | 43 |

| | |
|--|-----------|
| show ip igmp statistics | 44 |
| IGMP snooping | 47 |
| IGMP snooping defaults, protocols, and supported configuration | 47 |
| How IGMP snooping works | 48 |
| IGMP snooping configuration task list | 49 |
| Enabling or disabling IGMP snooping | 49 |
| Specifying the IGMP snooping version | 49 |
| Configuring IGMP snooping static groups | 50 |
| Enabling drop-unknown filters | 50 |
| Configuring IGMP snooping fast learn ports globally | 50 |
| Configuring IGMP snooping per port filtering | 51 |
| Disabling IGMP snooping | 51 |
| Viewing IGMP snooping information | 52 |
| IGMP snooping commands | 52 |
| ip igmp snooping {enable disable} | 52 |
| ip igmp snooping apply access-list | 53 |
| ip igmp snooping auto vlan | 54 |
| ip igmp snooping blocked vlan | 54 |
| ip igmp snooping drop-unknown | 55 |
| ip igmp snooping fastlearn | 56 |
| ip igmp snooping fastleave vlan | 57 |
| ip igmp snooping forced fastleave vlan | 57 |
| ip igmp snooping forward vlan | 58 |
| ip igmp snooping static-group | 59 |
| ip igmp snooping version | 60 |
| no ip igmp snooping | 60 |
| show ip igmp snooping | 61 |
| show ip igmp snooping counters | 61 |
| show ip igmp snooping groups | 62 |
| show ip igmp snooping static-groups | 63 |
| show ip igmp snooping statistics | 64 |
| show ip igmp snooping vlan <VLAN-ID> | 64 |
| show ip igmp snooping vlan <VLAN-ID> counters | 66 |
| show ip igmp snooping vlan <VLAN-ID> group port | 68 |
| show ip igmp snooping vlan <VLAN-ID> statistics | 69 |
| MLD snooping | 70 |
| MLD snooping functionality | 70 |
| MLD snooping global configuration commands | 70 |
| ipv6 mld snooping | 70 |
| MLD snooping VLAN configuration commands | 71 |
| ipv6 mld snooping | 71 |
| ipv6 mld snooping apply access-list | 71 |
| ipv6 mld snooping auto vlan | 72 |
| ipv6 mld snooping blocked vlan | 73 |
| ipv6 mld snooping fastlearn | 74 |
| ipv6 mld snooping fastleave vlan | 74 |
| ipv6 mld snooping forced fastleave | 75 |
| ipv6 mld snooping forward vlan | 76 |
| ipv6 mld snooping [static-group <X:X::X:X>] | 76 |
| ipv6 mld snooping [version <ver>] | 77 |
| MLD snooping show commands | 77 |
| show ipv6 mld snooping | 78 |
| show ipv6 mld snooping [counters] | 78 |
| show ipv6 mld snooping [groups] | 79 |

| | |
|---|-----|
| show ipv6 mld snooping [statistics] | 80 |
| show ipv6 mld snooping [vlan <vlan-id> [counters]] | 80 |
| show ipv6 mld snooping [vlan <vlan-id> [statistics]] | 82 |
| show ipv6 mld snooping [vlan <vlan-id> [group [<group-ip>] [source <source-ip>]]] | 82 |
| show ipv6 mld snooping [vlan <vlan-id> [group [port <port_id>]]] | 84 |
| show ipv6 mld snooping [static-groups] | 85 |
| MLD configuration commands for interface VLAN | 85 |
| ipv6 mld {enable disable} | 85 |
| ipv6 mld apply access-list | 86 |
| no ipv6 mld | 87 |
| ipv6 mld querier | 87 |
| ipv6 mld querier [interval <interval-value>] | 88 |
| ipv6 mld last-member-query-interval <interval-value> | 88 |
| ipv6 mld querier query-max-response-time <response-time> | 89 |
| ipv6 mld robustness | 89 |
| ipv6 mld static-group <MULTICAST-GROUP-IP> | 90 |
| ipv6 mld version <VERSION> | 90 |
| ipv6 mld version <VERSION> [strict] | 91 |
| MLD show commands for interface VLAN | 91 |
| show ipv6 mld | 91 |
| show ipv6 mld [interface <intf_id> vlan <vlan-id>] | 92 |
| show ipv6 mld [vrf <vrf_name> all-vrfs] | 93 |
| show ipv6 mld [interface <intf-id> vlan <vlan-id>] [counters]] | 94 |
| show ipv6 mld [interface <intf-id> vlan <vlan-id>] [groups]] | 95 |
| show ipv6 mld [interface (<intf-id> vlan <vlan-id>) [group <group_ip>] [source <source_ip>]]] | 96 |
| show ipv6 mld [groups] | 97 |
| show ipv6 mld groups [all-vrfs vrf <vrf_name>] | 98 |
| show ipv6 mld [interface <intf-id> [counters]] | 99 |
| show ipv6 mld [interface <intf-id> [statistics]] | 100 |
| show ipv6 mld [interface <intf-id> [groups]] | 101 |
| show ipv6 mld [interface (<intf-id> vlan <vlan-id>) [group <group_ip>] [source <source_ip>]]] | 101 |
| show ipv6 mld [group <group_ip> [all-vrfs vrf <vrf_name>]] | 102 |
| show ipv6 mld [group <group_ip> [source <source_ip> [all-vrfs vrf <vrf_name>]]] | 104 |
| show ipv6 mld [interface vlan <vlan-id> [statistics]] | 105 |
| show ipv6 mld [static-groups [vrf <vrf_name> all-vrfs]] | 106 |
| show ipv6 mld counters | 107 |
| MLD configuration commands for interface | 108 |
| ipv6 mld {enable disable} | 108 |
| ipv6 mld apply access-list | 108 |
| no ipv6 mld | 109 |
| ipv6 mld querier | 110 |
| ipv6 mld querier [interval <interval-value>] | 110 |
| ipv6 mld last-member-query-interval | 111 |
| ipv6 mld querier query-max-response-time | 111 |
| ipv6 mld robustness | 112 |
| ipv6 mld static-group | 112 |
| ipv6 mld version | 113 |
| ipv6 mld version [strict] | 113 |

Protocol Independent Multicast - Sparse Mode (V4 and V6)115

| | |
|--|-----|
| Protocol Independent Multicast - Sparse Mode (PIM-SM) overview | 115 |
| PIM-SM defaults, protocols, and supported configuration | 115 |
| PIM-SM router types | 116 |
| How PIM-SM works | 118 |

| | |
|--|-----|
| Enabling/disabling PIM-SM in an interface | 120 |
| Configuring PIM-SM options in an interface | 120 |
| Viewing PIM information | 123 |
| PIM-SM configuration example | 124 |
| PIM-SM configuration task list | 126 |
| Enabling or disabling PIM globally | 127 |
| Configuring join/prune interval | 127 |
| Enabling/disabling multicast traffic to SPT | 128 |
| Configuring an RP | 128 |
| Configuring a BSR | 130 |
| Configuring RPF override | 132 |
| Removing all PIM-SM related configurations on an interface | 132 |
| PIM graceful shutdown | 133 |
| PIM-SM commands for IPv4 | 134 |
| accept-register access-list | 134 |
| accept-rp | 135 |
| active-active | 136 |
| bfd all-interfaces | 137 |
| bsr-candidate bsm-interval | 138 |
| bsr-candidate hash-mask-length | 138 |
| bsr-candidate priority | 139 |
| bsr-candidate source-ip-interface | 139 |
| disable | 140 |
| enable | 141 |
| ip pim-sparse {enable disable} | 141 |
| ip pim-sparse bfd | 142 |
| ip pim-sparse dr-priority | 142 |
| ip pim-sparse hello-delay | 143 |
| ip pim-sparse hello-interval | 144 |
| ip pim-sparse ip-addr | 145 |
| ip pim-sparse lan-prune-delay | 145 |
| ip pim-sparse override-interval | 146 |
| ip pim-sparse propagation-delay | 147 |
| join-prune-interval | 148 |
| multicast-route-limit | 148 |
| no ip pim-sparse | 149 |
| register-rate-limit | 149 |
| router pim | 150 |
| rp-address <IP-ADDR> | 151 |
| rp-candidate group-prefix | 152 |
| rp-candidate hold-time | 152 |
| rp-candidate priority | 153 |
| rp-candidate source-ip-interface | 153 |
| rpf-override | 154 |
| show ip mroute | 155 |
| show ip mroute brief | 156 |
| show ip mroute <GROUP-ADDR> | 157 |
| show ip pim | 159 |
| show ip pim bsr | 159 |
| show ip pim bsr elected | 161 |
| show ip pim bsr local | 162 |
| show ip pim interface | 163 |
| show ip pim interface <INTERFACE-NAME> | 164 |
| show ip pim interface <INTERFACE-NAME> counters | 165 |
| show ip pim neighbor | 166 |
| show ip pim pending | 167 |

| | |
|---|-----|
| show ip pim rp-candidate | 168 |
| show ip pim rp-set | 169 |
| show ip pim rp-set learned | 170 |
| show ip pim rp-set static | 171 |
| show ip pim rpf-override | 172 |
| show ip pim rpf-override source | 173 |
| sources-per-group | 174 |
| spt-threshold | 175 |
| PIM-SM commands for IPv6 | 175 |
| accept-register access-list | 175 |
| accept-rp | 176 |
| bsr-candidate bsm-interval | 177 |
| bsr-candidate hash-mask-length | 178 |
| bsr-candidate priority | 178 |
| bsr-candidate source-ip-interface | 179 |
| disable | 180 |
| enable | 180 |
| ipv6 pim6-sparse {enable disable} | 181 |
| ipv6 pim6-sparse bfd | 181 |
| ipv6 pim6-sparse dr-priority | 182 |
| ipv6 pim6-sparse hello-delay | 183 |
| ipv6 pim6-sparse hello-interval | 184 |
| ipv6 pim6-sparse ipv6-addr | 184 |
| ipv6 pim6-sparse lan-prune-delay | 185 |
| ipv6 pim6-sparse override-interval | 186 |
| ipv6 pim6-sparse propagation-delay | 187 |
| join-prune-interval | 187 |
| no ipv6 pim6-sparse | 188 |
| router pim6 | 188 |
| rp-address <IPv6-ADDR> | 189 |
| rp-candidate group-prefix | 190 |
| rp-candidate hold-time | 190 |
| rp-candidate priority | 191 |
| rp-candidate source-ip-interface | 192 |
| rpf-override | 193 |
| show ipv6 mroute <GROUP-ADDR> | 194 |
| show ipv6 mroute | 195 |
| show ipv6 mroute brief | 196 |
| show ipv6 pim6 | 197 |
| show ipv6 pim6 bsr | 198 |
| show ipv6 pim6 bsr elected | 200 |
| show ipv6 pim6 bsr local | 201 |
| show ipv6 pim6 interface <INTERFACE-NAME> | 201 |
| show ipv6 pim6 interface | 202 |
| show ipv6 pim6 neighbor | 203 |
| show ipv6 pim6 pending | 204 |
| show ipv6 pim6 rp-candidate | 205 |
| show ipv6 pim6 rpf-override | 206 |
| show ipv6 pim6 rpf-override source | 207 |
| show ipv6 pim6 rp-set | 208 |
| show ipv6 pim6 rp-set learned | 209 |
| show ipv6 pim6 rp-set static | 210 |
| spt-threshold | 211 |

Protocol Independent Multicast - Dense Mode (V4 and V6) 212

| | |
|---|-----|
| Protocol Independent Multicast - Dense Mode (PIM-DM) overview | 212 |
|---|-----|

| | |
|--|------------|
| PIM-DM defaults, protocols, and supported configurations | 212 |
| PIM-DM configuration example | 213 |
| PIM-DM features | 213 |
| PIM-DM commands for IPv4 | 214 |
| disable | 214 |
| enable | 214 |
| no ip pim-dense {enable disable} | 215 |
| ip pim-dense bfd | 216 |
| ip pim-dense graft-retry-interval | 216 |
| ip pim-dense hello-delay | 217 |
| ip pim-dense hello-interval | 218 |
| ip pim-dense ip-addr | 219 |
| ip pim-dense lan-prune-delay | 219 |
| ip pim-dense max-graft-retries | 220 |
| ip pim-dense override-interval | 221 |
| ip pim-dense propagation-delay | 222 |
| ip pim-dense ttl-threshold | 222 |
| router pim | 223 |
| show ip mroute | 224 |
| show ip mroute <GROUP-ADDR> | 225 |
| show ip mroute brief | 227 |
| show ip pim | 227 |
| show ip pim interface | 228 |
| show ip pim interface <INTERFACE-NAME> | 229 |
| show ip pim interface <INTERFACE-NAME> counters | 230 |
| show ip pim neighbor | 231 |
| state-refresh-interval | 232 |
| PIM-DM commands for IPv6 | 232 |
| disable | 232 |
| enable | 233 |
| ipv6 pim6-dense {enable disable} | 233 |
| ipv6 pim6-dense bfd | 234 |
| ipv6 pim6-dense graft-retry-interval | 235 |
| ipv6 pim6-dense hello-delay | 236 |
| ipv6 pim6-dense hello-interval | 236 |
| ipv6 pim6-dense ipv6-addr | 237 |
| ipv6 pim6-dense lan-prune-delay | 238 |
| ipv6 pim6-dense max-graft-retries | 238 |
| ipv6 pim6-dense override-interval | 239 |
| ipv6 pim6-dense propagation-delay | 240 |
| ipv6 pim6-dense ttl-threshold | 241 |
| no ipv6 pim6-dense | 242 |
| show ipv6 pim6 | 242 |
| show ipv6 pim6 interface | 243 |
| show ipv6 pim6 interface <INTERFACE-NAME> | 244 |
| show ipv6 mroute | 244 |
| show ipv6 mroute brief | 246 |
| show ipv6 mroute <GROUP-ADDR> | 247 |
| show ipv6 pim6 neighbor | 249 |
| router pim6 | 249 |
| state-refresh-interval | 250 |
| Multicast Source Discovery Protocol (MSDP) | 252 |
| Multicast Source Discovery Protocol (MSDP) overview | 252 |
| MSDP router config commands | 252 |
| disable | 252 |

| | |
|--|------------|
| enable | 253 |
| router msdp | 253 |
| sa-interval | 254 |
| MSDP peer configuration commands | 254 |
| connection-retry-interval | 254 |
| connect-source | 255 |
| description | 255 |
| disable | 256 |
| enable | 257 |
| ip msdp peer | 257 |
| keepalive | 258 |
| mesh-group | 258 |
| password | 259 |
| sa-filter access-list | 260 |
| MSDP show commands | 261 |
| show ip msdp count | 261 |
| show ip msdp peer | 262 |
| show ip msdp sa-cache | 263 |
| show ip msdp summary | 263 |
| mDNS gateway | 265 |
| mDNS gateway overview | 265 |
| Configuring mDNS gateway | 266 |
| mDNS gateway commands | 267 |
| debug mdns | 267 |
| description | 268 |
| id | 268 |
| mdns-sd | 269 |
| mdns-sd apply-profile tx | 269 |
| mdns-sd enable | 270 |
| mdns-sd profile | 271 |
| mdns-sd service | 271 |
| clear mdns-sd statistics | 272 |
| <sequence-number> | 272 |
| show mdns-sd service-entries | 274 |
| show mdns-sd statistics | 275 |
| show mdns-sd statistics profile | 275 |
| show mdns-sd summary | 276 |
| show running-config interface | 277 |
| show running-config mdns-sd profile | 277 |
| show running-config mdns-sd service | 278 |
| Multicast VXLAN | 279 |
| IGMP | 280 |
| PIM-SM | 280 |
| Sample Multicast over VXLAN Config of a VSX Leaf in Symmetric IRB topology | 281 |
| Multicast VXLAN commands | 284 |
| ip pim-sparse vsx-virtual-neighbor | 284 |
| redistribute local-mac | 285 |
| show ip mroute | 285 |
| show ip pim neighbor | 287 |
| Support and other resources | 289 |
| Accessing Aruba Support | 289 |
| Accessing updates | 289 |
| Aruba Support Portal | 289 |

| | |
|------------------------------|-----|
| My Networking | 290 |
| Warranty information | 290 |
| Regulatory information | 290 |
| Documentation feedback | 290 |

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 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 |
|---|---|
| <code>example-text</code> | 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: <ul style="list-style-type: none">■ <code><example-text></code>■ <code><example-text></code>■ <i>example-text</i>■ <i>example-text</i> | Identifies a placeholder—such as a parameter or a variable—that you must substitute with an actual value in a command or in code: <ul style="list-style-type: none">■ 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: <ul style="list-style-type: none"> ■ 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:

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 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>

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.

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:
!
!
!
!
!
vlan 1
  no shutdown
vlan 2
  ip igmp snooping enable
  ip igmp snooping version 2
  ip igmp snooping forward 1/1/1
  ip igmp snooping blocked 1/1/3
  ip igmp snooping static group 239.1.1.10
  ip igmp snooping static group 239.1.1.11
interface 1/1/1
  no shutdown
  no routing
  vlan access 2
interface 1/1/2
  no shutdown
  no routing
  vlan access 2
interface 1/1/3
  no shutdown
  no routing
  vlan access 2
interface vlan2
  no shutdown
  ip address 20.1.1.1/24
  ip igmp enable
  ip igmp version 2
  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
```

IGMP commands

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

ip igmp

Syntax

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

Description

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

Command context

```
config-if-vlan  
config-if  
config-lag-if
```

Parameters

```
enable  
    Enable IGMP.  
disable  
    Disable IGMP.
```

Authority

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

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
```

ip igmp apply access-list

Syntax

```
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.

Command context

config-if-vlan

Parameters

access-list

Associates an ACL with the IGMP.

<ACL-NAME>

Specifies the name of the ACL.

Authority

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

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
```

ip igmp last-member-query-interval

Syntax

```
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.

Command context

config-if-vlan

config-if

config-lag-if

Parameters

<INTERVAL-VALUE>

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

Authority

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

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
```

ip igmp querier

Syntax

```
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.

Command context

```
config-if-vlan
config-if
config-lag-if
```

Authority

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

Examples

Configuring an IGMP querier on interface VLAN 2:

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

ip igmp querier interval

Syntax

```
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.

Command context

```
config-if-vlan
config-if
config-lag-if
```

Parameters

<INTERVAL-VALUE>

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

Authority

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

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
```

ip igmp querier query-max-response-time

Syntax

```
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.

Command context

```
config-if-vlan
config-if
config-lag-if
```

Parameters

<RESPONSE-TIME>

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

Authority

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

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
```

ip igmp robustness

Syntax

```
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.

Command context

```
config-if-vlan
config-if
config-lag-if
```

Parameters

<VALUE>

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

Authority

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

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
```

ip igmp static-group

Syntax

```
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.

Command context

```
config-if-vlan
config-if
config-lag-if
```

Parameters

<MULTICAST-GROUP-IP>

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

Authority

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

Examples

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
```

ip igmp version

Syntax

```
ip igmp version <VERSION>
```

Description

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

Command context

```
config-if-vlan
config-if
config-lag-if
```

Parameters

<VERSION>

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

Authority

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

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
```

ip igmp version strict

Syntax

```
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.

Command context

```
config-if-vlan
config-if
config-lag-if
```

Parameters

<VERSION>

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

Authority

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

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
```

no ip igmp

Syntax

```
no ip igmp
```

Description

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

Command context

```
config-if-vlan
config-if
config-lag-if
```

Authority

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

Examples

Removes IGMP on interface VLAN 2:

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

show ip igmp

Syntax

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

Description

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

Command context

Operator (>) or Manager (#)

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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

```

show ip igmp counters

Syntax

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

Description

Shows IGMP counter details, or shows counters by VRF.

Command context

Operator (>) or Manager (#)

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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 |

show ip igmp group

Syntax

```
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.

Command context

Operator (>) or Manager (#)

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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

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

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
```

| Vers | Mode | Uptime | Expires | V1 Timer | V2 Timer | Sources Forwarded | Sources 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
```

| Vers | Mode | Uptime | Expires | V1 Timer | V2 Timer | Sources Forwarded | Sources 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
```

show ip igmp groups

Syntax

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

Description

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

Command context

Operator (>) or Manager (#)

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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

| Vers | Mode | Uptime | Expires | V1 Timer | V2 Timer | Sources Forwarded | Sources 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

| Vers | Mode | Uptime | Expires | V1 Timer | V2 Timer | Sources Forwarded | Sources 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

| Vers | Mode | Uptime | Expires | V1 Timer | V2 Timer | Sources Forwarded | Sources 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

| Vers | Mode | Uptime | Expires | V1 Timer | V2 Timer | Sources Forwarded | Sources 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

| Vers | Mode | Uptime | Expires | V1 Timer | V2 Timer | Sources Forwarded | Sources 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
```

| Vers | Mode | Uptime | Expires | V1 Timer | V2 Timer | Sources Forwarded | Sources 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
```

| Vers | Mode | Uptime | Expires | V1 Timer | V2 Timer | Sources Forwarded | Sources 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
```

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

show ip igmp interface

Syntax

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

Description

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

Command context

Operator (>) or Manager (#)

Parameters

<INTF-ID>

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

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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
```

show ip igmp interface counters

Syntax

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

Description

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

Command context

Operator (>) or Manager (#)

Parameters

<INTF-ID>

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

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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 |

show ip igmp interface group

Syntax

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

Description

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

Command context

Operator (>) or Manager (#)

Parameters

<INTF-ID>

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

vlan <VLAN-ID>

Specifies a VLAN. Values: 1-4094.

<GROUP-ID>

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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

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

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
```

show ip igmp interface groups

Syntax

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

Description

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

Command context

Operator (>) or Manager (#)

Parameters

<INTF-ID>

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

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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

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

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

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

Group Address       : 239.1.1.2
Source Address      : 10.1.1.1

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

show ip igmp interface statistics

Syntax

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

Description

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

Command context

Operator (>) or Manager (#)

Parameters

<INTF-ID>

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

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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
```

show ip igmp static-groups

Syntax

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

Description

Shows IGMP static groups, or shows information by VRF.

Command context

Operator (>) or Manager (#)

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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
```

show ip igmp statistics

Syntax

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

Description

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

Command context

Operator (>) or Manager (#)

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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

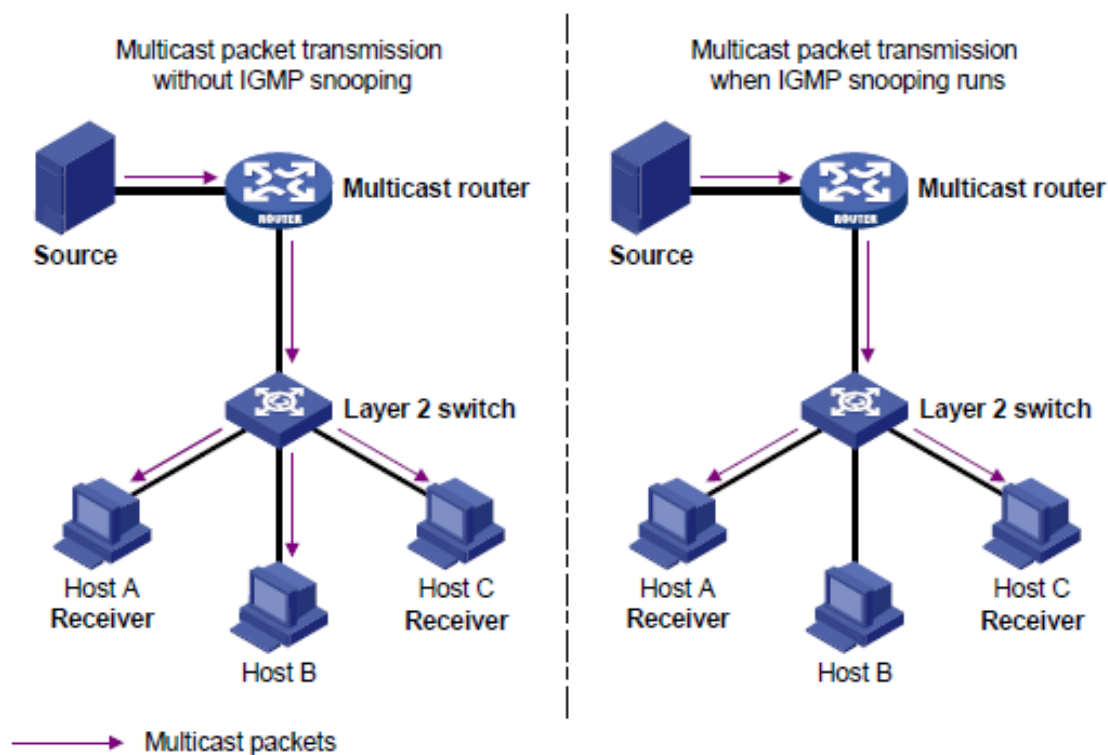
VRF Name      : test

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

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

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 {enable|disable}

Syntax

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

Description

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

Command context

```
config-vlan
```

Parameters

```
{enable | disable}
```

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

Authority

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

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
```

ip igmp snooping apply access-list

Syntax

```
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.

Command context

config-vlan

Parameters

access-list

Associates an ACL with the IGMP.

<ACL-NAME>

Specifies the name of the ACL.

Authority

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

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
```

ip igmp snooping auto vlan

Syntax

```
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.

Command context

config-if

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).

Authority

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

Example

On the 6400 Switch Series, interface identification differs.

Configuring 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
```

ip igmp snooping blocked vlan

Syntax

```
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.

Command context

`config-if`

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).

Authority

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

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
```

ip igmp snooping drop-unknown

Syntax

```
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.

Command context

`config`

Parameters

`vlan-shared`

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

`vlan-exclusive`

Enables exclusive drop unknown filter per VLAN.

Authority

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

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
```

ip igmp snooping fastlearn

Syntax

```
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.

Command context

config

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).

Authority

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

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
```


ip igmp snooping fastleave vlan

Syntax

```
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.

Command context

```
config-if
```

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).

Authority

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

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
```

ip igmp snooping forced fastleave vlan

Syntax

```
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.

Command context

config-if

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).

Authority

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

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
```

ip igmp snooping forward vlan

Syntax

```
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.

Command context

config-if

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).

Authority

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

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
```

ip igmp snooping static-group

Syntax

```
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.

Command context

config-vlan

Parameters

<MULTICAST-IP-ADDRESS>

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

Authority

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

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
```

ip igmp snooping version

Syntax

```
ip igmp snooping version <VERSION>
```

Description

Configures the IGMP snooping version on the VLAN.

Command context

```
config-vlan
```

Parameters

<VERSION>

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

Authority

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

Examples

Configuring IGMP snooping version on the VLAN:

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

no ip igmp snooping

Syntax

```
no ip igmp snooping
```

Description

Disables all IGMP snooping configurations on the VLAN.

Command context

```
config-vlan
```

Authority

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

Examples

Disabling all IGMP snooping configurations on the VLAN:

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

show ip igmp snooping

Syntax

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

Description

Shows IGMP snooping configuration information and status for all VLANs.

Command context

Operator (>) or Manager (#)

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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
```

show ip igmp snooping counters

Syntax

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

Description

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

Command context

Operator (>) or Manager (#)

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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
```

show ip igmp snooping groups

Syntax

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

Description

Shows IGMP snooping group information.

Command context

Operator (>) or Manager (#)

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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
```

show ip igmp snooping static-groups

Syntax

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

Description

Shows IGMP snooping static group details.

Command context

Operator (>) or Manager (#)

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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
```

show ip igmp snooping statistics

Syntax

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

Description

Shows IGMP snooping protocol information and the joined group statistics.

Command context

Operator (>) or Manager (#)

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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
```

show ip igmp snooping vlan <VLAN-ID>

Syntax

```
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.

Command context

Operator (>) or Manager (#)

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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

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

```

show ip igmp snooping vlan <VLAN-ID> counters

Syntax

```
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.

Command context

Operator (>) or Manager (#)

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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:
```



```
Last Reporter : 10.1.1.1
Group Type    : Filter
```

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

show ip igmp snooping vlan <VLAN-ID> statistics

Syntax

```
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.

Command context

Operator (>) or Manager (#)

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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
```

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

Syntax

```
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.

Command context

```
config
```

Parameters

```
vlan-shared
```

Required: Enable shared VLAN filter on the switch.

```
vlan-exclusive
```

Required: Enable exclusive drop unknown filter per VLAN.

Authority

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

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
```

MLD snooping VLAN configuration commands

ipv6 mld snooping

Syntax

```
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.

Command context

```
config-vlan-<VLAN-ID>
```

Parameters

`enable`

Required: Enable MLD snooping on the VLAN.

`disable`

Required: Disable MLD snooping on the VLAN.

Authority

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

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
```

ipv6 mld snooping apply access-list

Syntax

```
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.

Command context

config-vlan

Parameters

access-list

Associates an ACL with the IGMP.

<ACL-NAME>

Specifies the name of the ACL.

Authority

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

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
```

ipv6 mld snooping auto vlan

Syntax

```
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.

Command context

config-vlan-<VLAN-ID>

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).

Authority

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

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
```

ipv6 mld snooping blocked vlan

Syntax

```
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.

Command context

config-vlan-<VLAN-ID>

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).

Authority

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

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
```

ipv6 mld snooping fastlearn

Syntax

```
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.

Command context

```
config
```

Parameters

```
port-list
```

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

Authority

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

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
```

ipv6 mld snooping fastleave vlan

Syntax

```
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.

Command context

```
config-vlan-<VLAN-ID>
```

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).

Authority

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

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
```

ipv6 mld snooping forced fastleave

Syntax

```
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.

Command context

`config-vlan-<VLAN-ID>`

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).

Authority

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

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
```

ipv6 mld snooping forward vlan

Syntax

```
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.

Command context

config-vlan-<VLAN-ID>

Parameters

<VLAN-LIST>

Required: Specifies a list of VLANs on which ports should be configured as forward ports. 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).

Authority

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

Example

On the 6400 Switch Series, interface identification differs.

Configuring forward 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 forward vlan 10
switch(config-vlan)# ipv6 mld snooping forward vlan 10-20
```

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

Syntax

```
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.

Command context

```
config-vlan-<VLAN-ID>
```

Parameters

```
static-group
```

Required: <x:x::x:x>, MLD static multicast group.

Authority

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

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
```

ipv6 mld snooping [version <ver>]

Syntax

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

Description

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

Command context

```
config-vlan-<VLAN-ID>
```

Parameters

```
ver
```

Required: 1-2, MLD snooping version.

Authority

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

Example

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

MLD snooping show commands

show ipv6 mld snooping

Syntax

```
show ipv6 mld snooping
```

Description

This command shows MLD snooping configuration details for all VLANs.

Command context

Manager (#)

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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
```

show ipv6 mld snooping [counters]

Syntax

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

Description

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

Command context

Manager (#)

Parameters

counters

Optional, show MLD snooping counters.

Authority

Operators or Administrators or local user group members with execution rights for this command.
Operators can execute this command from the operator context (>) only.

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
```

show ipv6 mld snooping [groups]

Syntax

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

Description

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

Command context

Manager (#)

Parameters

groups

Optional, show MLD snooping groups information.

Authority

Operators or Administrators or local user group members with execution rights for this command.
Operators can execute this command from the operator context (>) only.

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            Filter
```

show ipv6 mld snooping [statistics]

Syntax

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

Description

This command shows MLD snooping statistics information.

Command context

Manager (#)

Parameters

statistics

Optional, show MLD snooping statistics.

Authority

Operators or Administrators or local user group members with execution rights for this command.
Operators can execute this command from the operator context (>) only.

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
```

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

Syntax


```
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.

Command context

Manager (#)

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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#
```

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

Syntax

```
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.

Command context

Manager (#)

Parameters

vlan-id

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

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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
```

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

Syntax

```
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.

Command context

Manager (#)

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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

Port      Vers Mode Uptime Expires V1      Sources Sources
-----
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 ipv6 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

```

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

Syntax

```
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.

Command context

Manager (#)

Parameters

port-id

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

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

Example

```

switch# show ipv6 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

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

```

```

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

```

show ipv6 mld snooping [static-groups]

Syntax

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

Description

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

Command context

Manager (#)

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

Example

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

```
MLD Static Group Address Information
```

```
VLAN ID Group Address
```

```
-----
```

```
10      ff12::1
```

```
10      ff12::2
```

MLD configuration commands for interface VLAN

ipv6 mld {enable | disable}

Syntax

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

Description

This command enables or disables MLD on the interface VLAN.

Command context

```
config-if-vlan
```

Parameters

```
enable
```

Required: Enable MLD on the interface VLAN.

```
disable
```

Required: Disable MLD on the interface VLAN.

Authority

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

Example

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

ipv6 mld apply access-list

Syntax

```
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.

Command context

```
config-vlan
```

Parameters

```
access-list
```

Associates an ACL with the IGMP.

```
<ACL-NAME>
```

Specifies the name of the ACL.

Authority

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

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
```

no ipv6 mld

Syntax

```
no ipv6 mld
```

Description

This command removes all MLD configurations on the interface.

Authority

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

Command context

```
config-if
```

Example

On the 6400 Switch Series, interface identification differs.

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

ipv6 mld querier

Syntax

```
ipv6 mld querier
```

Description

This command configures MLD querier.

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

Command context

```
config-if-vlan
```

Authority

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

Example

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

ipv6 mld querier [interval <interval-value>]

Syntax

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

Description

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

Command context

config-if-vlan

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.

Authority

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

Example

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

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

Syntax

```
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.

Command context

config-if-vlan

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.

Authority

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

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
```

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

Syntax

```
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.

Command context

config-if-vlan

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.

Authority

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

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
```

ipv6 mld robustness

Syntax

```
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.

Command context

config-if-vlan

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.

Authority

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

Example

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

ipv6 mld static-group <MULTICAST-GROUP-IP>

Syntax

```
ipv6 mld static-group <MULTICAST-GROUP-IP>
```

Description

This command configures MLD static group.

Command context

config-if-vlan

Parameters

<MULTICAST-GROUP-IP>

Required: X:X::X:X, configures MLD static group.

Authority

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

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
```

ipv6 mld version <VERSION>

Syntax

```
ipv6 mld version <VERSION>
```

Description

This command configures MLD version.

Command context

config-if-vlan

Parameters

<VERSION>

Required: 1-2, configures MLD version.

Authority

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

Example

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

ipv6 mld version <VERSION> [strict]

Syntax

```
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.

Command context

config-if-vlan

Parameters

<VERSION>

Required: 1-2, configures MLD version.

Authority

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

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
```

MLD show commands for interface VLAN

show ipv6 mld

Syntax

```
show ipv6 mld
```

Description

This command shows MLD configuration on VLAN.

Command context

Manager (#)

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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
```

show ipv6 mld [interface <intf_id> | vlan <vlan-id>]

Syntax

```
show ipv6 mld [interface <IFNAME> | vlan <VLAN-ID>]
```

Description

This command shows MLD configuration on a specific VLAN.

Command context

Manager (#)

Parameters

<VLAN-ID>

Required: 1-4094, shows MLD configuration on a specified VLAN.

<IFNAME>

Required: Shows MLD configuration on a specified interface.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

Example

```

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

```

show ipv6 mld [vrf <vrf_name> | all-vrfs]

Syntax

```
show ipv6 mld [vrf <VRF-NAME> | all-vrfs ]
```

Description

This command shows MLD information for the specified VRF.

Command context

Manager (#)

Parameters

<VRF-NAME>

Optional: shows MLD information status in a specific VRF.

all-vrfs

Optional: shows MLD information status for all VRFs.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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

```

show ipv6 mld [interface <intf-id> | vlan <vlan-id>] [counters]

Syntax

```
show ipv6 mld [interface <intf-id> | vlan <vlan-id>] [counters]
```

Description

This command shows MLD query packet Tx and Rx on a specific VLAN.

Command context

Manager (#)

Parameters

vlan-id

Required: 1-4094, shows MLD configuration on a specified VLAN.

intf-id

Required: IFNAME, shows MLD configuration on a specified interface.

counters

Optional: Shows MLD query packet counter Tx-Rx on a specified VLAN.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

Example

```
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 |

show ipv6 mld [interface <intf-id> | vlan <vlan-id>] [groups]

Syntax

```
show ipv6 mld [interface <intf-id> | vlan <vlan-id>] [groups]
```

Description

This command shows MLD groups joined details.

Command context

Manager (#)

Parameters

vlan-id

Required: 1-4094, shows MLD information on a specified VLAN.

intf-id

Required: IFNAME, shows MLD information on a specified interface.

groups

Optional: Shows MLD groups information on a specified interface.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

Example

```
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

Vers  Mode  Uptime      Expires      V1          Sources      Sources
-----  ---  -----  -----  ---  -----  -----
2      INC  6m 2s      0m 4s      Timer      Forwarded    Blocked

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

Mode  Uptime      Expire
-----  -----  -----
INC  6m 2s      0m 4s
```

show ipv6 mld [interface (<intf-id> | vlan <vlan-id>) [group <group_ip>] [source <source_ip>]]]

Syntax

```
show ipv6 mld [interface (<intf-id> | vlan <vlan-id>) [group <group_ip>] [source <source_ip>]]]
```

Description

This command shows MLD joined group details on a specified interface.

Command context

Manager (#)

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 specified source.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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

Vl      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

```

show ipv6 mld [groups]

Syntax

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

Description

This command shows MLD groups joined details.

Command context

Manager (#)

Parameters

groups

Options: shows MLD groups information.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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

Vers Mode Uptime   Expires   V1      Sources  Sources
-----
1          2m 27s    1m 53s  1m 53s  Forwarded Blocked
-----

MLD group information for group ff05::2:12

Interface Name   : vlan2
VRF Name        : default

Group Address    : ff05::2:12
Last Reporter    : 2001::1

Vers Mode Uptime   Expires   V1      Sources  Sources
-----
1          0m 3s     4m 18s  4m 18s  Forwarded Blocked
-----

```

show ipv6 mld groups [all-vrfs | vrf <vrf_name>]

Syntax

```
show ipv6 mld groups [all-vrfs | vrf <vrf_name>]
```

Description

This command shows MLD groups joined details on VRFs.

Command context

Manager (#)

Parameters

all-vrfs

Optional: shows MLD groups joined in all VRFs.

vrf-name

Optional: shows MLD groups joined in a specific VRF.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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

Vers Mode Uptime    Expires      V1          Sources    Sources
-----
1          4m 4s     2m 38s     2m 38s     Forwarded  Blocked
MLD group information for group ff05::2:12
Interface Name     : vlan3
VRF Name           : red

Group Address      : ff05::2:12
Last Reporter      : 2001::1

Vers Mode Uptime    Expires      V1          Sources    Sources
-----
1          1m 36s     2m 45s     2m 45s     Forwarded  Blocked
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

Vers Mode Uptime    Expires      V1          Sources    Sources
-----
1          5m 25s     1m 17s     1m 17s     Forwarded  Blocked

```

show ipv6 mld [interface <intf-id> [counters]]

Syntax

```
show ipv6 mld [interface <intf-id> [counters]]
```

Description

This command shows MLD query packet Tx and Rx on a specific interface.

Command context

Manager (#)

Parameters

intf-id

Required: shows MLD configuration on a specified interface.

counters

Optional: shows MLD query packet counter Tx-Rx on a specified interface.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

Example

```
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
```

show ipv6 mld [interface <intf-id> [statistics]]

Syntax

```
show ipv6 mld [interface <intf-id> [statistics]]
```

Description

This command shows MLD statistics on a specific interface.

Command context

Manager (#)

Parameters

intf-id

Required: shows MLD statistics on a specified interface.

statistics

Optional: shows MLD statistics on a specified interface.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

Example

```
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
```

show ipv6 mld [interface <intf-id> [groups]]

Syntax

```
show ipv6 mld [interface <intf-id> [groups]]
```

Description

This command shows MLD groups joined details.

Command context

Manager (#)

Parameters

intf-id

Required: shows MLD configuration on a specified interface.

groups

Optional: shows MLD groups information.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

Example

```
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

Vers Mode Uptime Expires V1 Sources Sources
-----
2 EXC 0m 14s 4m 6s Timer Forwarded Blocked
```

show ipv6 mld [interface (<intf-id> | vlan <vlan-id>) [group <group_ip>] [source <source_ip>]]]

Syntax

```
show ipv6 mld [interface (<intf-id> | vlan <vlan-id>) [group <group_ip>] [source <source_ip>]]]
```

Description

This command shows MLD joined group details on a specified interface.

Command context

Manager (#)

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 specified source.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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

Vers Mode Uptime    Expires      V1          Sources    Sources
-----|-----|-----|-----|-----|-----|-----
2      INC  6m 2s      0m 4s      Timer       Forwarded  Blocked

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
```

show ipv6 mld [group <group_ip> [all-vrfs | vrf <vrf_name>]]

Syntax

```
show ipv6 mld [group <group_ip> [all-vrfs | vrf <vrf_name>]]
```

Description

This command shows MLD joined group details on VRF.

Command context

Manager (#)

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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

Vers Mode Uptime Expires V1 Sources Sources
-----
2   EXC  3m 12s   3m 46s   3m 4s   Forwarded Blocked

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

Vers Mode Uptime Expires V1 Sources Sources
-----
1           1m 16s   3m 4s   3m 4s   Forwarded Blocked

MLD group information for group ff05::2:11

Interface Name   : vlan3
VRF Name         : red

Group Address    : ff05::2:11
Last Reporter    : 2001::1

Vers Mode Uptime Expires V1 Sources Sources
-----
1           0m 52s   3m 28s   3m 28s   Forwarded Blocked

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
```

| Vers | Mode | Uptime | Expires | V1 Timer | Sources Forwarded | Sources Blocked |
|------|------|--------|---------|-------------|----------------------|--------------------|
| 1 | | 1m 24s | 2m 56s | 2m 56s | | |

show ipv6 mld [group <group_ip> [source <source_ip> [all-vrfs | vrf <vrf_name>]]]

Syntax

```
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.

Command context

Manager (#)

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.

Optional: shows MLD groups joined in a specific VRF.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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

```

show ipv6 mld [interface vlan <vlan-id> [statistics]]

Syntax

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

Description

This command shows MLD statistics on a specific interface VLAN.

Command context

Manager (#)

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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
```

show ipv6 mld [static-groups [vrf <vrf_name> | all-vrfs]]

Syntax

```
show ipv6 mld [static-groups [vrf <vrf_name> | all-vrfs]]
```

Description

This command shows MLD static groups.

Command context

Manager (#)

Parameters

all-vrfs

Optional: shows MLD groups joined in all VRFs.

vrf

Optional: shows MLD groups joined in a specific VRF.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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
```

show ipv6 mld counters

Syntax

```
show ipv6 mld [counters [ vrf <vrf_name> ]]
```

Description

This command shows MLD counters.

Command context

Manager (#)

Parameters

vrf

Optional: shows MLD counter status in a specific VRF.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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 |

MLD configuration commands for interface

ipv6 mld {enable | disable}

Syntax

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

Description

This command enables or disables MLD on the interface.

Command context

```
config-if
```

Parameters

enable

Required: Enable MLD on the interface.

disable

Required: Disable MLD on the interface.

Authority

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

Example

On the 6400 Switch Series, interface identification differs.

```
switch(config)# interface 1/1/1
switch(config-if)# ipv6 mld enable
switch(config-if)# ipv6 mld disable
```

ipv6 mld apply access-list

Syntax

```
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.

Command context

```
config-vlan
```

Parameters

```
access-list
```

Associates an ACL with the IGMP.

```
<ACL-NAME>
```

Specifies the name of the ACL.

Authority

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

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 1/1/1
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
```

no ipv6 mld

Syntax

```
no ipv6 mld
```

Description

This command removes all MLD configurations on the interface.

Authority

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

Command context

```
config-if
```

Example

On the 6400 Switch Series, interface identification differs.

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

ipv6 mld querier

Syntax

```
ipv6 mld querier
```

Description

This command configures MLD querier. This functionality will allow the interface to join in the querier-election process.

Command context

```
config-if
```

Authority

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

Example

On the 6400 Switch Series, interface identification differs.

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

ipv6 mld querier [interval <interval-value>]

Syntax

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

Description

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

Command context

```
config-if
```

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.

Authority

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

Example

On the 6400 Switch Series, interface identification differs.

```
switch(config)# interface 1/1/1
switch(config-if)# ipv6 mld querier interval 100
switch(config-if)# no ipv6 mld querier interval
```

ipv6 mld last-member-query-interval

Syntax

```
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.

Command context

config-if

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.

Authority

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

Example

On the 6400 Switch Series, interface identification differs.

```
switch(config)# interface 1/1/1
switch(config-if)# ipv6 mld last-member-query-interval 2
switch(config-if)# no ipv6 mld last-member-query-interval
```

ipv6 mld querier query-max-response-time

Syntax

```
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.

Command context

config-if

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.

Authority

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

Example

On the 6400 Switch Series, interface identification differs.

```
switch(config)# interface 1/1/1
switch(config-if)# ipv6 mld query-max-response-time 50
switch(config-if)# no ipv6 mld query-max-response-time
```

ipv6 mld robustness

Syntax

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.

Command context

config-if

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.

Authority

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

Example

On the 6400 Switch Series, interface identification differs.

```
switch(config)# interface 1/11/1
switch(config-if)# ipv6 mld robustness 5
switch(config-if)# no ipv6 mld robustness
```

ipv6 mld static-group

Syntax

```
ipv6 mld static-group <multicast-group-ip>
```

Description

This command configures MLD static group.

Command context

```
config-if
```

Parameters

```
multicast-group-ip
```

Required: X:X::X:X, configures MLD static group.

Authority

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

Example

On the 6400 Switch Series, interface identification differs.

```
switch(config)# interface 1/1/1
switch(config-if)# ipv6 mld static-group ff12::c
switch(config-if)# no ipv6 mld static-group ff12::c
```

ipv6 mld version

Syntax

```
ipv6 mld version <version>
```

Description

This command configures MLD version.

Command context

```
config-if
```

Parameters

```
version
```

Required: 1-2, configures MLD version.

Authority

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

Example

On the 6400 Switch Series, interface identification differs.

```
switch(config)# interface 1/1/1
switch(config-if)# ipv6 mld version 2
```

ipv6 mld version [strict]

Syntax

```
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.

Command context

```
config-if
```

Parameters

```
version
```

Required: 1-2, configures MLD version.

Authority

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

Example

On the 6400 Switch Series, interface identification differs.

```
switch(config)# interface 1/1/1  
switch(config-if)# ipv6 mld version 2 strict  
switch(config-if)# no ipv6 mld version 2 strict
```

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.

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.

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 SPT 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 must be in 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.

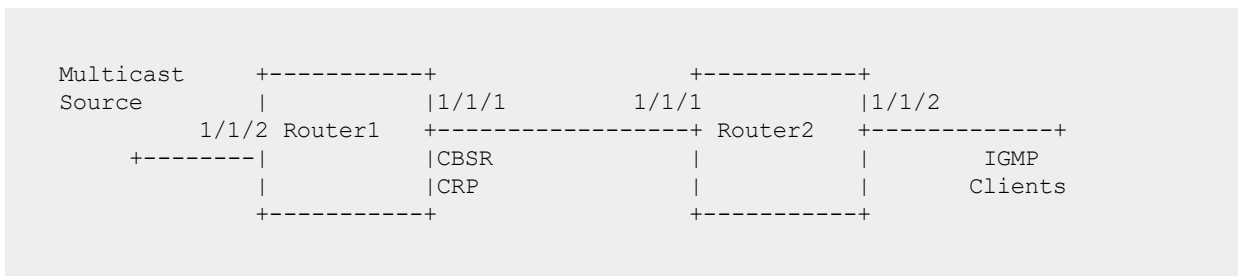
Procedure

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 neighborhood 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 graceful shutdown](#)

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.

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 graceful shutdown

The PIM active-active solution makes one of the VSX device 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 won't be 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 |
| < 8192 | 300 seconds |

| Number of MRoutes | Timer value |
|-------------------|-------------|
| < 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 <2-8>
```

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-SM commands for IPv4

accept-register access-list

Syntax

```
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.

Command context

```
config-pim
```

Parameters

```
<ACL-RULE>
```

Specifies the ACL rule name.

Authority

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

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
```

accept-rp

Syntax

```
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.

Command context

```
config-pim
```

Parameters

<IP-ADDR>

Specifies the IPv4 address of the static RP. Format: A.B.C.D

<ACL-RULE>

Specifies the ACL rule name.

Authority

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

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
```

active-active

Syntax

```
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.

Command context

```
config-pim
```

Authority

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

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
```

bfd all-interfaces

Syntax

```
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.

Command context

```
config-pim
```

Authority

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

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
```

bsr-candidate bsm-interval

Syntax

```
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.

Command context

```
config-pim
```

Parameters

<INTERVAL-VALUE>

Specifies the BSR-candidate BSM interval in seconds. Default: 60 seconds. Range: 5-300.

Authority

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

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
```

bsr-candidate hash-mask-length

Syntax

```
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.

Command context

```
config-pim
```

Parameters

<LENGTH-VALUE>

Specifies the length (in bits) of the hash mask. Default: 30. Range: 1-32.

Authority

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

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
```

bsr-candidate priority

Syntax

```
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.

Command context

```
config-pim
```

Parameters

<PRIORITY-VALUE>

Specifies the priority for the Candidate Bootstrap router. Default: 0. Range: 0-255

Authority

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

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
```

bsr-candidate source-ip-interface

Syntax

```
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.

Command context

`config-pim`

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).

Authority

Administrators or local user group members with execution rights for this 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
```

disable

Syntax

`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.

Command context

`config-pim`

Authority

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

Example

Disabling PIM router:

```
switch(config)# router pim
switch(config-pim)# disable
```

enable

Syntax

enable

Description

Enables PIM globally on the router.

Command context

config-pim

Authority

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

Example

Enabling PIM router:

```
switch(config)# router pim
switch(config-pim)# enable
```

ip pim-sparse {enable|disable}

Syntax

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.

Command context

config-if
config-if-vlan
config-lag-if

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.

Authority

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

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
```

ip pim-sparse bfd

Syntax

```
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.

Command context

```
config-if
config-if-vlan
```

Parameters

`disable`

Disables the BFD configuration on the interface.

Authority

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

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
```

ip pim-sparse dr-priority

Syntax

```
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.

Command context

```
config-if
config-if-vlan
config-lag-if
```

Parameters

<PRIORITY-VALUE>

Specifies the priority value to use on the interface in the DR election process. Required. Default: 1. Range: 0- to 294967295.

Authority

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

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
```

ip pim-sparse hello-delay

Syntax

```
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.

Command context

```
config-if
config-if-vlan
config-lag-if
```

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.

Authority

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

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
```

ip pim-sparse hello-interval

Syntax

```
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.

Command context

```
config-if
config-if-vlan
config-lag-if
```

Parameters

<INTERVAL-VALUE>

Specifies the frequency at which PIM Hello messages are transmitted on this interface. Range: 5 to 300.
Default: 30.

Authority

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

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
```

ip pim-sparse ip-addr

Syntax

```
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`.

Command context

```
config-if
config-if-vlan
config-lag-if
```

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.

Authority

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

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
```

ip pim-sparse lan-prune-delay

Syntax

```
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.

Command context

```
config-if
config-if-vlan
config-lag-if
```

Authority

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

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
```

ip pim-sparse override-interval

Syntax

```
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.

Command context

```
config-if
config-if-vlan
config-lag-if
```

Parameters

<INTERVAL-VALUE>

Specifies the override interval of a LAN Prune Delay option in ms. Range: 500 to 6000. Default: 2500.

Authority

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

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
```

ip pim-sparse propagation-delay

Syntax

```
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.

Command context

```
config-if
config-if-vlan
config-lag-if
```

Parameters

<DELAY-VALUE>

Specifies the propagation delay value in ms. Range: 250 to 2000. Default: 500.

Authority

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

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
```

join-prune-interval

Syntax

```
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.

Command context

```
config-pim
```

Parameters

<INTERVAL-VALUE>

Specifies the join-prune-interval in seconds. Range 5 to 65535 Default: 60.

Authority

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

Examples

Configuring join prune interval:

```
switch(config)# router pim  
switch(config-pim)# join-prune-interval 400  
switch(config-pim)# no join-prune-interval
```

multicast-route-limit

Syntax

```
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.

Command context

```
config-pim
```

Parameters

<limit>

Specifies the value to be configured as the multicast route limit. Range: 1 to 4294967295.

Authority

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

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)# mcast-route-limit 1024
switch(config-pim)# no mcast-route-limit
```

no ip pim-sparse

Syntax

```
no ip pim-sparse
```

Description

Removes all the PIM-SM related configurations for the interface.

Command context

```
config-if
config-if-vlan
config-lag-if
```

Authority

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

Example

Removing PIM-SM configuration:

```
switch(config)# interface vlan 40
switch(config-if-vlan)# no ip pim-sparse
```

register-rate-limit

Syntax

```
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.

Command context

config-pim

Parameters

<limit>

Specifies the value to be configured as the register rate limit. Range: 1 to 4294967295.

Authority

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

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
```

router pim

Syntax

```
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.

Command context

config

Parameters

vrf <VRF-NAME>

Specifies the name of a VRF.

Authority

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

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
```

rp-address <IP-ADDR>

Syntax

```
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.

Command context

config-pim

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.

Authority

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

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 override  
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
```

rp-candidate group-prefix

Syntax

```
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.

Command context

config-pim

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.

Authority

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

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
```

rp-candidate hold-time

Syntax

```
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.

Command context

config-pim

Parameters

<TIME-VALUE>

Specifies the hold-time value in seconds to be sent in C-RP-Adv messages. Range: 30 to 250. Default: 150.

Authority

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

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
```

rp-candidate priority

Syntax

```
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.

Command context

config-pim

Parameters

<PRIORITY-VALUE>

Specifies the priority value for the Candidate-RP router. Range: 0 to 255. Default: 192.

Authority

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

Example

Configuring and removing candidate priority:

```
switch(config)# router pim
switch(config-pim)# rp-candidate priority 250
switch(config-pim)# no rp-candidate priority
```

rp-candidate source-ip-interface

Syntax

```
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.

Command context

config-pim

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.

Authority

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

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
```

rpf-override

Syntax

```
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.

Command context

config-pim

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.

Authority

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

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
```

show ip mroute

Syntax

```
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.

Command context

Operator (>) or Manager (#)

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.

Authority

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

Operators can execute this command from the operator context (>) only.

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
```

show ip mroute brief

Syntax

```
show ip 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.

Command context

Operator (>) or Manager (#)

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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
```

show ip mroute <GROUP-ADDR>

Syntax

```
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.

Command context

Operator (>) or Manager (#)

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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

```

show ip pim

Syntax

```
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.

Command context

Operator (>) or Manager (#)

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

Example

Showing IP PIM router:

```

switch# show ip pim

PIM Global Parameters

VRF           : default
PIM Status    : enable
SPT Threshold : enabled

```

show ip pim bsr

Syntax

```
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.

Command context

Operator (>) or Manager (#)

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.

Authority

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

Operators can execute this command from the operator context (>) only.

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

```

show ip pim bsr elected

Syntax

```
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.

Command context

Operator (>) or Manager (#)

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.

Authority

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

Operators can execute this command from the operator context (>) only.

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
```

show ip pim bsr local

Syntax

```
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.

Command context

Operator (>) or Manager (#)

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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

```

show ip pim interface

Syntax

```
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.

Command context

Operator (>) or Manager (#)

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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 |

show ip pim interface <INTERFACE-NAME>

Syntax

```
show ip pim interface <INTERFACE-NAME> [vsx-peer]
```

Description

Shows detailed information about the PIM interface currently configured.

Command context

Operator (>) or Manager (#)

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.

Authority

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

Operators can execute this command from the operator context (>) only.

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
Propagation Delay (msec) : 500
Neighbor Timeout       : 105

Lan Prune Delay : Yes
DR Priority      : 1
```

show ip pim interface <INTERFACE-NAME> counters

Syntax

```
show ip pim interface <INTERFACE-NAME> counters [vsx-peer]
```

Description

Shows the PIM packet counters information for the specified interface.

Command context

Operator (>) or Manager (#)

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.

Authority

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

Operators can execute this command from the operator context (>) only.

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

```

show ip pim neighbor

Syntax

```

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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
```

show ip pim pending

Syntax

```
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.

Command context

Operator (>) or Manager (#)

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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
```

show ip pim rp-candidate

Syntax

```
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.

Command context

Operator (>) or Manager (#)

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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

```

show ip pim rp-set

Syntax

```
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.

Command context

Operator (>) or Manager (#)

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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

```

show ip pim rp-set learned

Syntax

```
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.

Command context

Operator (>) or Manager (#)

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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

```

show ip pim rp-set static

Syntax

```
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.

Command context

Operator (>) or Manager (#)

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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

```

show ip pim rpf-override

Syntax

```
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

Command context

Operator (>) or Manager (#)

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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

```

show ip pim rpf-override source

Syntax

```

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.

Command context

Operator (>) or Manager (#)

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.

`[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.

Authority

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

Operators can execute this command from the operator context (>) only.

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
```

sources-per-group

Syntax

```
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.

Command context

```
config-pim
```

Parameters

```
<limit>
```

Specifies the value to be configured as the sources allowed per group. Range: 1 to 4294967295.

Authority

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

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
```

spt-threshold

Syntax

```
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.

Command context

```
config-pim
```

Authority

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

Example

Enabling and disabling the SPT threshold:

```
switch(config)# router pim
switch(config-pim)# spt-threshold
switch(config-pim)# no spt-threshold
```

PIM-SM commands for IPv6

accept-register access-list

Syntax

```
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.

Command context

```
config-pim6
```

Parameters

<ACL-RULE>

Specifies the ACL rule name.

Authority

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

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
```

accept-rp

Syntax

```
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.

Command context

`config-pim6`

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.

Authority

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

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
```

bsr-candidate bsm-interval

Syntax

```
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.

Command context

```
config-pim6
```

Parameters

```
<INTERVAL-VALUE>
```

Specifies the BSR-candidate BSM interval in seconds. Range: 5 to 300. Default: 60.

Authority

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

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
```

bsr-candidate hash-mask-length

Syntax

```
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.

Command context

config-pim6

Parameters

<LENGTH-VALUE>

Specifies the length (in bits) of the hash mask. Range: 1 to 128. Default: 126.

Authority

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

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
```

bsr-candidate priority

Syntax

```
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.

Command context

```
config-pim6
```

Parameters

<PRIORITY-VALUE>

Specifies the priority for the Candidate Bootstrap router. Range: 0 to 255. Default: 0.

Authority

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

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
```

bsr-candidate source-ip-interface

Syntax

```
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.

Command context

```
config-pim6
```

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`.

Authority

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

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
```

disable

Syntax

disable

Description

Disables PIMv6 globally on the router.



Using the `disable` command will cause all the multicast routes to be erased from hardware.

Command context

config-pim6

Authority

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

Example

Disabling PIM router:

```
switch(config)# router pim6
switch(config-pim6)# disable
```

enable

Syntax

enable

Description

Enables PIMv6 globally on the router.

Command context

config-pim6

Authority

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

Example

Enabling PIM router:

```
switch(config)# router pim6  
switch(config-pim6)# enable
```

ipv6 pim6-sparse {enable|disable}

Syntax

```
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.

Command context

```
config-if  
config-if-vlan  
config-lag-if
```

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.

Authority

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

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
```

ipv6 pim6-sparse bfd

Syntax

```
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.

Command context

```
config-if
config-if-vlan
config-lag-if
```

Parameters

`disable`

Disables the BFD configuration on the interface.

Authority

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

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
```

ipv6 pim6-sparse dr-priority

Syntax

```
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.

Command context

```
config-if
config-if-vlan
config-lag-if
```

Parameters

<PRIORITY-VALUE>

Specifies the priority value to use on the interface in the DR election process. Range: 0 to 4294967295.
Default: 1.

Authority

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

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
```

ipv6 pim6-sparse hello-delay

Syntax

```
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.

Command context

```
config-if
config-if-vlan
config-lag-if
```

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.

Authority

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

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
```

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.

Command context

```
config-if
config-if-vlan
config-lag-if
```

Parameters

<INTERVAL-VALUE>

Specifies the frequency at which PIM Hello messages are transmitted on this interface in seconds. Range: 5 to 300. Default: 30.

Authority

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

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
```

ipv6 pim6-sparse ipv6-addr

Syntax

```
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`.

Command context

```
config-if
config-if-vlan
config-lag-if
```

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.

Authority

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

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
```

ipv6 pim6-sparse lan-prune-delay

Syntax

```
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.

Command context

```
config-if
config-if-vlan
config-lag-if
```

Authority

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

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
```

ipv6 pim6-sparse override-interval

Syntax

```
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.

Command context

```
config-if
config-if-vlan
config-lag-if
```

Parameters

<INTERVAL-VALUE>

Specifies the override interval of a LAN Prune Delay option in ms. Range: 500 to 6000. Default: 2500.

Authority

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

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
```

ipv6 pim6-sparse propagation-delay

Syntax

```
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.

Command context

```
config-if
config-if-vlan
config-lag-if
```

Parameters

<DELAY-VALUE>

Specifies the propagation delay value in ms. Range: 250 to 2000. Default: 500.

Authority

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

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
```

join-prune-interval

Syntax

```
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.

Command context

```
config-pim6
```

Parameters

<INTERVAL-VALUE>

Specifies the join-prune-interval in seconds. Range 5 to 65535. Default: 60.

Authority

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

Examples

Configuring join prune interval:

```
switch(config)# router pim6
switch(config-pim6)# join-prune-interval 400
switch(config-pim6)# no join-prune-interval
```

no ipv6 pim6-sparse

Syntax

```
no ipv6 pim6-sparse
```

Description

Removes all the PIM-SM related IPv6 configurations for the interface.

Command context

```
config-if
config-if-vlan
config-lag-if
```

Authority

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

Example

Removing PIM-SM configuration:

```
switch(config)# interface vlan40
switch(config-if-vlan)# no ipv6 pim6-sparse
```

router pim6

Syntax

```
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.

Command context

```
config
```

Parameters

vrf <VRF-NAME>

Specifies the name of a VRF. Default: default.

Authority

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

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
```

rp-address <IPv6-ADDR>

Syntax

```
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.

Command context

config-pim

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.

Authority

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

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 override
switch(config-pim6)# rp-address 2002::02 ff08::1:4/64
switch(config-pim6)# no rp-address 2002::02 ff08::1:4/64
```

rp-candidate group-prefix

Syntax

```
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.

Command context

config-pim6

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.

Authority

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

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
```

rp-candidate hold-time

Syntax

```
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.

Command context

```
config-pim6
```

Parameters

<TIME-VALUE>

Specifies the hold-time value in seconds to be sent in C-RP-Adv messages. Range: 30 - 255. Default: 150.

Authority

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

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
```

rp-candidate priority

Syntax

```
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.

Command context

```
config-pim
```

Parameters

<PRIORITY-VALUE>

Specifies the priority value for the Candidate-RP router. Range: 0 to 255. Default: 192.

Authority

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

Example

Configuring and removing candidate priority:

```
switch(config)# router pim6
switch(config-pim6)# rp-candidate priority 250
switch(config-pim6)# no rp-candidate priority
```

rp-candidate source-ip-interface

Syntax

```
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.

Command context

config-pim6

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.

Authority

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

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
```

Removing the candidate source IP interface:

```
switch(config-pim6)# no rp-candidate source-ip-interface vlan20
```

rpf-override

Syntax

```
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.

Command context

```
config-pim6
```

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.

Authority

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

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
```

show ipv6 mroute <GROUP-ADDR>

Syntax

```
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.

Command context

Operator (>) or Manager (#)

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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
```

show ipv6 mroute

Syntax

```
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.

Command context

Operator (>) or Manager (#)

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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
```

show ipv6 mroute brief

Syntax

```
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.

Command context

Operator (>) or Manager (#)

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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
```

show ipv6 pim6

Syntax

```
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.

Command context

Operator (>) or Manager (#)

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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
```

show ipv6 pim6 bsr

Syntax

```
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.

Command context

Operator (>) or Manager (#)

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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
```

show ipv6 pim6 bsr elected

Syntax

```
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.

Command context

Operator (>) or Manager (#)

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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
```


show ipv6 pim6 bsr local

Syntax

```
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.

Command context

Operator (>) or Manager (#)

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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
```

show ipv6 pim6 interface <INTERFACE-NAME>

Syntax

```
show ipv6 pim6 interface <INTERFACE-NAME> [vsx-peer]
```

Description

Shows detailed information about the PIM interface currently configured.

Command context

Operator (>) or Manager (#)

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.

Authority

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

Operators can execute this command from the operator context (>) only.

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
Propagation Delay (msec) : 350
Neighbor Timeout      : 0

Lan Prune Delay : Yes
DR Priority      : 3
```

show ipv6 pim6 interface

Syntax

```
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.

Command context

Operator (>) or Manager (#)

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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
```

show ipv6 pim6 neighbor

Syntax

```
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.

Authority

Operators or Administrators or local user group members with execution rights for this command.
Operators can execute this command from the operator context (>) only.

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
```

show ipv6 pim6 pending

Syntax

```
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.

Command context

Operator (>) or Manager (#)

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.

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.

Authority

Operators or Administrators or local user group members with execution rights for this command.
Operators can execute this command from the operator context (>) only.

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
```

show ipv6 pim6 rp-candidate

Syntax

```
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.

Command context

Operator (>) or Manager (#)

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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

```

show ipv6 pim6 rpf-override

Syntax

```
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

Command context

Operator (>) or Manager (#)

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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
```

show ipv6 pim6 rpf-override source

Syntax

```
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.

Command context

Operator (>) or Manager (#)

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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
```

show ipv6 pim6 rp-set

Syntax

```
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.

Command context

Operator (>) or Manager (#)

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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

```

show ipv6 pim6 rp-set learned

Syntax

```
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.

Command context

Operator (>) or Manager (#)

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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
```

show ipv6 pim6 rp-set static

Syntax

```
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.

Command context

Operator (>) or Manager (#)

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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
```

spt-threshold

Syntax

```
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.

Command context

```
config-pim6
```

Authority

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

Example

Enabling and disabling the SPT threshold:

```
switch(config)# router pim6
switch(config-pim6)# spt-threshold
switch(config-pim6)# no spt-threshold
```

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 *PIM-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

disable

Syntax

```
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.

Command context

```
config-pim
```

Authority

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

Example

Disabling PIM router:

```
switch(config)# router pim  
switch(config-pim)# disable
```

enable

Syntax

enable

Description

Enables PIM globally on the router.

Command context

config-pim

Authority

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

Example

Enabling PIM router:

```
switch(config)# router pim
switch(config-pim)# enable
```

no ip pim-dense {enable|disable}

Syntax

```
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.

Command context

```
config-if
config-if-vlan
config-lag-if
```

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.

Authority

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

Examples

Enabling and disabling PIM-SM 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
```

ip pim-dense bfd

Syntax

```
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.

Command context

```
config-if
config-if-vlan
config-lag-if
```

Parameters

`disable`

Disables the BFD configuration on the interface.

Authority

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

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
```

ip pim-dense graft-retry-interval

Syntax

```
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.

Command context

```
config-if
config-if-vlan
config-lag-if
```

Parameters

<INTERVAL-VALUE>

Specifies the interval the routing switch waits for the graft acknowledgement. Default: 3 seconds. Range: 1-10 seconds.

Authority

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

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)# ip pim-dense graft-retry-interval 5
switch(config-if-vlan)# no ip pim-dense graft-retry-interval
```

ip pim-dense hello-delay

Syntax

```
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.

Command context

```
config-if
config-if-vlan
config-lag-if
```

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.

Authority

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

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 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
```

ip pim-dense hello-interval

Syntax

```
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.

Command context

```
config-if
config-if-vlan
config-lag-if
```

Parameters

<INTERVAL-VALUE>

Specifies the frequency at which PIM Hello messages are transmitted on this interface. Default: 30 seconds. Range: 5-300 seconds.

Authority

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

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
```

ip pim-dense ip-addr

Syntax

```
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`.

Command context

```
config-if
config-if-vlan
config-lag-if
```

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.

Authority

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

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
```

ip pim-dense lan-prune-delay

Syntax

```
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.

Command context

```
config-if
config-if-vlan
config-lag-if
```

Authority

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

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
```

ip pim-dense max-graft-retries

Syntax

```
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.

Command context

```
config-if
config-if-vlan
config-lag-if
```

Parameters

<INTERVAL-VALUE>

Specifies the number of retries for the routing switch to resend the graft packet. Default: 3 attempts. Range: 1-10 attempts.

Authority

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

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
```

ip pim-dense override-interval

Syntax

```
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.

Command context

```
config-if
config-if-vlan
config-lag-if
```

Parameters

<INTERVAL-VALUE>

Specifies the override interval of a LAN Prune Delay option in ms. Default: 2500 ms. Range: 500-6000.

Authority

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

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
```

ip pim-dense propagation-delay

Syntax

```
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.

Command context

```
config-if
config-if-vlan
config-lag-if
```

Parameters

<DELAY-VALUE>

Specifies the propagation delay value in ms. Default: 500 ms. Range: 250-2000 ms.

Authority

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

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
```

ip pim-dense ttl-threshold

Syntax

```
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.

Command context

```
config-if  
config-if-vlan  
config-lag-if
```

Parameters

<THRESHOLD-VALUE>

Specifies the time to live threshold. Default: 3 attempts. Range: 0-255.

Authority

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

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
```

router pim

Syntax

```
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.

Command context

```
config
```

Parameters

vrf <VRF-NAME>

Specifies the name of a VRF.

Authority

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

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
```

show ip mroute

Syntax

```
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.

Command context

Operator (>) or Manager (#)

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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

```

show ip mroute <GROUP-ADDR>

Syntax

```

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.

Command context

Operator (>) or Manager (#)

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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

```

show ip mroute brief

Syntax

```
show ip 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.

Command context

Operator (>) or Manager (#)

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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

```

show ip pim

Syntax

```
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.

Command context

Operator (>) or Manager (#)

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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
```

show ip pim interface

Syntax

```
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.

Command context

Operator (>) or Manager (#)

Parameters

all-vrfs

Optional. Shows PIM interface information for all VRFs.

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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
```

show ip pim interface <INTERFACE-NAME>

Syntax

```
show ip pim interface <INTERFACE-NAME> [vsx-peer]
```

Description

Shows detailed information about the PIM interface currently configured.

Command context

Operator (>) or Manager (#)

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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
Propagation Delay (msec) : 500
Neighbor Timeout         : 105

Lan Prune Delay : Yes
DR Priority      : 1
```

show ip pim interface <INTERFACE-NAME> counters

Syntax

```
show ip pim interface <INTERFACE-NAME> counters [vsx-peer]
```

Description

Shows the PIM packet counters information for the specified interface.

Command context

Operator (>) or Manager (#)

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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

```

show ip pim neighbor

Syntax

```
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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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
```

state-refresh-interval

Syntax

```
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.

Command context

```
config-pim
```

Parameters

<INTERVAL-VALUE>

Specifies the state refresh interval in seconds. Default: 60 seconds. Range 10-100.

Authority

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

Examples

Configuring the state refresh interval:

```
switch(config)# router pim
switch(config-pim)# state-refresh 30
switch(config-pim)# no state-refresh
```

PIM-DM commands for IPv6

disable

Syntax

```
disable
```


Description

Disables PIMv6 globally on the router.



Using the `disable` command will cause all the multicast routes to be erased from hardware.

Command context

`config-pim6`

Authority

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

Example

Disabling PIM router:

```
switch(config)# router pim6
switch(config-pim6)# disable
```

enable

Syntax

`enable`

Description

Enables PIMv6 globally on the router.

Command context

`config-pim6`

Authority

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

Example

Enabling PIM router:

```
switch(config)# router pim6
switch(config-pim6)# enable
```

ipv6 pim6-dense {enable|disable}

Syntax

`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.

Command context

```
config-if  
config-if-vlan  
config-lag-if
```

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.

Authority

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

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
```

ipv6 pim6-dense bfd

Syntax

```
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.

Command context

```
config-if  
config-if-vlan  
config-lag-if
```

Parameters

`disable`

Disables the BFD configuration on the interface.

Authority

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

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
```

ipv6 pim6-dense graft-retry-interval

Syntax

```
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.

Command context

```
config-if
config-if-vlan
config-lag-if
```

Parameters

<INTERVAL-VALUE>

Specifies the interval the routing switch waits for the graft acknowledgement. Default: 3 seconds. Range: 1-10.

Authority

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

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
```

ipv6 pim6-dense hello-delay

Syntax

```
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.

Command context

```
config-if
config-if-vlan
config-lag-if
```

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.

Authority

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

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 vlan40
switch(config-if-vlan)# ipv6 pim6-dense hello-delay 4
switch(config-if-vlan)# no ipv6 pim6-dense hello-delay
```

ipv6 pim6-dense hello-interval

Syntax

```
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.

Command context

```
config-if  
config-if-vlan  
config-lag-if
```

Parameters

<INTERVAL-VALUE>

Specifies the frequency at which PIM Hello messages are transmitted on this interface. Default: 30 seconds. Range: 5-300.

Authority

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

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
```

ipv6 pim6-dense ipv6-addr

Syntax

```
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`.

Command context

```
config-if  
config-if-vlan  
config-lag-if
```

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.

Authority

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

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
```

ipv6 pim6-dense lan-prune-delay

Syntax

```
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.

Command context

```
config-if
config-if-vlan
config-lag-if
```

Authority

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

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
```

ipv6 pim6-dense max-graft-retries

Syntax

```
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.

Command context

```
config-if
config-if-vlan
config-lag-if
```

Parameters

<INTERVAL-VALUE>

Specifies the number of retries for the routing switch to resend the graft packet. Default: 3 attempts.
Range: 1-10.

Authority

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

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
```

ipv6 pim6-dense override-interval

Syntax

```
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.

Command context

```
config-if
config-if-vlan
```

config-lag-if

Parameters

<INTERVAL-VALUE>

Specifies the override interval of a LAN Prune Delay option in ms. Default: 2500 ms. Range: 500-6000.

Authority

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

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
```

ipv6 pim6-dense propagation-delay

Syntax

```
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.

Command context

```
config-if
config-if-vlan
config-lag-if
```

Parameters

<DELAY-VALUE>

Specifies the propagation delay value in ms. Default: 500 ms. Range: 250-2000.

Authority

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

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
```

ipv6 pim6-dense ttl-threshold

Syntax

```
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.

Command context

```
config-if
config-if-vlan
config-lag-if
```

Parameters

<THRESHOLD-VALUE>

Specifies the time to live threshold. Default: 3 attempts. Range: 0-255.

Authority

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

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
```

no ipv6 pim6-dense

Syntax

```
no ip pim-dense
```

Description

Removes PIM-DM for all IPv6 related configurations for the interface.

Command context

```
config-if
config-if-vlan
config-lag-if
```

Authority

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

Examples

Removing all PIM-DM configurations on an interface:

```
switch(config)# interface vlan40
switch(config-if-vlan)# no ipv6 pim6-dense
```

show ipv6 pim6

Syntax

```
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.

Command context

Operator (>) or Manager (#)

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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
```

show ipv6 pim6 interface

Syntax

```
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.

Command context

Operator (>) or Manager (#)

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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

```

show ipv6 pim6 interface <INTERFACE-NAME>

Syntax

```
show ipv6 pim6 interface <INTERFACE-NAME> [vsx-peer]
```

Description

Shows detailed information about the PIM interface currently configured.

Command context

Operator (>) or Manager (#)

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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
Propagation Delay : 350 msec
Neighbor Timeout  : 0
Graft Retry Interval : 9
LAN Prune Delay   : Yes
DR Priority       : 3
TTL Threshold     : 250
Max Graft Retries : 9

```

show ipv6 mroute

Syntax

```
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.

Command context

Operator (>) or Manager (#)

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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

```

show ipv6 mroute brief

Syntax

```
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.

Command context

Operator (>) or Manager (#)

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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
```

show ipv6 mroute <GROUP-ADDR>

Syntax

```
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.

Command context

Operator (>) or Manager (#)

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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

```

show ipv6 pim6 neighbor

Syntax

```

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.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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

```

router pim6

Syntax

```
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.

Command context

```
config
```

Parameters

```
vrf <VRF-NAME>
```

Specifies the name of a VRF. Default: default.

Authority

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

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
```

state-refresh-interval

Syntax

```
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.

Command context

```
config-pim6
```

Parameters

<INTERVAL-VALUE>

Specifies the state refresh interval in seconds. Default: 60 seconds. Range 10-100.

Authority

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

Examples

Configuring the state refresh interval:

```
switch(config)# router pim6  
switch(config-pim6)# state-refresh 30  
switch(config-pim6)# no state-refresh
```

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).

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

Syntax

```
disable
```

Description

Disables MSDP on the VRF.

Command context

```
config-msdp
```

Authority

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

Example

Disabling MSDP:

```
switch(config)# router msdp  
switch(config-msdp)# disable
```

enable

Syntax

```
enable
```

Description

Enables MSDP on the VRF.

Command context

```
config-msdp
```

Authority

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

Example

Enabling MSDP:

```
switch(config)# router msdp  
switch(config-msdp)# enable
```

router msdp

Syntax

```
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.

Command context

```
config
```

Parameters

```
vrf <VRF-NAME>
```

Specifies the context to the specified VRF.

Authority

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

Examples

Configuring default MSDP router context:

```
switch(config)# router msdp  
switch(config-msdp)#
```

Configuring specified router MSDP:

```
switch(config-msdp)# router msdp vrf red
```

sa-interval

Syntax

```
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.

Command context

config-msdp

Parameters

<INTERVAL-VALUE>

Specifies the sa-interval in seconds. Default: 60 seconds. Range 60-65535.

Authority

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

Examples

Configuring the sa-interval:

```
switch(config)# router msdp  
switch(config-msdp)# sa-interval 400  
switch(config-msdp)# no sa-interval
```

MSDP peer configuration commands

connection-retry-interval

Syntax

```
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.

Command context

`config-msdp-peer`

Parameters

`<INTERVAL-VALUE>`

Specify connection-retry-interval in seconds. Range: 1-65535.

Authority

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

Example

Configuring the connection-retry-interval:

```
switch(config-msdp-peer) # connection-retry-interval 120
switch(config-msdp-peer) # no connection-retry-interval
```

connect-source

Syntax

`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.

Command context

`config-msdp-peer`

Parameters

`<INTERFACE-NAME>`

Specifies the interface to use as a source.

Authority

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

Example

Configuring the connection source interface:

```
switch(config-msdp-peer) # connect-source 1/1/1
switch(config-msdp-peer) # no connect-source 1/1/1
```

description

Syntax

```
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.

Command context

```
config-msdp-peer
```

Parameters

<TEXT>

Specifies a description for the MSDP Peer.

Authority

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

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
```

disable

Syntax

```
disable
```

Description

Disables MSDP peer on the L3 interface.

Command context

```
config-msdp-peer
```

Authority

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

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
```

enable

Syntax

```
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.

Command context

```
config-msdp-peer
```

Authority

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

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
```

ip msdp peer

Syntax

```
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.

Command context

```
config-msdp
```

Parameters

<IP-ADDR>

Specifies the IPv4 address of the MSDP peer. Format: A.B.C.D

Authority

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

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)#
```

keepalive

Syntax

```
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.

Command context

config-msdp-peer

Parameters

<KEEPALIVE-INTERVAL>

Specifies the value for the keepalive interval.

<HOLD-TIME>

Specifies the value for the hold time.

Authority

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

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
```

mesh-group

Syntax

```
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.

Command context

config-msdp-peer

Parameters

<MESH-NAME>

Specifies the MSDP mesh group name.

Authority

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

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
```

password

Syntax

```
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.

Command context

config-msdp-peer

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.

Authority

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

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
```

sa-filter access-list

Syntax

```
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.

Command context

config-msdp-peer

Parameters

{in|out}

Enables the filter for incoming or outgoing SA messages.

<ACL-RULE>

Specifies the ACL rule name.

Authority

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

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
```

MSDP show commands

show ip msdp count

Syntax

```
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.

Command context

Operator (>) or Manager (#)

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.

Authority

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

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
```

show ip msdp peer

Syntax

```
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.

Command context

Operator (>) or Manager (#)

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.

Authority

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

Examples

Showing MSDP peer information for VRFs:

```
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

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
```

show ip msdp sa-cache

Syntax

```
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.

Authority

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

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
```

show ip msdp summary

Syntax

```
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.

Command context

Operator (>) or Manager (#)

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.

Authority

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

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
```


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 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 configure 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

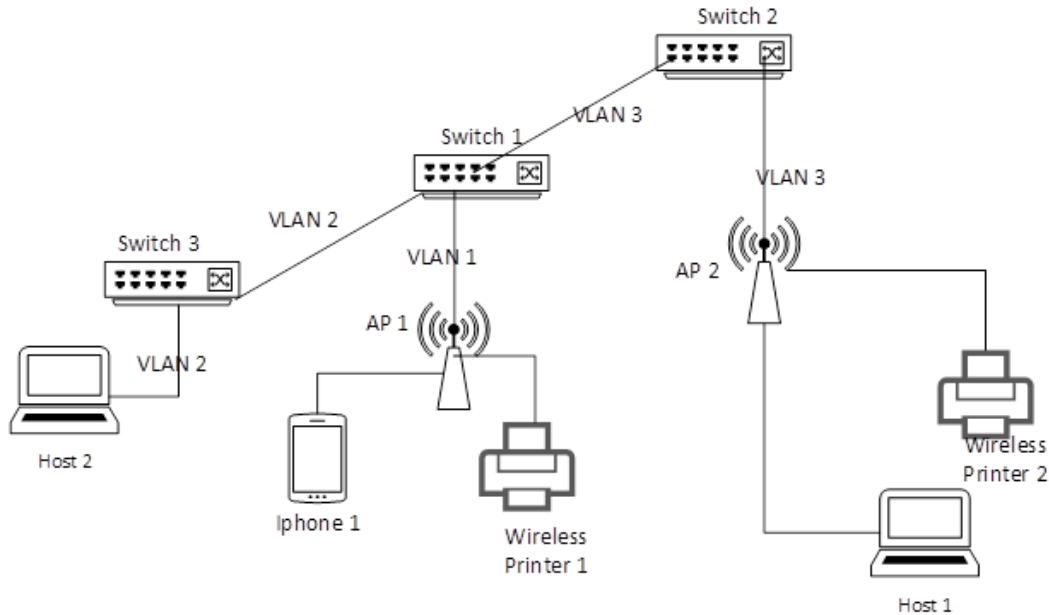
The following figure shows an example topology where mDNS gateway is useful. Consider the following:

- 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. Because, the switch allows the mDNS packets to be reflected in only 256 mDNS VLANs, 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 6300 and 6400 Switch Series only.

debug mdns

Syntax

```
debug mdns {all | config | init | packet | timer}
```

Description

Enables mDNS gateway debug logs for all or specific debug modules.

Command context

Manager (#)

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.

Authority

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

Examples

Enabling debug logs for all modules:

```
switch# debug mdns all
```

Enabling debug logs for config module:

```
switch# debug mdns config
```

description

Syntax

```
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.

Command context

```
config-mdns-sd-service
```

Parameters

```
<SERVICE-DESCRIPTION>
```

Specifies the service description. Maximum 128 characters.

Authority

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

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
```

id

Syntax

```
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.

Command context

```
config-mdns-sd-service
```

Parameters

```
<SERVICE-ID>
```

Specifies the service ID. Maximum 128 characters.

Authority

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

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
```

mdns-sd

Syntax

```
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.

Command context

```
config-if-vlan
```

Authority

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

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
```

mdns-sd apply-profile tx

Syntax

```
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.

Command context

config-if-vlan

Parameters

<PROFILE-NAME>

Specifies the profile name. Maximum 32 characters.

Authority

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

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
```

mdns-sd enable

Syntax

```
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.

Command context

config

Authority

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

Examples

Enable mDNS gateway:

```
switch(config)# mdns-sd enable
```

Disable mDNS gateway:

```
switch(config)# no mdns-sd enable
```

mdns-sd profile

Syntax

```
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.

Command context

```
config
```

Parameters

<PROFILE-NAME>

Specifies the name of the profile. Maximum 32 characters.

Authority

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

Examples

Creating a profile:

```
switch(config)# mdns-sd profile student
```

mdns-sd service

Syntax

```
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.

Command context

config

Parameters

<SERVICE-NAME>

Specifies the name of the service. Maximum 32 characters.

Authority

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

Examples

Configure a service for mDNS gateway:

```
switch(config)# mdns-sd service students
```

Delete a service:

```
switch(config)# no mdns-sd service students
```

clear mdns-sd statistics

Syntax

```
clear mdns-sd statistics
```

Description

Clears all mDNS gateway statistics.

Command context

config

Authority

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

Examples

Clear mDNS gateway statistics:

```
switch(config)# clear mdns-sd statistics
```

<sequence-number>

Syntax

```
<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.

Command context

`config-mdns-sd-profile`

Parameters

`<SERVICE-NAME>`

Specifies the service name. Maximum 128 characters.

`<SERVICE-INSTANCE-NAME>`

Specifies the service instance name. Maximum 128 characters.

Authority

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

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 instance-name office._pdl-datastream._tcp.local
switch(config-mdns-sd-profile)# 30 permit service-instance-name 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 instance-name office._pdl-datastream._tcp.local
switch(config-mdns-sd-profile)# 30 permit service-instance-name instance-name
library._pdl-datastream._tcp.local
switch(config-mdns-sd-profile)# no 30 permit service-instance-name instance-name
library._pdl-datastream._tcp.local
switch(config-mdns-sd-profile)# 40 deny
```

show mdns-sd service-entries

Syntax

```
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.

Command context

Operator (>) or Manager (#)

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

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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
```

show mdns-sd statistics

Syntax

```
show mdns-sd statistics [vlan [<VLAN-ID>]]
```

Description

Shows the mDNS packets received and sent globally, and per VLAN.

Command context

Operator (>) or Manager (#)

Parameters

<VLAN-ID>

Specifies the VLAN ID. Required. Range 1 to 4094.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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 10
Packets Recieved   : 100
Packets Sent       : 100
Packets Dropped    : 0

VLAN 20
Packets Recieved   : 0
Packets Sent       : 50
Packets Dropped    : 50
```

show mdns-sd statistics profile

Syntax

```
show mdns-sd statistics profile <PROFILE-NAME>
```

Description

Displays the number of packets permitted or denied by various filter rules in a profile.

Command context

Operator (>) or Manager (#)

Parameters

<PROFILE-NAME>

Specifies the profile name. Maximum 32 characters.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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
```

show mdns-sd summary

Syntax

```
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.

Command context

Operator (>) or Manager (#)

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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
```

show running-config interface

Syntax

```
show running-config interface <INTERFACE-NAME>
```

Description

Shows the configuration of profiles for an interface.

Command context

Operator (>) or Manager (#)

Parameters

<INTERFACE-NAME>

Specifies the interface name.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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
```

show running-config mdns-sd profile

Syntax

```
show running-config mdns-sd profile <PROFILE-NAME>
```

Description

Shows the configuration of all or a specific profile.

Command context

Operator (>) or Manager (#)

Parameters

<PROFILE-NAME>

Specifies the profile name. Maximum 32 characters.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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
```

show running-config mdns-sd service

Syntax

```
show running-config mdns-sd service <SERVICE-NAME>
```

Description

Shows the running configuration of all or a specific mDNS service.

Command context

Operator (>) or Manager (#)

Parameters

<SERVICE-NAME>

Specifies the service name. Maximum 32 characters.

Authority

Operators or Administrators or local user group members with execution rights for this command. Operators can execute this command from the operator context (>) only.

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

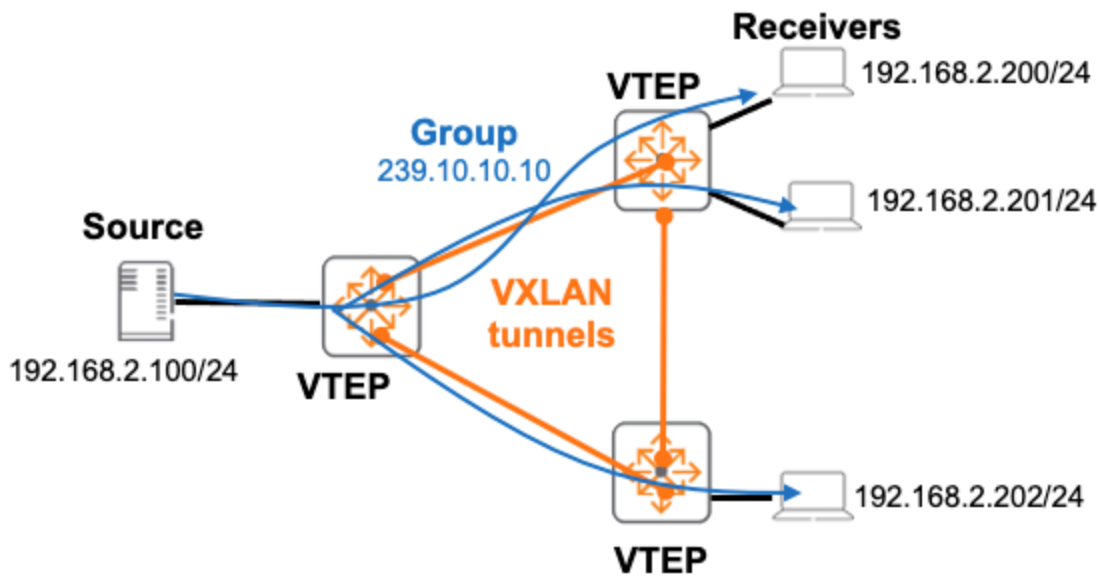
mdns-sd service itunes
  id _home-sharing._tcp
  id _apple-mobdev._dev
```



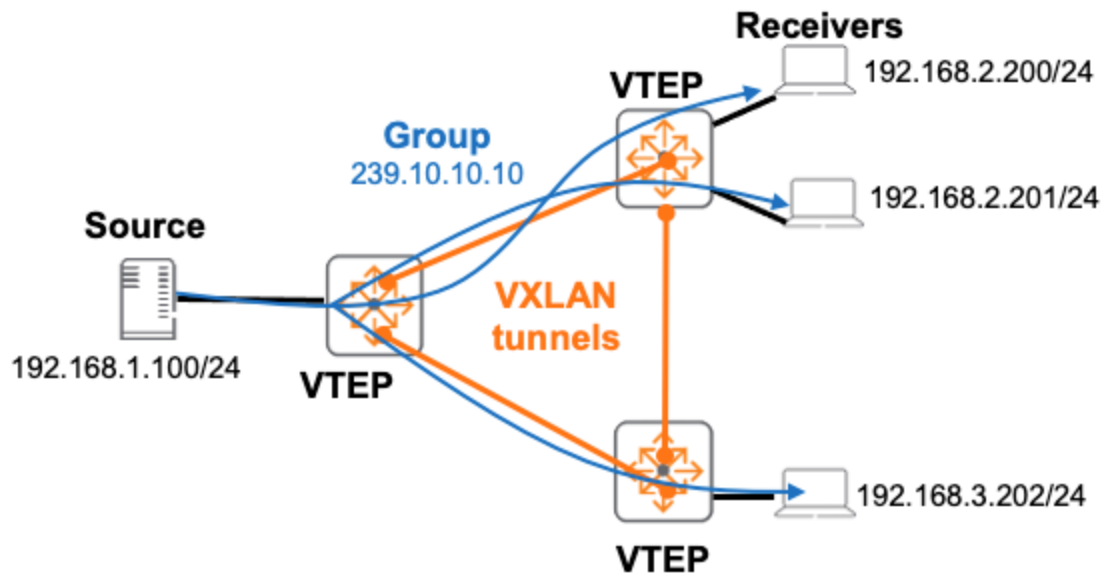
The Aruba 8320 Switch Series does not support VXLAN.

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 here:



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 here:



IGMP

In a VXLAN deployment, enabling igmp snooping prevents flooding of unknown multicast packets to all the VTEPs in the L2VNI. AHQ from the querier is sent to all the VTEPs in the L2VNI along with the regular ports in the associated VLAN. Additionally, IGMP Membership Reports from local hosts are forwarded to all the VTEPs in the L2VNI.

In a situation where a VSX pair is acting like a VTEP, IGMP Membership Reports from remote VTEPs are synchronized among the VSX peers. Both the VSX peers will learn the join on the same VTEP. In order to achieve this, `redistribute local-svi` or `redistribute local-mac` commands must be enabled under the EVPN context. When running VSX on a pair of switches, only one device will get the packet on the VTEP. IGMP snooping should be enabled on all devices in the fabric, otherwise all multicast traffic is flooded.

If the VTEP does not have any IGMP configurations, VXLAN encapsulated packets are copied to the CPU even though there is no IGMP configuration; the packets are forwarded by the software to the other ports.



In a VXLAN-enabled topology where there are tunnel endpoints configured on different platforms, the scale supported will be the lowest value among the different platforms. This is because the joins are synced across the Tunnel Endpoints.

PIM-SM

In a VXLAN deployment, when PIM is configured on the tenant VRF, PIM is automatically enabled on the L3VNI interface on that VRF. This interface is used to route multicast traffic across tunnels in a symmetric IRB network. PIM neighbors will be learned on this interface and the remote VTEP neighbors will be listed under this interface. Multicast traffic is forwarded through the same L3VNI interface to reach other VTEP clients.

PIM uses the VXLAN source IP as the DR priority and it overrides the default DR priority. It is recommended not to configure DR priorities. However, if you must configure the priority, the DR priority should be unique in each of the leaf nodes. For a VSX VTEP, the VSX peers should have the same DR priority.



- PIM-DM with VXLAN is not currently supported.
- Multicast over static VXLAN tunnels is currently not supported.
- PIM active-active is not applicable for Multicast over VXLAN.

Sample Multicast over VXLAN Config of a VSX Leaf in Symmetric IRB topology

Leaf-1A Config:

```
hostname Leaf-1A
vrf Test1
  rd 100.0.0.1:15000
  route-target export 1234567:15000 evpn
  route-target import 1234567:15000 evpn
vlan 1
vlan 101
#Enable IGMP snooping
  ip igmp snooping enable
vlan 200
virtual-mac 00:00:00:0a:0a:0a

#evpn configuration
evpn
  redistribute local-svi
  vlan 101
    rd 100.0.0.1:101
    route-target export 101:101
    route-target import 101:101

#L2vni svi configuration          Enable IGMP and PIM on the L2 VNI mapped SVI
interface vlan 101
  vrf attach Test1
  ip address 101.1.1.2/24
  active-gateway ip mac 00:00:20:00:10:01
  active-gateway ip 101.1.1.1
  ip igmp enable
  ip pim-sparse enable
  ip pim-sparse vsx-virtual-neighbor

#MC-LAG-AF SVI Connection to device Outside Fabric
interface vlan 200
  vrf attach Test1
  vsx active-forwarding
  ip address 101.2.1.2/24
  ip ospf 1 area 0.0.0.0
  ip pim-sparse enable
  ip pim-sparse vsx-virtual-neighbor

#vxlan configuration
interface vxlan 1
  source ip 100.0.0.1
  vxlan-counters aggregate
  no shutdown
  vni 101
  vlan 101
```

```

vni 15001
  vrf Test1
  routing

vsx
  inter-switch-link lag 1
  role primary
  keepalive peer 192.168.1.2 source 192.168.1.1
router ospf 1
  router-id 11.11.11.11
  area 0.0.0.0
router bgp 1
  bgp router-id 1.1.1.1
  neighbor 3.3.3.3 remote-as 1
  neighbor 3.3.3.3 update-source loopback 0
  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 3.3.3.3 activate
    neighbor 3.3.3.3 send-community extended
    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 Test1
    address-family ipv4 unicast
      redistribute connected
    exit-address-family
!
#Enable PIM
router pim vrf Test1
  enable

```

Leaf-1B Config:

```

hostname Leaf-1B
vrf Test1
  rd 100.0.0.1:15000
  route-target export 1234567:15000 evp
  route-target import 1234567:15000 evpn
vlan 1
vlan 101
  #Enable IGMP snooping
  ip igmp snooping enable
vlan 200
virtual-mac 00:00:00:0a:0a:0a

#evpn configuration
evpn
  redistribute local-svi
  vlan 101
    rd 100.0.0.1:101
    route-target export 101:101
    route-target import 101:101

```

```

#L2vni svi configuration. Configure IGMP and PIM on the L2 VNI mapped SVI
interface vlan 101
    vrf attach Test1
    ip address 101.1.1.3/24
    active-gateway ip mac 00:00:20:00:10:01
    active-gateway ip 101.1.1.1
    ip igmp enable
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor

#MC-LAG-AF SVI Connection to device Outside Fabric
interface vlan 200
    vrf attach Test1
    vsx active-forwarding
    ip address 101.2.1.1/24
    ip ospf 1 area 0.0.0.0
    ip pim-sparse enable
    ip pim-sparse vsx-virtual-neighbor

#vxlan configuration
interface vxlan 1
    source ip 100.0.0.1
    vxlan-counters aggregate
    no shutdown
    vni 101
        vlan 101
    vni 15001
        vrf Test1
        routing

vsx
    inter-switch-link lag 1
    role secondary
    keepalive peer 192.168.1.1 source 192.168.1.2
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 3.3.3.3 remote-as 1
    neighbor 3.3.3.3 update-source loopback 0
    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 3.3.3.3 activate
        neighbor 3.3.3.3 send-community extended
        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 Test1
    address-family ipv4 unicast
        redistribute connected
    exit-address-family

```

```
!  
#Enable PIM  
router pim vrf Test1  
    enable
```

RP config on PIM router outside Fabric:

```
# SVI Connection to VxLAN VSX Leaf-1  
interface vlan 200  
    ip address 101.2.1.3/24  
    ip ospf 1 area 0.0.0.0  
    ip pim-sparse enable  
  
router ospf 1  
    router-id 7.7.7.7  
    area 0.0.0.0  
  
router pim  
    enable  
    rp-candidate source-ip-interface loopback0  
    rp-candidate group-prefix 224.0.0.0/4  
    bsr-candidate source-ip-interface loopback0
```

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

10.07 or earlier

--

Command Information

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

redistribute local-mac

```
redistribute local-mac
no redistribute local-mac
```

Description

Enables Type-2 route advertisement for local MAC address of the SVI interfaces corresponding to the EVPN-enabled VLANs.

The `no` form of this command disables the Type-2 route advertisement.

Examples

```
switch(config)# evpn
switch(config)# redistribute local-mac
switch(config)# vlan 20
```

Command History

10.07 or earlier --

Command Information

All platforms `config-evpn` 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`

`[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

10.07 or earlier --

Command Information

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

10.07 or earlier --

Command Information

| | | |
|---------------|-----------------------------|--|
| 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. |
|---------------|-----------------------------|--|

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.